

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	JOHNS-001US3
		Application Number	
Title of Invention	System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2

Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove				
Legal Name				
Prefix	Given Name	Middle Name	Family Name	Suffix
	William	J.	Johnson	
Residence Information (Select One) <input checked="" type="radio"/> US Residency <input type="radio"/> Non US Residency <input type="radio"/> Active US Military Service				
City	Flower Mound	State/Province	TX	Country of Residence ⁱ
				US
Mailing Address of Inventor:				
Address 1	1704 Katherine Court			
Address 2				
City	Flower Mound	State/Province	TX	
Postal Code	75022	Country ⁱ	US	
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button. Add				

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).

An Address is being provided for the correspondence information of this application.

Customer Number	42640		
Email Address	patents@yudellisidore.com	Add Email	Remove Email

Application Information:

Title of the Invention	System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications		
Attorney Docket Number	JOHNS-001US3	Small Entity Status Claimed	<input checked="" type="checkbox"/>
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	70	Suggested Figure for Publication (if any)	

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	JOHNS-001US3
		Application Number	
Title of Invention	System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications		

Publication Information:

<input type="checkbox"/> Request Early Publication (Fee required at time of Request 37 CFR 1.219)
<input type="checkbox"/> Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.			
Please Select One:	<input checked="" type="radio"/> Customer Number	<input type="radio"/> US Patent Practitioner	<input type="radio"/> Limited Recognition (37 CFR 11.9)
Customer Number	42640		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.			
Prior Application Status	Pending	<input type="button" value="Remove"/>	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	12077041	2008-03-14
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			<input type="button" value="Add"/>

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).			
			<input type="button" value="Remove"/>
Application Number	Country i	Filing Date (YYYY-MM-DD)	Priority Claimed
			<input type="radio"/> Yes <input checked="" type="radio"/> No
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			<input type="button" value="Add"/>

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	JOHNS-001US3	
		Application Number		
Title of Invention	System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications			

Authorization to Permit Access:

<input checked="" type="checkbox"/> Authorization to Permit Access to the Instant Application by the Participating Offices
<p>If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.</p> <p>In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.</p> <p>In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.</p>

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.				
Applicant 1				
If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.				
<input type="button" value="Remove"/>				
<input type="radio"/> Assignee	<input type="radio"/> Legal Representative under 35 U.S.C. 117			
<input type="radio"/> Person to whom the inventor is obligated to assign.	<input type="radio"/> Person who shows sufficient proprietary interest			
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:				
Name of the Deceased or Legally Incapacitated Inventor : <input type="text"/>				
If the Assignee is an Organization check here. <input type="checkbox"/>				
Prefix	Given Name	Middle Name	Family Name	Suffix

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	JOHNS-001US3
		Application Number	
Title of Invention	System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications		

Mailing Address Information:			
Address 1			
Address 2			
City		State/Province	
Country ⁱ		Postal Code	
Phone Number		Fax Number	
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button.			<input type="button" value="Add"/>

Signature:

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications					
Signature	/Craig J. Yudell/		Date (YYYY-MM-DD)	2013-09-23	
First Name	Craig	Last Name	Yudell	Registration Number	39083
Additional Signature may be generated within this form by selecting the Add button.			<input type="button" value="Add"/>		

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

SYSTEM AND METHOD FOR LOCATION BASED EXCHANGES OF DATA FACILITATING DISTRIBUTED LOCATIONAL APPLICATIONS

CROSS-REFERENCES TO RELATED APPLICATIONS

5 This application is a continuation of application serial number 12/077,041 filed March 14, 2008 and entitled "System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications". This application contains an identical specification to serial number 12/077,041 except for the abstract, claims, and minor
10 modifications resulting from a Preliminary Amendment filed November 17, 2008 and a Preliminary Amendment B filed February 10, 2009.

FIELD OF THE INVENTION

15 The present disclosure relates generally to location based services for mobile data processing systems, and more particularly to location based exchanges of data between distributed mobile data processing systems for locational applications. A common connected service is not required for location based functionality and features. Location based exchanges of data between distributed mobile data processing systems enable location based features and functionality in a peer to peer manner.

20

BACKGROUND OF THE INVENTION

The internet has exploded with new service offerings. Websites yahoo.com, google.com, ebay.com, amazon.com, and iTunes.com have demonstrated well the ability to provide valuable services to a large dispersed geographic audience through the internet
25 (ebay, yahoo, google, amazon and iTunes (Apple) are trademarks of the respective companies). Thousands of different types of web services are available for many kinds of functionality. Advantages of having a service as the intermediary point between clients, users, and systems, and their associated services, includes centralized processing, centralized maintaining of data, for example to have an all knowing database for scope of
30 services provided, having a supervisory point of control, providing an administrator with

access to data maintained by users of the web service, and other advantages associated with centralized control. The advantages are analogous to those provided by the traditional mainframe computer to its clients wherein the mainframe owns all resources, data, processing, and centralized control for all users and systems (clients) that access its services. However, as computers declined in price and adequate processing power was brought to more distributed systems, such as Open Systems (i.e. Windows, UNIX, Linux, and Mac environments), the mainframe was no longer necessary for many of the daily computing tasks. In fact, adequate processing power is incorporated in highly mobile devices, various handheld mobile data processing systems, and other mobile data processing systems. Technology continues to drive improved processing power and data storage capabilities in less physical space of a device. Just as Open Systems took much of the load of computing off of mainframe computers, so to can mobile data processing systems offload tasks usually performed by connected web services. As mobile data processing systems are more capable, there is no need for a service to middleman interactions possible between them.

While a centralized service has its advantages, there are also disadvantages. A service becomes a clearinghouse for all web service transactions. Regardless of the number of threads of processing spread out over hardware and processor platforms, the web service itself can become a bottleneck causing poor performance for timely response, and can cause a large amount of data that must be kept for all connected users and/or systems. Even large web services mentioned above suffer from performance and maintenance overhead. A web service response will likely never be fast enough. Additionally, archives must be kept to ensure recovery in the event of a disaster because the service houses all data for its operations. Archives also require storage, processing power, planning, and maintenance. A significantly large and costly data center is necessary to accommodate millions of users and/or systems to connect to the service. There is a tremendous amount of overhead in providing such a service. Data center processing power, data capacity, data transmission bandwidth and speed, infrastructure entities, and various performance considerations are quite costly. Costs include real estate required, utility bills for electricity and cooling, system maintenance, personnel to operate a successful business with service(s), etc. A method is needed to prevent large data center costs while eliminating performance issues for features sought. It is inevitable

that as users are hungry for more features and functionality on their mobile data processing systems, processing will be moved closer to the device for optimal performance and infrastructure cost savings.

5 Service delivered location dependent content was disclosed in U.S. Patents 6,456,234; 6,731,238; 7,187,997 (Johnson). Anonymous location based services was disclosed in U.S. PTO Publication 2006/0022048 (Johnson). The Johnson patents and published application operate as most web services do in that the clients connecting to the service benefit from the service by having some connectivity to the service. U.S. Publication 2006/0022048 (Johnson) could cause large numbers of users to inundate the
10 service with device heartbeats and data to maintain, depending on the configurations made. While this may be of little concern to a company that has successfully deployed substantially large web service resources, it may be of great concern to other more frugal companies. A method is needed for enabling location dependent features and functionality without the burden of requiring a service.

15 Users are skeptical about their privacy as internet services proliferate. A service by its very nature typically holds information for a user maintained in a centralized service database. The user's preferences, credential information, permissions, customizations, billing information, surfing habits, and other conceivable user configurations and activity monitoring, can be housed by the service at the service. Company insiders, as well as
20 outside attackers, may get access. Most people are concerned with preventing personal information of any type being kept in a centralized database which may potentially become compromised from a security standpoint. Location based services are of even more concern, in particular when the locations of the user are to be known to a centralized service. A method and system is needed for making users comfortable with knowing that
25 their personal information is at less risk of being compromised.

A reasonable requirement is to push intelligence out to the mobile data processing systems themselves, for example, in knowing their own locations and perhaps the locations of other nearby mobile data processing systems. Mobile data processing systems can intelligently handle many of their own application requirements without
30 depending on some remote service. Just as two people in a business organization should not need a manager to speak to each other, no two mobile data processing systems should require a service middleman for useful location dependent features and

functionality. The knowing of its own location should not be the end of social interaction implementation local to the mobile data processing systems, but rather the starting place for a large number of useful distributed local applications that do not require a service.

5 Different users use different types of Mobile data processing Systems (MSs) which are also called mobile devices: laptops, tablet computers, Personal Computers (PCs), Personal Digital Assistants (PDAs), cell phones, automobile dashboard mounted data processing systems, shopping cart mounted data processing systems, mobile vehicle or apparatus mounted data processing systems, Personal Navigational Devices (PNDs), iPhones (iPhone is a trademark of Apple, Inc.), various handheld mobile data processing systems, etc. MSs move freely in the environment, and are unpredictably moveable (i.e. can be moved anywhere, anytime). Many of these Mobile data processing Systems (MSs) do not have capability of being automatically located, or are not using a service for being automatically located. Conventional methods use directly relative stationary references such as satellites, antennas, etc. to locate MSs. Stationary references are expensive to deploy, and risk obsolescence as new technologies are introduced to the marketplace. 10 Stationary references have finite scope of support for locating MSs.

While the United States E911 mandate for cellular devices documents requirements for automatic location of a Mobile data processing System (MS) such as a cell phone, the mandate does not necessarily promote real time location and tracking of the MSs, nor does it define architecture for exploiting Location Based Services (LBS). We are in an era where Location Based Services (LBS), and location dependent features and functionality, are among the most promising technologies in the world. Automatic locating of every Mobile data processing System (MS) is an evolutionary trend. A method is needed to shorten the length of time for automatically locating every MS. Such a goal can be costly using prior art technologies such as GPS (Global Positioning System), radio wave triangulation, coming within range to a known located sensor, or the like. Complex system infrastructure, or added hardware costs to the MSs themselves, make such ventures costly and time constrained by schedules and costs involved in engineering, construction, and deployment. 20

30 A method is needed for enabling users to get location dependent features and functionality through having their mobile locations known, regardless of whether or not

their MS is equipped for being located. Also, new and modern location dependent features and functionality can be provided to a MS unencumbered by a connected service.

BRIEF SUMMARY OF THE INVENTION

5 LBS (Location Based Services) is a term which has gained in popularity over the years as MSs incorporate various location capability. The word “Services” in that terminology plays a major role in location based features and functionality involving interaction between two or more users. This disclosure introduces a new terminology, system, and method referred to as Location Based eXchanges (LBX). LBX is an acronym used interchangeably/contextually throughout this disclosure for the singular term
10 “Location Based Exchange” and for the plural term “Location Based Exchanges”, much the same way LBS is used interchangeably/contextually for the single term “Location Based Service” and for the plural term “Location Based Services”. LBX describes leveraging the distributed nature of connectivity between MSs in lieu of leveraging a
15 common centralized service nature of connectivity between MSs. The line can become blurred between LBS and LBX since the same or similar features and functionality are provided, and in some cases strengths from both may be used. The underlying architectural shift differentiates LBX from LBS for depending less on centralized services, and more on distributed interactions between MSs. LBX provide server-free and server-
20 less location dependent features and functionality.

 Disclosed are many different aspects to LBX, starting with the foundation requirement for each participating MS to know, at some point in time, their own whereabouts. LBX is enabled when an MS knows its own whereabouts. It is therefore a goal to first make as many MSs know their own whereabouts as possible. When two or
25 more MSs know their own whereabouts, LBX enables distributed locational applications whereby a server is not required to middleman social interactions between the MSs. The MSs interact as peers. LBX disclosed include purely peer to peer interactions, peer to peer interactions for routing services, peer to peer interactions for delivering distributed services, and peer to peer interactions for location dependent features and functionality.
30 One embodiment of an LBX enabled MS is referred to as an lbxPhone™.

 It is an advantage herein to have no centralized service governing location based features and functionality among MSs. Avoiding a centralized service prevents

performance issues, infrastructure costs, and solves many of the issues described above. No centralized service also prevents a user's information from being kept in one accessible place. LBS contain centralized data that is personal in nature to its users. This is a security concern. Having information for all users in one place increases the likelihood that a disaster to the data will affect more than a single user. LBX spreads data out across participating systems so that a disaster affecting one user does not affect any other user.

It is an advantage herein for enabling useful distributed applications without the necessity of having a service, and without the necessity of users and/or systems registering with a service. MSs interact as peers in preferred embodiments, rather than as clients to a common service (e.g. internet connected web service).

It is an advantage herein for locating as many MSs as possible in a wireless network, and without additional deployment costs on the MSs or the network. Conventional locating capability includes GPS (Global Positioning System) using stationary orbiting satellites, improved forms of GPS, for example AGPS (Adjusted GPS) and DGPS (Differential GPS) using stationary located ground stations, wireless communications to stationary located cell tower base stations, TDOA (Time Difference of Arrival) or AOA (Angle of Arrival) triangulation using stationary located antennas, presence detection in vicinity of a stationary located antenna, presence detection at a wired connectivity stationary network location, or other conventional locating systems and methods. Mobile data processing systems, referred to as Indirectly Located Mobile data processing systems (ILMs), are automatically located using automatically detected locations of Directly Located Mobile data processing systems (DLMs) and/or automatically detected locations of other ILMs. ILMs are provided with the ability to participate in the same LBS, or LBX, as a DLM (Directly Located Mobile data processing system). DLMs are located using conventional locating capability mentioned above. DLMs provide reference locations for automatically locating ILMs, regardless of where any one is currently located. DLMs and ILMs can be highly mobile, for example when in use by a user. There are a variety of novel methods for automatically locating ILMs, for example triangulating an ILM (Indirectly Located Mobile data processing system) location using a plurality of DLMs, detecting the ILM being within the vicinity of at least one DLM, triangulating an ILM location using a plurality of other ILMs, detecting the ILM being within the vicinity of at least one other ILM, triangulating an ILM location using a mixed set of

DLM(s) and ILM(s), determining the ILM location from heterogeneously located DLMs and/or ILMs, and other novel methods.

MSs are automatically located without using direct conventional means for being automatically located. The conventional locating capability (i.e. conventional locating methods) described above is also referred to as direct methods. Conventional methods are direct methods, but not all direct methods are conventional. There are new direct techniques disclosed below. Provided herein is an architecture, as well as systems and methods, for immediately bringing automatic location detection to every MS in the world, regardless of whether that MS is equipped for being directly located. MSs without capability of being directly located are located by leveraging the automatically detected locations of MSs that are directly located. This is referred to as being indirectly located. An MS which is directly located is hereinafter referred to as a Directly Located Mobile data processing system (DLM). For a plural acronym, MSs which are directly located are hereinafter referred to as Directly Located Mobile data processing systems (DLMs). MSs without capability of being directly located are located using the automatically detected locations of MSs that have already been located. An MS which is indirectly located is hereinafter referred to as an Indirectly Located Mobile data processing system (ILM). For a plural acronym, MSs which are indirectly located are hereinafter referred to as Indirectly Located Mobile data processing systems (ILMs). A DLM can be located in the following ways:

- A) New triangulated wave forms;
- B) Missing Part Triangulation (MPT) as disclosed below;
- C) Heterogeneous direct locating methods;
- D) Assisted Direct Location Technology (ADLT) using a combination of direct and indirect methods;
- E) Manually specified; and/or
- F) Any combinations of A) through E);

DLMs provide reference locations for automatically locating ILMs, regardless of where the DLMs are currently located. It is preferable to assure an accurate location of every DLM, or at least provide a confidence value of the accuracy. A confidence value of the accuracy is used by relative ILMs to determine which are the best set (e.g. which are of highest

priority for use to determine ILM whereabouts) of relative DLMs (and/or ILMs) to use for automatically determining the location of the ILM.

In one example, the mobile locations of several MSs are automatically detected using their local GPS chips. Each is referred to as a DLM. The mobile location of a non-locatable MS is triangulated using radio waves between it and three (3) of the GPS equipped DLMs. The MS becomes an ILM upon having its location determined relative the DLMs. ILMs are automatically located using DLMs, or other already located ILMs. An ILM can be located in the following ways:

- G) Triangulating an ILM location using a plurality of DLMs with wave forms of any variety (e.g. AOA, TDOA, MPT (a heterogeneous location method));
- H) Detecting the ILM being within the reasonably close vicinity of at least one DLM;
- I) Triangulating an ILM location using a plurality of other ILMs with wave forms of any variety;
- J) Detecting the ILM being within the reasonable close vicinity of at least one other ILM;
- K) Triangulating an ILM location using a mixed set of DLM(s) and ILM(s) with wave forms of any variety (referred to as ADLT);
- L) Determining the ILM location from heterogeneously located DLMs and/or ILMs (i.e. heterogeneously located, as used here, implies having been located relative different location methodologies);
- M) A) through F) Above; and/or
- N) Any combinations of A) through M).

Locating functionality may leverage GPS functionality, including but not limited to GPS, AGPS (Adjusted GPS), DGPS, (Differential GPS), or any improved GPS embodiment to achieve higher accuracy using known locations, for example ground based reference locations. The Nextel GPS enabled iSeries cell phones provide excellent examples for use as DLMs (Nextel is a trademark of Sprint/Nextel). Locating functionality may incorporate triangulated locating of the MS, for example using a class of Radio Frequency (RF) wave spectrum (cellular, WiFi, bluetooth, etc), and may use measurements from different wave spectrums for a single location determination (depends on communications interface(s) 70 available). A MS may have its whereabouts

determined using a plurality of wave spectrum classes available to it (cellular, WiFi, bluetooth, etc). Locating functionality may include in-range proximity detection for detecting the presence of the MS. Wave forms for triangulated locating also include microwaves, infrared wave spectrum relative infrared sensors, visible light wave spectrum relative light visible light wave sensors, ultraviolet wave spectrum relative ultraviolet wave sensors, X-ray wave spectrum relative X-ray wave sensors, gamma ray wave spectrum relative gamma ray wave sensors, and longwave spectrum (below AM) relative longwave sensors. While there are certainly more common methods for automatically locating a MS (e.g. radio wave triangulation, GPS, in range proximity detection), those skilled in the art recognize there are methods for different wave spectrums being detected, measured, and used for carrying information between data processing systems.

Kubler et al (U.S. PTO publications 2004/0264442, 2004/0246940, 2004/0228330, 2004/0151151) disclosed methods for detecting presence of mobile entities as they come within range of a sensor. In Kubler et al, accuracy of the location of the detected MS is not well known, so an estimated area of the whereabouts of the MS is enough to accomplish intended functionality, for example in warehouse installations. A confidence value of this disclosure associated with Kubler et al tends to be low (i.e. not confident), with lower values for long range sensors and higher values for short range sensors.

GPS and the abundance of methods for improving GPS accuracy has led to many successful systems for located MSs with high accuracy. Triangulation provides high accuracies for locating MSs. A confidence value of this disclosure associated with GPS and triangulating location methods tends to be high (i.e. confident). It is preferred that DLMs use the highest possible accuracy method available so that relative ILMs are well located. Not all DLMs need to use the same location methods. An ILM can be located relative DLMs, or other ILMs, that each has different locating methodologies utilized.

Another advantage herein is to generically locate MSs using varieties and combinations of different technologies. MSs can be automatically located using direct conventional methods for accuracy to base on the locating of other MSs. MSs can be automatically located using indirect methods. Further, it is an advantage to indirectly locate a MS relative heterogeneously located MSs. For example, one DLM may be automatically located using GPS. Another DLM may be automatically located using cell tower triangulation. A third DLM may be automatically located using within range proximity.

An ILM can be automatically located at a single location, or different locations over time, relative these three differently located DLMs. The automatically detected location of the ILM may be determined using a form of triangulation relative the three DLMs just discussed, even though each DLM had a different direct location method used. In a preferred embodiment, industry standard IEEE 802.11 Wi-Fi is used to locate (triangulate) an ILM relative a plurality of DLMs (e.g. TDOA in one embodiment). This standard is prolific among more compute trended MSs. Any of the family of 802.11 wave forms such as 802.11a, 802.11b, 802.11g, or any other similar class of wave spectrum can be used, and the same spectrum need not be used between a single ILM and multiple DLMs. 802.x used herein generally refers to the many 802.whatever variations.

Another advantage herein is to make use of existing marketplace communications hardware, communications software interfaces, and communications methods and location methods where possible to accomplish locating an MS relative one or more other MSs. While 802.x is widespread for Wi-Fi communications, other RF wave forms can be used (e.g. cell phone to cell tower communications). In fact, any wave spectrum for carrying data applies herein.

Still another advantage is for support of heterogeneous locatable devices. Different people like different types of devices as described above. Complete automation of locating functionality can be provided to a device through local automatic location detection means, or by automatic location detection means remote to the device. Also, an ILM can be located relative a laptop, a cell phone, and a PDA (i.e. different device types).

Yet another advantage is to prevent the unnecessary storing of large amounts of positioning data for a network of MSs. Keeping positioning data for knowing the whereabouts of all devices can be expensive in terms of storage, infrastructure, performance, backup, and disaster recovery. A preferred embodiment simply uses a distributed approach to determining locations of MSs without the overhead of an all-knowing database maintained somewhere. Positions of MSs can be determined “on the fly” without storing information in a master database. However, there are embodiments for storing a master database, or a subset thereof, to configurable storage destinations, when it makes sense. A subset can be stored at a MS.

Another advantage includes making use of existing location equipped MSs to expand the network of locatable devices by locating non-equipped MSs relative the

location of equipped MSs. MSs themselves help increase dimensions of the locatable network of MSs. The locatable network of MSs is referred to as an LN-Expanse (i.e. Location-Network Expanse). An LN-Expanse dynamically grows and shrinks based on where MSs are located at a particular time. For example, as users travel with their personal MSs, the personal MSs themselves define the LN-Expanse since the personal MSs are used to locate other MSs. An ILM simply needs location awareness relative located MSs (DLMs and/or ILMs).

Yet another advantage is a MS interchangeably taking on the role of a DLM or ILM as it travels. MSs are chameleons in this regard, in response to location technologies that happen to be available. A MS may be equipped for DLM capability, but may be in a location at some time where the capability is inoperable. In these situations the DLM takes on the role of an ILM. When the MS again enters a location where it can be a DLM, it automatically takes on the role of the DLM. This is very important, in particular for emergency situations. A hiker has a serious accident in the mountains which prevents GPS equipped DLM capability from working. Fortunately, the MS automatically takes on the role of an ILM and is located within the vicinity of neighboring (nearby) MSs. This allows the hiker to communicate his location, operate useful locational application functions and features at his MS, and enable emergency help that can find him.

It is a further advantage that MS locations be triangulated using any wave forms (e.g. RF, microwaves, infrared, visible light, ultraviolet, X-ray, gamma ray). X-ray and gamma ray applications are special in that such waves are harmful to humans in short periods of times, and such applications should be well warranted to use such wave forms. In some medical embodiments, micro-machines may be deployed within a human body. Such micro-machines can be equipped as MSs. Wave spectrums available at the time of deployment can be used by the MSs for determining exact positions when traveling through a body.

It is another advantage to use TDOA (Time Difference Of Arrival), AOA (Angle Of Arrival), and Missing Part Triangulation (MPT) when locating a MS. TDOA uses time information to determine locations, for example for distances of sides of a triangle. AOA uses angles of arrival to antennas to geometrically assess where a MS is located by intersecting lines drawn from the antennas with detected angles. MPT is disclosed herein as using combinations of AOA and TDOA to determine a location. Exclusively using all

AOA or exclusively using all TDOA is not necessary. MPT can be a direct method for locating MSs.

Yet another advantage is to locate MSs using Assisted Direct Location Technology (ADLT). ADLT is disclosed herein as using direct (conventional) location capability together with indirect location capability to confidently determine the location of a MS.

Still another advantage is to permit manual specification for identifying the location of a MS (a DLM). The manual location can then in turn be used to facilitate locating other MSs. A user interface may be used for specification of a DLM location. The user interface can be local, or remote, to the DLM. Various manual specification methods are disclosed. Manual specification is preferably used with less mobile MSs, or existing MSs such as those that use dodgeball.com (trademark of Google). The confidence value depends on how the location is specified, whether or not it was validated, and how it changes when the MS moves after being manually set. Manual specification should have limited scope in an LN-expanse unless inaccuracies can be avoided.

Another advantage herein is locating a MS using any of the methodologies above, any combinations of the methodologies above, and any combinations of direct and/or indirect location methods described.

Another advantage is providing synergy between different locating technologies for smooth operations as an MS travels. There are large numbers of methods and combinations of those methods for keeping an MS informed of its whereabouts. Keeping an MS informed of its whereabouts in a timely manner is critical in ensuring LBX operate optimally, and for ensuring nearby MSs without certain locating technologies can in turn be located.

It is another advantage for locating an MS with multiple location technologies during its travels, and in using the best of breed data from multiple location technologies to infer a MS location confidently. Confidence values are associated with reference location information to ensure an MS using the location information can assess accuracy. A DLM is usually an “affirmifier”. An affirmifier is an MS with its whereabouts information having high confidence of accuracy and can serve as a reference for other MSs. An ILM can also be an affirmifier provided there is high confidence that the ILM location is known. An MS (e.g. ILM) may be a “pacifier”. A pacifier is an MS having location information for its

whereabouts with a low confidence for accuracy. While it can serve as a reference to other ILMs, it can only do so by contributing a low confidence of accuracy.

It is an advantage to synergistically make use of the large number of locating technologies available to prevent one particular type of technology to dominate others while using the best features of each to assess accurate mobile locations of MSs.

A further advantage is to leverage a data processing system with capability of being located for co-locating another data processing system without any capability of being located. For example, a driver owns an older model automobile, has a useful second data processing system in the automobile without means for being automatically located. The driver also own a cell phone, called a first data processing system, which does have means for being automatically located. The location of the first data processing system can be shared with the second data processing system for locating the second data processing system. Further still, the second data processing system without means for being automatically located is located relative a first set (plurality) of data processing systems which are not at the same location as the second data processing system. So, data processing systems are automatically located relative at least one other data processing which can be automatically located.

Another advantage is a LBX enabled MS includes a service informant component for keeping a supervisory service informed. This prevents an MS from operating in total isolation, and prevents an MS from operating in isolation with those MSs that are within its vicinity (e.g. within maximum range 1306) at some point in time, but to also participate when the same MSs are great distances from each other. There are LBX which would fit well into an LBS model, but a preferred embodiment chooses to use the LBX model. For example, multiple MS users are seeking to carpool to and from a common destination. The service informant component can perform timely updates to a supervisory service for route comparisons between MSs, even though periods of information are maintained only at the MSs. For example, users find out that they go to the same church with similar schedules, or coworkers find out they live nearby and have identical work schedules. The service informant component can keep a service informed of MS whereabouts to facilitate novel LBX applications.

It is a further advantage in leveraging the vast amount of MS WiFi deployment underway in the United States. More widespread WiFi availability enhances the ability for well performing peer to peer types of features and functionality disclosed.

5 It is a further advantage to prevent unnecessary established connections from interfering with successfully triangulating a MS position. As the MS roams and encounters various wave spectrum signals, that is all that is required for determining the MS location. Broadcast signaling contains the necessary location information for automatically locating the MS.

10 Yet another advantage is to leverage Network Time Protocol (NTP) for eliminating bidirectional communications in determining Time of Arrival (TOA) and TDOA (Time Difference Of Arrival) measurements (TDOA as used in the disclosure generally refers to both TOA and TDOA). NTP enables a single unidirectional transmission of data to carry all that is necessary in determining TDOA, provided the sending data processing system and the receiving data processing system are NTP synchronized to an adequate granulation of
15 time.

A further advantage herein is to leverage existing “usual communications” data transmissions for carrying new data that is ignored by existing MS processing, but observed by new MS processing, for carrying out processing maximizing location functions and features across a large geography. Alternatively, new data can be transmitted
20 between systems for the same functionality.

Further features and advantages of the disclosure, as well as the structure and operation of various embodiments of the disclosure, are described in detail below with reference to the accompanying drawings. In the drawings, like reference numbers
25 generally indicate identical, functionally similar, and/or structurally similar elements. The drawing in which an element first appears is indicated by the leftmost digit(s) in the corresponding reference number, except that reference numbers 1 through 99 may be found on the first 4 drawings of Figs. 1A through 1D. None of the drawings, discussions, or materials herein is to be interpreted as limiting to a particular embodiment. The
30 broadest interpretation is intended. Other embodiments accomplishing same functionality are within the spirit and scope of this disclosure. It should be understood that information

is presented by example and many embodiments exist without departing from the spirit and scope of this disclosure.

BRIEF DESCRIPTION OF THE DRAWINGS

5 There is no guarantee that there are descriptions in this specification for explaining every novel feature found in the drawings. The present disclosure will be described with reference to the accompanying drawings, wherein:

 Fig. 1A depicts a preferred embodiment high level example componentization of a MS in accordance with the present disclosure;

10 Fig. 1B depicts a Location Based eXchanges (LBX) architectural illustration for discussing the present disclosure;

 Fig. 1C depicts a Location Based Services (LBS) architectural illustration for discussing prior art of the present disclosure;

 Fig. 1D depicts a block diagram of a data processing system useful for
15 implementing a MS, ILM, DLM, centralized server, or any other data processing system disclosed herein;

 Fig. 1E depicts a network illustration for discussing various deployments of whereabouts processing aspects of the present disclosure;

 Fig. 2A depicts an illustration for describing automatic location of a MS through the
20 MS coming into range of a stationary cellular tower;

 Fig. 2B depicts an illustration for describing automatic location of a MS through the MS coming into range of some stationary antenna;

 Fig. 2C depicts an illustration for discussing an example of automatically locating a MS through the MS coming into range of some stationary antenna;

25 Fig. 2D depicts a flowchart for describing a preferred embodiment of a service whereabouts update event of an antenna in-range detected MS when MS location awareness is monitored by a stationary antenna or cell tower;

 Fig. 2E depicts a flowchart for describing a preferred embodiment of an MS whereabouts update event of an antenna in-range detected MS when MS location
30 awareness is monitored by the MS;

 Fig. 2F depicts a flowchart for describing a preferred embodiment of a procedure for inserting a Whereabouts Data Record (WDR) to an MS whereabouts data queue;

Fig. 3A depicts a locating by triangulation illustration for discussing automatic location of a MS;

Fig. 3B depicts a flowchart for describing a preferred embodiment of the whereabouts update event of a triangulated MS when MS location awareness is monitored by some remote service;

Fig. 3C depicts a flowchart for describing a preferred embodiment of the whereabouts update event of a triangulated MS when MS location awareness is monitored by the MS;

Fig. 4A depicts a locating by GPS triangulation illustration for discussing automatic location of a MS;

Fig. 4B depicts a flowchart for describing a preferred embodiment of the whereabouts update event of a GPS triangulated MS;

Fig. 5A depicts a locating by stationary antenna triangulation illustration for discussing automatic location of a MS;

Fig. 5B depicts a flowchart for describing a preferred embodiment of the whereabouts update event of a stationary antenna triangulated MS;

Fig. 6A depicts a flowchart for describing a preferred embodiment of a service whereabouts update event of a physically or logically connected MS;

Fig. 6B depicts a flowchart for describing a preferred embodiment of a MS whereabouts update event of a physically or logically connected MS;

Figs. 7A, 7B and 7C depict a locating by image sensory illustration for discussing automatic location of a MS;

Fig. 7D depicts a flowchart for describing a preferred embodiment of graphically locating a MS, for example as illustrated by Figs. 7A through 7C;

Fig. 8A heterogeneously depicts a locating by arbitrary wave spectrum illustration for discussing automatic location of a MS;

Fig. 8B depicts a flowchart for describing a preferred embodiment of locating a MS through physically contacting the MS;

Fig. 8C depicts a flowchart for describing a preferred embodiment of locating a MS through a manually entered whereabouts of the MS;

Fig. 9A depicts a table for illustrating heterogeneously locating a MS;

Fig. 9B depicts a flowchart for describing a preferred embodiment of heterogeneously locating a MS;

Figs. 10A and 10B depict an illustration of a Locatable Network expanse (LN-Expanse) for describing locating of an ILM with all DLMs;

5 Fig. 10C depicts an illustration of a Locatable Network expanse (LN-Expanse) for describing locating of an ILM with an ILM and DLM;

Figs. 10D, 10E, and 10F depict an illustration of a Locatable Network expanse (LN-Expanse) for describing locating of an ILM with all ILMs;

10 Fig. 10G and 10H depict an illustration for describing the infinite reach of a Locatable Network expanse (LN-Expanse) according to MSs;

Fig. 10I depicts an illustration of a Locatable Network expanse (LN-Expanse) for describing a supervisory service;

Fig. 11A depicts a preferred embodiment of a Whereabouts Data Record (WDR) 1100 for discussing operations of the present disclosure;

15 Figs. 11B, 11C and 11D depict an illustration for describing various embodiments for determining the whereabouts of an MS;

Fig. 11E depicts an illustration for describing various embodiments for automatically determining the whereabouts of an MS;

20 Fig. 12 depicts a flowchart for describing an embodiment of MS initialization processing;

Figs. 13A through 13C depict an illustration of data processing system wireless data transmissions over some wave spectrum;

Fig. 14A depicts a flowchart for describing a preferred embodiment of MS LBX configuration processing;

25 Fig. 14B depicts a continued portion flowchart of Fig. 14A for describing a preferred embodiment of MS LBX configuration processing;

Fig. 15A depicts a flowchart for describing a preferred embodiment of DLM role configuration processing;

30 Fig. 15B depicts a flowchart for describing a preferred embodiment of ILM role configuration processing;

Fig. 15C depicts a flowchart for describing a preferred embodiment of a procedure for Manage List processing;

Fig. 16 depicts a flowchart for describing a preferred embodiment of NTP use configuration processing;

Fig. 17 depicts a flowchart for describing a preferred embodiment of WDR maintenance processing;

5 Fig. 18 depicts a flowchart for describing a preferred embodiment of a procedure for variable configuration processing;

Fig. 19 depicts an illustration for describing a preferred embodiment multithreaded architecture of peer interaction processing of a MS in accordance with the present disclosure;

10 Fig. 20 depicts a flowchart for describing a preferred embodiment of MS whereabouts broadcast processing;

Fig. 21 depicts a flowchart for describing a preferred embodiment of MS whereabouts collection processing;

15 Fig. 22 depicts a flowchart for describing a preferred embodiment of MS whereabouts supervisor processing;

Fig. 23 depicts a flowchart for describing a preferred embodiment of MS timing determination processing;

Fig. 24A depicts an illustration for describing a preferred embodiment of a thread request queue record;

20 Fig. 24B depicts an illustration for describing a preferred embodiment of a correlation response queue record;

Fig. 24C depicts an illustration for describing a preferred embodiment of a WDR request record;

25 Fig. 25 depicts a flowchart for describing a preferred embodiment of MS WDR request processing;

Fig. 26A depicts a flowchart for describing a preferred embodiment of MS whereabouts determination processing;

Fig. 26B depicts a flowchart for describing a preferred embodiment of processing for determining a highest possible confidence whereabouts;

30 Fig. 27 depicts a flowchart for describing a preferred embodiment of queue prune processing;

Fig. 28 depicts a flowchart for describing a preferred embodiment of MS termination processing;

Fig. 29A depicts a flowchart for describing a preferred embodiment of a process for starting a specified number of threads in a specified thread pool; and

5 Fig. 29B depicts a flowchart for describing a preferred embodiment of a procedure for terminating the process started by Fig. 29A.

DETAILED DESCRIPTION OF THE INVENTION

With reference now to detail of the drawings, the present disclosure is described. Obvious error handling is omitted from the flowcharts in order to focus on the key aspects of the present disclosure. Obvious error handling includes database I/O errors, field validation errors, errors as the result of database table/data constraints or unique keys, data access errors, communications interface errors or packet collision, hardware failures, checksum validations, bit error detections/corrections, and any other error handling as well known to those skilled in the relevant art in context of this disclosure. A semicolon may be used in flowchart blocks to represent, and separate, multiple blocks of processing within a single physical block. This allows simpler flowcharts with less blocks in the drawings by placing multiple blocks of processing description in a single physical block of the flowchart. Flowchart processing is intended to be interpreted in the broadest sense by example, and not for limiting methods of accomplishing the same functionality. Preferably, field validation in the flowcharts checks for SQL injection attacks, communications protocol sniff and hack attacks, preventing of spoofing MS addresses, syntactical appropriateness, and semantics errors where appropriate. Disclosed user interface processing and/or screenshots are also preferred embodiment examples that can be implemented in other ways without departing from the spirit and scope of this disclosure. Alternative user interfaces (since this disclosure is not to be limiting) will use similar mechanisms, but may use different mechanisms without departing from the spirit and scope of this disclosure.

Locational terms such as whereabouts, location, position, area, destination, perimeter, radius, geofence, situational location, or any other related two or three dimensional locational term used herein to described position(s) and/or locations and/or whereabouts is to be interpreted in the broadest sense. Location field 1100c may include an area (e.g. on earth), a point (e.g. on earth), or a three dimensional bounds in space. In

another example, a radius may define a sphere in space, rather than a circle in a plane. In some embodiments, a planet field forms part of the location (e.g. Earth, Mars, etc as part of field 1100c) for which other location information (e.g. latitude and longitude on Mars also part of field 1100c) is relative. In some embodiments, elevations (or altitudes) from known locatable point(s), distances from origin(s) in the universe, etc. can denote where exactly is a point of three dimensional space, or three dimensional sphere, area, or solid, is located. That same point can provide a mathematical reference to other points of the solid area/region in space. Descriptions for angles, pitches, rotations, etc from some reference point(s) may be further provided. Three dimensional areas/regions include a conical shape, cubical shape, spherical shape, pyramidal shape, irregular shapes, or any other shape either manipulated with a three dimensional graphic interface, or with mathematical model descriptions. Areas/regions in space can be occupied by a MS, passed through (e.g. by a traveler) by a MS, or referenced through configuration by a MS. In a three dimensional embodiment, nearby/nearness is determined in terms of three dimensional information, for example, a spherical radius around one MS intersecting a spherical radius around another MS. In a two dimensional embodiment, nearby/nearness is determined in terms of two dimensional information, for example, a circular radius around one MS intersecting a circular radius around another MS. Points can be specified as a point in a x-y-z plane, a point in polar coordinates, or the like, perhaps the center of a planet (e.g. Earth) or the Sun, some origin in the Universe, or any other origin for distinctly locating three dimensional location(s), positions, or whereabouts in space. Elevation (e.g. for earth, or some other planet, etc) may be useful to the three dimensional point of origin, and/or for the three dimensional region in space. A region in space may also be specified with connecting x-y-z coordinates together to bound the three dimensional region in space. There are many methods for representing a location (field 1100c) without departing from the spirit and scope of this disclosure. MSs, for example as carried by users, can travel by airplane through three dimensional areas/regions in space, or travel under the sea through three dimensional regions in space.

Various embodiments of communications between MSs, or an MS and service(s), will share channels (e.g. frequencies) to communicate, depending on when in effect. Sharing a channel will involve carrying recognizable and processable signature to distinguish transmissions for carrying data. Other embodiments of communications

between MSs, or an MS and service(s), will use distinct channels to communicate, depending on when in effect. The number of channels that can be concurrently listened on and/or concurrently transmitted on by a data processing system will affect which embodiments are preferred. The number of usable channels will also affect which
5 embodiments are preferred. This disclosure avoids unnecessary detail in different communication channel embodiments so as to not obfuscate novel material. Independent of various channel embodiments within the scope and spirit of the present disclosure, MSs communicate with other MSs in a peer to peer manner, in some aspects like automated walkie-talkies.

10 Novel features disclosed herein need not be provided as all or none. Certain features may be isolated in some MS embodiments, or may appear as any subset of features and functionality in other embodiments.

Location Based eXchanges (LBX) Architecture

15 Fig. 1A depicts a preferred embodiment high level example componentization of a MS in accordance with the present disclosure. A MS 2 includes processing behavior referred to as LBX Character 4 and Other Character 32. LBX character 4 provides processing behavior causing MS 2 to take on the character of a Location Based Exchange (LBX) MS according to the present disclosure. Other Character 32 provides processing
20 behavior causing MS to take on character of prior art MSs in context of the type of MS. Other character 32 includes at least other processing code 34, other processing data 36, and other resources 38, all of which are well known to those skilled in the art for prior art MSs. In some embodiments, LBX character 4 components may, or may not, make use of other character 32 components 34, 36, and 38. Other character 32 components may, or
25 may not, make use of LBX character 4 components 6 through 30.

LBX character 4 preferably includes at least Peer Interaction Processing (PIP) code 6, Peer Interaction Processing (PIP) data 8, self management processing code 18, self management processing data 20, WDR queue 22, send queue 24, receive queue 26, service informant code 28, and LBX history 30. Peer interaction processing (PIP) code 6
30 comprises executable code in software, firmware, or hardware form for carrying out LBX processing logic of the present disclosure when interacting with another MS. Peer interaction processing (PIP) data 8 comprises data maintained in any sort of memory of

MS 2, for example hardware memory, flash memory, hard disk memory, a removable memory device, or any other memory means accessible to MS 2. PIP data 8 contains intelligence data for driving LBX processing logic of the present disclosure when interacting with other MSs. Self management processing code 18 comprises executable code in software, firmware, or hardware form for carrying out the local user interface LBX processing logic of the present disclosure. Self management processing data 20 contains intelligence data for driving processing logic of the present disclosure as disclosed for locally maintained LBX features. WDR queue 22 contains Whereabouts Data Records (WDRs) 1100, and is a First-In-First-Out (FIFO) queue when considering housekeeping for pruning the queue to a reasonable trailing history of inserted entries (i.e. remove stale entries). WDR queue 22 is preferably designed with the ability of queue entry retrieval processing similar to Standard Query Language (SQL) querying, wherein one or more entries can be retrieved by querying with a conditional match on any data field(s) of WDR 1100 and returning lists of entries in order by an ascending or descending key on one or any ascending/descending ordered list of key fields.

All disclosed queues (e.g. 22, 24, 26, 1980 and 1990 (See Fig. 19)) are implemented with an appropriate thread-safe means of queue entry peeking (makes copy of sought queue entry without removing), discarding, retrieval, insertion, and queue entry field sorted search processing. Queues are understood to have an associated implicit semaphore to ensure appropriate synchronous access to queue data in a multi-threaded environment to prevent data corruption and misuse. Such queue interfaces are well known in popular operating systems. In MS operating system environments which do not have an implicit semaphore protected queue scheme, queue accesses in the present disclosure flowcharts are to be understood to have a previous request to a queue-assigned semaphore lock prior to queue access, and a following release of the semaphore lock after queue access. Operating systems without semaphore control may use methods to achieve similar thread-safe synchronization functionality. Queue functionality may be accomplished with lists, arrays, databases (e.g. SQL) and other methodologies without departing from the spirit and scope of queue descriptions herein.

Queue 22 alternate embodiments may maintain a plurality of WDR queues which segregate WDRs 1100 by field(s) values to facilitate timely processing. WDR queue 22 may be at least two (2) separate queues: one for maintaining the MS 2 whereabouts, and

one for maintaining whereabouts of other MSs. WDR queue 22 may be a single instance WDR 1100 in some embodiments which always contains the most current MS 2 whereabouts for use by MS 2 applications (may use a sister queue 22 for maintaining WDRs from remote MSs). At least one entry is to be maintained to WDR queue 22 at all times for MS 2 whereabouts.

Send queue 24 (Transmit (Tx) queue) is used to send communications data, for example as intended for a peer MS within the vicinity (e.g. nearby as indicated by maximum range 1306) of the MS 2. Receive queue 26 (Receive (Rx) queue) is used to receive communications data, for example from peer MSs within the vicinity (e.g. nearby as indicated by maximum range 1306) of the MS 2. Queues 24 and 26 may also each comprise a plurality of queues for segregating data thereon to facilitate performance in interfacing to the queues, in particular when different queue entry types and/or sizes are placed on the queue. A queue interface for sending/receiving data to/from the MS is optimal in a multi-threaded implementation to isolate communications transport layers to processing behind the send/receive queue interfaces, but alternate embodiments may send/receive data directly from a processing thread disclosed herein. Queues 22, 24, and/or 26 may be embodied as a purely data form, or SQL database, maintained at MS 2 in persistent storage, memory, or any other storage means. In some embodiments, queues 24 and 26 are not necessary since other character 32 will already have accessible resources for carrying out some LBX character 4 processing.

Queue embodiments may contain fixed length records, varying length records, pointers to fixed length records, or pointers to varying length records. If pointers are used, it is assumed that pointers may be dynamically allocated for record storage on insertions and freed upon record use after discards or retrievals.

As well known to those skilled in the art, when a thread sends on a queue 24 in anticipation of a corresponding response, there is correlation data in the data sent which is sought in a response received by a thread at queue 26 so the sent data is correlated with the received data. In a preferred embodiment, correlation is built using a round-robin generated sequence number placed in data for sending along with a unique MS identifier (MS ID). If data is not already encrypted in communications, the correlation can be encrypted. While the unique MS identifier (MS ID) may help the MS identify which (e.g. wireless) data is destined for it, correlation helps identify which data at the MS caused the

response. Upon receipt of data from a responder at queue 26, correlation processing uses the returned correlation (e.g. field 1100m) to correlate the sent and received data. In preferred embodiments, the sequence number is incremented each time prior to use to ensure a unique number, otherwise it may be difficult to know which data received is a response to which data was sent, in particular when many data packets are sent within seconds. When the sequence number reaches a maximum value (e.g. $2^{32} - 1$), then it is round-robbined to 0 and is incremented from there all over again. This assures proper correlation of data between the MS and responders over time. There are other correlation schemes (e.g. signatures, random number generation, checksum counting, bit patterns, date/time stamp derivatives) to accomplish correlation functionality. If send and receive queues of Other Character 32 are used, then correlation can be used in a similar manner to correlate a response with a request (i.e. a send with a receipt).

There may be good reason to conceal the MS ID when transmitting it wirelessly. In this embodiment, the MS ID is a dependable and recognizable derivative (e.g. a pseudo MS ID) that can be detected in communications traffic by the MS having the pseudo MS ID, while concealing the true MS ID. This would conceal the true MS ID from would-be hackers sniffing wireless protocol. The derivative can always be reliably the same for simplicity of being recognized by the MS while being difficult to associate to a particular MS. Further still, a more protected MS ID (from would-be hackers that take time to deduce how an MS ID is scrambled) can itself be a dynamically changing correlation anticipated in forthcoming communications traffic, thereby concealing the real MS ID (e.g. phone number or serial number), in particular when anticipating traffic in a response, yet still useful for directing responses back to the originating MS (with the pseudo MS ID (e.g. correlation)). A MS would know which correlation is anticipated in a response by saving it to local storage for use until it becomes used (i.e. correlated in a matching response), or becomes stale. In another embodiment, a correlation response queue (like CR queue 1990) can be deployed to correlate responses with requests that contain different correlations for pseudo MS IDs. In all embodiments, the MS ID (or pseudo MS ID) of the present disclosure should enable targeting communications traffic to the MS.

Service informant code 28 comprises executable code in software, firmware, or hardware form for carrying out of informing a supervisory service. The present disclosure does not require a connected web service, but there are features for keeping a service

informed with activities of MS LBX. Service informant code 28 can communicate as requested any data 8, 20, 22, 24, 26, 30, 36, 38, or any other data processed at MS 2.

LBX history 30 contains historical data useful in maintaining at MS 2, and possibly useful for informing a supervisory service through service informant code 28. LBX History 30 preferably has an associated thread of processing for keeping it pruned to the satisfaction of a user of MS 2 (e.g. prefers to keep last 15 days of specified history data, and 30 days of another specified history data, etc). With a suitable user interface to MS 2, a user may browse, manage, alter, delete, or add to LBX History 30 as is relevant to processing described herein. Service informant code 28 may be used to cause sending of an outbound email, SMS message, outbound data packet, or any other outbound communication in accordance with LBX of the MS.

PIP data 8 preferably includes at least permissions 10, charters 12, statistics 14, and a service directory 16. Permissions 10 are configured to grant permissions to other MS users for interacting the way the user of MS 2 desires for them to interact. Therefore, permissions 10 contain permissions granted from the MS 2 user to other MS users. In another embodiment, permissions 10 additionally, or alternatively, contain permissions granted from other MS users to the MS 2 user. Permissions are maintained completely local to the MS 2. Charters 12 provide LBX behavior conditional expressions for how MSs should interact with MS 2. Charters 12 are configured by the MS 2 user for other MS users. In another embodiment, charters 12 additionally, or alternatively, are configured by other MS users for the MS 2 user. Some charters expressions depend on permissions 10. Statistics 14 are maintained at MS 2 for reflecting peer (MS) to peer (MS) interactions of interest that occurred at MS 2. In another embodiment, statistics 14 additionally, or alternatively, reflect peer (MS) to peer (MS) interactions that occurred at other MSs, preferably depending on permissions 10. Service informant code 28 may, or may not, inform a service of statistics 14 maintained. Service directory 16 includes routing entries for how MS 2 will find a sought service, or how another MS can find a sought service through MS 2.

In some embodiments, any code (e.g. 6, 18, 28, 34, 38) can access, manage, use, alter, or discard any data (e.g. 8, 20, 22, 24, 26, 30, 36, 38) of any other component in MS 2. Other embodiments may choose to keep processing of LBX character 4 and other character 32 disjoint from each other. Rectangular component boundaries are logical

component representations and do not have to delineate who has access to what. MS (also MSs) references discussed herein in context for the new and useful features and functionality disclosed is understood to be an MS 2 (MSs 2).

5 Fig. 1B depicts a Location Based eXchanges (LBX) architectural illustration for discussing the present disclosure. LBX MSs are peers to each other for locational features and functionality. An MS 2 communicates with other MSs without requiring a service for interaction. For example, Fig. 1B depicts a wireless network 40 of five (5) MSs. Each is able to directly communicate with others that are in the vicinity (e.g. nearby as indicated by maximum range 1306). In a preferred embodiment, communications are limited reliability wireless broadcast datagrams having recognizable data packet identifiers. In another embodiment, wireless communications are reliable transport protocols carried out by the MSs, such as TCP/IP. In other embodiments, usual communications data associated with other character 32 include new data (e.g. Communications Key 1304) in transmissions for being recognized by MSs within the vicinity. For example, as an MS conventionally communicates, LBX data is added to the protocol so that other MSs in the vicinity can detect, access, and use the data. The advantage to this is that as MSs use wireless communications to carry out conventional behavior, new LBX behavior is provided by simply incorporating additional information (e.g. Communications Key 1304) to existing communications.

20 Regardless of the embodiment, an MS 2 can communicate with any of its peers in the vicinity using methods described below. Regardless of the embodiment, a communication path 42 between any two MSs is understood to be potentially bidirectional, but certainly at least unidirectional. The bidirectional path 42 may use one communications method for one direction and a completely different communications method for the other, but ultimately each can communicate to each other. When considering that a path 42 comprises two unidirectional communications paths, there are $N * (N - 1)$ unidirectional paths for N MSs in a network 40. For example, 10 MSs results in 90 (i.e. $10 * 9$) one way paths of communications between all 10 MSs for enabling them to talk to each other. Sharing of the same signaling channels is preferred to minimize the number of MS threads listening on distinct channels. Flowcharts are understood to

process at incredibly high processing speeds, in particular for timely communications processing.

5 Fig. 1C depicts a Location Based Services (LBS) architectural illustration for discussing prior art of the present disclosure. In order for a MS to interact for LBS with another MS, there is service architecture 44 for accomplishing the interaction. For example, to detect that MS 1 is nearby MS N, the service is indispensably involved in maintaining data and carrying out processing. For example, to detect that MS 1 is arriving to, or departing from, a geofenced perimeter area configured by MS N, the service was
10 indispensably involved in maintaining data and carrying out processing. For example, for MS N to locate MS 1 on a live map, the service was indispensably involved in maintaining data and carrying out processing. In another example, to grant and revoke permissions from MS 1 to MS N, the service was indispensably involved in maintaining data and carrying out processing. While it is advantageous to require a single bidirectional path 46
15 for each MS (i.e. two unidirectional communications paths; $(2 * N)$ unidirectional paths for N MSs), there are severe requirements for service(s) when there are lots of MSs (i.e. when N is large). Wireless MSs have advanced beyond cell phones, and are capable of housing significant parallel processing, processing speed, increased wireless transmission speeds and distances, increased memory, and richer features.

20

Fig. 1D depicts a block diagram of a data processing system useful for implementing a MS, ILM, DLM, centralized server, or any other data processing system described herein. An MS 2 is a data processing system 50. Data processing system 50 includes at least one processor 52 (e.g. Central Processing Unit (CPU)) coupled to a bus
25 54. Bus 54 may include a switch, or may in fact be a switch 54 to provide dedicated connectivity between components of data processing system 50. Bus (and/or switch) 54 is a preferred embodiment coupling interface between data processing system 50 components. The data processing system 50 also includes main memory 56, for example, random access memory (RAM). Memory 56 may include multiple memory cards, types,
30 interfaces, and/or technologies. The data processing system 50 may include secondary storage devices 58 such as persistent storage 60, and/or removable storage device 62, for example as a compact disk, floppy diskette, USB flash, or the like, also connected to bus

(or switch) 54. In some embodiments, persistent storage devices could be remote to the data processing system 50 and coupled through an appropriate communications interface. Persistent storage 60 may include flash memory, disk drive memory, magnetic, charged, or bubble storage, and/or multiple interfaces and/or technologies, perhaps in software interface form of variables, a database, shared memory, etc.

The data processing system 50 may also include a display device interface 64 for driving a connected display device (not shown). The data processing system 50 may further include one or more input peripheral interface(s) 66 to input devices such as a keyboard, keypad, Personal Digital Assistant (PDA) writing implements, touch interfaces, mouse, voice interface, or the like. User input (“user input”, “user events” and “user actions” used interchangeably) to the data processing system are inputs accepted by the input peripheral interface(s) 66. The data processing system 50 may still further include one or more output peripheral interface(s) 68 to output devices such as a printer, facsimile device, or the like. Output peripherals may also be available via an appropriate interface.

Data processing system 50 will include a communications interface(s) 70 for communicating to another data processing system 72 via analog signal waves, digital signal waves, infrared proximity, copper wire, optical fiber, or other wave spectrums described herein. A MS may have multiple communications interfaces 70 (e.g. cellular connectivity, 802.x, etc). Other data processing system 72 may be an MS. Other data processing system 72 may be a service. Other data processing system 72 is a service data processing system when MS 50 communicates to other data processing system 72 by way of service informant code 28. In any case, the MS and other data processing system are said to be interoperating when communicating.

Data processing system programs (also called control logic) may be completely inherent in the processor(s) 52 being a customized semiconductor, or may be stored in main memory 56 for execution by processor(s) 52 as the result of a read-only memory (ROM) load (not shown), or may be loaded from a secondary storage device into main memory 56 for execution by processor(s) 52. Such programs, when executed, enable the data processing system 50 to perform features of the present disclosure as discussed herein. Accordingly, such data processing system programs represent controllers of the data processing system.

In some embodiments, the disclosure is directed to a control logic program product comprising at least one processor 52 having control logic (software, firmware, hardware microcode) stored therein. The control logic, when executed by processor(s) 52, causes the processor(s) 52 to provide functions of the disclosure as described herein. In another embodiment, this disclosure is implemented primarily in hardware, for example, using a prefabricated component state machine (or multiple state machines) in a semiconductor element such as a processor 52.

Those skilled in the art will appreciate various modifications to the data processing system 50 without departing from the spirit and scope of this disclosure. A data processing system, and more particularly a MS, preferably has capability for many threads of simultaneous processing which provide control logic and/or processing. These threads can be embodied as time sliced threads of processing on a single hardware processor, multiple processors, multi-core processors, Digital Signal Processors (DSPs), or the like, or combinations thereof. Such multi-threaded processing can concurrently serve large numbers of concurrent MS tasks. Concurrent processing may be provided with distinct hardware processing and/or as appropriate software driven time-sliced thread processing. Those skilled in the art recognize that having multiple threads of execution on an MS is accomplished in many different ways without departing from the spirit and scope of this disclosure. This disclosure strives to deploy software to existing MS hardware configurations, but the disclosed software can be deployed as burned-in microcode to new hardware of MSs.

Data processing aspects of drawings/flowcharts are preferably multi-threaded so that many MSs and applicable data processing systems are interfaced with in a timely and optimal manner. Data processing system 50 may also include its own clock mechanism (not shown), if not an interface to an atomic clock or other clock mechanism, to ensure an appropriately accurate measurement of time in order to appropriately carry out processing described below. In some embodiments, Network Time Protocol (NTP) is used to keep a consistent universal time for MSs and other data processing systems in communications with MSs. This is most advantageous to prevent unnecessary round-tripping of data between data processing systems to determine timing (e.g. Time Difference of Arrival (TDOA)) measurements. A NTP synchronized date/time stamp maintained in communications is compared by a receiving data processing system for comparing with its

own NTP date/time stamp to measure TOA (time of arrival (i.e. time taken to arrive)). Of course, in the absence of NTP used by the sender and receiver, TOA is also calculated in a bidirectional transmission using correlation. In this disclosure, TOA measurements from one location technology are used for triangulating with TOA measurements from another location technology, not just for determining “how close”. Therefore, TDOA terminology is generally used herein to refer to the most basic TOA measurement of a wave spectrum signal being the difference between when it was sent and when it was received. TDOA is also used to describe using the difference of such measurements to locate (triangulate). NTP use among participating systems has the advantage of a single unidirectional broadcast data packet containing all a receiving system requires to measure TDOA, by knowing when the data was sent (date/time stamp in packet) and when the data was received (signal detected and processed by receiving system). A NTP clock source (e.g. atomic clock) used in a network is to be reasonably granular to carry out measurements, and ensures participating MSs are updated timely according to anticipated time drifts of their own clocks. There are many well known methods for accomplishing NTP, some which require dedicated thread(s) for NTP processing, and some which use certain data transmitted to and from a source to keep time in synch.

Those skilled in the art recognize that NTP accuracy depends on participating MS clocks and processing timing, as well as time server source(s). Radio wave connected NTP time server(s) is typically accurate to as granular as 1 millisecond. Global Positioning System (GPS) time servers provide accuracy as granular as 50 microseconds. GPS timing receivers provide accuracy to around 100 nanoseconds, but this may be reduced by timing latencies in time server operating systems. With advancements in hardware, microcode, and software, obvious improvements are being made to NTP. In NTP use embodiments of this disclosure, an appropriate synchronization of time is used for functional interoperability between MSs and other data processing systems using NTP. NTP is not required in this disclosure, but it is an advantage when in use.

LBX Directly Located Mobile Data Processing Systems (DLMs)

Fig. 1E depicts a network illustration for discussing various deployments of whereabouts processing aspects of the present disclosure. In some embodiments, a

cellular network cluster 102 and cellular network cluster 104 are parts of a larger cellular network. Cellular network cluster 102 contains a controller 106 and a plurality of base stations, shown generally as base stations 108. Each base station covers a single cell of the cellular network cluster, and each base station 108 communicates through a wireless connection with the controller 106 for call processing, as is well known in the art. Wireless devices communicate via the nearest base station (i.e. the cell the device currently resides in), for example base station 108b. Roaming functionality is provided when a wireless device roams from one cell to another so that a session is properly maintained with proper signal strength. Controller 106 acts like a telephony switch when a wireless device roams across cells, and it communicates with controller 110 via a wireless connection so that a wireless device can also roam to other clusters over a larger geographical area. Controller 110 may be connected to a controller 112 in a cellular cluster through a physical connection, for example, copper wire, optical fiber, or the like. This enables cellular clusters to be great distances from each other. Controller 112 may in fact be connected with a physical connection to its base stations, shown generally as base stations 114. Base stations may communicate directly with the controller 112, for example, base station 114e. Base stations may communicate indirectly to the controller 112, for example base station 114a by way of base station 114d. It is well known in the art that many options exist for enabling interoperating communications between controllers and base stations for the purpose of managing a cellular network. A cellular network cluster 116 may be located in a different country. Base controller 118 may communicate with controller 110 through a Public Service Telephone Network (PSTN) by way of a telephony switch 120, PSTN 122, and telephony switch 124, respectively. Telephony switch 120 and telephony switch 124 may be private or public. In one cellular network embodiment of the present disclosure, the services execute at controllers, for example controller 110. In some embodiments, the MS includes processing that executes at a wireless device, for example mobile laptop computer 126, wireless telephone 128, a personal digital assistant (PDA) 130, an iPhone 170, or the like. As the MS moves about, positional attributes are monitored for determining location. The MS may be handheld, or installed in a moving vehicle. Locating a wireless device using wireless techniques such as Time Difference of Arrival (TDOA) and Angle Of Arrival (AOA) are well known in the art. The service may also execute on a server computer accessible to controllers, for example server computer 132, provided an

appropriate timely connection exists between cellular network controller(s) and the server computer 132. Wireless devices (i.e. MSs) are preferably known by a unique identifier, for example a phone number, caller id, device identifier, or like appropriate unique handle.

In another embodiment of the present disclosure, GPS satellites such as satellite 134, satellite 136, and satellite 138 provide information, as is well known in the art, to GPS devices on earth for triangulation locating of the GPS device. In this embodiment, a MS has integrated GPS functionality so that the MS monitors its positions. The MS is preferably known by a unique identifier, for example a phone number, caller id, device identifier, or like appropriate unique handle.

In yet another embodiment of the present disclosure, a physically connected device, for example, telephone 140, computer 142, PDA 144, telephone 146, and fax machine 148, may be newly physically connected to a network. Each is a MS, although the mobility is limited. Physical connections include copper wire, optical fiber, USB, or any other physical connection, by any communications protocol thereon. Devices are preferably known by a unique identifier, for example a phone number, caller id, device identifier, physical or logical network address, or like appropriate unique handle. The MS is detected for being newly located when physically connected. A service can be communicated to upon detecting connectivity. The service may execute at an Automatic Response Unit (ARU) 150, a telephony switch, for example telephony switch 120, a web server 152 (for example, connected through a gateway 154), or a like data processing system that communicates with the MS in any of a variety of ways as well known to those skilled the art. MS detection may be a result of the MS initiating a communication with the service directly or indirectly. Thus, a user may connect his laptop to a hotel network, initiate a communication with the service, and the service determines that the user is in a different location than the previous communication. A local area network (LAN) 156 may contain a variety of connected devices, each an MS that later becomes connected to a local area network 158 at a different location, such as a PDA 160, a server computer 162, a printer 164, an internet protocol telephone 166, a computer 168, or the like. Hard copy presentation could be made to printer 164 and fax 148.

Current technology enables devices to communicate with each other, and other systems, through a variety of heterogeneous system and communication methods. Current technology allows executable processing to run on diverse devices and systems.

Current technology allows communications between the devices and/or systems over a plethora of methodologies at close or long distance. Many technologies also exist for automatic locating of devices. It is well known how to have an interoperating communications system that comprises a plurality of individual systems communicating with each other with one or more protocols. As is further known in the art of developing software, executable processing of the present disclosure may be developed to run on a particular target data processing system in a particular manner, or customized at install time to execute on a particular data processing system in a particular manner.

Fig. 2A depicts an illustration for describing automatic location of a MS, for example a DLM 200, through the MS coming into range of a stationary cellular tower. A DLM 200, or any of a variety of MSs, travels within range of a cell tower, for example cell tower 108b. The known cell tower location is used to automatically detect the location of the DLM 200. In fact, any DLM that travels within the cell served by cell tower 108b is identified as the location of cell tower 108b. The confidence of a location of a DLM 200 is low when the cell coverage of cell tower 108b is large. In contrast, the confidence of a location of a DLM 200 is higher when the cell coverage of cell tower 108b is smaller. However, depending on the applications locating DLMs using this method, the locating can be quite acceptable. Location confidence is improved with a TDOA measurement for the elapsed time of communication between DLM 200 and cell tower to determine how close the MS is to the cell tower. Cell tower 108b can process all locating by itself, or with interoperability to other services as connected to cell tower 108b in Figure 1E. Cell tower 108b can communicate the location of DLM 200 to a service, to the DLM 200, to other MSs within its coverage area, any combination thereof, or to any connected data processing system, or MS, of Figure 1E.

Fig. 2B depicts an illustration for describing automatic location of a MS, for example a DLM 200, through the MS coming into range of some stationary antenna. DLM 200, or any of a variety of MSs, travels within range of a stationary antenna 202 that may be mounted to a stationary object 204. The known antenna location is used to automatically detect the location of the DLM 200. In fact, any DLM that travels within the coverage area served by antenna 202 is identified as the location of antenna 202. The confidence of a

location of a DLM 200 is low when the antenna coverage area of antenna 202 is large. In contrast, the confidence of a location of a DLM 200 is higher when the antenna coverage area of antenna 202 is smaller. However, depending on the applications locating DLMs using this method, the locating can be quite acceptable. Location confidence is improved with a TDOA measurement for the elapsed time of communication between DLM 200 and a particular antenna to determine how close the MS is to the antenna. Antenna 202 can process all locating by itself (with connected data processing system (not shown) as well known to those skilled in the art), or with interoperability to other services as connected to antenna 202, for example with connectivity described in Figure 1E. Antenna 202 can be used to communicate the location of DLM 200 to a service, to the DLM 200, to other MSs within its coverage area, any combination thereof, or to any connected data processing system, or MS, of Figure 1E.

Fig. 2C depicts an illustration for discussing an example of automatically locating a MS, for example a DLM 200, through the MS coming into range of some stationary antenna. DLM 200, or any of a variety of MSs, travels within range of a stationary antenna 212 that may be mounted to a stationary object, such as building 210. The known antenna location is used to automatically detect the location of the DLM 200. In fact, any DLM that travels within the coverage area served by antenna 212 is identified as the location of antenna 212. The confidence of a location of a DLM 200 is low when the antenna coverage area of antenna 212 is large. In contrast, the confidence of a location of a DLM 200 is higher when the antenna coverage area of antenna 212 is smaller. However, depending on the applications locating DLMs using this method, the locating can be quite acceptable. Location confidence is improved with a TDOA measurement as described above. Antenna 212 can process all locating by itself (with connected data processing system (not shown) as well known to those skilled in the art), or with interoperability to other services as connected to antenna 212, for example with connectivity described in Figure 1E. Antenna 212 can be used to communicate the location of DLM 200 to a service, to the DLM 200, to other MSs within its coverage area, any combination thereof, or to any connected data processing system, or MS, of Figure 1E.

Once DLM 200 is within the building 210, a strategically placed antenna 216 with a desired detection range within the building is used to detect the DLM 200 coming into its

proximity. Wall breakout 214 is used to see the antenna 216 through the building 210. The known antenna 216 location is used to automatically detect the location of the DLM 200. In fact, any DLM that travels within the coverage area served by antenna 216 is identified as the location of antenna 216. The confidence of a location of a DLM 200 is low when the antenna coverage area of antenna 216 is large. In contrast, the confidence of a location of a DLM 200 is higher when the antenna coverage area of antenna 216 is smaller. Travels of DLM 200 can be limited by objects, pathways, or other limiting circumstances of traffic, to provide a higher confidence of location of DLM 200 when located by antenna 216, or when located by any locating antenna described herein which detects MSs coming within range of its location. Location confidence is improved with a TDOA measurement as described above. Antenna 216 can process all locating by itself (with connected data processing system (not shown) as well known to those skilled in the art), or with interoperability to other services as connected to antenna 216, for example with connectivity described in Figure 1E. Antenna 216 can be used to communicate the location of DLM 200 to a service, to the DLM 200, to other MSs within its coverage area, any combination thereof, or to any connected data processing system, or MS, of Figure 1E. Other in-range detection antennas of a Figure 2C embodiment may be strategically placed to facilitate warehouse operations such as in Kubler et al.

Fig. 2D depicts a flowchart for describing a preferred embodiment of a service whereabouts update event of an antenna in-range detected MS, for example a DLM 200, when MS location awareness is monitored by a stationary antenna, or cell tower (i.e. the service thereof). Figs. 2A through 2C location detection processing are well known in the art. Fig. 2D describes relevant processing for informing MSs of their own whereabouts. Processing begins at block 230 when a MS signal deserving a response has been received and continues to block 232 where the antenna or cell tower service has authenticated the MS signal. A MS signal can be received for processing by blocks 230 through 242 as the result of a continuous, or pulsed, broadcast or beaconing by the MS (Fig. 13A), perhaps as part of usual communication protocol in progress for the MS (Fig. 13A usual data 1302 with embedded Communications Key (CK) 1304), or an MS response to continuous, or pulsed, broadcast or beaconing via the service connected antenna (Fig. 13C). MS and/or service transmission can be appropriately correlated for a

response (as described above) which additionally facilitates embodiments using TDOA measurements (time of communications between the MS and antenna, or cell tower) to determine at least how close is the MS in range (or use in conjunction with other data to triangulate the MS location). The MS is preferably authenticated by a unique MS identifier such as a phone number, address, name, serial number, or any other unique handle to the MS. In this, and any other embodiments disclosed, an MS may be authenticated using a group identifier handle indicating membership to a supported/known group deserving further processing. Authentication will preferably consult a database for authenticating that the MS is known. Block 232 continues to block 234 where the signal received is immediately responded back to the MS, via the antenna, containing at least correlation along with whereabouts information for a Whereabouts Data Record (WDR) 1100 associated with the antenna (or cell tower). Thereafter, the MS receives the correlated response containing new data at block 236 and completes a local whereabouts data record 1100 (i.e. WDR 1100) using data received along with other data determined by the MS.

In another embodiment, blocks 232 through 234 are not required. A service connected antenna (or cell tower) periodically broadcasts its whereabouts (WDR info (e.g. Fig. 13C)) and MSs in the vicinity use that directly at block 236. The MS can choose to use only the confidence and location provided, or may determine a TDOA measurement for determining how close it is. If the date/time stamp field 1100b indicates NTP is in use by the service, and the MS is also using NTP, then a TDOA measurement can be determined using the one unidirectional broadcast via the antenna by using the date/time stamp field 1100b received with when the WDR information was received by the MS (subtract time difference and use known wave spectrum for distance). If either the service or MS is not NTP enabled, then a bidirectional correlated data flow between the service and MS is used to assess a TDOA measurement in terms of time of the MS. One embodiment provides the TDOA measurement from the service to the MS. Another embodiment calculates the TDOA measurement at the MS.

Network Time protocol (NTP) can ensure MSs have the same atomic clock time as the data processing systems driving antennas (or cell towers) they will encounter. Then, date/time stamps can be used in a single direction (unidirectional) broadcast packet to determine how long it took to arrive to/from the MS. In an NTP embodiment, the MS (Fig.

13A) and/or the antenna (Fig. 13C) sends a date/time stamp in the pulse, beacon, or protocol. Upon receipt, the antenna (or cell tower) service data processing system communicates how long the packet took from an MS to the antenna (or cell tower) by comparing the date/time stamp in the packet and a date/time stamp of when it was received. The service may also set the confidence value, before sending WDR information to the MS. Similarly, an MS can compare a date/time stamp in the unidirectional broadcast packet sent from a locating service (Fig. 13C) with when received by the MS. So, NTP facilitates TDOA measurements in a single broadcast communication between systems through incorporation to usual communications data 1302 with a date/time stamp in Communications Key (CK) 1304, or alternatively in new data 1302. Similarly, NTP facilitates TDOA measurement in a single broadcast communication between systems through incorporation to usual communications data 1312 with a date/time stamp in Communications Key (CK) 1314, or alternatively in new data 1312.

The following template is used in this disclosure to highlight field settings. See Fig. 11A descriptions. Fields are set to the following upon exit from block 236:

MS ID field 1100a is preferably set with: Unique MS identifier of the MS invoking block 240. This field is used to uniquely distinguish this MS WDRs on queue 22 from other originated WDRs.

DATE/TIME STAMP field 1100b is preferably set with: Date/time stamp for WDR completion at block 236 to the finest granulation of time achievable by the MS. The NTP use indicator is set appropriately.

LOCATION field 1100c is preferably set with: Location of stationary antenna (or cell tower) as communicated by the service to the MS.

CONFIDENCE field 1100d is preferably set with: The same value (e.g. 76) for any range within the antenna (or cell tower), or may be adjusted using the TDOA measurement (e.g. amount of time detected by the MS for the response at block 234). The longer time it takes between the MS sending a signal detected at block 232 and the response with data back received by the MS (block 234), the less confidence there is for being located

because the MS must be a larger distance from the antenna or cell tower. The less time it takes between the MS sending a signal detected at block 232 and the response with data back, the more confidence there is for being located because the MS must be a closer distance to the antenna or cell tower. Confidence values are standardized for all location technologies. In some embodiments of Fig. 2D processing, a confidence value can be set for 1 through 100 (1 being lowest confidence and 100 being highest confidence) wherein a unit of measurement between the MS and antenna (or cell tower) is used directly for the confidence value. For example, 20 meters is used as the unit of measurement. For each unit of 20 meters distance determined by the TDOA measurement, assign a value of 1, up to a worst case of 100 (i.e. 2000 meters). Round the 20 meter unit of distance such that 0 meters to < 25 meters is 20 meters (i.e. 1 unit of measurement), 26 meters to < 45 meters is 40 meters (i.e. 2 units of measurement), and so on. Once the number of units is determined, subtract that number from 101 for the confidence value (i.e. 1 unit = confidence value 100, 20 units = confidence value 81; 100 units or greater = confidence value of 1). Yet another embodiment will use a standard confidence value for this “coming in range” technology such as 76 and then further increase or decrease the confidence using the TDOA measurement. Many embodiments exist for quantifying a higher versus lower confidence. In any case, a confidence value (e.g. 76) is determined by the MS, service, or both (e.g. MS uses TDOA measurement to modify confidence sent by service).

LOCATION TECHNOLOGY field 1100e is preferably set with: “Server Antenna Range” for an antenna detecting the MS, and is set to “Server Cell Range” for a cell tower detecting the MS. The originator indicator is set to DLM.

LOCATION REFERENCE INFO field 1100f is preferably set with: The period of time for communications between the antenna and the MS (a TDOA measurement), if known; a communications signal strength, if available; wave spectrum used (e.g. from MS receive processing), if available; particular communications interface 70, if available. The TDOA measurement may be converted to a distance using wave spectrum information. The values populated here should have already been factored into the confidence value at block 236.

COMMUNICATIONS REFERENCE INFO field 1100g is preferably set with: Parameters uniquely identifying a/the service (e.g. antenna (or cell tower)) and how to best communicate with it again, if available. May not be set, regardless if received from the service.

5

SPEED field 1100h is preferably set with: Data received by MS at block 234, if available.

HEADING field 1100i is preferably set with: Data received by MS at block 234, if available.

10

ELEVATION field 1100j is preferably set with: data received by MS at block 234, if available. Elevation field 1100j is preferably associated with the antenna (or cell tower) by the elevation/altitude of the antenna (or cell tower).

15

APPLICATION FIELDS field 1100k is preferably set with: Data received at block 234 by the MS, or set by data available to the MS, or set by both the locating service for the antenna (or cell tower) and the MS itself. Application fields include, and are not limited to, MS navigation APIs in use, social web site identifying information, application information for applications used, accessed, or in use by the MS, or any other information complementing whereabouts of the MS.

20

CORRELATION FIELD 1100m is preferably set with: Not Applicable (i.e. not maintained to queue 22).

25

SENT DATE/TIME STAMP field 1100n is preferably set with: Not Applicable (i.e. not maintained to queue 22).

RECEIVED DATE/TIME STAMP field 1100p is preferably set with: Not Applicable (i.e. not maintained to queue 22).

30

A service connected to the antenna (or cell tower) preferably uses historical information and artificial intelligence interrogation of MS travels to determine fields 1100h and 1100i. Block 236 continues to block 238 where parameters are prepared for passing

to Fig. 2F processing invoked at block 240. Parameters are set for: WDRREF = a reference or pointer to the WDR; DELETEQ = Fig. 2D location queue discard processing; and SUPER = Fig. 2D supervisory notification processing. Thereafter, block 240 invokes Fig. 2F processing and Fig. 2D processing terminates at block 242. Fig. 2F processing will insert to queue 22 so this MS knows at least its own whereabouts whenever possible. A single data instance embodiment of WDR queue 22 will cause Fig. 2F to update the single record of WDR information for being current upon exit from block 240 (this is true for all flowchart blocks invoking Fig. 2F processing).

With reference now to Fig. 2F, depicted is a flowchart for describing a preferred embodiment of a procedure for inserting a Whereabouts Data Record (WDR) 1100 to MS WDR queue 22. Appropriate semaphores are used for variables which can be accessed simultaneously by another thread other than the caller. With reference now to Fig. 2F, procedure processing starts at block 270 and continues to block 272 where parameters passed from the invoking block of processing, for example block 240, are determined. The variable WDRREF is set by the caller to a reference or pointer to the WDR so subsequent blocks of Fig. 2F can access the WDR. The variable DELETEQ is set by the caller so that block 292 knows how to discard obsolete location queue entries. The DELETEQ variable can be a multi-field record (or reference thereof) for how to prune. The variable SUPER is set by the caller so that block 294 knows under what condition(s), and which data, to contact a supervisory service. The SUPER variable can be a multi-field record (or reference thereof) for instruction.

Block 272 continues to block 274 where the DLMV (see Fig. 12 and later discussions for DLMV (DLM role(s) List Variable)), or ILMV (see Fig. 12 and later discussions for ILMV (ILM role(s) List Variable)), is checked for an enabled role matching the WDR for insertion (e.g. DLM: location technology field 1100e (technology and originator indicator) when MS ID = this MS; ILM: DLM or ILM indicator when MS ID not this MS). If no corresponding DLMV/ILMV role is enabled for the WDR to insert, then processing continues to block 294 (the WDR is not inserted to queue 22). If the ILMV/DLMV role for the WDR is enabled, then processing continues to block 276 where the confidence of the WDR 1100 is validated prior to insertion. An alternate embodiment to Fig. 2F will not have block 274 (i.e. block 272 continues directly to block 276) since

appropriate DLM and/or ILM processing may be terminated anyway when DLM/ILM role(s) are disabled (see Fig. 14A/B).

If block 276 determines the data to be inserted is not of acceptable confidence (e.g. field 1100d < confidence floor value (see Fig. 14A/B)), then processing continues to block 294 described below. If block 276 determines the data to be inserted is of acceptable confidence (e.g. field 1100d > 70), then processing continues to block 278 for checking the intent of the WDR insertion.

If block 278 determines the WDR for insert is a WDR describing whereabouts for this MS (i.e. MS ID matching MS of Fig. 2F processing (DLM: Figs. 2A through 9B, or ILM: Fig. 26A/B)), then processing continues to block 280. If block 278 determines the WDR for insert is from a remote ILM or DLM (i.e. MS ID does not match MS of Fig. 2F processing), then processing continues to block 290. Block 280 peeks the WDR queue 22 for the most recent highest confidence entry for this MS whereabouts by searching queue 22 for: the MS ID field 1100a matching the MS ID of Fig. 2F processing, and a confidence field 1100d greater than or equal to the confidence floor value, and a most recent date/time stamp field 1100b. Thereafter, if block 282 determines one was found, then processing continues to block 284, otherwise processing continues to block 286 where a Last Whereabouts date/Time stamp (LWT) variable is set to field 1100b of the WDR for insert (e.g. first MS whereabouts WDR), and processing continues to block 288.

If block 284 determines the WDR for insertion has significantly moved (i.e. using a movement tolerance configuration (e.g. 3 meters) with fields 1100c of the WDR for insert and the WDR peeked at block 280), then block 286 sets the LWT (Last Whereabouts date/Time stamp) variable (with appropriate semaphore) to field 1100b of the WDR for insert, and processing continues to block 288, otherwise processing continues directly to block 288 (thereby keeping the LWT as its last setting). The LWT is to hold the most recent date/time stamp of when the MS significantly moved as defined by a movement tolerance. The movement tolerance can be system defined or configured, or user configured in Fig. 14 by an option for configuration detected at block 1408, and then using the Configure Value procedure of Fig. 18 (like confidence floor value configuration).

Block 288 accesses the DLMV and updates it with a new DLM role if there is not one present for it. This ensures a correct list of DLMV roles are available for configuration by Fig. 14. Preferably, by default an unanticipated DLMV role is enabled (helps inform the

user of its availability). Likewise in another embodiment, ILMV roles can be similarly updated, in particular if a more granulated list embodiment is maintained to the ILMV, or if unanticipated results help to identify another configurable role. By default, block 274 should allow unanticipated roles to continue with WDR insertion processing, and then
5 block 288 can add the role, enable it, and a user can decide what to do with it in configuration (Fig. 14A/B).

Thereafter, the WDR 1100 is inserted to the WDR queue 22 at block 290, block 292 discards any obsolete records from the queue as directed by the caller (invoker), and processing continues to block 294. The WDR queue 22 preferably contains a list of
10 historically MS maintained Whereabouts Data Records (WDRs) as the MS travels. When the MS needs its own location, for example from an application access, or to help locate an ILM, the queue is accessed for returning the WDR with the highest confidence value (field 1100d) in the most recent time (field 1100b) for the MS (field 1100a). Block 292 preferably discards by using fields 1100b and 1100d relative to other WDRs. The queue
15 should not be allowed to get too large. This will affect memory (or storage) utilization at the MS as well as timeliness in accessing a sought queue entry. Block 292 also preferably discards WDRs from queue 22 by moving selected WDRs to LBX History 30.

As described above, queue interfaces assume an implicit semaphore for properly accessing queue 22. There may be ILMs requesting to be located, or local applications of
20 the MS may request to access the MS whereabouts. Executable thread(s) at the MS can access the queue in a thread-safe manner for responding to those requests. The MS may also have multiple threads of processing for managing whereabouts information from DLMS, ILMs, or stationary location services. The more concurrently executable threads available to the MS, the better the MS is able to locate itself and respond to others (e.g.
25 MSs). There can be many location systems and methods used to keeping a MS informed of its own whereabouts during travel. While the preferred embodiment is to maximize thread availability, the obvious minimum requirement is to have at least 1 executable thread available to the MS. As described above, in operating system environments without proper queue interfaces, queue access blocks are first preceded by an explicit request for
30 a semaphore lock to access queue 22 (waits until obtained), and then followed by a block for releasing the semaphore lock to another thread for use. Also, in the present disclosure it is assumed in blocks which access data accessible to more than 1 concurrent thread

(e.g. shared memory access to DLMV or ILMV at block 274) that an appropriate semaphore (created at block 1220) protect synchronous access.

If block 294 determines information (e.g. whereabouts) should be communicated by service informant code 28 to a supervisory service, for example a service 1050, then block 296 communicates specified data to the service and processing terminates at block 298 by returning to the invoker (caller). If block 294 determines a supervisory service is not to be informed, then processing terminates with an appropriate return to the caller at block 298. Service informant code 28, at block 296, can send information as data that is reliably acknowledged on receipt, or as a datagram which most likely (but unreliably) is received.

Depending on the SUPER variable, block 294 may opt to communicate every time a WDR is placed to the queue, or when a reasonable amount of time has passed since last communicating to the supervisory service, or when a WDR confidence reaches a certain sought value, or when any WDR field or fields contain certain sought information, or when a reasonably large number of entries exist in WDR queue 22, or for any processing condition encountered by blocks 270 through 298, or for any processing condition encountered by caller processing up to the invocation of Fig. 2F processing. Different embodiments will send a single WDR 1100 at block 296, a plurality of WDRs 1100, or any other data. Various SUPER parameter(s) embodiments for Fig. 2F caller parameters can indicate what, when, where and how to send certain data. Block 296 may send an email, an SMS message, or use other means for conveying data. Service informant code 28 may send LBX history 30, statistics 14 and/or any other data 8, data 20, queue data, data 36 or resources 38. Service informant code 28 may update data in history 30, statistics 14 or any other data 8, data 20, queue data, data 36 and/or resources 38, possibly using conditions of this data to determine what is updated. Blocks 294 and 296 may be omitted in some embodiments.

If a single WDR is sent at block 296 as passed to Fig. 2F processing, then the WDR parameter determined at block 272 is accessed. If a plurality of WDRs is sent at block 296, then block 296 appropriately interfaces in a thread-safe manner to queue 22, and sends the WDRs.

Some preferred embodiments do not incorporate blocks 278 through 286. (i.e. block 276 continues to block 288 if confidence ok). Blocks 278 through 286 are for the purpose of implementing maintaining a date/time stamp of last MS significant movement

(using a movement tolerance). Architecture 1900 uses Fig. 2F, as does DLM processing. Fig. 2F must perform well for the preferred multithreaded architecture 1900. Block 280 performs a peek, and block 284 can be quite timely depending on embodiments used for location field 1100c. A movement tolerance incorporated at the MS is not necessary, but may be nice to have. Therefore, blocks 278 through 286 are optional blocks of processing.

Fig. 2F may also maintain (with appropriate semaphore) the most recent WDR describing whereabouts of the MS of Fig. 2F processing to a single data record every time a new one is to be inserted. This allows applications needing current whereabouts to simply access a current WDR, rather than interface to a plurality of WDRs at queue 22. For example, there could be a new block 289 for updating the single WDR 1100 (just prior to block 290 such that incoming blocks to block 290 go to new block 289, and new block 289 continues to block 290).

With reference now to Fig. 2E, depicted is a flowchart for describing a preferred embodiment of an MS whereabouts update event of an antenna in-range detected MS, for example a DLM 200, when MS location awareness is monitored by the MS. Fig. 2E describes relevant processing for MSs to maintain their own whereabouts. Processing begins at block 250 when the MS receives a signal from an antenna (or cell tower) deserving a response and continues to block 252 where the antenna or cell tower signal is authenticated by the MS as being a legitimate signal for processing. The signal can be received for processing by blocks 250 through 264 as the result of a continuous, or pulsed, broadcast or beaconing by the antenna, or cell tower (Fig. 13C), or as part of usual communication protocol in progress with at least one MS (Fig. 13C usual data 1312 with embedded Communications Key 1314), or as a response via antenna to a previous MS signal (Fig. 13A). The signal is preferably authenticated by a data parsed signature deserving further processing. Block 252 continues to block 254 where the MS sends an outbound request for soliciting an immediate response from the antenna (or cell tower) service. The request by the MS is appropriately correlated (e.g. as described above) for a response, which additionally facilitates embodiments using TDOA measurements (time of communications between the MS and antenna, or cell tower) to determine how close is the MS in range. Block 254 waits for a response, or waits until a reasonable timeout, whichever occurs first. There are also multithreaded embodiments to breaking up Fig. 2E

where block 254 does not wait, but rather terminates Fig. 2E processing and depends on another thread to correlate the response and then continue processing blocks 256 through 260 (like architecture 1900).

Thereafter, if block 256 determines the request timed out, then processing terminates at block 264. If block 256 determines the response was received, then processing continues to block 258. Block 258 completes a WDR 1100 with appropriate response data received along with data set by the MS. See Fig 11A descriptions. Fields are set to the following upon exit from block 258:

MS ID field 1100a is preferably set with: Same as was described for Fig. 2D (block 236) above.

DATE/TIME STAMP field 1100b is preferably set with: Same as was described for Fig. 2D (block 236) above.

LOCATION field 1100c is preferably set with: Same as was described for Fig. 2D (block 236) above.

CONFIDENCE field 1100d is preferably set with: Same as was described for Fig. 2D (block 236) above.

LOCATION TECHNOLOGY field 1100e is preferably set with: "Client Antenna Range" for an antenna detecting the MS, and is set to "Client Cell Range" for a cell tower detecting the MS. The originator indicator is set to DLM.

LOCATION REFERENCE INFO field 1100f is preferably set with: Same as was described for Fig. 2D (block 236) above.

COMMUNICATIONS REFERENCE INFO field 1100g is preferably set with: Same as was described for Fig. 2D (block 236) above.

SPEED field 1100h is preferably set with: Same as was described for Fig. 2D (block 236) above.

5 *HEADING field 1100i is preferably set with: Same as was described for Fig. 2D (block 236) above.*

ELEVATION field 1100j is preferably set with: Same as was described for Fig. 2D (block 236) above.

10 *APPLICATION FIELDS field 1100k is preferably set with: Same as was described for Fig. 2D (block 236) above.*

CORRELATION FIELD 1100m is preferably set with: Not Applicable (i.e. not maintained to queue 22).

15 *SENT DATE/TIME STAMP field 1100n is preferably set with: Not Applicable (i.e. not maintained to queue 22).*

20 *RECEIVED DATE/TIME STAMP field 1100p is preferably set with: Not Applicable (i.e. not maintained to queue 22).*

25 The longer time it takes between sending a request and getting a response at block 254, the less confidence there is for being located because the MS must be a larger distance from the antenna or cell tower. The less time it takes, the more confidence there is for being located because the MS must be a closer distance to the antenna or cell tower. Confidence values are analogously determined as described for Fig. 2D. Fig. 2D NTP embodiments also apply here. NTP can be used so no bidirectional communications is required for TDOA measurement. In this embodiment, the antenna (or cell tower) sets a NTP date/time stamp in the pulse, beacon, or protocol. Upon receipt, the MS instantly
30 knows how long the packet took to be received by comparing the NTP date/time stamp in the packet and a MS NTP date/time stamp of when it was received (i.e. no request/response pair required). If location information is also present with the NTP

date/time stamp in data received at block 252, then block 252 can continue directly to block 258.

An alternate MS embodiment determines its own (direction) heading and/or speed for WDR completion based on historical records maintained to the WDR queue 22 and/or LBX history 30.

Block 258 continues to block 260 for preparing parameters for: WDRREF = a reference or pointer to the WDR; DELETEQ = Fig. 2E location queue discard processing; and SUPER = Fig. 2E supervisory notification processing. Thereafter, block 262 invokes the procedure (Fig. 2F processing) to insert the WDR to queue 22. After Fig. 2F processing of block 262, Fig. 2E processing terminates at block 264.

In alternative “coming within range” (same as “in range”, “in-range”, “within range”) embodiments, a unique MS identifier, or MS group identifier, for authenticating an MS for locating the MS is not necessary. An antenna emitting signals (Fig. 13C) will broadcast (in CK 1314 of data 1312) not only its own location information (e.g. location field 1100c), but also an NTP indicated date/time stamp field 1100b, which the receiving MS (also having NTP for time synchronization) uses to perform a TDOA measurement upon receipt. This will enable a MS to determine at least how close (e.g. radius 1318 range, radius 1320 range, radius 1322 range, or radius 1316 range) it is located to the location of the antenna by listening for and receiving the broadcast (e.g. of Fig. 13C). Similarly, in another embodiment, an NTP synchronized MS emits signals (Fig. 13A) and an NTP synchronized data processing system associated with a receiving antenna can make a TDOA measurement upon signal receipt. In other embodiments, more than a single unidirectional signal may be used while still preventing the requirement to recognize the MS to locate it. For example, an antenna emitting signals (e.g. Fig. 13C hotspot WiFi 802.x) will contain enough information for a MS to respond with correlation for being located, and visa-versa. In any case, there can be multi-directional exchanged signals for determining a TDOA measurement.

Fig. 3A depicts a locating by triangulation illustration for discussing automatic location of a MS, for example DLM 200. DLM 200 is located through triangulation, as is well known in the art. At least three base towers, for example, base tower 108b, base

tower 108d, and base tower 108f, are used for locating the MS. A fourth base tower may be used if elevation (or altitude) was configured for use in locating DLM 200. There are cases where only two base towers are necessary given routes of travel are limited and known, for example, in spread out roadways or limited configured locations. Base towers may also be antennas 108b, 108d, and 108f in similar triangulation embodiments.

Fig. 3B depicts a flowchart for describing a preferred embodiment of the whereabouts update event of a triangulated MS, for example DLM 200, when MS location awareness is monitored by some remote service. While Fig. 3A location determination with TDOA and AOA is well known in the art, Figs. 3B and 3C include relevant processing for MSs to maintain their own whereabouts. Processing begins at block 310 and continues to block 312 where base stations able to communicate to any degree with a MS continue reporting to their controller the MS signal strength with an MS identifier (i.e. a unique handle) and Time Difference of Arrival (TDOA) information, Angle of Arrival (AOA) information, or heterogeneously both TDOA and AOA (i.e. MPT), depending on the embodiment. The MS can pick signals from base stations. In some embodiments, the MS monitors a paging channel, called a forward channel. There can be multiple forward channels. A forward channel is the transmission frequency from the base tower to the MS. Either the MS provides broadcast heartbeats (Fig. 13A) for base stations, or the base stations provide heartbeats (Fig. 13C) for a response from the MS, or usual MS use protocol signals are detected and used (incorporating CK 1304 in usual data 1302 by MS, or CK 1314 in "usual data" 1312 by service). Usual data is the usual communications traffic data in carrying out other character 32 processing. Communication from the MS to the base tower is on what is called the reverse channel. Forward channels and reverse channel are used to perform call setup for a created session channel.

TDOA is calculated from the time it takes for a communication to occur from the MS back to the MS via the base tower, or alternatively, from a base tower back to that base tower via the MS. NTP may also be used for time calculations in a unidirectional broadcast from a base tower (Fig. 13C) to the MS, or from the MS (Fig. 13A) to a base tower (as described above). AOA is performed through calculations of the angle by which a signal from the MS encounters the antenna. Triangle geometry is then used to calculate a location. The AOA antenna is typically of a phased array type.

See “Missing Part Triangulation (MPT)” section below with discussions for Figs. 11A through 11E for details on heterogeneously locating the MS using both TDOA and AOA (i.e. Missing Part Triangulation (MPT)). Just as high school taught geometry for solving missing parts of a triangle, so to does MPT triangulate an MS location. Think of the length of a side of a triangle as a TDOA measurement – i.e. length of time, translatable to a distance. Think of the AOA of a signal to an antenna as one of the angles of a triangle vertice. Solving with MPT analogously uses geometric and trigonometric formulas to solve the triangulation, albeit at fast processing speeds.

Thereafter, if the MS is determined to be legitimate and deserving of processing (similar to above), then block 314 continues to block 316. If block 314 determines the MS is not participating with the service, in which case block 312 did little to process it, then processing continues back to block 312 to continue working on behalf of legitimate participating MSs. The controller at block 316 may communicate with other controllers when base stations in other cellular clusters are picking up a signal, for example, when the MS roams. In any case, at block 316, the controller(s) determines the strongest signal base stations needed for locating the MS, at block 316. The strongest signals that can accomplish whereabouts information of the MS are used. Thereafter, block 318 accesses base station location information for base stations determined at block 316. The base station provides stationary references used to (relatively) determine the location of the MS. Then, block 320 uses the TDOA, or AOA, or MPT (i.e. heterogeneously both AOA and TDOA) information together with known base station locations to calculate the MS location.

Thereafter, block 322 accesses historical MS location information, and block 324 performs housekeeping by pruning location history data for the MS by time, number of entries, or other criteria. Block 326 then determines a heading (direction) of the MS based on previous location information. Block 326 may perform Artificial Intelligence (AI) to determine where the MS may be going by consulting many or all of the location history data. Thereafter, block 328 completes a service side WDR 1100, block 330 appends the WDR information to location history data and notifies a supervisory service if there is one outside of the service processing of Fig. 3B. Processing continues to block 332 where the service communicates the WDR to the located MS.

Thereafter, the MS completes its own WDR at block 334 for adding to WDR queue 22 to know its own whereabouts whenever possible, and block 336 prepares parameters for invoking WDR insertion processing at block 338. Parameters are set for: WDRREF = a reference or pointer to the MS WDR; DELETEQ = Fig. 3B location queue discard processing; and SUPER = Fig. 3B supervisory notification processing (e.g. no supervisory notification processing because it was already handled at block 330, or by being in context of the Fig. 3B service processing). At block 338, the MS invokes Fig. 2F processing already described. After block 338, processing continues back to block 312. Of course, block 332 continues directly to block 312 at the service(s) since there is no need to wait for MS(s) processing in blocks 334 through 338. Fig. 3B processing is continuous for every MS in the wireless network 7 days a week, 24 hours a day.

See Fig 11A descriptions. Fields are set to the following upon exit from block 334:

MS ID field 1100a is preferably set with: Same as was described for Fig. 2D (block 236) above.

DATE/TIME STAMP field 1100b is preferably set with: Same as was described for Fig. 2D (block 236) above.

LOCATION field 1100c is preferably set with: The triangulated location of the MS as communicated by the service.

CONFIDENCE field 1100d is preferably set with: Confidence of triangulation determined by the service which is passed to the MS at block 332. The confidence value may be set with the same value (e.g. 85) regardless of how the MS was triangulated. In other embodiments, field 1100d will be determined (completely, or adjusting the value of 85) by the service for TDOA measurements used, AOA measurements, signal strengths, wave spectrum involved, and/or the abundance of particular MS signals available for processing by blocks 312 through 320. Higher confidences are assigned for smaller TDOA measurements (shorter distances), strong signal strengths, and numerous additional data points beyond what is necessary to locate the MS. Lower confidences are assigned for larger TDOA measurements, weak signal strengths, and minimal data points necessary to

locate the MS. A reasonable confidence can be assigned using this information as guidelines where 1 is the lowest confidence and 100 is the highest confidence.

5 *LOCATION TECHNOLOGY field 1100e is preferably set with:* “Server Cell TDOA”, “Server Cell AOA”, “Server Cell MPT”, “Server Antenna TDOA”, “Server Antenna AOA”, or “Server Antenna MPT”, depending on how the MS was located and what flavor of service was used. The originator indicator is set to DLM.

10 *LOCATION REFERENCE INFO field 1100f is preferably set with:* null (not set) for indicating that all triangulation data was factored into determining confidence, and none is relevant for a single TDOA or AOA measurement in subsequent processing (i.e. service did all the work).

15 *COMMUNICATIONS REFERENCE INFO field 1100g is preferably set with:* Same as was described for Fig. 2D (block 236) above.

20 *SPEED field 1100h is preferably set with:* Service WDR information at block 332, wherein the service used historical information and artificial intelligence interrogation of MS travels to determine, if available.

HEADING field 1100i is preferably set with: Service WDR information at block 332, wherein the service used historical information and artificial intelligence interrogation of MS travels to determine, if available.

25 *ELEVATION field 1100j is preferably set with:* Elevation/altitude, if available.

APPLICATION FIELDS field 1100k is preferably set with: Same as was described for Fig. 2D (block 236) above.

30 *CORRELATION FIELD 1100m is preferably set with:* Not Applicable (i.e. not maintained to queue 22).

SENT DATE/TIME STAMP field 1100n is preferably set with: Not Applicable (i.e. not maintained to queue 22).

RECEIVED DATE/TIME STAMP field 1100p is preferably set with: Not Applicable (i.e. not maintained to queue 22).

5
10
15
20
25
30

Fig. 3C depicts a flowchart for describing a preferred embodiment of the whereabouts update event of a triangulated MS, for example a DLM 200, when MS location awareness is monitored by the MS. Communications between the base stations and MS is similar to Fig. 3B processing except the MS receives information (Fig. 13C) for performing calculations and related processing. Processing begins at block 350 and continues to block 352 where the MS continues receiving (Fig. 13C) pulse reporting from base stations (or antennas). AOA, TDOA, and MPT (See “Missing Part Triangulation (MPT)” section below with discussions for Figs. 11A through 11E for details on heterogeneously locating the MS using both TDOA and AOA) can be used to locate the MS, so there are many possible signal types received at block 352. Then, block 354 determines the strongest signals which can accomplish a completed WDR, or at least a location, of the MS. Thereafter, block 356 parses base station location information from the pulse messages that are received by the MS. Block 358 communicates with base stations to perform TDOA and/or AOA measurements and calculations. The time it takes for a communication to occur from the MS back to the MS for TDOA, or alternatively, from a base tower back to that base tower can be used. NTP may also be used, as described above, so that base towers (or antennas) broadcast signals (Fig. 13C) picked up by the MS which already contain the base tower locations and NTP date/time stamps for TDOA calculations. Block 358 uses the TDOA and/or AOA information with the known base station information to determine the MS location. While AOA information from the base stations (or antennas) is used by the MS, various MS embodiments can use AOA information detected at an MS antenna provided the heading, yaw, pitch, and roll is known at the MS during the same time as signal reception by the MS. A 3-axis accelerometer (e.g. in iPhone) may also provide yaw, pitch and roll means for proper AOA calculation.

Thereafter, block 360 accesses historical MS location information (e.g. WDR queue 22 and/or LBX history 30) to prevent redundant information kept at the MS, and block 362

performs housekeeping by pruning the LBX history 30 for the MS by time, number of entries, or other criteria. Block 364 then determines a heading (direction) of the MS based on previous location information (unless already known from block 358 for AOA determination). Block 364 may perform Artificial Intelligence (AI) to determine where the MS may be going by consulting queue 22 and/or history 30. Thereafter, block 366 completes a WDR 1100, and block 368 prepares parameters for Fig. 2F processing: WDRREF = a reference or pointer to the MS WDR; DELETEQ = Fig. 3C location queue discard processing; and SUPER = Fig. 3B supervisory notification processing. Block 368 continues to block 370 for invoking Fig. 2F processing already described above. After block 370, processing continues back to block 352. Fig. 3C processing is continuous for the MS as long as the MS is enabled. In various multithreaded embodiments, many threads at the MS work together for high speed processing at blocks 352 through 358 for concurrently communicating to many stationary references.

See Fig 11A descriptions. Fields are set to the following upon exit from block 366:

MS ID field 1100a is preferably set with: Same as was described for Fig. 2D (block 236) above.

DATE/TIME STAMP field 1100b is preferably set with: Same as was described for Fig. 2D (block 236) above.

LOCATION field 1100c is preferably set with: The triangulated location of the MS as determined by the MS.

CONFIDENCE field 1100d is preferably set with: The confidence of triangulation as determined by the MS. Confidence may be set with the same value (e.g. 80 since MS may be moving during triangulation) regardless of how the MS was triangulated. In other embodiments, field 1100d will be determined (completely, or adjusting the value of 80) by the MS for TDOA measurements used, AOA measurements, signal strengths, wave spectrum involved, and/or the abundance of particular service signals available for processing. Higher confidences are assigned for smaller TDOA measurements (shorter distances), strong signal strengths, and numerous additional data points beyond what is

necessary to locate the MS. Lower confidences are assigned for larger TDOA measurements, weak signal strengths, and minimal data points necessary to locate the MS. A reasonable confidence can be assigned using this information as guidelines where 1 is the lowest confidence and 100 is the highest confidence.

5

LOCATION TECHNOLOGY field 1100e is preferably set with: “Client Cell TDOA”, “Client Cell AOA”, “Client Cell MPT”, “Client Antenna TDOA”, “Client Antenna AOA”, or “Client Antenna MPT”, depending on how the MS located itself. The originator indicator is set to DLM.

10

LOCATION REFERENCE INFO field 1100f is preferably set with: Data associated with selected best stationary reference(s) used by the MS: the selection location/whereabouts, TDOA measurement to it, and wave spectrum (and/or particular communications interface 70) used, if reasonable. The TDOA measurement may be converted to a distance using wave spectrum information. Also, preferably set herein is data associated with a selected best stationary reference used by the MS (may be same or different than for TDOA measurement): the selection location, AOA measurement to it, and heading, yaw, pitch, and roll values (or accelerometer readings), if reasonable. Values that may be populated here should have already been factored into the confidence value. There may be one or more stationary reference whereabouts with useful measurements maintained here for Fig. 26B processing of block 2652.

15

20

COMMUNICATIONS REFERENCE INFO field 1100g is preferably set with: Parameters referencing MS internals, if desired.

25

SPEED field 1100h is preferably set with: Speed determined by the MS using historical information (queue 22 and/or history 30) and artificial intelligence interrogation of MS travels to determine, if reasonable.

30

HEADING field 1100i is preferably set with: Heading determined by the MS using historical information (queue 22 and/or history 30) and artificial intelligence interrogation of MS travels to determine, if reasonable.

ELEVATION field 1100j is preferably set with: Elevation/altitude, if available.

5 *APPLICATION FIELDS field 1100k is preferably set with: Same as was described for Fig. 2D (block 236) above.*

CORRELATION FIELD 1100m is preferably set with: Not Applicable (i.e. not maintained to queue 22).

10 *SENT DATE/TIME STAMP field 1100n is preferably set with: Not Applicable (i.e. not maintained to queue 22).*

RECEIVED DATE/TIME STAMP field 1100p is preferably set with: Not Applicable (i.e. not maintained to queue 22).

15
20
25
30
In alternative triangulation embodiments, a unique MS identifier, or MS group identifier, for authenticating an MS for locating the MS is not necessary. An antenna emitting signals (Fig. 13C) will broadcast (CK 1314 of data 1312) not only its own location information, but also an NTP date/time stamp, which the receiving MS (also having NTP for time synchronization) uses to perform TDOA measurements upon receipt. This will enable a MS to determine how close (e.g. radius 1318 range, radius 1320 range, radius 1322 range, or radius 1316 range) it is located to the location of the antenna by listening for and receiving the broadcast (e.g. of Fig. 13C). Similarly, in another embodiment, an NTP synchronized MS emits signals (Fig. 13A) and an NTP synchronized data processing system associated with a receiving antenna can determine a TDOA measurement upon signal receipt. In other embodiments, more than a single unidirectional signal may be used while still preventing the requirement to recognize the MS to locate it. For example, an antenna emitting signals will contain enough information for a MS to respond with correlation for being located. Alternatively, an MS emitting signals will contain enough information for a service to respond with correlation for being located. In any case, there can be multi-directional exchanged signals for determining TDOA. Similarly, a service side

data processing system can interact with a MS for AOA information without requiring a known identifier of the MS (use request/response correlation).

5 Fig. 4A depicts a locating by GPS triangulation illustration for discussing automatic location of a MS, for example a DLM 200. A MS, for example DLM 200, is located through GPS triangulation as is well known in the art. At least three satellites, for example, satellite 134, satellite 136, and satellite 138, are necessary for locating the MS. A fourth satellite would be used if elevation, or altitude, was configured for use by the present disclosure. Ground based stationary references can further enhance whereabouts determination.

10 Fig. 4B depicts a flowchart for describing a preferred embodiment of the whereabouts update event of a GPS triangulated MS, for example a DLM 200. Repeated continuous GPS location processing begins at block 410 and continues to block 412 where the MS initializes to the GPS interface, then to block 414 for performing the conventional locating of the GPS enabled MS, and then to block 416 for calculating location information. In some embodiments, block 412 may only be necessary a first time prior to repeated invocations of Fig. 4B processing. Block 414 may be an implicit wait for pulses from satellites, or an event driven mechanism when GPS satellite pulses are received for synchronized collection, or a multithreaded implementation concurrently listening for, and processing collaboratively, the signals. Block 414 and block 416 processing is well known in the art. Thereafter, the MS completes a WDR 1100 at block 418, block 420 prepares parameters for Fig. 2F invocation, and block 422 invokes, with the WDR, the Fig. 2F processing (described above). Processing then terminates at block 424. Parameters prepared at block 420 are: WDRREF = a reference or pointer to the WDR; DELETEQ = Fig. 4B location queue discard processing; and SUPER = Fig. 4B supervisory notification processing. GPS location processing is preferably continuous for the MS as long as the MS is enabled.

See Fig. 11A descriptions. Fields are set to the following upon exit from block 418:

30 *MS ID field 1100a is preferably set with: Same as was described for Fig. 2D (block 236) above.*

DATE/TIME STAMP field 1100b is preferably set with: Same as was described for Fig. 2D (block 236) above.

LOCATION field 1100c is preferably set with: The GPS location of the MS.

5

CONFIDENCE field 1100d is preferably set with: Confidence of GPS variety (usually high) which may be set with the same value (e.g. 95 for DGPS, 93 for AGPS, and 90 for GPS). In other embodiments, field 1100d will be determined (completely, or amending the defaulted value) by the MS for timing measurements, signal strengths, and/or the abundance of particular signals available for processing, similarly to as described above. An MS may not be aware of the variety of GPS, in which case straight GPS is assumed.

10

LOCATION TECHNOLOGY field 1100e is preferably set with: “GPS”, “A-GPS”, or “D-GPS”, depending on (if known) flavor of GPS. The originator indicator is set to DLM.

15

LOCATION REFERENCE INFO field 1100f is preferably set with: null (not set) for indicating that data was factored into determining confidence, and none is relevant for a single TDOA or AOA measurement in subsequent processing.

20

COMMUNICATIONS REFERENCE INFO field 1100g is preferably set with: Parameters referencing MS internals, if desired.

SPEED field 1100h is preferably set with: Speed determined by the MS using a suitable GPS interface, or historical information (queue 22 and/or history 30) and artificial intelligence interrogation of MS travels to determine, if reasonable.

25

HEADING field 1100i is preferably set with: Heading determined by the MS using a suitable GPS interface, or historical information (queue 22 and/or history 30) and artificial intelligence interrogation of MS travels to determine, if reasonable.

30

ELEVATION field 1100j is preferably set with: Elevation/altitude, if available.

APPLICATION FIELDS field 1100k is preferably set with: Same as was described for Fig. 2D (block 236) above.

5 *CORRELATION FIELD 1100m is preferably set with:* Not Applicable (i.e. not maintained to queue 22).

SENT DATE/TIME STAMP field 1100n is preferably set with: Not Applicable (i.e. not maintained to queue 22).

10 *RECEIVED DATE/TIME STAMP field 1100p is preferably set with:* Not Applicable (i.e. not maintained to queue 22).

15 Fig. 5A depicts a locating by stationary antenna triangulation illustration for discussing automatic location of a MS, for example DLM 200. There may be communication/transmission issues when an MS is taken indoors. Shown is a top view of an indoor floor plan 502. Antenna stations 504 (shown generally as 504) are strategically placed over the area so that an MS can be located. Triangulation techniques again apply. At least three antenna stations, for example, station 504f, station 504h, and station 504i are used to locate the MS, for example DLM 200. In floor plan embodiments where aisles delimit travel, only two antenna stations may be necessary, for example at either end of the particular aisle. While most stations 504 may receive signals from the MS, only the strongest stations are used. Fig. 5A and associated discussions can also be used for an outside triangulation embodiment using a similar strategic antenna placement scheme. Processing described for Figs. 3A to 3C can also be used for an indoor embodiment as described by Fig. 5A.

20

25

30 Fig. 5B depicts a flowchart for describing a preferred embodiment of the whereabouts update event of a stationary antenna triangulated MS, for example a DLM 200. In one embodiment, indoor location technology of Pinpoint corporation (Pinpoint is a trademark of Pinpoint Corporation) is utilized to locate any MS that moves about the indoor location. The Pinpoint corporation methodology begins at block 510 and continues to block 512. A cell controller drives antenna stations to emit a broadcast signal from

every station. Any MS within range (i.e. indoors) will phase modulate its unique identifier onto a return signal it transmits, at block 514. Stations at block 516 receive the transmission and strength of signal. The cell controller that drives stations sorts out and selects the strongest (e.g. 3) signals. The cell controller, at block 518, also extracts the unique MS identifier from the return signal, and TDOA is used to calculate distances from the stations receiving the strongest signals from the MS at block 520. Alternative embodiments can use AOA or MPT to determine locations. The locations of the controller selected stations are registered in an overlay map in an appropriate coordinate system, landmark system, or grid of cells. Block 522 locates the MS using the overlay map, locations of the (e.g. 3) selected stations, and the calculated distances triangulated from the selected stations, using TDOA, AOA, or MPT in various embodiments. Thereafter, block 524 calculates location information of the MS. Processing continues with repeated broadcast at block 512 and subsequent processing for every MS within range.

Thereafter, block 526 accesses historical MS location information, performs housekeeping by pruning location history data for the MS by time, number of entries, or other criteria, and determines a heading (direction) of the MS based on previous location information. Block 526 may perform Artificial Intelligence (AI) to determine where the MS may be going by consulting many or all of the location history data. Thereafter, block 528 completes a service side WDR 1100, block 530 appends the WDR information to location history data and notifies a supervisory service if there is one outside of the service processing of Fig. 5B. Processing continues to block 532 where the service communicates the WDR to the located MS.

Thereafter, the MS completes the WDR at block 534 for adding to WDR queue 22. Thereafter, block 536 prepares parameters passed to Fig. 2F processing for: WDRREF = a reference or pointer to the MS WDR; DELETEQ = Fig. 5B location queue discard processing; and SUPER = Fig. 5B supervisory notification processing (e.g. no supervisory notification processing because it was already handled at block 530, or by being in context of the Fig. 5B service processing). Block 536 continues to block 538 where the MS invokes Fig. 2F processing already described above. After block 538, processing continues back to block 514. Of course, block 532 continues directly to block 514 at the service(s) since there is no need to wait for MS(s) processing in blocks 534 through 538.

Fig. 5B processing is continuous for every MS in the wireless network 7 days a week, 24 hours a day.

See Fig 11A descriptions. Fields are set to the following upon exit from block 534:

5 *MS ID field 1100a is preferably set with:* Same as was described for Fig. 2D (block 236) above.

DATE/TIME STAMP field 1100b is preferably set with: Same as was described for Fig. 2D (block 236) above.

10

LOCATION field 1100c is preferably set with: The triangulated location of the MS as communicated by the service.

15 *CONFIDENCE field 1100d is preferably set with:* Confidence of triangulation determined by the service which is passed to the MS at block 532. The confidence value may be set with the same value (e.g. 95 (normally high for triangulation using densely positioned antennas)) regardless of how the MS was triangulated. In other embodiments, field 1100d will be determined (completely, or adjusting the value of 95) by the service for TDOA measurements used, AOA measurements, signal strengths, wave spectrum involved,
20 and/or the abundance of particular MS signals available for processing. Higher confidences are assigned for smaller TDOA measurements (shorter distances), strong signal strengths, and numerous additional data points beyond what is necessary to locate the MS. Lower confidences are assigned for larger TDOA measurements, weak signal strengths, and minimal data points necessary to locate the MS. A reasonable confidence
25 can be assigned using this information as guidelines where 1 is the lowest confidence and 100 is the highest confidence.

30 *LOCATION TECHNOLOGY field 1100e is preferably set with:* "Server Antenna TDOA", "Server Antenna AOA", or "Server Antenna MPT", depending on how the MS was located and what flavor of service was used. The originator indicator is set to DLM.

LOCATION REFERENCE INFO field 1100f is preferably set with: null (not set) for indicating that all triangulation data was factored into determining confidence, and none is relevant for a single TDOA or AOA measurement in subsequent processing (i.e. service did all the work).

5

COMMUNICATIONS REFERENCE INFO field 1100g is preferably set with: Same as was described for Fig. 2D (block 236) above.

10

SPEED field 1100h is preferably set with: Service WDR information at block 532, wherein the service used historical information and artificial intelligence interrogation of MS travels to determine, if available.

15

HEADING field 1100i is preferably set with: Service WDR information at block 532, wherein the service used historical information and artificial intelligence interrogation of MS travels to determine, if available.

ELEVATION field 1100j is preferably set with: Elevation/altitude, if available.

20

APPLICATION FIELDS field 1100k is preferably set with: Same as was described for Fig. 2D (block 236) above.

CORRELATION FIELD 1100m is preferably set with: Not Applicable (i.e. not maintained to queue 22).

25

SENT DATE/TIME STAMP field 1100n is preferably set with: Not Applicable (i.e. not maintained to queue 22).

RECEIVED DATE/TIME STAMP field 1100p is preferably set with: Not Applicable (i.e. not maintained to queue 22).

30

Fig. 6A depicts a flowchart for describing a preferred embodiment of a service whereabouts update event of a physically, or logically, connected MS, for example a DLM

200. A MS may be newly located and physically, or logically, connected, whereby communications between the MS and service is over a physical/logical connection. Physical connections may occur by connecting a conduit for communications to the MS, or from the MS to a connection point. Conduits include ethernet cables, optical fiber, firewire, USB, or any other means for conduit for communications through a physical medium. Conduits also include wireless mediums (air) for transporting communications, such as when an MS comes into physical wireless range eligible for sending and receiving communications. Logical connections may occur, after a physical connection already exists, for example through a successful communication, or authenticated, bind between a MS and other MS, or MS and service. Logical connections also include the result of: successfully logging into an application, successfully authenticated for access to some resource, successfully identified by an application, or any other logical status upon a MS being certified, registered, signed in, authenticated, bound, recognized, affirmed, or the like.

Relevant processing begins at block 602 and continues to block 604 where an MS device is physically/logically connected to a network. Thereafter, the MS accesses a service at block 606. Then, at block 608, the service accesses historical MS location history along with the connectivity address, and block 610 performs housekeeping by pruning the location history data maintained for the MS by time, number of entries, or other criteria. Block 610 may perform Artificial Intelligence (AI) to determine where the MS may be going (e.g. using heading based on previous locations) by consulting much or all of the location history data. Thereafter, service processing at block 612 completes a service side WDR 1100, then the service appends WDR information to location history data at block 614, and may notify a supervisory service if there is one outside of the service processing of Fig. 6A. Processing continues to block 616 where the service communicates WDR information to the newly physically/logically connected MS. There are many embodiments for determining a newly connected MS location using a physical or logical address, for example consulting a database which maps locations to network addresses (e.g. location to logical ip address; location to physical wall jack/port; etc). Then, at block 618 the MS completes its own WDR using some information from block 616, Fig. 2F parameters are prepared at block 620, block 622 invokes Fig. 2F processing already described above, and processing terminates at block 624. Parameters are set at

block 620 for: WDRREF = a reference or pointer to the MS WDR; DELETEQ = Fig. 6A location queue discard processing; and SUPER = Fig. 6A supervisory notification processing (e.g. no supervisory notification processing because it was already handled at block 614, or by being in context of the Fig. 6A service processing). Of course, block 616
5 continues directly to block 624 at the service(s) since there is no need to wait for MS processing in blocks 618 through 622. Fig. 6A processing is available at any appropriate time in accordance with the underlying service.

See Fig 11A descriptions. Fields are set to the following upon exit from block 618:

10 *MS ID field 1100a is preferably set with:* Same as was described for Fig. 2D (block 236) above.

DATE/TIME STAMP field 1100b is preferably set with: Same as was described for Fig. 2D (block 236) above.

15 *LOCATION field 1100c is preferably set with:* The location of the MS as communicated by the service.

CONFIDENCE field 1100d is preferably set with: Confidence (determined by the service) according to how the MS was connected, or may be set with the same value (e.g. 100 for physical connect, 77 for logical connect (e.g. short range wireless)) regardless of how the MS was located. In other embodiments, field 1100d will be determined by the service for anticipated physical conduit range, wireless logical connect range, etc. The resulting confidence value can be adjusted based on other parameters analogously to as described
20 above.

LOCATION TECHNOLOGY field 1100e is preferably set with “Service Physical Connect” or “Service Logical Connect”, depending on how the MS connected. The originator indicator is set to DLM.

30 *LOCATION REFERENCE INFO field 1100f is preferably set with:* null (not set), but if a TDOA measurement can be made (e.g. short range logical connect, and using

methodologies described above), then a TDOA measurement, a communications signal strength, if available; and wave spectrum (and/or particular communications interface 70) used, if available. The TDOA measurement may be converted to a distance using wave spectrum information. Possible values populated here should have already been factored into the confidence value.

COMMUNICATIONS REFERENCE INFO field 1100g is preferably set with: Same as was described for Fig. 2D (block 236) above.

SPEED field 1100h is preferably set with: null (not set), but can be set with speed required to arrive to the current location from a previously known location, assuming same time scale is used.

HEADING field 1100i is preferably set with: null (not set), but can be set to heading determined when arriving to the current location from a previously known location.

ELEVATION field 1100j is preferably set with: Elevation/altitude (e.g. of physical connection, or place of logical connection detection), if available.

APPLICATION FIELDS field 1100k is preferably set with: Same as was described for Fig. 2D (block 236) above.

CORRELATION FIELD 1100m is preferably set with: Not Applicable (i.e. not maintained to queue 22).

SENT DATE/TIME STAMP field 1100n is preferably set with: Not Applicable (i.e. not maintained to queue 22).

RECEIVED DATE/TIME STAMP field 1100p is preferably set with: Not Applicable (i.e. not maintained to queue 22).

Fig. 6B depicts a flowchart for describing a preferred embodiment of a MS whereabouts update event of a physically, or logically, connected MS, for example a DLM 200. A MS may be newly located and physically/logically connected, whereby communications between the MS and service is over a physical/logical connection as described in Fig. 6A above. Relevant processing begins at block 640 and continues to block 642 where an MS device is physically/logically connected. Thereafter, at block 644 the MS accesses the connectivity service and waits for an acknowledgement indicating a successful connection. Upon acknowledgement receipt, processing continues to block 646 where the MS requests WDR information via the connectivity service and waits for the data (i.e. connectivity service may be different than the location service, or may be one in the same). As part of connectivity, location service pointer(s) (e.g. ip address for <http://112.34.323.18> referencing or a Domain Name Service (DNS) name like <http://www.servicename.com>) are provided with the connectivity acknowledgement from the connectivity service at block 644, so the MS knows how to proceed at block 646 for retrieving location information. There are various embodiments for the location service determining a MS location as described above for Fig. 6A. In an alternative embodiment, the MS already knows how to locate itself wherein block 644 continues directly to block 648 (no block 646) because the MS maintains information for determining its own whereabouts using the physical or logical address received in the acknowledgement at block 644. Similar mapping of a network address to the MS location can be in MS data, for example data 36, data 8, or data 20. At block 648, the MS completes its WDR 1100. Thereafter, block 650 prepares Fig. 2F parameters, block 652 invokes Fig. 2F processing already described above, and processing terminates at block 654. Parameters set at block 650 are: WDRREF = a reference or pointer to the MS WDR; DELETEQ = Fig. 6B location queue discard processing; and SUPER = Fig. 6B supervisory notification processing. Fig. 6B processing is available at any appropriate time to the MS.

See Fig 11A descriptions. Fields are set to the following upon exit from block 648:

MS ID field 1100a is preferably set with: Same as was described for Fig. 2D (block 236) above.

DATE/TIME STAMP field 1100b is preferably set with: Same as was described for Fig. 2D (block 236) above.

LOCATION field 1100c is preferably set with: The location determined for the MS.

5

CONFIDENCE field 1100d is preferably set with: Confidence (determined by the service) according to how the MS was connected, or may be set with the same value (e.g. 100 for physical connect, 77 for logical connect (e.g. short range wireless)) regardless of how the MS was located. In other embodiments, field 1100d will be determined by the service for anticipated physical conduit range, wireless logical connect range, etc. The resulting confidence value can be adjusted based on other parameters analogously to as described above.

10

LOCATION TECHNOLOGY field 1100e is preferably set with “Client Physical Connect” or “Client Logical Connect”, depending on how the MS connected. The originator indicator is set to DLM.

15

LOCATION REFERENCE INFO field 1100f is preferably set with: null (not set), but if a TDOA measurement can be made (e.g. short range logical connect, and using methodologies described above), then a TDOA measurement, a communications signal strength, if available; and wave spectrum (and/or particular communications interface 70) used, if available. The TDOA measurement may be converted to a distance using wave spectrum information. Possible values populated here should have already been factored into the confidence value.

20

25

COMMUNICATIONS REFERENCE INFO field 1100g is preferably set with: Same as was described for Fig. 2D (block 236) above.

SPEED field 1100h is preferably set with: null (not set), but can be set with speed required to arrive to the current location from a previously known location using, assuming same time scale is used.

30

HEADING field 1100i is preferably set with: null (not set), but can be set to heading determined when arriving to the current location from a previously known location.

ELEVATION field 1100j is preferably set with: Elevation/altitude (e.g. of physical connection, or place of logical connection detection), if available.

APPLICATION FIELDS field 1100k is preferably set with: Same as was described for Fig. 2D (block 236) above.

CORRELATION FIELD 1100m is preferably set with: Not Applicable (i.e. not maintained to queue 22).

SENT DATE/TIME STAMP field 1100n is preferably set with: Not Applicable (i.e. not maintained to queue 22).

RECEIVED DATE/TIME STAMP field 1100p is preferably set with: Not Applicable (i.e. not maintained to queue 22).

Figs. 7A, 7B and 7C depict a locating by image sensory illustration for discussing automatic location of a MS, for example a DLM 200. With reference now to Fig. 7A, an image capture device 702 is positioned for monitoring MSs that come into the field of view 704 of device 702. Device 702 may be a camcorder, video camera, image camera that takes at least one snapshot, timely snapshots, or motion/presence detection snapshots, or any other device capable of producing at least a snapshot image at some point in time containing objects in the field of view 704. In one preferred embodiment, DLM 200 is sensed within the vicinity of device 702, perhaps by antenna (or cell tower) 701, prior to being photographed by device 702. In another embodiment, DLM 200 is sensed by movement within the vicinity of device 702 with well know motion detection means. In yet another embodiment, device 702 periodically or continually records. Device 702 is connected to a locating service 700 for processing as described by Fig. 7D. Locating service 700 has means for communicating wirelessly to DLM 200, for example through a connected antenna (or cell tower) 701. Fig. 7A illustrates that device 702 participates in

pattern recognition for identifying the location of a MS. The MS can have on its exterior a string of characters, serial number, barcode, license plate, graphic symbol(s), textual symbols, combinations thereof, or any other visually perceptible, or graphical, identification 708 that can be recognized optically, or in a photograph. Device 702 is to have graphical/pixel resolution capability matching the requirements for identifying a MS with the sought graphical identification. Graphical identification 708 can be formed on the perceptible exterior of DLM 200, or can be formed as part of a housing/apparatus 706 which hosts DLM 200. Graphical identification 708 can be automatically read from an image using well known barcode reader technology, an Optical Character Recognition (OCR) process, a license tag scanner, general pattern recognition software, or the like. Housing 706 is generally shown for representing an automobile (license plate recognition, for example used in prior art toll tag lanes), a shopping cart, a package, or any other hosting article of manufacture which has a DLM 200 as part of it. Upon recognition, DLM 200 is associated with the location of device 702. Error in locating an MS will depend on the distance within the field of view 704 from device 702. A distance may be estimated based on the anticipated size of identification 708, relative its size determined within the field of view 704.

With reference now to Fig. 7B, image capture device 702 is positioned for monitoring MSs that come into the field of view 704 of device 702. MSs are preferably distinguishable by appearance (e.g. color, shape, markings, labels, tags, etc), or as attached (e.g. recognized mount to host) or carried (e.g. recognized by its recognized user). Such techniques are well known to those skilled in the art. Device 702 is as described above with connectivity to locating service 700 and antenna (or cell tower) 701. Fig. 7B illustrates that device 702 uses known measurements within its field of view for determining how large, and where located, are objects that come into the field of view 704. For example, a well placed and recognizable vertical line 710a and horizontal line 710b, which are preferably perpendicular to each other, have known lengths and positions. The objects which come into the field of view are measured based on the known lengths and positions of the lines 710a and 710b which may be landscape markings (e.g. parking lot lines) for additional purpose. Field of view 704 may contain many lines and/or objects of known dimensions strategically placed or recognized within the field of view 704 to facilitate image processing by service 700. Building 714 may serve as a reference point

having known dimension and position in measuring objects such as a person 716 or DLM 200. A moving object such as a shopping cart 712 can have known dimensions, but not a specific position, to facilitate service 700 in locating an MS coming into the field of view 704. Those skilled in the art recognize that known dimensions and/or locations of anticipated objects in field of view 704 have measurements facilitating discovering positions and measurements of new objects that may travel into the field of view 704. Using Fig. 7B techniques with Fig. 7A techniques provides additional locating accuracy. A distance may be estimated based on the anticipated sizes of references in the field of view, relative size of the recognized MS.

With reference now to Fig. 7C, image capture device 702 is positioned for monitoring MSs that come into the field of view 704 of device 702. Device 702 is as described above with connectivity to locating service 700 and antenna (or cell tower) 701. MSs are preferably distinguishable by appearance (e.g. color, shape, markings, labels, tags, etc), or as attached (e.g. recognized mount to host) or carried (e.g. recognized by its user), or as identified by Fig. 7A and/or Fig. 7B methodologies. Fig. 7C illustrates that device 702 uses known locations within its field of view for determining how large, and where located, are objects that come into the field of view 704. For example, building 714, tree 720, and traffic sign 722 have its locations known in field of view 704 by service 700. Solving locations of objects that move into the field of view is accomplished with graphical triangulation measurements between known object reference locations (e.g. building 714, tree 720, and sign 722) and the object to be located. Timely snapshots by device 702 provide an ongoing locating of an MS, for example DLM 200. Line segment distances 724 (a, b, c) can be measured using references such as those of Fig. 7B. Whereabouts are determined by providing known coordinates to anticipated objects such as building 714, tree 720, and sign 722. Similarly, graphical AOA measurements (i.e. graphical angle measurements) and graphical MPT measurements can be used in relation to anticipated locations of objects within the field of view 704. There may be many anticipated (known) object locations within field of view 704 to further facilitate locating an MS. Being nearby an object may also be enough to locate the MS by using the object's location for the location of the MS. Using Fig. 7C techniques with Fig. 7A and/or Fig. 7B techniques provides additional locating accuracy.

The system and methodologies illustrated by Figs. 7A through 7C are preferably used in optimal combination by locating service 700 to provide a best location of an MS. In some embodiments, MS whereabouts is determined as the location of a device 702 by simply being recognized by the device 702. In other embodiments, multiple devices 702 can be strategically placed within a geographic area for being used in combination to a common locating service 700 for providing a most accurate whereabouts of an MS. Multiple field of views 704 from difference angles of different devices 702 enable more precise locating within three dimensional space, including precise elevations.

Fig. 7D depicts a flowchart for describing a preferred embodiment of graphically locating a MS in accordance with locating service 700 described above, for example as illustrated by Figs. 7A through 7C. Locating service 700 may be a single capable data processing system, or many connected data processing systems for enhanced parallel processing. Locating service 700 may be connected to services involved with any other locating technology described in this application for synergistic services as an MS is mobile. Locating service 700 begins at block 732 and continues to block 734 where the service 700 is initialized in preparation of MS whereabouts analysis. Block 734 initializes its table(s) of sought identifying criteria which can be pattern recognized. In one preferred embodiment, color/shade, shape, appearance and applicable sought information is initialized for each sought identifying criteria. Pattern recognition is well known in the art and initialization is specific for each technology discussed above for Figs. 7A through 7C. For Figs. 7B and 7C discussions, positions, measurements, and reference points of known landmarks are additionally accounted. Thereafter, block 736 gets the next snapshot from device(s) 702. If there is none waiting to get, block 736 waits for one. If there is one queued up for processing, then block 736 continues to block 738. Fig. 7D is processing of a service, and is preferably multi-threaded. For example, blocks 736 through 754 can occur concurrently in many threads for processing a common queue of snapshots received from a device 702, or many devices 702. Each thread may process all sought criteria, or may specialize in a subset of sought criteria wherein if nothing is found, the thread can place the snapshot back on a queue for thread processing for another sought criteria after marking the queue entry as having been processed for one particular subset. So, threads may be specialized and work together in seeking all criteria, or may each work

in parallel seeking the same criteria. In preferred embodiments, there is at least one queue of snapshots received by block(s) 736. Block 736 continues to block 738 which attempts to detect an MS having sought criteria using pattern recognition techniques of Figs. 7A through 7C, in particular, or in combination. In one example embodiment, as
5 device 702 provides service 700 with at least one timely snapshot to block 736, the snapshot graphic is scanned at block 738 for identifying characters/symbols/appearance of sought criteria. Block 738 continues with its search result to block 740. If block 740 determines no MS was detected, then processing continues back to block 736. If block 738 detected at least one MS (as determined at block 740), then block 742 calculates
10 WDR information for the MS(s) detected, block 744 notifies a supervisory service of MS whereabouts if applicable, block 746 communicates the WDR information to MS(s) detected (for example via antenna 701), and processing continues to block 748.

There may be a plurality of MSs in the field of view, so communications at block 746 targets each MS recognized. A MS should not rely on the service to have done its job
15 correctly. At a MS, block 748 checks the MS ID communicated for validation. If block 748 determines the MS ID is incorrect, then processing continues back to block 736 (for the particular MS). If block 748 determines the MS ID is correct, then processing continues to block 750 where the particular MS completes its WDR 1100 received from service 700. Thereafter, MS(s) prepare parameters at block 752, invoke local Fig. 2F processing
20 already described above (at block 754), and processing continues for service 700 back to block 736. Of course, block 746 continues directly to block 736 at the service(s) since there is no need to wait for MS(s) processing in blocks 748 through 754. Parameters set at block 752 are: WDRREF = a reference or pointer to the MS WDR; DELETEQ = Fig. 7D location queue discard processing; and SUPER = Fig. 7D supervisory notification (e.g. no
25 supervisory notification processing because it was already handled at block 744, or by being in context of the Fig. 7D service processing). No snapshots from device 702 are to be missed at block 736.

See Fig 11A descriptions. Fields are set to the following upon exit from block 750:

30 *MS ID field 1100a is preferably set with:* Unique MS identifier of the MS, after validating at the MS that the service 700 has correctly identified it. This field is used to uniquely distinguish this MS WDRs on queue 22 from other originated WDRs. The service 700 may

determine a MS ID from a database lookup using above appearance criteria. Field 1100a may also be determined using the transmission methods as described for Figs. 2A through 2E, for example by way of antenna 701. For example, when the MS comes within range of antenna 701, Fig. 7D processing commences. Another embodiment prevents recognizing more than one MS within the field of view 704 at any time (e.g. a single file entryway), in which case the service can solicit a “who are you” transmission to identify the MS and then send back its whereabouts (in which case the MS sets its own MS ID here).

DATE/TIME STAMP field 1100b is preferably set with: Same as was described for Fig. 2D (block 236) above.

LOCATION field 1100c is preferably set with: The location determined for the MS by the service.

CONFIDENCE field 1100d is preferably set with: same value (e.g. 76) regardless of how the MS location was determined. In other embodiments, field 1100d will be determined by the number of distance measurements and/or the abundance of particular objects used in the field of view 704. The resulting confidence value can be adjusted based on other graphical parameters involved, analogously to as described above.

LOCATION TECHNOLOGY field 1100e is preferably set with: “Server Graphic-Patterns” “Server Graphic-Distances”, “Server Graphic Triangulate”, or a combination field value depending on how the MS was located and what flavor of service was used. The originator indicator is set to DLM.

LOCATION REFERENCE INFO field 1100f is preferably set with: null (not set) for indicating that all whereabouts determination data was factored into the confidence, and none is relevant for a single TDOA or AOA measurement in subsequent processing (i.e. service did all the work).

COMMUNICATIONS REFERENCE INFO field 1100g is preferably set with: Same as was described for Fig. 2D (block 236) above.

SPEED field 1100h is preferably set with: null (not set), but can be set with speed required to arrive to the current location from a previously known time at a location (e.g. using previous snapshots processed), assuming the same time scale is used.

5

HEADING field 1100i is preferably set with: null (not set), but can be set to heading determined when arriving to the current location from a previously known location (e.g. using previous snapshots processed).

10

ELEVATION field 1100j is preferably set with: Elevation/altitude, if available, if available.

APPLICATION FIELDS field 1100k is preferably set with: Same as was described for Fig. 2D (block 236) above.

15

CORRELATION FIELD 1100m is preferably set with: Not Applicable (i.e. not maintained to queue 22).

SENT DATE/TIME STAMP field 1100n is preferably set with: Not Applicable (i.e. not maintained to queue 22).

20

RECEIVED DATE/TIME STAMP field 1100p is preferably set with: Not Applicable (i.e. not maintained to queue 22).

In an alternative embodiment, MS 2 may be equipped (e.g. as part of resources 38) with its own device 702 and field of view 704 for graphically identifying recognizable environmental objects or places to determine its own whereabouts. In this embodiment, the MS would have access to anticipated objects, locations and dimensions much the same way described for Figs. 7A through 7D, either locally maintained or verifiable with a connected service. Upon a successful recognition of an object, place, or other graphically perceptible image which can be mapped to a location, the MS would complete a WDR similarly to above. The MS may recognize addresses, buildings, landmarks, of other pictorial data. Thus, the MS may graphically determine its own location. The MS would

30

then complete a WDR 1100 for Fig. 2F processing exactly as described for Fig. 7D with the exceptions of fields that follow:

5 *MS ID field 1100a is preferably set with:* Same as was described for Fig. 2D (block 236) above.

LOCATION field 1100c is preferably set with: The location determined for the MS by the MS.

10 *LOCATION TECHNOLOGY field 1100e is preferably set with:* "Client Graphic-Patterns" "Client Graphic-Distances", "Client Graphic Triangulate", or a combination field value depending on how the MS located itself. The originator indicator is set to DLM.

COMMUNICATIONS REFERENCE INFO field 1100g is preferably set with: null (not set).

15
20
25
30
Fig. 8A heterogeneously depicts a locating by arbitrary wave spectrum illustration for discussing automatic location of a MS. In the case of acoustics or sound, prior art has shown that a noise emitting animal or object can be located by triangulating the sound received using TDOA by strategically placed microphones. It is known that by figuring out time delay between a few strategically spaced microphones, one can infer the location of the sound. In a preferred embodiment, an MS, for example DLM 200, emits a pulsed or constant sound (preferably beyond the human hearing range) which can be sensed by microphones 802 through 806. Data is superimposed on the sound wave spectrum with variations in pitch or tone, or data occurs in patterned breaks in sound transmission. Data may contain a unique identifier of the MS so service(s) attached to microphones 802 through 806 can communicate uniquely to an MS. In some embodiments, sound used by the MS is known to repel certain pests such as unwanted animals, rodents, or bugs in order to prevent the person carrying the MS from encountering such pests during travel, for example during outdoor hiking or mountain climbing. In submarine acoustics, AOA is a method to locate certain objects. The Figs. 3B and 3C flowcharts occur analogously for sound signals received by microphones 802 through 806 which are connected to service processing of Figs. 3B and 3C. The only difference is wave spectrum used.

It has been shown that light can be used to triangulate position or location information (e.g. U.S. Patents 6,549,288 (Migdal et al) and 6,549,289 (Ellis)). Optical sensors 802 through 806 detect a light source of, or illumination of, an MS, for example DLM 200. Data is superimposed on the light wave spectrum with specified frequency/wavelength and/or periodicity, or data occurs in patterned breaks in light transmission. Data may contain a unique identifier of the MS so service(s) attached to sensors 802 through 806 can communicate uniquely to an MS. Mirrors positioned at optical sensors 802 through 806 may be used to determine an AOA of light at the sensor, or alternatively TDOA of recognizable light spectrum is used to position an MS. The Figs. 3B and 3C flowcharts occur analogously for light signals received by sensors 802 through 806 which are connected to service processing of Figs. 3B and 3C. The only difference is wave spectrum used.

Heterogeneously speaking, Fig. 8A illustrates having strategically placed sensors 802 through 806 for detecting a wave spectrum and using TDOA, AOA, or MPT. Those skilled in the art appreciate that a wave is analogously dealt with by Figs. 3B and 3C regardless of the wave type, albeit with different sensor types 802 through 806 and different sensor interface to service(s) of Figs. 3B and 3C. Wave signal spectrums for triangulation by analogous processing to Figs. 3B and 3C include microwaves, infrared, visible light, ultraviolet light, X-rays, gamma rays, longwaves, magnetic spectrum, or any other invisible, visible, audible, or inaudible wave spectrum. Sensors 802 through 806 are appropriately matched according to the requirements. Alternatively, a MS may be sensing wave spectrums emitted by transmitters 802 through 806.

Those skilled in the relevant arts appreciate that the point in all this discussion is all the wave forms provide methods for triangulating whereabouts information of an MS. Different types of wave forms that are available for an MS can be used solely, or in conjunction with each other, to determine MS whereabouts. MSs may be informed of their location using the identical wave spectrum used for whereabouts determination, or may use any other spectrum available for communicating WDR information back to the MS. Alternatively, the MS itself can determine WDR information relative applicable sensors/transmitters. In any case, a WDR 1100 is completed analogously to Figs. 3B and 3C.

Fig. 8B depicts a flowchart for describing a preferred embodiment of locating a MS through physically sensing a MS, for example a DLM 200. Processing begins at block 810 upon contact with a candidate MS and continues to block 812 where initialization takes place. Initialization includes determining when, where, and how the contact was made. Then, block 814 takes the contact sample and sets it as input containing a unique identifier or handle of the MS which was sensed. There are various known embodiments of how the MS is sensed:

- a) Touching sensors contact the MS (or host/housing having MS) to interpret physical characteristics of the MS in order to uniquely identify it (e.g. Braille, embossed/raised/depressed symbols or markings, shape, temperature, depressions, size, combinations thereof, etc);
- b) Purchase is made with MS while in vicinity of device accepting purchase, and as part of that transaction, the MS is sensed as being at the same location as the device accepting purchase, for example using a cell phone to purchase a soft drink from a soft drink dispensing machine;
- c) Barcode reader is used by person to scan the MS (or host/housing having MS), for example as part of shipping, receiving, or transporting;
- d) The MS, or housing with MS, is sensed by its odor (or host/housing having MS), perhaps an odor indicating where it had been, where it should not be, or where it should be. Various odor detection techniques may be used;
- e) Optical sensing wherein the MS is scanned with optical sensory means, for example to read a serial number; and/or
- f) Any sensing means which can identify the MS through physical contact, or by nearby/close physical contact with some wave spectrum.

Block 814 continues to block 816 where a database is accessed for recognizing the MS identifier (handle) by mapping sensed information with an associated MS handle. If a match is found at block 818, then block 822 determines WDR 1100 information using the location of where sensing took place. If block 818 determines no match was found, then data is saved at block 820 for an unrecognized entity such as is useful when an MS should have been recognized, but was not. In another embodiment, the MS handle is directly sensed so block 814 continues directly to block 818 (no block 816). Block 820

continues to block 834 where processing terminates. Block 816 may not use the entire MS identifier for search, but some portion of it to make sure it is a supported MS for being located by sensing. The MS identifier is useful when communicating wirelessly the WDR information to the MS (at block 826).

5 Referring now back to block 822, processing continues to block 824 where a supervisory service may be updated with the MS whereabouts (if applicable), and block 826 communicates the WDR information to the MS. Any available communication method can be used for communicating the WDR information to the MS, as described above. Thereafter, the MS completes the WDR at block 828, block 830 prepares Fig. 2F
10 parameters, and block 832 invokes Fig. 2F processing already described above. Processing terminates thereafter at block 834. Parameters set at block 830 are: WDRREF = a reference or pointer to the MS WDR; DELETEQ = Fig. 8B location queue discard processing; and SUPER = Fig. 8B supervisory notification (e.g. no supervisory notification processing because it was already handled at block 824, or by being in context of the Fig.
15 8B service processing). Fig. 8B processing is available at any appropriate time for the MS. In an alternate embodiment, the MS senses its environment to determine whereabouts.

See Fig 11A descriptions. Fields are set to the following upon exit from block 828:

20 *MS ID field 1100a is preferably set with:* Same as was described for Fig. 2D (block 236) above.

DATE/TIME STAMP field 1100b is preferably set with: Same as was described for Fig. 2D (block 236) above.

25 *LOCATION field 1100c is preferably set with:* Location of the sensor sensing the MS.

CONFIDENCE field 1100d is preferably set with: Should be high confidence (e.g. 98) for indisputable contact sensing and is typically set with the same value.

30 *LOCATION TECHNOLOGY field 1100e is preferably set with:* "Contact", or a specific type of Contact. The originator indicator is set to DLM.

LOCATION REFERENCE INFO field 1100f is preferably set with: null (not set).

COMMUNICATIONS REFERENCE INFO field 1100g is preferably set with: Same as was described for Fig. 2D (block 236) above.

5

SPEED field 1100h is preferably set with: null (not set), but can be set with speed required to arrive to the current location from a previously known time at a location, assuming the same time scale is used.

10

HEADING field 1100i is preferably set with: null (not set), but can be set to heading determined when arriving to the current location from a previously known location.

ELEVATION field 1100j is preferably set with: Elevation/altitude, if available.

15

APPLICATION FIELDS field 1100k is preferably set with: Same as was described for Fig. 2D (block 236) above.

CORRELATION FIELD 1100m is preferably set with: Not Applicable (i.e. not maintained to queue 22).

20

SENT DATE/TIME STAMP field 1100n is preferably set with: Not Applicable (i.e. not maintained to queue 22).

RECEIVED DATE/TIME STAMP field 1100p is preferably set with: Not Applicable (i.e. not maintained to queue 22).

25

Fig. 8C depicts a flowchart for describing a preferred embodiment of locating a MS, for example a DLM 200, through a manually entered location of the MS. MS user interface processing begins at block 850 when a user starts the user interface from code 18 and continues to block 852. Any of a variety of user interfaces, dependent on the type of MS, is used for manually entering the location of the MS. A user interfaces with the MS at block 852 until one of the monitored actions relevant to this disclosure are detected.

30

5 Thereafter, if block 854 determines the user has selected to set his location manually, then processing continues to block 860. If block 854 determines the user did not select to manually set his location, then block 856 determines if the user selected to force the MS to determine its location. If the user did select to force the MS to get its own location, then block 856 continues to block 862. If the user did not select to force the MS to get its own location as determined by block 856, then processing continues to block 858. If block 858 determines the user wanted to exit the user interface, then block 880 terminates the interface and processing terminates at block 882. If block 858 determines the user did not want to exit the user interface, then block 884 handles any user interface actions which caused exit from block 852 yet were not handled by any action processing relevant to this disclosure.

10 With reference back to block 860, the user interfaces with the MS user interface to manually specify WDR information. The user can specify:

- 15 1) An address or any address subset such as a zip code;
- 2) Latitude, longitude, and elevation;
- 3) MAPSCO identifier;
- 4) FEMA map identifier;
- 5) USDA map identifier;
- 6) Direct data entry to a WDR 1100; or
- 20 7) Any other method for user specified whereabouts of the MS.

The user can specify a relevant confidence value for the manually entered location, however, processing at block 860 preferably automatically defaults a confidence value for the data entered. For example, a complete address, validated at block 860, will have a high confidence. A partial address such as city and state, or a zip code will have a low confidence value. The confidence value will reflect how large an area is candidate for where the MS is actually located. To prevent completely relying on the user at block 860 for accurate WDR information, validation embodiments may be deployed. Some examples:

- 30
 - Upon specification (e.g. FEMA), the MS will access connected service(s) to determine accuracy (FEMA conversion tables);

- Upon specification (e.g. MAPSCO), the MS will access local resources to help validate the specification (e.g. MAPSCO conversion tables); and/or
- Upon specification (e.g. address), the MS can access queue 22 and/or history 30 for evidence proving likelihood of accuracy. The MS may also access services, or local resources, for converting location information for proper comparisons.

In any case, a confidence field 1100d value can be automatically set based on the validation results, and the confidence may, or may not, be enabled for override by the user.

After WDR information is specified at block 860, the MS completes the WDR at block 874, block 876 prepares parameters for Fig. 2F processing, and (at block 878) the MS invokes Fig. 2F processing already described above before returning back to block 852. Parameters set at block 876 are: WDRREF = a reference or pointer to the MS WDR; DELETEQ = Fig. 8C location queue discard processing; and SUPER = Fig. 8C supervisory notification processing. Various embodiments permit override of the confidence floor value by the user, or by Fig. 8C processing. Block 874 may convert the user specified information into a standardized more usable form in an LN-expanse (e.g. convert to latitude and longitude if possible, truncated precision for more area coverage). WDR 1100 fields (see Fig. 11A) are set analogously in light of the many variations already described above.

With reference back to block 862, if it is determined that the MS is equipped with capability (e.g. in range, or in readiness) to locate itself, then processing continues to block 864 where the MS locates itself using MS driven capability described by Figs. 2E, 3C, 4B, 6B, and 8A or MS driven alternative embodiments to Figs. 2D, 3B, 5B, 6A, 7D, 8A, and 8B, or any other MS capability for determining its own whereabouts with or without help from other data processing systems or services. Interfacing to locating capability preferably involves a timeout in case there is no, or slow, response, therefore block 864 continues to block 868 where it determined whether or not block 864 timed out prior to determining a location. If block 868 determines a timeout was encountered, then block 872 provides the user with an error to the user interface, and processing continues back to block 852. Block 872 preferably requires use acknowledgement prior to continuing to block 852.

If block 868 determines there was no timeout (i.e. whereabouts successfully determined), then block 870 interfaces to the locating interface to get WDR information, block 874 completes a WDR, and blocks 876 and 878 do as described above. If block 862 determines the MS cannot locate itself and needs help, then block 866 emits at least one broadcast request to any listening service which can provide the MS its location. Appropriate correlation is used for an anticipated response. Example services listening are service driven capability described by Figs. 2D, 3B, 5B, 6A, 7D, 8A, and 8B, or service side alternative embodiments of Figs. 2E, 3C, 4B, 6B, and 8A, or any other service capability for determining MS whereabouts with or without help from the MS or other data processing systems or services. Block 866 then continues to block 868.

If block 868 determines a timeout was encountered from the service broadcast request, then block 872 provides the user with an error to the user interface, and processing continues back to block 852. If block 868 determines there was no timeout (i.e. whereabouts successfully determined), then block 870 receives WDR information from the locating interface of the responding service, block 874 completes a WDR, and blocks 876 and 878 do as already described above.

See Fig 11A descriptions. Depending how the MS was located via processing started at block 856 to block 862, a WDR is completed analogous to as described in Figs. above. If the user manually specified whereabouts at block 860, fields are set to the following upon exit from block 874:

MS ID field 1100a is preferably set with: Same as was described for Fig. 2D (block 236) above.

DATE/TIME STAMP field 1100b is preferably set with: Same as was described for Fig. 2D (block 236) above.

LOCATION field 1100c is preferably set with: Location entered by the user, or converted from entry by the user; preferably validated.

CONFIDENCE field 1100d is preferably set with: User specified confidence value, or a system assigned value per a validated manual specification. Confidence should reflect

confidence of location precision (e.g. validated full address high; city and zip code low, etc). Manually specified confidences are preferably lower than other location technologies since users may abuse or set incorrectly, unless validated. Specifying lower confidence values than technologies above, for completely manual WDR specifications (i.e. no validation), ensures that manual specifications are only used by the MS in absence of other technologies.

LOCATION TECHNOLOGY field 1100e is preferably set with: "Manual", or "Manual Validated". Types of validations may further be elaborated. The originator indicator is set to DLM.

LOCATION REFERENCE INFO field 1100f is preferably set with: null (not set).

COMMUNICATIONS REFERENCE INFO field 1100g is preferably set with: null (not set).

SPEED field 1100h is preferably set with: null (not set).

HEADING field 1100i is preferably set with: null (not set).

ELEVATION field 1100j is preferably set with: null (not set).

APPLICATION FIELDS field 1100k is preferably set with: Same as was described for Fig. 2D (block 236) above; or as decided by the user.

CORRELATION FIELD 1100m is preferably set with: Not Applicable (i.e. not maintained to queue 22).

SENT DATE/TIME STAMP field 1100n is preferably set with: Not Applicable (i.e. not maintained to queue 22).

RECEIVED DATE/TIME STAMP field 1100p is preferably set with: Not Applicable (i.e. not maintained to queue 22).

Fig. 9A depicts a table for illustrating heterogeneously locating a MS, for example a DLM 200. While many location methods and systems have been exhausted above, there may be other system and methods for locating an MS which apply to the present disclosure. The requirement for LBX is that the MS be located, regardless of how that occurs. MSs disclosed herein can be located by one or many location technologies discussed. As MS prices move lower, and capabilities increase, an affordable MS will contain multiple abilities for being located. GPS, triangulation, in-range detection, and contact sensory may all be used in locating a particular MS as it travels. Equipping the MS with all techniques is straightforward and is compelling when there are competing, or complementary, technologies that the MS should participate in.

The Fig. 9A table has DLM location methods for rows and a single column for the MS (e.g. DLM 200). Each location technology can be driven by the client (i.e. the MS), or a service (i.e. the location server(s)) as denoted by a row qualifier "C" for client or "S" for service. An MS may be located by many technologies. The table illustrated shows that the MS with unique identifier 0A12:43EF:985B:012F is able to be heterogeneously located, specifically with local MS GPS capability, service side cell tower in-range detection, service side cell tower TDOA, service side cell tower MPT (combination of TDOA and AOA), service side antenna in-range detection, service side antenna AOA, service side antenna TDOA, service side antenna MPT, service side contact/sensory, and general service side MPT. The unique identifier in this example is a universal product identifier (like Host Bus Adapter (HBA) World Wide Name (WWN) identifiers are generated), but could be in other form as described above (e.g. phone # 214-403-4071). An MS can have any subset of technologies used to locate it, or all of the technologies used to locate it at some time during its travels. An MS is heterogeneously located when two or more location technologies are used to locate the MS during MS travels and/or when two or more location technologies with incomplete results are used in conjunction with each other to locate the MS during MS travels, such as MPT. MPT is a heterogeneous location technology because it uses at least two different methods to accomplish a single location determination. Using combinations of different location technologies can be used, for example a TDOA measurement from an in-range antenna with a TDOA measurement relative a cell tower (e.g. as accomplished in MS processing of Fig. 26B), using completely

different services that have no knowledge of each other. Another combination is to use a synergy of whereabouts data from one technology with whereabouts data from another technology. For example, in-range detection is used in combination with graphical identification to provide better whereabouts of a MS. In another example, a GPS equipped MS travels to an area where GPS does not work well (e.g. downtown amidst large and tall buildings). The DLM becomes an ILM, and is triangulated relative other MSs. So, an MS is heterogeneously located using two or more technologies to determine a single whereabouts, or different whereabouts of the MS during travel.

Fig. 9B depicts a flowchart for describing a preferred embodiment of heterogeneously locating a MS, for example DLM 200. While heterogeneously locating an MS can occur by locating the MS at different times using different location technologies, flowchart 9B is shown to discuss a generalization of using different location technologies with each other at the same time to locate an MS. Processing begins at block 950 and continues to block 952 where a plurality of parameters from more than one location technology are examined for locating an MS. Processing begins at block 950 by a service (or the MS) when a location technology by itself cannot be used to confidently locate the MS. Data deemed useful at block 952, when used in conjunction with data from a different location technology to confidently locate the MS, is passed for processing to block 954. Block 954 heterogeneously locates the MS using data from at least two location technologies to complement each other and to be used in conjunction with each other in order to confidently locate the MS. Once the MS whereabouts are determined at block 954, WDR information is communicated to the MS for further processing at block 956. In some embodiments where a service is heterogeneously locating the MS, block 956 communicates WDR information wirelessly to the MS before processing begins at block 958. In another embodiment where the MS is heterogeneously locating itself, block 956 communicates WDR information internally to WDR completion processing at block 958. In preferred embodiments, the MS completes its WDR information at block 958, Fig. 2F parameters are prepared at block 960, and the MS invokes Fig. 2F processing already described above (at block 962), before processing terminates at block 964. Parameters set at block 960 are: WDRREF = a reference or pointer to the MS WDR; DELETEQ = Fig. 9B location queue discard processing; and SUPER = Fig. 9B supervisory notification

processing. WDR 1100 fields (see Fig. 11A) are set analogously in light of many variations already described above.

5 In some embodiments of Fig. 9B processing, Missing Part Triangulation (MPT) is used to heterogeneously locate an MS. For a service side embodiment example, block 950 begins service processing when TDOA information itself cannot be used to confidently locate the MS, or AOA information itself cannot be used to confidently locate the MS, however using angles and distances from each in conjunction with each other enables solving whereabouts confidently. See “Missing Part Triangulation (MPT)” section
10 below with discussions for Figs. 11A through 11E for MPT processing of blocks 952 and 954. Data discovered at block 952 and processed by block 954 depends on the embodiment, what stationary reference point locations are known at the time of blocks 952 and 954 processing, and which parts are missing for triangulating the MS. Having three (3) sides (all TDOA) with known stationary vertices location(s) solves the triangle for locating the MS. Three (3) angles (all AOA) with known stationary vertices location(s)
15 solves the triangle for locating the MS. Those skilled in the art appreciate that solving triangulation can make complementary use of different distances (time used to determine length in TDOA) and angles (from AOA) for deducing a MS location confidently (e.g. MPT). Those skilled in the art recognize that having stationary reference locations facilitates requiring less triangular information for deducing a MS location confidently.
20

While MPT has been discussed by example, flowchart 9B is not to be interpreted in a limiting sense. Any location technologies, for example as shown in Fig. 9A, can be used in conjunction with each other when not all information required is available in a single location technology to confidently deduce an MS location. Data available from the different
25 location technologies available will be examined on its own merits, and optionally used in conjunction to deduce a confident location. For example, a TDOA (difference between when signal sent and when received) measurement from “coming within range” technology can be used to distinguish how close, or how far, is an MS in the vicinity. That measurement may be used to more confidently locate the MS using other TDOA
30 measurements from other unrelated “coming within range” whereabouts information.

With the many DLM examples above, it should be clear now to the reader how to set the WDR 1100 for DLM invoked Fig. 2F processing. There can be other location technologies that will set WDR 1100 fields analogously. Locating methodologies of Figs. 2A through 9B can be used in any combination, for example for more timely or accurate locating. Furthermore, a MS automatically takes on a role of a DLM or ILM depending on what capability is available at the time, regardless of whether or not the MS is equipped for being directly located. As a DLM roams to unsupported areas, it can remain a DLM using different DLM technologies, and it can become an ILM to depend on other MSs (ILMs or DLMs) in the vicinity to locate it.

LBX Indirectly Located Mobile Data Processing Systems (ILMs)

Figs. 10A and 10B depict an illustration of a Locatable Network expanse (LN-Expanse) 1002 for describing locating of an ILM with all DLMs. With reference now to Fig. 10A, DLM 200a, DLM 200b, DLM 200c, DLM 200d, and DLM 200e (referred to generally in Figs. 10A and 10B discussions as DLMs 200) are each automatically and directly located, for example using any of the automatic location technologies heretofore described. ILM 1000b is automatically located using the reference locations of DLM 200b, DLM 200c, and DLM 200e. DLMs 200 can be mobile while providing reference locations for automatically determining the location of ILM 1000b. Timely communications between MSs is all that is required for indirectly locating MSs. In some embodiments, DLMs 200 are used to triangulate the position of ILM 1000b using aforementioned wave spectrum(s) reasonable for the MSs. Different triangulation embodiments can triangulate the location of ILM 1000b using TDOA, AOA, or MPT, preferably by the ILM 1000b seeking to be located. In other embodiments, TDOA information is used to determine how close ILM 1000b is to a DLM for associating the ILM at the same location of a DLM, but with how close nearby. In other embodiments, an ILM is located by simply being in communications range to another MS. DLMs 200 can be referenced for determining elevation of an ILM. The same automatic location technologies used to locate a DLM can be used to automatically locate an ILM, except the DLMs are mobile and serve as the reference points. It is therefore important that DLM locations be timely known when references are needed for locating ILMs. Timely ILM interactions with other MSs, and protocol considerations are discussed in architecture 1900 below. DLMs 200b, 200c, and 200e are

preferably selected for locating ILM 1000b by their WDR high confidence values, however any other WDR data may be used whereby wave spectrum, channel signal strength, time information, nearness, surrounded-ness, etc is considered for generating a confidence field 1100d of the WDR 1100 for the located ILM. Preferably, those considerations are factored into a confidence value, so that confidence values can be completely relied upon.

With reference now to Fig. 10B, ILM 1000c has been located relative a plurality of DLMs, namely DLM 200b, DLM 200d, and DLM 200e. ILM 1000c is located analogously to ILM 1000b as described for Fig. 10A, except there are different DLMs involved with doing the locating of ILM 1000c because of a different location of ILM 1000c. Figs. 10A and 10B illustrate that MSs can be located using other MSs, rather than fixed stationary references described for Figs. 2A through 9B. ILM 1000b and ILM 1000c are indirectly located using DLMs 200.

Fig. 10C depicts an illustration of a Locatable Network expense (LN-Expense) 1002 for describing locating of an ILM with an ILM and DLM. ILM 1000a is automatically located using the reference locations of DLM 200c, DLM 200b, and ILM 1000b. DLM 200b, DLM 200c and ILM 1000b can be mobile while providing reference locations for automatically determining the location of ILM 1000a. In some embodiments, MSs are used to triangulate the position of ILM 1000a using any of the aforementioned wave spectrum(s) (e.g. WiFi 802.x, cellular radio, etc) reasonable for the MSs. Different triangulation embodiments can triangulate the location of ILM 1000a using TDOA, AOA, or MPT, preferably by the ILM 1000a seeking to be located. In other embodiments, TDOA information is used to determine how close ILM 1000a is to a MS (DLM or ILM) for associating the ILM at the same location of a MS, but with how close nearby. In other embodiments, an ILM is located by simply being in communications range to another MS. DLMs or ILMs can be referenced for determining elevation of ILM 1000a. The same automatic location technologies used to locate a MS (DLM or ILM) are used to automatically locate an ILM, except the MSs are mobile and serve as the reference points. It is therefore important that MS (ILM and/or DLM) locations be timely known when references are needed for locating ILMs. Timely ILM interactions with other MSs, and protocol considerations are discussed in architecture 1900 below. DLM 200b, DLM 200c, and ILM 1000b are preferably selected for locating ILM 1000a by their WDR high confidence values, however any other WDR

data may be used whereby wave spectrum, channel signal strength, time information, nearness, surrounded-ness, etc is considered for generating a confidence field 1100d of the WDR 1100 for the located ILM. Preferably, those considerations were already factored into a confidence value so that confidence values can be completely relied upon. ILM 1000a is indirectly located using DLM(s) and ILM(s).

Figs. 10D, 10E, and 10F depict an illustration of a Locatable Network expanse (LN-Expanse) 1002 describing locating of an ILM with all ILMs. With reference now to Fig. 10D, ILM 1000e is automatically located using the reference locations of ILM 1000a, ILM 1000b, and ILM 1000c. ILM 1000a, ILM 1000b and ILM 1000c can be mobile while providing reference locations for automatically determining the location of ILM 1000e. Timely communications between MSs is all that is required. In some embodiments, MSs are used to triangulate the position of ILM 1000e using any of the aforementioned wave spectrum(s) reasonable for the MSs. Different triangulation embodiments can triangulate the location of ILM 1000e using TDOA, AOA, or MPT processing (relative ILMs 1000a through 1000c), preferably by the ILM 1000e seeking to be located. ILMs can be referenced for determining elevation of ILM 1000e. The same automatic location technologies used to locate a MS (DLM or ILM) are used to automatically locate an ILM, except the MSs are mobile and serve as the reference points. It is therefore important that ILM locations be timely known when references are needed for locating ILMs. Timely ILM interactions with other MSs, and protocol considerations are discussed in architecture 1900 below. ILM 1000a, ILM 1000b, and ILM 1000c are preferably selected for locating ILM 1000e by their WDR high confidence values, however any other WDR data may be used whereby wave spectrum, channel signal strength, time information, nearness, surrounded-ness, etc is considered for generating a confidence field 1100d of the WDR 1100 for the located ILM. Preferably, those considerations were already factored into a confidence value so that confidence values can be completely relied upon. ILM 1000e is indirectly located using ILM 1000a, ILM 1000b, and ILM 1000c.

With reference now to Fig. 10E, ILM 1000g is automatically located using the reference locations of ILM 1000a, ILM 1000c, and ILM 1000e. ILM 1000a, ILM 1000c and ILM 1000e can be mobile while providing reference locations for automatically determining

the location of ILM 1000g. ILM 1000g is located analogously to ILM 1000e as described for Fig. 10D, except there are different ILMs involved with doing the locating of ILM 1000g because of a different location of ILM 1000g. Note that as ILMs are located in the LN-expanse 1002, the LN-expanse expands with additionally located MSs.

5

With reference now to Fig. 10F, ILM 1000i is automatically located using the reference locations of ILM 1000f, ILM 1000g, and ILM 1000h. ILM 1000f, ILM 1000g and ILM 1000h can be mobile while providing reference locations for automatically determining the location of ILM 1000i. ILM 1000i is located analogously to ILM 1000e as described for Fig. 10D, except there are different ILMs involved with doing the locating of ILM 1000i because of a different location of ILM 1000i. Figs. 10D through 10F illustrate that an MS can be located using all ILMs, rather than all DLMS (Figs 10A and 10B), a mixed set of DLMS and ILMs (Fig. 10C), or fixed stationary references (Figs. 2A through 9B). ILMs 1000e, 1000g, and 1000i are indirectly located using ILMs. Note that in the Fig. 10 illustrations the LN-expanse 1002 has expanded down and to the right from DLMS directly located up and to the left. It should also be noted that locating any MS can be done with at least one other MS. Three are not required as illustrated. It is preferable that triangulation references used surround an MS.

Figs. 10G and 10H depict an illustration for describing the reach of a Locatable Network expanse (LN-Expanse) according to MSs. Location confidence will be dependent on the closest DLMS, how stale an MS location becomes for serving as a reference point, and how timely an MS refreshes itself with a determined location. An MS preferably has highest available processing speed with multithreaded capability in a plurality of hardware processors and/or processor cores. A substantially large number of high speed concurrent threads of processing that can occur within an MS provides for an optimal capability for being located quickly among its peer MSs, and for serving as a reference to its peer MSs. MS processing described in flowcharts herein assumes multiple threads of processing with adequate speed to accomplish an optimal range in expanding the LN-Expanse 1002.

With reference now to Fig. 10G, an analysis of an LN-Expanse 1002 will contain at least one DLM region 1022 containing a plurality of DLMS, and at least one DLM indirectly located region 1024 containing at least one ILM that has been located with all DLMS.

Depending on the range, or scope, of an LN-Expanse 1002, there may be a mixed region 1026 containing at least one ILM that has been indirectly located by both an ILM and DLM, and there may be an exclusive ILM region 1028 containing at least one ILM that has been indirectly located by all ILMs. The further in distance the LN-Expanse has expanded from DLM region 1022 with a substantial number of MSs, the more likely there will an exclusive ILM region 1028. NTP may be available for use in some regions, or some subset of a region, yet not available for use in others. NTP is preferably used where available to minimize communications between MSs, and an MS and service(s). An MS has the ability to make use of NTP when available.

With reference now to Fig. 10H, all MSs depicted know their own locations. The upper left-hand portion of the illustration consists of region 1022. As the reader glances more toward the rightmost bottom portion of the illustration, there can be regions 1024 and regions 1026 in the middle of the illustration. At the very rightmost bottom portion of the illustration, remaining ILMs fall in region 1028. An ILM is indirectly located relative all DLMs, DLMs and ILMs, or all ILMs. An “Affirmifier” in a LN-expanse confidently knows its own location and can serve as a reference MS for other MSs. An affirmifier is said to “affirmify” when in the act of serving as a reference point to other MSs. A “Pacifier” can contribute to locating other systems, but with a low confidence of its own whereabouts. The LN-Expanse is a network of located/locatable MSs, and is preferably expanded by a substantial number of affirmifiers.

Fig. 10I depicts an illustration of a Locatable Network expanse (LN-Expanse) for describing a supervisory service, for example supervisory service 1050. References in flowcharts for communicating information to a supervisory service can refer to communicating information to supervisory service 1050 (e.g. blocks 294 and 296 from parameters passed to block 272 for many processing flows). The only requirement is that supervisory service 1050 be contactable from an MS (DLM or ILM) that reports to it. An MS reporting to service 1050 can communicate directly to it, through another MS (i.e. a single hop), or through a plurality of MSs (i.e. a plurality of hops). Networks of MSs can be preconfigured, or dynamically reconfigured as MSs travel to minimize the number of hops between a reporting MS and service 1050. A purely peer to peer preferred embodiment includes a peer to peer network of located/locatable MSs that interact with each other as

described herein. The purely peer to peer preferred embodiment may have no need to include a service 1050. Nevertheless, a supervisory service may be warranted to provide certain processing centralization, or for keeping information associated with MSs. In some embodiments, supervisory service 1050 includes at least one database to house data (e.g. data 8; data 20; data 36; data 38, queue data 22, 24, 26; and/or history 30) for any subset of MSs which communicate with it, for example to house MS whereabouts information.

Fig. 11A depicts a preferred embodiment of a Whereabouts Data Record (WDR) 1100 for discussing operations of the present disclosure. A WDR takes on a variety of formats depending on the context of use. There are several parts to a WDR depending on use. There is an identity section which contains a MS ID field 1100a for identifying the WDR. Field 1100a can contain a null value if the WDR is for whereabouts information received from a remote source which has not identified itself. MSs do not require identities of remote data processing systems in order to be located. There is a core section which is required in WDR uses. The core section includes date/time stamp field 1100b, location field 1100c, and confidence field 1100d. There is a transport section of fields wherein any one of the fields may be used when communicating WDR information between data processing systems. Transport fields include correlation field 1100m, sent date/time stamp field 1100n, and received date/time stamp field 1100p. Transport fields may also be communicated to send processing (e.g. queue 24), or received from receive processing (e.g. queue 26). Other fields are of use depending on the MS or applications thereof, however location technology field 1100e and location reference info field 1100f are of particular interest in carrying out additional novel functionality of the present disclosure. Communications reference information field 1100g may be valuable, depending on communications embodiments in the LN-expanse.

Some fields are multi-part fields (i.e. have sub-fields). Whereabouts Data Records (WDRs) 1100 may be fixed length records, varying length records, or a combination with field(s) in one form or the other. Some WDR embodiments will use anticipated fixed length record positions for subfields that can contain useful data, or a null value (e.g. -1). Other WDR embodiments may use varying length fields depending on the number of sub-fields to be populated. Other WDR embodiments will use varying length fields and/or sub-fields

which have tags indicating their presence. Other WDR embodiments will define additional fields to prevent putting more than one accessible data item in one field. In any case, processing will have means for knowing whether a value is present or not, and for which field (or sub-field) it is present. Absence in data may be indicated with a null indicator (-1), or indicated with its lack of being there (e.g. varying length record embodiments).

When a WDR is referenced in this disclosure, it is referenced in a general sense so that the contextually reasonable subset of the WDR of Fig. 11A is used. For example, when communicating WDRs (sending/receiving data 1302 or 1312) between data processing systems, a reasonable subset of WDR 1100 is communicated in preferred embodiments as described with flowcharts. When a WDR is maintained to queue 22, preferably most (if not all) fields are set for a complete record, regardless if useful data is found in a particular field (e.g. some fields may be null (e.g. -1)). Most importantly, Whereabouts Data Records (WDRs) are maintained to queue 22 for maintaining whereabouts of the MS which owns queue 22. LBX is most effective the more timely (and continuous) a MS has valid whereabouts locally maintained. WDRs are designed for maintaining whereabouts information independent of any location technology applied. Over time, a MS may encounter a plurality of location technologies used to locate it. WDRs maintained to a first MS queue 22 have the following purpose:

- 1) Maintain timely DLM whereabouts information of the first MS independent of any location technology applied;
- 2) Maintain whereabouts information of nearby MSs independent of any location technology applied;
- 3) Provide DLM whereabouts information to nearby MSs for determining their own locations (e.g. provide whereabouts information to at least a second MS for determining its own location);
- 4) Maintain timely ILM whereabouts information of the first MS independent of any location technology applied; and
- 5) Provide ILM whereabouts information to nearby MSs so they can determine their own locations (e.g. first MS providing whereabouts information to at least a second MS for the second MS determining its own whereabouts).

A MS may go in and out of DLM or ILM roles as it is mobile. Direct location methods are not always available to the MS as it roams, therefore the MS preferably does all of 1 through 5 above. When the WDR 1100 contains a MS ID field 1100a matching the MS which owns queue 22, that WDR contains the location (location field 1100c) with a specified confidence (field 1100d) at a particular time (date/time stamp field 1100b) for that MS. Preferably the MS ID field 1100a, date/time stamp field 1100b and confidence field 1100d is all that is required for searching from the queue 22 the best possible, and most timely, MS whereabouts at the time of searching queue 22. Other embodiments may consult any other fields to facilitate the best possible MS location at the time of searching and/or processing queue 22. The WDR queue 22 also maintains affirmifier WDRs, and acceptable confidence pacifier WDRs (block 276), which are used to calculate a WDR having matching MS field 1100a so the MS knows its whereabouts via indirect location methods. Affirmifier and pacifier WDRs have MS ID field 1100a values which do not match the MS owning queue 22. This distinguishes WDRs of queue 22 for A) accessing the current MS location; from B) the WDRs from other MSs. All WDR fields of affirmifier and pacifier originated WDRs are of importance for determining a best location of the MS which owns queue 22, and in providing LBX functionality.

MS ID field 1100a is a unique handle to an MS as previously described. Depending on the installation, MS ID field 1100a may be a phone #, physical or logical address, name, machine identifier, serial number, encrypted identifier, concealable derivative of a MS identifier, correlation, pseudo MS ID, or some other unique handle to the MS. An MS must be able to distinguish its own unique handle from other MS handles in field 1100a. For indirect location functionality disclosed herein, affirmifier and pacifier WDRs do not need to have a correct originating MS ID field 1100a. The MS ID may be null, or anything to distinguish WDRs for MS locations. However, to accomplish other LBX features and functionality, MS Identifiers (MS IDs) of nearby MSs (or unique correlations thereof) maintained in queue 22 are to be known for processing by an MS. MS ID field 1100a may contain a group identifier of MSs in some embodiments for distinguishing between types of MSs (e.g. to be treated the same, or targeted with communications, as a group), as long as the MS containing queue 22 can distinguish its own originated WDRs 1100. A defaulted value may also be set for a "do not care" setting (e.g. null).

Date/Time stamp field 1100b contains a date/time stamp of when the WDR record 1100 was completed by an MS for its own whereabouts prior to WDR queue insertion. It is in terms of the date/time scale of the MS inserting the local WDR (NTP derived or not). Date/Time stamp field 1100b may also contain a date/time stamp of when the WDR record 1100 was determined for the whereabouts of an affirmifier or pacifier originating record 1100 to help an MS determine its own whereabouts, but it should still be in terms of the date/time scale of the MS inserting the local WDR (NTP derived or not) to prevent time conversions when needed, and to promote consistent queue 22 searches/sorts/etc. The date/time stamp field 1100b should use the best possible granulation of time, and may be in synch with other MSs and data processing systems according to NTP. A time zone, day/light savings time, and NTP indicator is preferably maintained as part of field 1100b. The NTP indicator (e.g. bit) is for whether or not the date/time stamp is NTP derived (e.g. the NTP use setting is checked for setting this bit when completing the WDR for queue 22 insertion). In some embodiments, date/time stamp field 1100b is measured in the same granulation of time units to an atomic clock available to MSs of an LN-Expanse 1002. When NTP is used in a LN-Expanse, identical time server sources are not a requirement provided NTP derived date/time stamps have similar accuracy and dependability.

Location field 1100c depends on the installation of the present disclosure, but can include a latitude and longitude, cellular network cell identifier, geocentric coordinates, geodetic coordinates, three dimensional space coordinates, area described by GPS coordinates, overlay grid region identifier or coordinates, GPS descriptors, altitude/elevation (e.g. in lieu of using field 1100j), MAPSCO reference, physical or logical network address (including a wildcard (e.g. ip addresses 145.32.*.*)), particular address, polar coordinates, or any other two/three dimensional location methods/means used in identifying the MS location. Data of field 1100c is preferably a consistent measure (e.g. all latitude and longitude) for all location technologies that populate WDR queue 22. Some embodiments will permit using different measures to location field 1100c (e.g. latitude and longitude for one, address for another; polar coordinates for another, etc) which will be translated to a consistent measure at appropriate processing times.

Confidence field 1100d contains a value for the confidence that location field 1100c accurately describes the location of the MS when the WDR is originated by the MS for its own whereabouts. Confidence field 1100d contains a value for the confidence that

location field 1100c accurately describes the location of an affirmifier or pacifier that originated the WDR. A confidence value can be set according to known timeliness of processing, communications and known mobile variables (e.g. MS speed, heading, yaw, pitch, roll, etc) at the time of transmission. Confidence values should be standardized for all location technologies used to determine which location information is of a higher/lower confidence when using multiple location technologies (as determined by fields 1100e and 1100f) for enabling determination of which data is of a higher priority to use in determining whereabouts. Confidence value ranges depend on the implementation. In a preferred embodiment, confidence values range from 1 to 100 (as discussed previously) for denoting a percentage of confidence. 100% confidence indicates the location field 1100c is guaranteed to describe the MS location. 0% confidence indicates the location field 1100c is guaranteed to not describe the MS location. Therefore, the lowest conceivable value of a queue 22 for field 1100d should be 1. Preferably, there is a lowest acceptable confidence floor value configured (by system, administrator, or user) as used at points of queue entry insertion – see block 276 to prevent frivolous data to queue 22. In most cases, WDRs 1100 contain a confidence field 1100d up to 100. In confidence value preferred embodiments, pacifiers know their location with a confidence of less than 75, and affirmifiers know their location with a confidence value 75 or greater. The confidence field is skewed to lower values as the LN-expanse 1002 is expanded further from region 1022. Confidence values are typically lower when ILMs are used to locate a first set of ILMs (i.e. first tier), and are then lower when the first set of ILMs are used to locate a second set of ILMs (second tier), and then lower again when the second set of ILMs are used to locate a third set of ILMs (third tier), and so on. Often, examination of a confidence value in a WDR 1100 can indicate whether the MS is a DLM, or an ILM far away from DLMs, or an MS which has been located using accurate (high confidence) or inaccurate (low confidence) locating techniques.

Location Technology field 1100e contains the location technology used to determine the location of location field 1100c. An MS can be located by many technologies. Location Technology field 1100e can contain a value from a row of Fig. 9A or any other location technology used to locate a MS. WDRs inserted to queue 22 for MS whereabouts set field 1100e to the technology used to locate the MS. WDRs inserted to queue 22 for facilitating a MS in determining whereabouts set field 1100e to the

technology used to locate the affirmifier or pacifier. Field 1100e also contains an originator indicator (e.g. bit) for whether the originator of the WDR 1100 was a DLM or ILM. When received from a service that has not provided confidence, this field may be used by a DLM to determine confidence field 1100d.

5 Location Reference Info field 1100f preferably contains one or more fields useful to locate a MS in processing subsequent of having been inserted to queue 22. In other embodiments, it contains data that contributed to confidence determination. Location Reference Info field 1100f may contain information (TDOA measurement and/or AOA measurement – see inserted field 1100f for Figs. 2D, 2E and 3C) useful to locate a MS in
10 the future when the WDR originated from the MS for its own whereabouts. Field 1100f will contain selected triangulation measurements, wave spectrum used and/or particular communications interfaces 70, signal strength(s), TDOA information, AOA information, or any other data useful for location determination. Field 1100f can also contain reference whereabouts information (Fig. 3C) to use relative a TDOA or AOA (otherwise WDR
15 location field assumed as reference). In one embodiment, field 1100f contains the number of DLMs and ILMs which contributed to calculating the MS location to break a tie between using WDRs with the same confidence values. In another embodiment, a tier of ILMs used to locate the MS is maintained so there is an accounting for the number of ILMs in the LN-expanse between the currently located MS and a DLM. In other embodiments, MS
20 heading, yaw, pitch and roll, or accelerometer values are maintained therein, for example for antenna AOA positioning. When wave spectrum frequencies or other wave characteristics have changed in a transmission used for calculating a TDOA measurement, appropriate information may be carried along, for example to properly convert a time into a distance. Field 1100f should be used to facilitate correct
25 measurements and uses, if needed conversions have not already taken place.

 Communications reference information field 1100g is a multipart record describing the communications session, channel, and bind criteria between the MS and MSs, or service(s), that helped determine its location. In some embodiments, field 1100g contains unique MS identifiers, protocol used, logon/access parameters, and useful statistics of the
30 MSs which contributed to data of the location field 1100c. An MS may use field 1100g for WDRs originated from affirmifiers and pacifiers for subsequent LBX processing.

Speed field 1100h contains a value for the MS speed when the WDR is originated by the MS for its own whereabouts. Speed field 1100d may contain a value for speed of an affirmifier or pacifier when the WDR was originated elsewhere. Speed is maintained in any suitable units.

5 Heading field 1100i contains a value for the MS heading when the WDR is originated by the MS for its own whereabouts. Heading field 1100i may contain a value for heading of an affirmifier or pacifier when the WDR was originated elsewhere. Heading values are preferably maintained in degrees up to 360 from due North, but is maintained in any suitable directional form.

10 Elevation field 1100j contains a value for the MS elevation (or altitude) when the WDR is originated by the MS for its own whereabouts. Elevation field 1100j may contain a value for elevation (altitude) of an affirmifier or pacifier when the WDR was originated elsewhere. Elevation (or altitude) is maintained in any suitable units.

15 Application fields 1100k contains one or more fields for describing application(s) at the time of completing, or originating, the WDR 1100. Application fields 1100k may include field(s) for:

- a) MS Application(s) in use at time;
- b) MS Application(s) context(s) in use at time;
- c) MS Application(s) data for state information of MS Application(s) in use at time;
- 20 d) MS Application which caused WDR 1100;
- e) MS Application context which caused WDR 1100;
- f) MS Application data for state information of MS Application which caused WDR 1100;
- g) Application(s) in use at time of remote MS(s) involved with WDR;
- 25 h) Application(s) context(s) in use at time of remote MS(s) involved with WDR;
- i) MS Application(s) data for state information of remote MS(s) involved with WDR;
- j) Remote MS(s) criteria which caused WDR 1100;
- k) Remote MS(s) context criteria which caused WDR 1100;
- l) Remote MS(s) data criteria which caused WDR 1100;
- 30 m) Application(s) in use at time of service(s) involved with WDR;
- n) Application(s) context(s) in use at time of service(s) involved with WDR;
- o) MS Application(s) data for state information of service(s) involved with WDR;

- p) Service(s) criteria which caused WDR 1100;
- q) Service(s) context criteria which caused WDR 1100;
- r) Service(s) data criteria which caused WDR 1100;
- s) MS navigation APIs in use;
- 5 t) Web site identifying information;
- u) Physical or logical address identifying information;
- v) Situational location information as described in U.S. Patents 6,456,234; 6,731,238; 7,187,997 (Johnson);
- w) Transactions completed at a MS;
- 10 x) User configurations made at a MS;
- y) Environmental conditions of a MS;
- z) Application(s) conditions of a MS;
- aa) Service(s) conditions of a MS;
- bb) Date/time stamps (like field 1100b) with, or for, any item of a) through aa); and/or
- 15 cc) Any combinations of a) through bb).

Correlation field 1100m is optionally present in a WDR when the WDR is in a transmission between systems (e.g. wireless communications) such as in data 1302 or 1312. Field 1100m provides means for correlating a response to an earlier request, or to correlate a response to an earlier broadcast. Correlation field 1100m contains a unique handle. In a LN-expanse which globally uses NTP, there is no need for correlation in data 1302 or 1312. Correlation field 1100m may be present in WDRs of queues 24 or 26. Alternatively, a MS ID is used for correlation.

Sent date/time stamp field 1100n is optionally present in a WDR when the WDR is in transmission between systems (e.g. wireless communications) such as in data 1302 or 1312. Field 1100n contains when the WDR was transmitted. A time zone, day/light savings time, and NTP indicator is preferably maintained as part of field 1100n. Field 1100n is preferably not present in WDRs of queue 22 (but can be if TDOA measurement calculation is delayed to a later time). In some embodiments, there is no need for field 1100n. Whereabouts determined for MSs of an LN-Expanse may be reasonably timely, facilitating simplicity of setting outbound field 1100b to the transmission date/time stamp at the sending data processing system, rather than when the WDR was originally completed

for whereabouts (e.g. when substantially the same time anyway). Sent date/time field 1100n may be present in WDRs of queues 24 or 26.

Received date/time stamp field 1100p is preferably present in a WDR when inserted to queue 26 by receiving thread(s) upon received data 1302 or 1312. Field 1100p contains when the WDR was received by the MS. A time zone, day/light savings time, and NTP indicator is preferably maintained as part of field 1100p. Field 1100p is preferably not present in WDRs of queue 22 (but can be if TDOA measurement calculation is delayed to a later time). In some embodiments, there is no need for field 1100p. For example, thread(s) 1912 may be listening directly on applicable channel(s) and can determine when the data is received. In another embodiment, thread(s) 1912 process fast enough to determine the date/time stamp of when data 1302 or 1312 is received since minimal time has elapsed between receiving the signal and determining when received. In fact, known processing duration between when received and when determined to be received can be used to correctly alter a received date/time stamp. Received date/time stamp field 1100p is preferably added to records placed to queue 26 by receiving thread(s) feeding queue 26.

Any fields of WDR 1100 which contain an unpredictable number of subordinate fields of data preferably use a tagged data scheme, for example an X.409 encoding for a Token, Length, and Value (called a TLV encoding). Therefore, a WDR 1100, or field therein, can be a variable sized record. For example, Location Reference info field 1100f may contain TTA, 8, .1456 where the Token = "TTA" for Time Till Arrival (TDOA measurement between when sent and when received), Length = 8 for 8 bytes to follow, and Value = .1456 in time units contained within the 8 bytes; also SS, 4, 50 where Token = "Signal Strength", 4 = 4 for 4 bytes to follow, and Value = 50 dBu for the signal strength measurement. This allows on-the-fly parsing of unpredictable, but interpretable, multipart fields. The TLV encoding also enables-on-the-fly configuration for parsing new subordinate fields to any WDR 1100 field in a generic implementation, for example in providing parse rules to a Lex and Yacc implementation, or providing parse rules to a generic top down recursive TLV encoding parser and processor.

Any field of WDR 1100 may be converted: a) prior to insertion to queue 22; or b) after access to queue 22; or c) by queue 22 interface processing; for standardized processing. Any field of WDR 1100 may be converted when

sending/receiving/broadcasting, or related processing, to ensure a standard format. Other embodiments will store and access values of WDR 1100 field(s) which are already in a standardized format. WDR 1100 fields can be in any order, and a different order when comparing what is in data transmitted versus data maintained to queue 22.

5 An alternate embodiment to WDRs maintained to queue 22 preserves transport fields 1100m, 1100n and/or 1100p, for example for use on queue 22. This would enable 1952 thread(s) to perform TDOA measurements that are otherwise calculated in advance and kept in field 1100f. However, queue 22 size should be minimized and the preferred embodiment uses transport fields when appropriate to avoid carrying them along to other
10 processing.

Figs. 11B, 11C and 11D depict an illustration for describing various embodiments for determining the whereabouts of an MS, for example an ILM 1000e. With reference now to Fig. 11B, a MS 1000e location is located by using locations of three (3) other MSs: MS₄, MS₅, and MS₆ (referred to generally as MS_j). MS_j are preferably located with a
15 reasonably high level of confidence. In some embodiments, MS_j are all DLMs. In some embodiments, MS_j are all ILMs. In some embodiments, MS_j are mixed DLMs and ILMs. Any of the MSs may be mobile during locating of MS 1000e. Wave spectrums in use, rates of data communications and MS processing speed, along with timeliness of
20 processing described below, provide timely calculations for providing whereabouts of ILM 1000e with a high level of confidence. The most confident MSs (MS_j) were used to determine the MS 1000e whereabouts. For example, MS_j were all located using a form of GPS, which in turn was used to triangulate the whereabouts of MS 1000e. In another example, MS₄ was located by a form of triangulation technology, MS₅ was located by a
25 form of “coming into range” technology, and MS₆ was located by either of the previous two, or some other location technology. It is not important how an MS is located. It is important that each MS know its own whereabouts and maintain a reasonable confidence to it, so that other MSs seeking to be located can be located relative highest confidence locations available. The WDR queue 22 should always contain at least one entry
30 indicating the location of the MS 2 which owns WDR queue 22. If there are no entries contained on WDR queue 22, the MS 2 does not know its own location.

With reference now to Fig. 11C, a triangulation of MS 1000e at location 1102 is explained using location (whereabouts) 1106 of MS₄, location (whereabouts) 1110 of MS₅, and location (whereabouts) 1114 of MS₆. Signal transmission distance from MS_j locations are represented by the radiuses, with r_1 the TDOA measurement (time difference between when sent and when received) between MS₄ and MS 1000e, with r_2 the TDOA measurement (time difference between when sent and when received) between MS₅ and MS 1000e, with r_3 the TDOA measurement (time difference between when sent and when received) between MS₆ and MS 1000e. In this example, the known locations of MS_j which are used to determine the location of MS 1000e allow triangulating the MS 1000e whereabouts using the TDOA measurements. In fact, less triangular data in the illustration can be necessary for determining a highly confident whereabouts of MS 1000e.

With reference now to Fig. 11D, a triangulation of MS 1000e at location 1102 is explained using location (whereabouts) 1106 of MS₄, location (whereabouts) 1110 of MS₅, and location (whereabouts) 1114 of MS₆. In some embodiments, AOA measurements taken at a positioned antenna of MS 1000e at location 1102 are used relative the whereabouts 1106, whereabouts 1110, whereabouts 1114 (AOA 1140, AOA 1144 and AOA 1142), wherein AOA measurements are detected for incoming signals during known values for MS heading 1138 with MS yaw, pitch, and roll (or accelerometer readings). AOA triangulation is well known in the art. Line segment 1132 represents the direction of signal arrival to the antenna at whereabouts 1102 from MS₄ at whereabouts 1106. Line segment 1134 represents the direction of signal arrival to the antenna at whereabouts 1102 from MS₅ at whereabouts 1110. Line segment 1136 represents the direction of signal arrival to the antenna at whereabouts 1102 from MS₆ at whereabouts 1114. In this example, the known locations of MS_j which are used to determine the location of MS 1000e allow triangulating the MS 1000e whereabouts using the AOA measurements. In fact, less triangular data in the illustration can be necessary for determining a highly confident whereabouts of MS 1000e. Alternative embodiments will use AOA measurements of outbound signals from the MS at whereabouts 1102 detected at antennas of whereabouts 1106 and/or 1110 and/or 1114.

Missing Part Triangulation (MPT)

Figs. 11C and 11D illustrations can be used in a complementary manner when only one or two TDOA measurements are available and/or not all stationary locations, or MS reference locations, are known at the time of calculation. Another example is when only one or two AOA angles is available and/or not all stationary locations, or MS reference locations, are known at the time of calculation. However, using what is available from each technology in conjunction with each other allows solving the MS whereabouts (e.g. blocks 952/954 processing above). MPT is one example of solving for missing parts using more than one location technology. Condition of data known for locating a MS (e.g. whereabouts 1106, 1110 and 1114) may be the following:

- 1) AAS = two angles and a side;
- 2) ASA = two angles and a common side;
- 3) SAS = two sides and the included angle; or
- 4) SSA = two sides and a non-included angle.

TDOA measurements are distances (e.g. time difference between when sent and when received), and AOA measurements are angles. Each of the four conditions are recognized (e.g. block 952 above), and data is passed for each of the four conditions for processing (e.g. block 954 above). For AAS (#1) and ASA (#2), processing (e.g. block 954) finds the third angle by subtracting the sum of the two known angles from 180 degrees (i.e. using mathematical law that triangles' interior angles add up to 180 degrees), and uses the mathematical law of Sines (i.e. $a / \sin A = b / \sin B = c / \sin C$) twice to find the second and third sides after plugging in the knowns and solving for the unknowns. For SAS (#3), processing (e.g. block 954) uses the mathematical law of Cosines (i.e. $a^2 = b^2 + c^2 - 2bc \cos A$) to find the third side, and uses the mathematical law of Sines ($\sin A / a = \sin B / b = \sin C / c$ (derived from law of Sines above)) to find the second angle. For SSA (#4), processing (e.g. block 954) uses the mathematical law of Sines (i.e. $\sin A / a = \sin B / b = \sin C / c$) twice to get the second angle, and mathematical law of Sines ($a / \sin A = b / \sin B = c / \sin C$) to get the third side. Those skilled in the art recognize other useful trigonometric functions and formulas, and similar uses of the same trigonometric functions, for MPT depending on what data is known. The data discovered and processed depends on an embodiment, what reference locations are available, and which parts are missing for MPT. MPT uses different distances (time used to determine length in TDOA) and/or angles (from AOA or TDOA technologies) for deducing a MS location confidently

(e.g. MPT). Those skilled in the art recognize that having known reference locations facilitates requiring less triangular information for deducing a MS location confidently. MPT embodiments may exist for any aforementioned wave spectrums.

5 Fig. 11E depicts an illustration for describing various embodiments for automatically determining the location of an MS. An MS can be located relative other MSs which were located using any of a variety of location technologies, for example any of those of Fig. 9A. An MS is heterogeneously located when one of the following conditions are met:

- More than one location technology is used during travel of the MS;
- 10 • More than one location technology is used to determine a single whereabouts of the MS;
- MPT is used to locate the MS; and/or
- ADLT is used to locate the MS.

The WDR queue 22 and interactions between MSs as described below cause the MS to be heterogeneously located without special consideration to any particular location technology. While WDR 1100 contains field 1100e, field 1100d provides a standard and generic measurement for evaluating WDRs from different location technologies, without concern for the location technology used. The highest confidence entries to a WDR queue 22 are used regardless of which location technology contributed to the WDR queue 22.

LBX Configuration

Fig. 12 depicts a flowchart for describing an embodiment of MS initialization processing. Depending on the MS, there are many embodiments of processing when the MS is powered on, started, restarted, rebooted, activated, enabled, or the like. Fig. 12 describes the blocks of processing relevant to the present disclosure as part of that initialization processing. It is recommended to first understand discussions of Fig. 19 for knowing threads involved, and variables thereof. Initialization processing starts at block 1202 and continues to block 1204 where the MS Basic Input Output System (BIOS) is initialized appropriately, then to block 1206 where other character 32 processing is initialized, and then to block 1208 to see if NTP is enabled for this MS. Block 1206 may start the preferred number of listen/receive threads for feeding queue 26 and the preferred number of send threads for sending data inserted to queue 24, in particular when

transmitting CK 1304 embedded in usual data 1302 and receiving CK 1304 or 1314 embedded in usual data 1302 or 1312, respectively. The number of threads started should be optimal for parallel processing across applicable channel(s). In this case, other character 32 threads are appropriately altered for embedded CK processing (sending at first opportune outbound transmission; receiving in usual inbound transmission).

If block 1208 determines NTP is enabled (as defaulted or last set by a user (i.e. persistent variable)), then block 1210 initializes NTP appropriately and processing continues to block 1212. If block 1208 determines NTP was not enabled, then processing continues to block 1212. Block 1210 embodiments are well known in the art of NTP implementations (also see block 1626). Block 1210 may cause the starting of thread(s) associated with NTP. In some embodiments, NTP use is assumed in the MS. In other embodiments, appropriate NTP use is not available to the MS. Depending on the NTP embodiment, thread(s) may pull time synchronization information, or may listen for and receive pushed time information. Resources 38 (or other MS local resource) provides interface to an MS clock for referencing, maintaining, and generating date/time stamps at the MS. After block 1210 processing, the MS clock is synchronized to NTP. Because of initialization of the MS in Fig. 12, block 1210 may rely on a connected service to initially get the startup synchronized NTP date/time. MS NTP processing will ensure the NTP enabled/disabled variable is dynamically set as is appropriate (using semaphore access) because an MS may not have continuous clock source access during travel when needed for resynchronization. If the MS does not have access to a clock source when needed, the NTP use variable is disabled. When the MS has (or again gets) access to a needed clock source, then the NTP use variable is enabled.

Thereafter, block 1212 creates shared memory to maintain data shared between processes/threads, block 1214 initializes persistent data to shared memory, block 1216 initializes any non-persistent data to shared memory (e.g. some statistics 14), block 1218 creates system queues, and block 1220 creates semaphore(s) used to ensure synchronous access by concurrent threads to data in shared memory, before continuing to block 1222. Shared memory data accesses appropriately utilize semaphore lock windows (semaphore(s) created at block 1220) for proper access. In one embodiment, block 1220 creates a single semaphore for all shared memory accesses, but this can deteriorate performance of threads accessing unrelated data. In the preferred embodiment, there is a

semaphore for each reasonable set of data of shared memory so all threads are fully executing whenever possible. Persistent data is that data which maintains values during no power, for example as stored to persistent storage 60. This may include data 8 (including permissions 10, charters 12, statistics 14, service directory 16), data 20, LBX history 30, data 36, resources 38, and/or other data. Persistent data preferably includes at least the DLMV (see DLM role(s) list Variable below), ILMV (see ILM role(s) list Variable below), process variables 19xx-Max values (19xx = 1902, 1912, 1922, 1932, 1942 and 1952 (see Fig. 19 discussions below)) for the last configured maximum number of threads to run in the respective process, process variables 19xx-PID values (19xx = 1902, 1912, 1922, 1932, 1942 and 1952 (see Fig. 19 discussions below)) for multi-purpose of: a) holding an Operating System Process Identifier (i.e. O/S PID) for a process started; and b) whether or not the respective process was last enabled (i.e. PID > 0) or disabled (i.e. PID <= 0), the confidence floor value (see Fig. 14A), the WTV (see Whereabouts Timeliness Variable (see Fig. 14A)), the NTP use variable (see Fig. 14A) for whether or not NTP was last set to disabled or enabled (used at block 1208), and the Source Periodicity Time Period (SPTP) value (see Fig. 14B). There are reasonable defaults for each of the persistent data prior to the first use of MS 2 (e.g. NTP use is disabled, and only becomes enabled upon a successful enabling of NTP at least one time). Non-persistent data may include data involved in some regard to data 8 (and subsets of permissions 10, charters 12, statistics 14, service directory 16), data 20, LBX history 30, data 36, resources 38, queues, semaphores, etc. Block 1218 creates queues 22, 24, and 26. Queues 1980 and 1990 are also created there if required. Queues 1980 and 1990 are not required when NTP is in use globally by participating data processing systems. Alternate embodiments may use less queues by threads sharing a queue and having a queue entry type field for directing the queue entry to the correct thread. Alternate embodiments may have additional queues for segregating entries of a queue disclosed for best possible performance. Other embodiments incorporate queues figuratively to facilitate explanation of interfaces between processing.

All queues disclosed herein are understood to have their own internally maintained semaphore for queue accesses so that queue insertion, peeking, accessing, etc uses the internally maintained semaphore to ensure two or more concurrently executing threads do not corrupt or misuse data to any queue. This is consistent with most operating system

queue interfaces wherein a thread stays blocked (preempted) after requesting a queue entry until a queue entry appears in the queue. Also, no threads will collide with another thread when inserting, peeking, or otherwise accessing the same queue. Therefore, queues are implicitly semaphore protected. Other embodiments may use an explicit semaphore protected window around queue data accessing, in which case those semaphore(s) are created at block 1220.

Thereafter, block 1222 checks for any ILM roles currently enabled for the MS (for example as determined from persistent storage of an ILM role(s) list Variable (ILMV) preferably preconfigured for the MS at first use, or configured as last configured by a user of the MS). ILM roles are maintained to the ILM role(s) list Variable (ILMV). The ILMV contains one or more entries for an ILM capability (role), each entry with a flag indicating whether it is enabled or disabled (marked = enabled, unmarked = disabled). If block 1222 determines there is at least one ILM role enabled (i.e. as marked by associated flag), then block 1224 artificially sets the corresponding 19xx-PID variables to a value greater than 0 for indicating the process(es) are enabled, and are to be started by subsequent Fig. 12 initialization processing. The 19xx-PID will be replaced with the correct Process Identifier (PID) upon exit from block 1232 after the process is started. Preferably, every MS can have ILM capability. However, a user may want to (configure) ensure a DLM has no ILM capability enabled (e.g. or having no list present). In some embodiments, by default, every MS has an unmarked list of ILM capability maintained to the ILMV for 1) USE DLM REFERENCES and 2) USE ILM REFERENCES. USE DLM REFERENCES, when enabled (marked) in the ILMV, indicates to allow the MS of Fig. 12 processing to determine its whereabouts relative remote DLMs. USE ILM REFERENCES, when enabled (marked) in the ILMV, indicates to allow the MS of Fig. 12 processing to determine its whereabouts relative remote ILMs. Having both list items marked indicates to allow determining MS whereabouts relative mixed DLMs and ILMs. An alternative embodiment may include a USE MIXED REFERENCES option for controlling the MS of Fig. 12 processing to determine its whereabouts relative mixed DLMs and/or ILMs. Alternative embodiments will enforce any subset of these options without exposing user configurations, for example on a MS without any means for being directly located.

For any of the ILMV roles of USE DLM REFERENCES, USE ILM REFERENCES, or both, all processes 1902, 1912, 1922, 1932, 1942 and 1952 are preferably started (i.e.

1902-PID, 1912-PID, 1922-PID, 1932-PID, 1942-PID and 1952-PID are artificially set at block 1224 to cause subsequent process startup at block 1232). Characteristics of an anticipated LN-expanse (e.g. anticipated location technologies of participating MSs, MS capabilities, etc) will start a reasonable subset of those processes with at least process 1912 started. Block 1224 continues to block 1226. If block 1222 determines there are no ILMV role(s) enabled, then block processing continues to block 1226.

Block 1226 initializes an enumerated process name array for convenient processing reference of associated process specific variables described in Fig. 19, and continues to block 1228 where the first member of the set is accessed for subsequent processing. The enumerated set of process names has a prescribed start order for MS architecture 1900. Thereafter, if block 1230 determines the process identifier (i.e. 19xx-PID such that 19xx is 1902, 1912, 1922, 1932, 1942, 1952 in a loop iteration of blocks 1228 through 1234) is greater than 0 (e.g. this first iteration of 1952-PID > 0 implies it is to be started here; also implies process 1952 is enabled as used in Figs. 14A, 28, 29A and 29B), then block 1232 spawns (starts) the process (e.g. 1952) of Fig. 29A to start execution of subordinate worker thread(s) (e.g. process 1952 thread(s)) and saves the real PID (Process Identifier) to the PID variable (e.g. 1952-PID) returned by the operating system process spawn interface. Block 1232 passes as a parameter to the process of Fig. 29A which process name to start (e.g. 1952), and continues to block 1234. If block 1230 determines the current process PID variable (e.g. 1952-PID) is not greater than 0 (i.e. not to be started; also implies is disabled as used in Figs. 14A, 28, 29A and 29B), then processing continues to block 1234. Block 1234 checks to see if all process names of the enumerated set (pattern of 19xx) have been processed (iterated) by blocks 1228 through 1234. If block 1234 determines that not all process names in the set have been processed (iterated), then processing continues back to block 1228 for handling the next process name in the set. If block 1234 determines that all process names of the enumerated set were processed, then block 1236 checks the DLMV (DLM role(s) list Variable). Blocks 1228 through 1234 iterate every process name of Fig. 19 to make sure that each is started in accordance with non-zero 19xx-PID variable values at Fig. 12 initialization.

Block 1236 checks for any DLM roles currently enabled for the MS (for example as determined from persistent storage of a DLM role(s) list Variable (DLMV) preferably preconfigured for the MS at first use if the MS contains DLM capability). DLM capability

(roles), whether on-board at the MS, or determined during MS travels (see block 288), is maintained to the DLM role(s) list Variable (DLMV). The DLMV contains one or more entries for a DLM capability (role), each (role) entry with a flag indicating whether it is enabled or disabled (marked = enabled, unmarked = disabled). If block 1236 determines there is at least one DLM role enabled (i.e. as marked by associated flag), then block 1238 initializes enabled role(s) appropriately and processing continues to block 1240. Block 1238 may cause the starting of thread(s) associated with enabled DLM role(s), for DLM processing above (e.g. Figs. 2A through 9B). Block 1238 may invoke API(s), enable flag(s), or initialize as is appropriate for DLM processing described above. Such initializations are well known in the art of prior art DLM capabilities described above. If block 1236 determines there are no DLM roles to initialize at the MS, then processing continues to block 1240. Any of the Fig. 9A technologies are eligible in the DLMV as determined to be present at the MS and/or as determined by historical contents of the WDR queue 22 (e.g. location technology field 1100e with MS ID field 1100a for this MS) and/or determined by LBX history 30. Application Programming Interfaces (APIs) may also be used to determine MS DLM capability (role(s)) for entry(s) to the DLMV.

Block 1240 completes LBX character initialization, and Fig. 12 initialization processing terminates thereafter at block 1242. Depending on what threads were started as part of block 1206, Block 1240 may startup the preferred number of listen/receive threads for feeding queue 26 and the preferred number of send threads for sending data inserted to queue 24, in particular when transmitting new data 1302 and receiving new data 1302 or 1312. The number of threads started should be optimal for parallel processing across applicable channel(s). Upon encounter of block 1242, the MS is appropriately operational, and a user at the MS of Fig. 12 processing will have the ability to use the MS and applicable user interfaces thereof.

With reference now to Fig. 29A, depicted is a flowchart for describing a preferred embodiment of a process for starting a specified number of threads in a specified thread pool. Fig. 29A is in itself an O/S process, has a process identifier (PID) after being started, will contain at least two threads of processing after being started, and is generic in being able to take on the identity of any process name passed to it (e.g. 19xx) with a parameter (e.g. from block 1232). Fig. 29A represents the parent thread of a 19xx process. The Fig.

29A process is generic for executing any of processes 19xx (i.e. 1902, 1912, 1922, 1932, 1942 and 1952) with the prescribed number of worker threads using the 19xx-Max configuration (i.e. 1902-Max, 1912-Max, 1922-Max, 1932-Max, 1942-Max and 1952-Max). Fig. 29A will stay running until it (first all of its worker thread(s)) is terminated. Fig. 29A consists of an O/S Process 19xx with at least a parent thread (main thread) and one worker thread (or number of worker threads for Fig. 19 processing as determined by 19xx-Max). The parent thread has purpose to stay running while all worker threads are running, and to own intelligence for starting worker threads and terminating the process when all worker threads are terminated. The worker threads are started subordinate to the Fig. 29A process at block 2912 using an O/S start thread interface.

A 19xx (i.e. 1902, 1912, 1922, 1932, 1942 and 1952) process starts at block 2902 and continues to block 2904 where the parameter passed for which process name to start (i.e. take on identity of) is determined (e.g. 1952). Thereafter, block 2906 creates a RAM semaphore (i.e. operating system term for a well performing Random Access Memory (RAM) semaphore with scope only within the process (i.e. to all threads of the process)). The local semaphore name preferably uses the process name prefix (e.g. 1952-Sem), and is used to synchronize threads within the process. RAM semaphores perform significantly better than global system semaphores. Alternate embodiments will have process semaphore(s) created at block 1220 in advance. Thereafter, block 2908 initializes a thread counter (e.g. 1952-Ct) to 0 for counting the number of worker threads actually started within the 19xx process (e.g. 1952), block 2910 initializes a loop variable J to 0, and block 2912 starts a worker thread (the first one upon first encounter of block 2912 for a process) in this process (e.g. process 1902 starts worker thread Fig. 20, ... , process 1952 starts worker thread Fig. 26A – see architecture 1900 description below).

Thereafter, block 2914 increments the loop variable by 1 and block 2916 checks if all prescribed worker threads have been started. Block 2916 accesses the 19xx-Max (e.g. 1952-Max) variable from shared memory using a semaphore for determining the maximum number of threads to start in the process worker thread pool. If block 2916 determines all worker threads have been started, then processing continues to block 2918. If block 2916 determines that not all worker threads have been started for the process of Fig. 29A, then processing continues back to block 2912 for starting the next

worker thread. Blocks 2912 through 2916 ensure the 19xx-Max (e.g. 1952-Max) number of worker threads are started within the process of Fig. 29A.

Block 2918 waits until all worker threads of blocks 2912 through 2916 have been started, as indicated by the worker threads themselves. Block 2918 waits until the process 19xx-Ct variable has been updated to the prescribed 19xx-Max value by the started worker threads, thereby indicating they are all up and running. When all worker threads are started (e.g. 1952-Ct = 1952-Max), thereafter block 2920 waits (perhaps a very long time) until the worker thread count (e.g. 1952-Ct) has been reduced back down to 0 for indicating that all worker threads have been terminated, for example when the user gracefully powers off the MS. Block 2920 continues to block 2922 when all worker threads have been terminated. Block 2922 sets the shared memory variable for the 19xx process (e.g. 1952-PID) to 0 using a semaphore for indicating that the 19xx (e.g. 1952) process is disabled and no longer running. Thereafter, the 19xx process terminates at block 2924. Waiting at blocks 2918 and 2920 are accomplished in a variety of well known methods:

- Detect signal sent to process by last started (or terminated) worker thread that thread count is now MAX (or 0); or
- Loop on checking the thread count with sleep time between checks, wherein within the loop there is a check of the current count (use RAM semaphore to access), and processing exits the loop (and block) when the count has reached the sought value; or
- Use of a semaphore for a count variable which causes the parent thread of Fig. 29A to stay blocked prior to the count reaching its value, and causes the parent thread to become cleared (will leave wait block) when the count reaches its sought value.

Starting threads of processing in Fig. 29A has been presented from a software perspective, but there are hardware/firmware thread embodiments which may be started appropriately to accomplish the same functionality. If the MS operating system does not have an interface for returning the PID at block 1232, then Fig. 29A can have a block (e.g. 2905) used to determine its own PID for setting the 19xx-PID variable.

Figs. 13A through 13C depict an illustration of data processing system wireless data transmissions over some wave spectrum. Embodiments may exist for any of the

5
10
15
20
25

forementioned wave spectrums, and data carried thereon may or may not be encrypted (e.g. encrypted WDR information). With reference now to Fig. 13A, a MS, for example a DLM 200a, sends/broadcasts data such as a data 1302 in a manner well known to those skilled in the art, for example other character 32 processing data. When a Communications Key (CK) 1304 is embedded within data 1302, data 1302 is considered usual communications data (e.g. protocol, voice, or any other data over conventional forward channel, reverse channel, voice data channel, data transmission channel, or any other prior art use channel) which has been altered to contain CK 1304. Data 1302 contains a CK 1304 which can be detected, parsed, and processed when received by another MS or other data processing system in the vicinity of the MS (e.g. DLM 200a) as determined by the maximum range of transmission 1306. CK 1304 permits “piggy-backing” on current transmissions to accomplish new functionality as disclosed herein. Transmission from the MS radiate out from it in all directions in a manner consistent with the wave spectrum used. The radius 1308 represents a first range of signal reception from the MS 200a, perhaps by another MS (not shown). The radius 1310 represents a second range of signal reception from the MS 200a, perhaps by another MS (not shown). The radius 1311 represents a third range of signal reception from the MS 200a, perhaps by another MS (not shown). The radius 1306 represents a last and maximum range of signal reception from the MS 200a, perhaps by another MS (not shown). MS design for maximum radius 1306 may take into account the desired maximum range versus acceptable wave spectrum exposure health risks for the user of the MS. The time of transmission from MS 200a to radius 1308 is less than times of transmission from MS 200a to radiuses 1310, 1311, or 1306. The time of transmission from MS 200a to radius 1310 is less than times of transmission from MS 200a to radiuses 1311 or 1306. The time of transmission from MS 200a to radius 1311 is less than time of transmission from MS 200a to radius 1306.

30

In another embodiment, data 1302 contains a Communications Key (CK) 1304 because data 1302 is new transmitted data in accordance with the present disclosure. Data 1302 purpose is for carrying CK 1304 information for being detected, parsed, and processed when received by another MS or other data processing system in the vicinity of the MS (e.g. DLM 200a) as determined by the maximum range of transmission 1306.

With reference now to Fig. 13B, a MS, for example an ILM 1000k, sends/broadcasts data such as a data 1302 in a manner well known to those skilled in the art. Data 1302 and CK 1304 are as described above for Fig. 13A. Data 1302 or CK 1304 can be detected, parsed, and processed when received by another MS or other data processing system in the vicinity of the MS (e.g. ILM 1000k) as determined by the maximum range of transmission 1306. Transmission from the MS radiate out from it in all directions in a manner consistent with the wave spectrum used, and as described above for Fig. 13A.

With reference now to Fig. 13C, a service or set of services sends/broadcasts data such as a data packet 1312 in a manner well known to those skilled in the art, for example to service other character 32 processing. When a Communications Key (CK) 1314 is embedded within data 1312, data 1312 is considered usual communications data (e.g. protocol, voice, or any other data over conventional forward channel, reverse channel, voice data channel, data transmission channel, or any other prior art use channel) which has been altered to contain CK 1314. Data 1312 contains a CK 1314 which can be detected, parsed, and processed when received by an MS or other data processing system in the vicinity of the service(s) as determined by the maximum range of transmission 1316. CK 1314 permits “piggy-backing” on current transmissions to accomplish new functionality as disclosed herein. Transmissions radiate out in all directions in a manner consistent with the wave spectrum used, and data carried thereon may or may not be encrypted (e.g. encrypted WDR information). The radius 1318 represents a first range of signal reception from the service (e.g. antenna thereof), perhaps by a MS (not shown). The radius 1320 represents a second range of signal reception from the service (e.g. antenna thereof), perhaps by a MS (not shown). The radius 1322 represents a third range of signal reception from the service (e.g. antenna thereof), perhaps by a MS (not shown). The radius 1316 represents a last and maximum range of signal reception from the service (e.g. antenna thereof), perhaps by a MS (not shown). The time of transmission from service to radius 1318 is less than times of transmission from service to radiuses 1320, 1322, or 1316. The time of transmission from service to radius 1320 is less than times of transmission from service to radiuses 1322 or 1316. The time of transmission from service to radius 1322 is less than time of

transmission from service to radius 1316. In another embodiment, data 1312 contains a Communications Key (CK) 1314 because data 1312 is new transmitted data in accordance with the present disclosure. Data 1312 purpose is for carrying CK 1314 information for being detected, parsed, and processed when received by another MS or data processing system in the vicinity of the service(s) as determined by the maximum range of transmission.

In some embodiments, data 1302 and 1312 are prior art wireless data transmission packets with the exception of embedding a detectable CK 1304 and/or CK 1314, respectively. Usual data communications of MSs are altered to additionally contain the CK so data processing systems in the vicinity can detect, parse, and process the CK. Appropriate send and/or broadcast channel processing is used. In other embodiments, data 1302 and 1312 are new broadcast wireless data transmission packets for containing CK 1304 and CK 1314, respectively. A MS may use send queue 24 for sending/broadcasting packets to data processing systems in the vicinity, and may use the receive queue 26 for receiving packets from other data processing systems in the vicinity. Contents of CKs (Communications Keys) depend on which LBX features are in use and the functionality intended.

In the case of “piggybacking” on usual communications, receive queue 26 insertion processing simply listens for the usual data and when detecting CK presence, inserts CK information appropriately to queue 26 for subsequent processing. Also in the case of “piggybacking” on usual communications, send queue 24 retrieval processing simply retrieves CK information from the queue and embeds it in an outgoing data 1302 at first opportunity. In the case of new data communications, receive queue 26 insertion processing simply listens for the new data containing CK information, and inserts CK information appropriately to queue 26 for subsequent processing. Also in the case of new data communications, send queue 24 retrieval processing simply retrieves CK information from the queue and transmits CK information as new data.

LBX: LN-EXPANSE Configuration

Fig. 14A depicts a flowchart for describing a preferred embodiment of MS LBX configuration processing. Fig. 14 is of Self Management Processing code 18. MS LBX

configuration begins at block 1402 upon user action to start the user interface and continues to block 1404 where user interface objects are initialized for configurations described below with current settings that are reasonable for display to available user interface real estate. Thereafter, applicable settings are presented to the user at block 5 1406 with options. Block 1406 preferably presents to the user at least whether or not DLM capability is enabled (i.e. MS to behave as a DLM = at least one role of DLMV enabled), whether or not ILM capability is enabled (i.e. MS to behave as an ILM = at least one role of ILMV enabled), and/or whether or not this MS should participate in the LN-expanse as a source location for other MSs (e.g. process 1902 and/or 1942 enabled). Alternative 10 embodiments will further present more or less information for each of the settings, or present information associated with other Fig. 14 blocks of processing. Other embodiments will not configure DLM settings for an MS lacking DLM capability (or when all DLMV roles disabled). Other embodiments will not configure ILM settings when DLM capability is present. Block 1406 continues to block 1408 where processing waits for user action in response to options. Block 1408 continues to block 1410 when a user action is 15 detected. If block 1410 determines the user selected to configure DLM capability (i.e. DLMV role(s)), then the user configures DLM role(s) at block 1412 and processing continues back to block 1406. Block 1412 processing is described by Fig. 15A. If block 1410 determines the user did not select to configure DLM capability (i.e. DLMV role(s)), 20 then processing continues to block 1414. If block 1414 determines the user selected to configure ILM capability (i.e. ILMV role(s)), then the user configures ILM role(s) at block 1416 and processing continues back to block 1406. Block 1416 processing is described by Fig. 15B. If block 1414 determines the user did not select to configure ILM capability (i.e. ILMV role(s)), then processing continues to block 1418. If block 1418 determines the 25 user selected to configure NTP use, then the user configures NTP use at block 1420 and processing continues back to block 1406. Block 1420 processing is described by Fig. 16. If block 1418 determines the user did not select to configure NTP use, then processing continues to block 1422.

If block 1422 determines the user selected to maintain the WDR queue, then the 30 user maintains WDRs at block 1424 and processing continues back to block 1406. Block 1424 processing is described by Fig. 17. Blocks 1412, 1416, 1420 and 1424 are understood to be delimited by appropriate semaphore control to avoid multi-threaded

access problems. If block 1422 determines the user did not select to maintain the WDR queue, then processing continues to block 1426. If block 1426 determines the user selected to configure the confidence floor value, then block 1428 prepares parameters for invoking a Configure Value procedure (parameters for reference (address) of value to configure; and validity criteria of value to configure), and the Configure Value procedure of Fig. 18 is invoked at block 1430 with the two (2) parameters. Thereafter, processing continues back to block 1406. Blocks 1428 and 1430 are understood to be delimited by appropriate semaphore control when modifying the confidence floor value since other threads can access the floor value.

The confidence floor value is the minimum acceptable confidence value of any field 1100d (for example as checked by block 276). No WDR with a field 1100d less than the confidence floor value should be used to describe MS whereabouts. In an alternative embodiment, the confidence floor value is enforced as the same value across an LN-expanse with no user control to modify it. One embodiment of Fig. 14 does not permit user control over a minimum acceptable confidence floor value. Various embodiments will default the floor value. Block 1812 enforces an appropriate value in accordance with the confidence value range implemented (e.g. value from 1 to 100). Since the confidence of whereabouts is likely dependent on applications in use at the MS, the preferred embodiment is to permit user configuration of the acceptable whereabouts confidence for the MS. A new confidence floor value can be put to use at next thread(s) startup, or can be used instantly with the modification made, depending on the embodiment. The confidence floor value can be used to filter out WDRs prior to inserting to queue 22, filter out WDRs when retrieving from queue 22, filter out WDR information when listening on channel(s) prior to inserting to queue 26, and/or used in accessing queue 22 for any reason (depending on embodiments). While confidence is validated on both inserts and queries (retrievals/peeks), one or the other validation is fine (preferably on inserts). It is preferred that executable code incorporate checks where applicable since the confidence floor value can be changed after queue 22 is in use. Also, various present disclosure embodiments may maintain all confidences to queue 22, or a particular set of acceptable confidences.

If block 1426 determines the user did not select to configure the confidence floor value, then processing continues to block 1432. If block 1432 determines the user

selected to configure the Whereabouts Timeliness Variable (WTV), then block 1434 prepares parameters for invoking the Configure Value procedure (parameters for reference (address) of value to configure; and validity criteria of value to configure), and the Configure Value procedure of Fig. 18 is invoked at block 1430 with the two (2) parameters. Thereafter, processing continues back to block 1406. Blocks 1434 and 1430 are understood to be delimited by appropriate semaphore control when modifying the WTV since other threads can access the WTV.

A critical configuration for MS whereabouts processing is whereabouts timeliness. Whereabouts timeliness is how often (how timely) an MS should have accurate whereabouts. Whereabouts timeliness is dependent on how often the MS is updated with whereabouts information, what technologies are available or are in the vicinity, how capable the MS is of maintaining whereabouts, processing speed(s), transmission speed(s), known MS or LN-expanse design constraints, and perhaps other factors. In some embodiments, whereabouts timeliness is as soon as possible. That is, MS whereabouts is updated whenever possible as often as possible. In fact, the present disclosure provides an excellent system and methodology to accomplish that by leveraging location technologies whenever and wherever possible. However, there should be balance when considering less capable processing of a MS to prevent hogging CPU cycles from other applications at the MS. In other embodiments, a hard-coded or preconfigured time interval is used for keeping an MS informed of its whereabouts in a timely manner. For example, the MS should know its own whereabouts at least every second, or at least every 5 seconds, or at least every minute, etc. Whereabouts timeliness is critical depending on the applications in use at the MS. For example, if MS whereabouts is updated once at the MS every 5 minutes during high speeds of travel when using navigation, the user has a high risk of missing a turn during travel in downtown cities where timely decisions for turns are required. On the other hand, if MS whereabouts is updated every 5 seconds, and an application only requires an update accuracy to once per minute, then the MS may be excessively processing.

In some embodiments, there is a Whereabouts Timeliness Variable (WTV) configured at the MS (blocks 1432, 1434, 1430). Whether it is user configured, system configured, or preset in a system, the WTV is used to:

- Define the maximum period of time for MS whereabouts to become stale at any particular time;
- Cause the MS to seek its whereabouts if whereabouts information is not up to date in accordance with the WTV; and
- Prevent keeping the MS too busy with keeping abreast of its own whereabouts.

In another embodiment, the WTV is automatically adjusted based on successes or failures of automatically locating the MS. As the MS successfully maintains timely whereabouts, the WTV is maintained consistent with the user configured, system configured, or preset value, or in accordance with active applications in use at the time. However, as the MS fails in maintaining timely whereabouts, the WTV is automatically adjusted (e.g. to longer periods of time to prevent unnecessary wasting of power and/or CPU resources). Later, as whereabouts become readily available, the WTV can be automatically adjusted back to the optimal value. In an emergency situation, the user always has the ability to force the MS to determine its own whereabouts anyway. (Blocks 856 and 862 through 878, in light of a WDR request and WDR response described for architecture 1900). In embodiments where the WTV is adjusted in accordance with applications in use at the time, the most demanding requirement of any application started is maintained to the WTV. Preferably, each application of the MS initializes to an API of the MS with a parameter of its WTV requirements. If the requirement is more timely than the current value, then the more timely value is used. The WTV can be put to use at next thread(s) startup, or can be used instantly with the modification made, depending on the embodiment.

If block 1432 determines the user did not select to configure the WTV, then processing continues to block 1436. If block 1436 determines the user selected to configure the maximum number of threads in a 19xx process (see 19xx-Max variable in Fig. 19 discussions), then block 1438 interfaces with the user until a valid 19xx-max variable is selected, and processing continues to block 1440. If block 1440 determines the 19xx process is already running (i.e. 19xx-PID > 0 implies it is enabled), then an error is provided to the user at block 1442, and processing continues back to block 1406. Preferably, block 1442 does not continue back to block 1406 until the user acknowledges the error (e.g. with a user action). If block 1440 determines the user selected 19xx process

(process 1902, process 1912, process 1922, process 1932, process 1942, or process 1952) is not already running (i.e. 19xx-PID = 0 implies it is disabled), then block 1444 prepares parameters for invoking the Configure Value procedure (parameters for reference (address) of 19xx-Max value to configure; and validity criteria of value to configure), and the Configure Value procedure of Fig. 18 is invoked at block 1430 with the two (2) parameters. Thereafter, processing continues back to block 1406. Blocks 1438, 1440, 1444 and 1430 are understood to be delimited by appropriate semaphore control when modifying the 19xx-Max value since other threads can access it. The 19xx-Max value should not be modified while the 19xx process is running because the number of threads to terminate may be changed prior to terminating. An alternate embodiment of modifying a process number of threads will dynamically modify the number of threads in anticipation of required processing.

If block 1436 determines the user did not select to configure a process thread maximum (19xx-Max), then block 1446 checks to see if the user selected to (toggle) disable or enable a particular process (i.e. a 19xx process of Fig. 19). If block 1446 determines the user did select to toggle enabling/disabling a particular Fig. 19 process, then block 1448 interfaces with the user until a valid 19xx process name is selected, and processing continues to block 1450. If block 1450 determines the 19xx process is already running (i.e. 19xx-PID > 0 implies it is enabled), then block 1454 prepares parameters (just as does block 2812). Thereafter, block 1456 invokes Fig. 29B processing (just as does block 2814). Processing then continues back to block 1406. If block 1450 determines the 19xx process is not running (i.e. 19xx-PID = 0 implies it is disabled), then block 1452 invokes Fig. 29A processing (just as does block 1232). Processing then continues back to block 1406. Block 1456 does not continue back to block 1406 until the process is completely terminated. Blocks 1448, 1450, 1452, 1454 and 1456 are understood to be delimited by appropriate semaphore control.

Preferred embodiments of blocks 1446 and 1448 use convenient names of processes being started or terminated, rather than convenient brief process names such as 1902, 1912, 1922, 1932, 1942, or 1952 used in flowcharts. In some embodiments, the long readable name is used, such as whereabouts broadcast process (1902), whereabouts collection process (1912), whereabouts supervisor process (1922), timing determination process (1932), WDR request process (1942), and whereabouts

determination process (1952). For example, the user may know that the whereabouts supervisor process enabled/disabled indicates whether or not to have whereabouts timeliness monitored in real time. Enabling the whereabouts supervisor process enables monitoring for the WTV in real time, and disabling the whereabouts supervisor process
5 disables monitoring the WTV in real time.

In another embodiment of blocks 1446 and 1448, a completely new name or description may be provided to any of the processes to facilitate user interface usability. For example, a new name Peer Location Source Variable (PLSV) can be associated to the whereabouts broadcast process 1902 and/or 1942. PLSV may be easier to remember.
10 If the PLSV was toggled to disabled, the whereabouts broadcast process 1902 and/or 1942 terminates. If the PLSV was toggled to enabled, the whereabouts broadcast process 1902 and/or 1942 is started. It may be easier to remember that the PLSV enables/disables whether or not to allow this MS to be a location source for other MSs in an LN-expanse.

In other embodiments, a useful name (e.g. PLSV) represents starting and terminating any subset of 19xx processes (a plurality (e.g. 1902 and 1942)) for simplicity. In yet other embodiments, Fig. 14A/14B can be used to start or terminate worker thread(s) in any process, for example to throttle up more worker threads in a process, or to throttle
15 down for less worker threads in a process, perhaps modifying thread instances to accommodate the number of channels for communications, or for the desired performance. There are many embodiments for fine tuning the architecture 1900 for optimal peer to peer interaction. In yet other embodiments, toggling may not be used. There may be individual options available at block 1408 for setting any data of this disclosure. Similarly, the 19xx-Max variables may be modified via individual user friendly
20 names and/or as a group of 19xx-Max variables.

Referring back to block 1446, if it is determined the user did not select to toggle for enabling/disabling process(es), then processing continues to block 1458. If block 1458 determines the user selected to exit Fig. 14A/14B configuration processing, then block 1460 terminates the user interface appropriately and processing terminates at block 1462.
25 If block 1458 determines the user did not select to exit the user interface, then processing continues to block 1466 of Fig. 14B by way of off page connector 1464.

With reference now to Fig. 14B, depicted is a continued portion flowchart of Fig. 14A for describing a preferred embodiment of MS LBX configuration processing. If block 1466 determines the user selected to configure the Source Periodicity Time Period (SPTP) value, then block 1468 prepares parameters for invoking the Configure Value procedure (parameters for reference (address) of value to configure; and validity criteria of value to configure), and the Configure Value procedure of Fig. 18 is invoked at block 1470 with the two (2) parameters. Thereafter, processing continues back to block 1406 by way of off page connector 1498. Blocks 1468 and 1470 are understood to be delimited by appropriate semaphore control when modifying the SPTP value since other threads can access it. The SPTP configures the time period between broadcasts by thread(s) 1902, for example 5 seconds. Some embodiments do not permit configuration of the SPTP.

If block 1466 determines the user did not select to configure the SPTP value, then processing continues to block 1472. If block 1472 determines the user selected to configure service propagation, then the user configures service propagation at block 1474 and processing continues back to block 1406 by way of off page connector 1498. If block 1472 determines the user did not select to configure service propagation, then processing continues to block 1476.

If block 1476 determines the user selected to configure permissions 10, then the user configures permissions at block 1478 and processing continues back to block 1406 by way of off page connector 1498. If block 1476 determines the user did not select to configure permissions 10, then processing continues to block 1480. If block 1480 determines the user selected to configure charters 12, then the user configures charters 12 at block 1482 and processing continues back to block 1406 by way of off page connector 1498. If block 1480 determines the user did not select to configure charters 12, then processing continues to block 1484. If block 1484 determines the user selected to configure statistics 14, then the user configures statistics 14 at block 1486 and processing continues back to block 1406 by way of off page connector 1498. If block 1484 determines the user did not select to configure statistics 14, then processing continues to block 1488. If block 1488 determines the user selected to configure service informant code 28, then the user configures code 28 at block 1490 and processing continues back to block 1406 by way of off page connector 1498. If block 1488 determines the user did not select to configure code 28, then processing continues to block 1492. If block 1492 determines the

user selected to maintain LBX history 30, then the user maintains LBX history at block 1494 and processing continues back to block 1406 by way of off page connector 1498. If block 1492 determines the user did not select to maintain LBX history 30, then processing continues to block 1496.

5 Block 1496 handles other user interface actions leaving block 1408, and processing continues back to block 1406 by way of off page connector 1498.

 Details of blocks 1474, 1478, 1482, 1486, 1490, 1494, and perhaps more detail to block 1496, are described with other flowcharts. Appropriate semaphores are requested at the beginning of block processing, and released at the end of block processing, for thread
10 safe access to applicable data at risk of being accessed by another thread of processing at the same time of configuration. In some embodiments, a user/administrator with secure privileges to the MS has ability to perform any subset of configurations of Figs. 14A and 14B processing, while a general user may not. Any subset of Fig. 14 configuration may appear in alternative embodiments, with or without authenticated administrator access to
15 perform configuration.

 Fig. 15A depicts a flowchart for describing a preferred embodiment of DLM role configuration processing of block 1412. Processing begins at block 1502 and continues to block 1504 which accesses current DLMV settings before continuing to block 1506. If
20 there were no DLMV entries (list empty) as determined by block 1506, then block 1508 provides an error to the user and processing terminates at block 1518. The DLMV may be empty when the MS has no local DLM capability and there hasn't yet been any detected DLM capability, for example as evidenced by WDRs inserted to queue 22. Preferably, the error presented at block 1508 requires the user to acknowledge the error (e.g. with a user
25 action) before block 1508 continues to block 1518. If block 1506 determines at least one entry (role) is present in the DLMV, then the current DLMV setting(s) are saved at block 1510, the manage list processing procedure of Fig. 15C is invoked at block 1512 with the DLMV as a reference (address) parameter, and processing continues to block 1514.

 Block 1514 determines if there were any changes to the DLMV from Fig. 15C
30 processing by comparing the DLMV after block 1512 with the DLMV saved at block 1510. If there were changes via Fig. 15C processing, such as a role which was enabled prior to block 1512 which is now disabled, or such as a role which was disabled prior to block

1512 which is now enabled, then block 1514 continues to block 1516 which handles the DLMV changes appropriately. Block 1516 continues to block 1518 which terminates Fig. 15A processing. If block 1514 determines there were no changes via block 1512, then processing terminates at block 1518.

5 Block 1516 enables newly enabled role(s) as does block 1238 described for Fig. 12. Block 1516 disables newly disabled role(s) as does block 2804 described for Fig. 28.

10 Fig. 15B depicts a flowchart for describing a preferred embodiment of ILM role configuration processing of block 1416. Processing begins at block 1522 and continues to block 1524 which accesses current ILMV settings before continuing to block 1526. If there were no ILMV entries (list empty) as determined by block 1526, then block 1528 provides an error to the user and processing terminates at block 1538. The ILMV may be empty when the MS is not meant to have ILM capability. Preferably, the error presented at block 1528 requires the user to acknowledge the error before block 1528 continues to block 1538. If block 1526 determines at least one entry (role) is present in the ILMV, then the current ILMV setting(s) are saved at block 1530, the manage list processing procedure of Fig. 15C is invoked with a reference (address) parameter of the ILMV at block 1532, and processing continues to block 1534.

15 Block 1534 determines if there were any changes to the ILMV from Fig. 15C processing by comparing the ILMV after block 1532 with the ILMV saved at block 1530. If there were changes via Fig. 15C processing, such as a role which was enabled prior to block 1532 which is now disabled, or such as a role which was disabled prior to block 1532 which is now enabled, then block 1534 continues to block 1536 which handles the ILMV changes appropriately. Block 1536 continues to block 1538 which terminates Fig. 15B processing. If block 1534 determines there were no changes via block 1532, then processing terminates at block 1538.

20 Block 1536 enables newly enabled role(s) as does blocks 1224 through 1234 described for Fig. 12. Block 1536 disables newly disabled role(s) as does blocks 2806 through 2816 described for Fig. 28.

30 Fig. 15C depicts a flowchart for describing a preferred embodiment of a procedure for Manage List processing. Processing starts at block 1552 and continues to block 1554.

Block 1554 presents the list (DLM capability if arrived to by way of Fig. 15A; ILM capability if arrived to by way of Fig. 15B) to the user, as passed to Fig. 15C processing with the reference parameter by the invoker, with which list items are marked (enabled) and which are unmarked (disabled) along with options, before continuing to block 1556 for awaiting user action. Block 1554 highlights currently enabled roles, and ensures disabled roles are not highlighted in the presented list. When a user action is detected at block 1556, thereafter, block 1558 checks if a list entry was enabled (marked) by the user, in which case block 1560 marks the list item as enabled, saves it to the list (e.g. DLMV or ILMV), and processing continues back to block 1554 to refresh the list interface. If block 1558 determines the user did not respond with an enable action, then block 1562 checks for a disable action. If block 1562 determines the user wanted to disable a list entry, then block 1564 marks (actually unmarks it) the list item as disabled, saves it to the list (e.g. DLMV or ILMV), and processing continues back to block 1554. If block 1562 determines the user did not want to disable a list item, then block 1566 checks if the user wanted to exit Fig. 15C processing. If block 1566 determines the user did not select to exit list processing, then processing continues to block 1568 where other user interface actions are appropriately handled and then processing continues back to block 1554. If block 1566 determines the user did select to exit manage list processing, then Fig. 15C processing appropriately returns to the caller at block 1570.

Fig. 15C interfaces with the user for desired DLMV (via Fig. 15A) or ILMV (via Fig. 15B) configurations. In some embodiments, it makes sense to have user control over enabling or disabling DLM and/or ILM capability (roles) to the MS, for example for software or hardware testing.

Fig. 16 depicts a flowchart for describing a preferred embodiment of NTP use configuration processing of block 1420. Processing starts at block 1602 and continues to block 1604 where the current NTP use setting is accessed. Thereafter, block 1606 presents the current NTP use setting to its value of enabled or disabled along with options, before continuing to block 1608 for awaiting user action. When a user action is detected at block 1608, block 1610 checks if the NTP use setting was disabled at block 1608, in which case block 1612 terminates NTP use appropriately, block 1614 sets (and

saves) the NTP use setting to disabled, and processing continues back to block 1606 to refresh the interface. Block 1612 disables NTP as does block 2828.

5 If block 1610 determines the user did not respond for disabling NTP, then block 1616 checks for a toggle to being enabled. If block 1616 determines the user wanted to enable NTP use, then block 1618 accesses known NTP server address(es) (e.g. ip
addresses preconfigured to the MS, or set with another user interface at the MS), and pings each one, if necessary, at block 1620 with a timeout. As soon as one NTP server is determined to be reachable, block 1620 continues to block 1622. If no NTP server was
10 reachable, then the timeout will have expired for each one tried at block 1620 for continuing to block 1622. Block 1622 determines if at least one NTP server was reachable at block 1620. If block 1622 determines no NTP server was reachable, then an error is presented to the user at block 1624 and processing continues back to block 1606. Preferably, the error presented at block 1624 requires the user to acknowledge the error before block 1624 continues to block 1606. If block 1622 determines that at least one NTP
15 server was reachable, then block 1626 initializes NTP use appropriately, block 1628 sets the NTP use setting to enabled (and saves), and processing continues back to block 1606. Block 1626 enables NTP as does block 1210.

Referring back to block 1616, if it is determined the user did not want to enable NTP use, then processing continues to block 1630 where it is checked if the user wanted
20 to exit Fig. 16 processing. If block 1630 determines the user did not select to exit Fig. 16 processing, then processing continues to block 1632 where other user interface actions leaving block 1608 are appropriately handled, and then processing continues back to block 1606. If block 1630 determines the user did select to exit processing, then Fig. 16 processing terminates at block 1634.

25 Fig. 17 depicts a flowchart for describing a preferred embodiment of WDR maintenance processing of block 1424. Processing starts at block 1702 and continues to block 1704 where it is determined if there are any WDRs of queue 22. If block 1704 determines there are no WDRs for processing, then block 1706 presents an error to the
30 user and processing continues to block 1732 where Fig. 17 processing terminates. Preferably, the error presented at block 1706 requires the user to acknowledge the error before block 1706 continues to block 1732. If block 1704 determines there is at least one

WDR, then processing continues to block 1708 where the current contents of WDR queue 22 is appropriately presented to the user (in a scrollable list if necessary). Thereafter, block 1710 awaits user action. When a user action is detected at block 1710, block 1712 checks if the user selected to delete a WDR from queue 22, in which case block 1714 discards the selected WDR, and processing continues back to block 1708 for a refreshed presentation of queue 22. If block 1712 determines the user did not select to delete a WDR, then block 1716 checks if the user selected to modify a WDR. If block 1716 determines the user wanted to modify a WDR of queue 22, then block 1718 interfaces with the user for validated WDR changes before continuing back to block 1708. If block 1716 determines the user did not select to modify a WDR, then block 1720 checks if the user selected to add a WDR to queue 22. If block 1720 determines the user selected to add a WDR (for example, to manually configure MS whereabouts), then block 1722 interfaces with the user for a validated WDR to add to queue 22 before continuing back to block 1708. If block 1720 determines the user did not select to add a WDR, then block 1724 checks if the user selected to view detailed contents of a WDR, perhaps because WDRs are presented in an abbreviated form at block 1708. If it is determined at block 1724 the user did select to view details of a WDR, then block 1726 formats the WDR in detail form, presents it to the user, and waits for the user to exit the view of the WDR before continuing back to block 1708. If block 1724 determines the user did not select to view a WDR in detail, then block 1728 checks if the user wanted to exit Fig. 17 processing. If block 1728 determines the user did not select to exit Fig. 17 processing, then processing continues to block 1730 where other user interface actions leaving block 1710 are appropriately handled, and then processing continues back to block 1708. If block 1728 determines the user did select to exit processing, then Fig. 17 processing terminates at block 1732.

There are many embodiments for maintaining WDRs of queue 22. In some embodiments, Fig. 17 (i.e. block 1424) processing is only provided for debug of an MS. In a single instance WDR embodiment, block 1708 presents the one and only WDR which is used to keep current MS whereabouts whenever possible. Other embodiments incorporate any subset of Fig. 17 processing.

Fig. 18 depicts a flowchart for describing a preferred embodiment of a procedure for variable configuration processing, namely the Configure Value procedure, for example for processing of block 1430. Processing starts at block 1802 and continues to block 1804 where parameters passed by the invoker of Fig. 18 are determined, namely the reference (address) of the value for configuration to be modified, and the validity criteria for what makes the value valid. Passing the value by reference simply means that Fig. 18 has the ability to directly change the value, regardless of where it is located. In some embodiments, the parameter is an address to a memory location for the value. In another embodiment, the value is maintained in a database or some persistent storage, and Fig. 18 is passed enough information to know how to permanently affect/change the value.

Block 1804 continues to block 1806 where the current value passed is presented to the user (e.g. confidence floor value), and then to block 1808 for awaiting user action. When a user action is detected at block 1808, block 1810 checks if the user selected to modify the value, in which case block 1812 interfaces with the user for a validated value using the validity criteria parameter before continuing back to block 1806. Validity criteria may take the form of a value range, value type, set of allowable values, or any other criteria for what makes the value a valid one.

If block 1810 determines the user did not select to modify the value, then block 1814 checks if the user wanted to exit Fig. 18 processing. If block 1814 determines the user did not select to exit Fig. 18 processing, then processing continues to block 1816 where other user interface actions leaving block 1808 are appropriately handled, and then processing continues back to block 1806. If block 1814 determines the user did select to exit processing, then Fig. 18 processing appropriately returns to the caller at block 1818.

LBX: LN-EXPANSE Interoperability

Fig. 19 depicts an illustration for describing a preferred embodiment multithreaded architecture of peer interaction processing of a MS in accordance with the present disclosure. MS architecture 1900 preferably includes a set of Operating System (O/S) processes (i.e. O/S terminology “process” with O/S terminology “thread” or “threads (i.e. thread(s))”, including a whereabouts broadcast process 1902, a whereabouts collection process 1912, a whereabouts supervisor process 1922, a timing determination process 1932, a WDR request process 1942, and a whereabouts determination process 1952.

Further included are queues for interaction of processing, and process associated variables to facilitate processing. All of the Fig. 19 processes are of PIP code 6. There is preferably a plurality (pool) of worker threads within each of said 19xx processes (i.e. 1902, 1912, 1922, 1932, 1942 and 1952) for high performance asynchronous processing. Each 19xx process (i.e. 1902, 1912, 1922, 1932, 1942 and 1952) preferably has at least two (2) threads:

- 1) "parent thread"; and
- 2) "worker thread".

A parent thread (Fig. 29A) is the main process thread for:

- starting the particular process;
- starting the correct number of worker thread(s) of that particular process;
- staying alive while all worker threads are busy processing; and
- properly terminating the process when worker threads are terminated.

The parent thread is indeed the parent for governing behavior of threads at the process whole level. Every process has a name for convenient reference, such as the names 1902, 1912, 1922, 1932, 1942 and 1952. Of course, these names may take on the associated human readable forms of whereabouts broadcast process, whereabouts collection process, whereabouts supervisor process, timing determination process, WDR request process, and whereabouts determination process, respectively. For brevity, the names used herein are by the process label of Fig. 19 in a form 19xx. There must be at least one worker thread in a process. Worker thread(s) are described with a flowchart as follows:

- 1902 – Fig. 20;
- 1912 – Fig. 21;
- 1922 – Fig. 22;
- 1932 – Fig. 23;
- 1942 – Fig. 25; and
- 1952 – Fig. 26A.

Threads of architecture MS are presented from a software perspective, but there are applicable hardware/firmware process thread embodiments accomplished for the same functionality. In fact, hardware/firmware embodiments are preferred when it is known that processing is mature (i.e. stable) to provide the fastest possible performance. Architecture 1900 processing is best achieved at the highest possible performance speeds for optimal wireless communications processing. There are two (2) types of processes for describing the types of worker threads:

- 1) "Slave to Queue"; and
- 2) "Slave to Timer".

10

A 19xx process is a slave to queue process when its worker thread(s) are driven by feeding from a queue of architecture 1900. A slave to queue process stays "blocked" (O/S terminology "blocked" = preempted) on a queue entry retrieval interface until the sought queue item is inserted to the queue. The queue entry retrieval interface becomes "cleared" (O/S terminology "cleared" = clear to run) when the sought queue entry is retrieved from the queue by a thread. These terms (blocked and cleared) are analogous to a semaphore causing a thread to be blocked, and a thread to be cleared, as is well known in the art. Queues have semaphore control to ensure no more than one thread becomes clear at a time for a single queue entry retrieved (as done in an O/S). One thread sees a particular queue entry, but many threads can feed off the same queue to do the same work concurrently. Slave to queue type of processes are 1912, 1932, 1942 and 1952. A slave to queue process is properly terminated by inserting a special termination queue entry for each worker thread to terminate itself after queue entry retrieval.

A 19xx process is a slave to timer process when its worker thread(s) are driven by a timer for peeking a queue of architecture 1900. A timer provides the period of time for a worker thread to sleep during a looped iteration of checking a queue for a sought entry (without removing the entry from the queue). Slave to timer threads periodically peek a queue, and based on what is found, will process appropriately. A queue peek does not alter the peeked queue. The queue peek interface is semaphore protected for preventing peeking at an un-opportune time (e.g. while thread inserting or retrieving from queue). Queue interfaces ensure one thread is acting on a queue with a queue interface at any particular time. Slave to timer type of processes are 1902 and 1922. A slave to timer

30

process is properly terminated by inserting a special termination queue entry for each worker thread to terminate itself by queue entry peek.

Block 2812 knows the type of 19xx process for preparing the process type parameter for invocation of Fig. 29B at block 2814. The type of process has slightly different termination requirements because of the worker thread(s) processing type. Alternate embodiments of slave to timer processes will make them slave to queue processes by simply feeding off Thread Request (TR) queue 1980 for driving a worker thread when to execute (and when to terminate). New timer(s) would insert timely queue entries to queue 1980, and processes 1902 and 1922 would retrieve from the queue (Fig. 24A record 2400). The queue entries would become available to queue 1980 when it is time for a particular worker thread to execute. Worker threads of processes 1902 and 1922 could retrieve, and stay blocked on, queue 1980 until an entry was inserted by a timer for enabling a worker thread (field 2400a set to 1902 or 1912). TR queue 1980 is useful for starting any threads of architecture 1900 in a slave to queue manner. This may be a cleaner architecture for all thread pools to operate the same way (slave to queue). Nevertheless, the two thread pool methods are implemented.

Each 19xx process has at least four (4) variables for describing present disclosure processing:

- 19xx-PID = The O/S terminology "Process Identifier (PID)" for the O/S PID of the 19xx process. This variable is also used to determine if the process is enabled (PID > 0), or is disabled (PID = 0 (i.e. <= 0));
- 19xx-Max = The configured number of worker thread(s) for the 19xx process;
- 19xx-Sem = A process local semaphore for synchronizing 19xx worker threads, for example in properly starting up worker threads in process 19xx, and for properly terminating worker threads in process 19xx; and
- 19xx-Ct = A process local count of the number of worker thread(s) currently running in the 19xx process.

19xx-PID and 19xx-Max are variables of PIP data 8. 19xx-Sem and 19xx-Ct are preferably process 19xx stack variables within the context of PIP code 6. 19xx-PID is a semaphore protected global variable in architecture 1900 so that it can be used to determine whether or not a particular 19xx process is enabled (i.e. running) or disabled (not running). 19xx-

Max is a semaphore protected global variable in architecture 1900 so that user configuration processing outside of architecture 1900 can be used to administrate a desired number of worker threads for a 19xx process. Alternate embodiments will not provide user configuration of 19xx-Max variables (e.g. hard coded maximum number of threads), in which case no 19xx-Max global variable is necessary. “Thread(s) 19xx” is a brief form of stating “worker thread(s) of the 19xx process”.

Receive (Rx) queue 26 is for receiving CK 1304 or CK 1314 data (e.g. WDR or WDR requests), for example from wireless transmissions. Queue 26 will receive at least WDR information (destined for threads 1912) and WDR requests (Fig. 24C records 2490 destined for threads 1942). At least one thread (not shown) is responsible for listening on appropriate channel(s) and immediately depositing appropriate records to queue 26 so that they can be processed by architecture 1900. Preferably, there is a plurality (pool) of threads for feeding queue 26 based on channel(s) being listened on, and data 1302 or 1312 anticipated for being received. Alternative embodiments of thread(s) 1912 may themselves directly be listening on appropriate channels and immediately processing packets identified, in lieu of a queue 26. Alternative embodiments of thread(s) 1942 may themselves directly be listening on appropriate channels and immediately processing packets identified, in lieu of a queue 26. Queue 26 is preferred to isolate channel(s) (e.g. frequency(s)) and transmission reception processing in well known modular (e.g. Radio Frequency (RF)) componentry, while providing a high performance queue interface to other asynchronous threads of architecture 1900 (e.g. thread(s) of process 1912). Wave spectrums (via particular communications interface 70) are appropriately processed for feeding queue 26. As soon as a record is received by an MS, it is assumed ready for processing at queue 26. All queue 26 accesses are assumed to have appropriate semaphore control to ensure synchronous access by any thread at any particular time to prevent data corruption and misuse. Queue entries inserted to queue 26 may have arrived on different channel(s), and in such embodiments a channel qualifier may further direct queue entries from queue 26 to a particular thread 1912 or 1942 (e.g. thread(s) dedicated to channel(s)). In other embodiments, receive processing feeds queue 26 independent of any particular channel(s) monitored, or received on (the preferred embodiment described). Regardless of how data is received and then immediately placed on queue 26, a received date/time stamp (e.g. fields 1100p or 2490c) is added to the applicable record for

communicating the received date/time stamp to a thread (e.g. thread(s) 1912 or 1942) of when the data was received. Therefore, the queue 26 insert interface tells the waiting thread(s) when the data was actually received. This ensures a most accurate received date/time stamp as close to receive processing as possible (e.g. enabling most accurate TDOA measurements). An alternate embodiment could determine applicable received date/time stamps in thread(s) 1912 or thread(s) 1942. Other data placed into received WDRs are: wave spectrum and/or particular communications interface 70 of the channel received on, and heading/yaw/pitch/roll (or accelerometer readings) with AOA measurements, signal strength, and other field 1100f eligible data of the receiving MS. Depending on alternative embodiments, queue 26 may be viewed metaphorically for providing convenient grounds of explanation.

Send (Tx) queue 24 is for sending/communicating CK 1304 data, for example for wireless transmissions. At least one thread (not shown) is responsible for immediately transmitting (e.g. wirelessly) anything deposited to queue 24. Preferably, there is a plurality (pool) of threads for feeding off of queue 24 based on channel(s) being transmitted on, and data 1302 anticipated for being sent. Alternative embodiments of thread(s) of processes 1902, 1922, 1932 and 1942 may themselves directly transmit (send/broadcast) on appropriate channels anything deposited to queue 24, in lieu of a queue 24. Queue 24 is preferred to isolate channel(s) (e.g. frequency(s)) and transmission processing in well known modular (e.g. RF) componentry, while providing a high performance queue interface to other asynchronous threads of architecture 1900 (e.g. thread(s) 1942). Wave spectrums and/or particular communications interface 70 are appropriately processed for sending from queue 24. All queue 24 accesses are assumed to have appropriate semaphore control to ensure synchronous access by any thread at any particular time to prevent data corruption and misuse. As soon as a record is inserted to queue 24, it is assumed sent immediately. Preferably, fields sent depend on fields set. Queue entries inserted to queue 24 may contain specification for which channel(s) to send on in some embodiments. In other embodiments, send processing feeding from queue 24 has intelligence for which channel(s) to send on (the preferred embodiment described). Depending on alternative embodiments, queue 24 may be viewed metaphorically for providing convenient grounds of explanation.

When interfacing to queue 24, the term “broadcast” refers to sending outgoing data in a manner for reaching as many MSs as possible (e.g. use all participating communications interfaces 70), whereas the term “send” refers to targeting a particular MS or group of MSs.

5 WDR queue 22 preferably contains at least one WDR 1100 at any point in time, for at least describing whereabouts of the MS of architecture 1900. Queue 22 accesses are assumed to have appropriate semaphore control to ensure synchronous access by any thread at any particular time to prevent data corruption and misuse. A single instance of data embodiment of queue 22 may require an explicit semaphore control for access. In a
10 WDR plurality maintained to queue 22, appropriate queue interfaces are again provided to ensure synchronous thread access (e.g. implicit semaphore control). Regardless, there is still a need for a queue 22 to maintain a plurality of WDRs from remote MSs. The preferred embodiment of all queue interfaces uses queue interface maintained semaphore(s) invisible to code making use of queue (e.g. API) interfaces. Depending on
15 alternative embodiments, queue 22 may be viewed metaphorically for providing convenient grounds of explanation.

Thread Request (TR) queue 1980 is for requesting processing by either a timing determination (worker) thread of process 1932 (i.e. thread 1932) or whereabouts determination (worker) thread of process 1952 (i.e. thread 1952). When requesting
20 processing by a thread 1932, TR queue 1980 has requests (retrieved via processing 1934 after insertion processing 1918) from a thread 1912 to initiate TDOA measurement. When requesting processing by a thread 1952, TR queue 1980 has requests (retrieved via processing 1958 after insertion processing 1918 or 1930) from a thread 1912 or 1922 so that thread 1952 performs whereabouts determination of the MS of architecture 1900.
25 Requests of queue 1980 comprise records 2400. Preferably, there is a plurality (pool) of threads 1912 for feeding queue 1980 (i.e. feeding from queue 26), and for feeding a plurality each of threads 1932 and 1952 from queue 1980. All queue 1980 accesses are assumed to have appropriate semaphore control to ensure synchronous access by any thread at any particular time to prevent data corruption and misuse. Depending on
30 alternative embodiments, queue 1980 may be viewed metaphorically for providing convenient grounds of explanation.

With reference now to Fig. 24A, depicted is an illustration for describing a preferred embodiment of a thread request queue record, as maintained to Thread Request (TR) queue 1980. TR queue 1980 is not required when a LN-expanse globally uses NTP, as found in thread 19xx processing described for architecture 1900, however it may be required at a MS which does not have NTP, or a MS which interacts with another data processing system (e.g. MS) that does not have NTP. Therefore, TR queue record 2400 (i.e. queue entry 2400) may, or may not, be required. This is the reason Fig. 1A does not depict queue 1980. When NTP is in use globally (in LN-expanse), TDOA measurements can be made using a single unidirectional data (1302 or 1312) packet containing a sent date/time stamp (of when the data was sent). Upon receipt, that sent date/time stamp received is compared with the date/time of receipt to determine the difference. The difference is a TDOA measurement. Knowing transmission speeds with a TDOA measurement allows calculating a distance. In this NTP scenario, no thread(s) 1932 are required.

Threads 1912 and/or DLM processing may always insert the MS whereabouts without requirement for thread(s) 1952 by incorporating thread 1952 logic into thread 1912, or by directly starting (without queue 1980) a thread 1952 from a thread 1912. Therefore, threads 1952 may not be required. If threads 1952 are not required, queue 1980 may not be required by incorporating thread 1932 logic into thread 1912, or by directly starting (without queue 1980) a thread 1932 from a thread 1912. Therefore, queue 1980 may not be required, and threads 1932 may not be required.

Records 2400 (i.e. queue entries 2400) contain a request type field 2400a and data field 2400b. Request type field 2400a simply routes the queue entry to destined thread(s) (e.g. thread(s) 1932 or thread(s) 1952). A thread 1932 remains blocked on queue 1980 until a record 2400 is inserted which has a field 2400a containing the value 1932. A thread 1952 remains blocked on queue 1980 until a record 2400 is inserted which has a field 2400a containing the value 1952. Data field 2400b is set to zero (0) when type field 2400a contains 1952 (i.e. not relevant). Data field 2400b contains an MS ID (field 1100a) value, and possibly a targeted communications interface 70 (or wave spectrum if one to one), when type field contains 1932. Field 2400b will contain information for appropriately targeting the MS ID with data (e.g. communications interface to use if MS has multiple of

them). An MS with only one communications interface can store only a MS ID in field 2400b.

Records 2400 are used to cause appropriate processing by 19xx threads (e.g. 1932 or 1952) as invoked when needed (e.g. by thread(s) 1912). Process 1932 is a slave to queue type of process, and there are no queue 1980 entries 2400 which will not get timely processed by a thread 1932. No interim pruning is necessary to queue 1980.

With reference now back to Fig. 19, Correlation Response (CR) queue 1990 is for receiving correlation data for correlating requests transmitted in data 1302 with responses received in data 1302 or 1312. Records 2450 are inserted to queue 1990 (via processing 1928) from thread(s) 1922 so that thread(s) 1912 (after processing 1920) correlate data 1302 or 1312 with requests sent by thread(s) 1922 (e.g. over interface 1926), for the purpose of calculating a TDOA measurement. Additionally, records 2450 are inserted to queue 1990 (via processing 1936) from thread(s) 1932 so that thread(s) 1912 (after processing 1920) correlate data 1302 or 1312 with requests sent by thread(s) 1932 (e.g. over interface 1938), for the purpose of calculating a TDOA measurement. Preferably, there is a plurality (pool) of threads for feeding queue 1990 and for feeding from queue 1990 (feeding from queue 1990 with thread(s) 1912). All queue 1990 accesses are assumed to have appropriate semaphore control to ensure synchronous access by any thread at any particular time to prevent data corruption and misuse. Depending on alternative embodiments, queue 1990 may be viewed metaphorically for providing convenient grounds of explanation.

With reference now to Fig. 24B, depicted is an illustration for describing a preferred embodiment of a correlation response queue record, as maintained to Correlation Response (CR) queue 1990. CR queue 1990 is not required when a LN-expanse globally uses NTP, as found in thread 19xx processing described for architecture 1900, however it may be required at a MS which does not have NTP, or a MS which interacts with another data processing system (e.g. MS) that does not have NTP. Therefore, CR record 2450 (i.e. queue entry 2450) may, or may not, be required. This is the reason Fig. 1A does not depict queue 1990. The purpose of CR queue 1990 is to enable calculation of TDOA measurements using correlation data to match a request with a response. When NTP is

used globally in the LN-expanse, no such correlations between a request and response is required, as described above. In the NTP scenario, thread(s) 1912 can deduce TDOA measurements directly from responses (see Fig. 21), and there is no requirement for threads 1932.

5 TDOA measurements are best taken using date/time stamps as close to the processing points of sending and receiving as possible, otherwise critical regions of code may be required for enabling process time adjustments to the measurements when processing is “further out” from said points. This is the reason MS receive processing provides received date/time stamps with data inserted to queue 26 (field 1100p or 2490c).
10 In a preferred embodiment, send queue 24 processing inserts to queue 1990 so the date/time stamp field 2450a for when sent is as close to just prior to having been sent as possible. However, there is still the requirement for processing time spent inserting to queue 1990 prior to sending anyway. Anticipated processing speeds of architecture 1900 allow reasonably moving sent date/time stamp setting just a little “further out” from actually
15 sending to keep modular send processing isolated. A preferred embodiment (as presented) assumes the send queue 24 interface minimizes processing instructions from when data is placed onto queue 24 and when it is actually sent, so that the sending thread(s) 19xx (1902, 1922, 1932 and 1942) insert to queue 1990 with a reasonably accurate sent/date stamp field 2450a. This ensures a most accurate sent date/time stamp
20 (e.g. enabling most accurate TDOA measurements). An alternate embodiment makes appropriate adjustments for more accurate time to consider processing instructions up to the point of sending after queue 1990 insertion.

Records 2450 (i.e. queue entries 2450) contain a date/time stamp field 2450a and a correlation data field 2450b. Date/time stamp field 2450a contains a date/time stamp of
25 when a request (data 1302) was sent as set by the thread inserting the queue entry 2450. Correlation data field 2450b contains unique correlation data (e.g. MS id with suffix of unique number) used to provide correlation for matching sent requests (data 1302) with received responses (data 1302 or 1312), regardless of the particular communications interface(s) used (e.g. different wave spectrums supported by MS). Upon a correlation
30 match, a TDOA measurement is calculated using the time difference between field 2450a and a date/time stamp of when the response was received (e.g. field 1100p). A thread 1912 accesses queue 1990 for a record 2450 using correlation field 2450b to match,

when data 1302 or 1312 contains correlation data for matching. A thread 1912 then uses the field 2450a to calculate a TDOA measurement. Process 1912 is not a slave to queue 1990 (but is to queue 26). A thread 1912 peeks queue 1990 for a matching entry when appropriate. Queue 1990 may contain obsolete queue entries 2450 until pruning is performed. Some WDR requests may be broadcasts, therefore records 2450 may be used for correlating a plurality of responses. In another record 2450 embodiment, an additional field 2450c is provided for specification of which communication interface(s) and/or channel(s) to listen on for a response.

With reference now back to Fig. 19, any reasonable subset of architecture 1900 processing may be incorporated in a MS. For example in one minimal subset embodiment, a DLM which has excellent direct locating means only needs a single instance WDR (queue 22) and a single thread 1902 for broadcasting whereabouts data to facilitate whereabouts determination by other MSs. In a near superset embodiment, process 1942 processing may be incorporated completely into process 1912, thereby eliminating processing 1942 by having threads 1912 feed from queue 26 for WDR requests as well as WDR information. In another subset embodiment, process 1922 may only send requests to queue 24 for responses, or may only start a thread 1952 for determining whereabouts of the MS. There are many viable subset embodiments depending on the MS being a DLM or ILM, capabilities of the MS, LN-expanse deployment design choices, etc. A reference to Fig. 19 accompanies thread 19xx flowcharts (Figs. 20, 21, 22, 23, 25 and 26A). The user, preferably an administrator type (e.g. for lbxPhone™ debug) selectively configures whether or not to start or terminate a process (thread pool), and perhaps the number of threads to start in the pool (see Fig. 14A). Starting a process (and threads) and terminating processes (and threads) is shown in flowcharts 29A and 29B. There are other embodiments for properly starting and terminating threads without departing from the spirit and scope of this disclosure.

Fig. 20 depicts a flowchart for describing a preferred embodiment of MS whereabouts broadcast processing, for example to facilitate other MSs in locating themselves in an LN-expanse. Fig. 20 processing describes a process 1902 worker thread, and is of PIP code 6. Thread(s) 1902 purpose is for the MS of Fig. 20 processing

(e.g. a first, or sending, MS) to periodically transmit whereabouts information to other MSs (e.g. at least a second, or receiving, MS) to use in locating themselves. It is recommended that validity criteria set at block 1444 for 1902-Max be fixed at one (1) in the preferred embodiment. Multiple channels for broadcast at block 2016 should be isolated to modular send processing (feeding from a queue 24).

In an alternative embodiment having multiple transmission channels visible to process 1902, there can be a worker thread 1902 per channel to handle broadcasting on multiple channels. If thread(s) 1902 (block 2016) do not transmit directly over the channel themselves, this embodiment would provide means for communicating the channel for broadcast to send processing when interfacing to queue 24 (e.g. incorporate a channel qualifier field with WDR inserted to queue 24). This embodiment could allow specification of at least one (1) worker thread per channel, however multiple worker threads configurable for process 1902 as appropriated for the number of channels configurable for broadcast.

Processing begins at block 2002, continues to block 2004 where the process worker thread count 1902-Ct is accessed and incremented by 1 (using appropriate semaphore access (e.g. 1902-Sem)), and continues to block 2006 for peeking WDR queue 22 for a special termination request entry. Block 2004 may also check the 1902-Ct value, and signal the process 1902 parent thread that all worker threads are running when 1902-Ct reaches 1902-Max. Thereafter, if block 2008 determines that a worker thread termination request was not found in queue 22, processing continues to block 2010. Block 2010 peeks the WDR queue 22 (using interface 1904) for the most recent highest confidence entry for this MS whereabouts by searching queue 22 for: the MS ID field 1100a matching the MS ID of Fig. 20 processing, and a confidence field 1100d greater than or equal to the confidence floor value, and a most recent NTP enabled date/time stamp field 1100b within a prescribed trailing period of time (e.g. preferably less than or equal to 2 seconds). For example, block 2010 peeks the queue (i.e. makes a copy for use if an entry found for subsequent processing, but does not remove the entry from queue) for a WDR of this MS (i.e. MS of Fig. 20 processing) which has the greatest confidence over 75 and has been most recently inserted to queue 22 with an NTP date/time stamp in the last 2 seconds. Date/time stamps for MS whereabouts which are not NTP derived have little use in the overall palette of process 19xx choices of architecture 1900 because

receiving data processing systems (e.g. MSs) will have no means of determining an accurate TDOA measurement in the unidirectional transmission from an NTP disabled MS. A receiving data processing system will still require a bidirectional correlated exchange with the MS of Fig. 20 processing to determine an accurate TDOA measurement in its own time scale (which is accomplished with thread(s) 1922 pulling WDR information anyway). An alternate embodiment to block 2010 will not use the NTP indicator as a search criteria so that receiving data processing systems can receive to a thread 1912, and then continue for appropriate correlation processing, or can at least maintain whereabouts to queue 22 to know who is nearby.

Thread 1902 is of less value to the LN-expanse when it broadcasts outdated/invalid whereabouts of the MS to facilitate locating other MSs. In an alternate embodiment, a movement tolerance (e.g. user configured or system set (e.g. 3 meters)) is incorporated at the MS, or at service(s) used to locate the MS, for knowing when the MS has significantly moved (e.g. more than 3 meters) and how long it has been (e.g. 45 seconds) since last significantly moving. In this embodiment, the MS is aware of the period of time since last significantly moving and the search time criteria is set using the amount of time since the MS significantly moved (whichever is greater). This way a large number of (perhaps more confident candidates) WDRs are searched in the time period when the MS has not significantly moved. Optional blocks 278 through 284 may have been incorporated to Fig. 2F for movement tolerance processing just described, in which case the LWT is compared to the current date/time of block 2010 processing to adjust block 2010 search time criteria for the correct trailing period. In any case, a WDR is sought at block 2010 which will help other MSs in the LN-expanse locate themselves, and to let other MSs know who is nearby.

Thereafter, if block 2012 determines a useful WDR was found, then block 2014 prepares the WDR for send processing, block 2016 broadcasts the WDR information (using send interface 1906) by inserting to queue 24 so that send processing broadcasts data 1302 (e.g. on all available communications interface(s) 70), for example as far as radius 1306, and processing continues to block 2018. The broadcast is for reception by data processing systems (e.g. MSs) in the vicinity. At least fields 1100b, 1100c, 1100d, and 1100n are broadcast. See Fig 11A descriptions. Fields are set to the following upon exit from block 2014:

5 *MS ID field 1100a is preferably set with:* Field 1100a from queue 22, or transformed (if not already) into a pseudo MS ID (possibly for future correlation) if desired. This field may also be set to null (not set) because it is not required when the NTP indicator of field 1100b is enabled and the broadcast is sent with an NTP enabled field 1100n.

DATE/TIME STAMP field 1100b is preferably set with: Field 1100b from queue 22.

10 *LOCATION field 1100c is preferably set with:* Field 1100c from queue 22.

CONFIDENCE field 1100d is preferably set with: Field 1100d from queue 22.

LOCATION TECHNOLOGY field 1100e is preferably set with: Field 1100e from queue 22.

15 *LOCATION REFERENCE INFO field 1100f is preferably set with:* null (not set). Null indicates to send processing feeding from queue 24 to use all available comm. interfaces 70 (i.e. Broadcast). Specifying a comm. interface targets the specified interface (i.e. send).

20 *COMMUNICATIONS REFERENCE INFO field 1100g is preferably set with:* null (not set). If MS ID (or pseudo MS ID) is sent, this is all that is required to target this MS.

SPEED field 1100h is preferably set with: Field 1100h from queue 22.

25 *HEADING field 1100i is preferably set with:* Field 1100i from queue 22.

ELEVATION field 1100j is preferably set with: Field 1100j from queue 22.

30 *APPLICATION FIELDS field 1100k is preferably set with:* Field 1100k from queue 22. An alternate embodiment will add, alter, or discard data (with or without date/time stamps) here at the time of block 2014 processing.

CORRELATION FIELD 1100m is preferably set with: null (not set).

SENT DATE/TIME STAMP field 1100n is preferably set with: Sent date/time stamp as close in processing the broadcast of block 2016 as possible.

5 *RECEIVED DATE/TIME STAMP field 1100p is preferably set with:* Not Applicable (i.e. N/A for sending).

10 Block 2018 causes thread 1902 to sleep according to the SPTP setting (e.g. a few seconds). When the sleep time has elapsed, processing continues back to block 2006 for another loop iteration of blocks 2006 through 2016. Referring back to block 2012, if a useful WDR was not found (e.g. candidates too old), then processing continues to block 2018. Referring back to block 2008, if a worker thread termination request entry was found at queue 22, then block 2020 decrements the worker thread count by 1 (using appropriate semaphore access (e.g. 1902-Sem)), and thread 1902 processing terminates at block 2022. Block 2020 may also check the 1902-Ct value, and signal the process 1902 parent thread that all worker threads are terminated when 1902-Ct equals zero (0).

15 Block 2016 causes broadcasting data 1302 containing CK 1304 wherein CK 1304 contains WDR information prepared as described above for block 2014. Alternative embodiments of block 2010 may not search a specified confidence value, and broadcast the best entry available anyway so that listeners in the vicinity will decide what to do with it. A semaphore protected data access (instead of a queue peek) may be used in embodiments where there is always one WDR current entry maintained for the MS.

20 In the embodiment wherein usual MS communications data 1302 of the MS is altered to contain CK 1304 for listening MSs in the vicinity, send processing feeding from queue 24, caused by block 2016 processing, will place WDR information as CK 1304 embedded in usual data 1302 at the next opportune time of sending usual data 1302. If an opportune time is not timely, send processing should discard the send request of block 2016 to avoid broadcasting outdated whereabouts information (unless using a movement tolerance and time since last significant movement). As the MS conducts its normal communications, transmitted data 1302 contains new data CK 1304 to be ignored by receiving MS other character 32 processing, but to be found by listening MSs within the vicinity which anticipate presence of CK 1304. Otherwise, when LN-Expanse deployments

have not introduced CK 1304 to usual data 1302 communicated on a receivable signal by MSs in the vicinity, Fig. 20 sends repeated timely pulsed broadcasts of new data 1302 (per SPTP) for MSs in the vicinity of the first MS to receive. In any case, appropriate implementation should ensure field 1100n is as accurate as possible for when data 1302 is actually sent.

An alternate embodiment to architecture 1900 for elimination of process 1902 incorporates a trigger implementation for broadcasting MS whereabouts at the best possible time – i.e. when the MS whereabouts is inserted to queue 22. As soon as a new (preferably NTP enabled) WDR candidate becomes available, it can be broadcast at a new block 279 of Fig. 2F. (e.g. new block 279 continued to from block 278 and then continuing to block 280). Fields are set as described above for Fig. 20. Preferably, the new block 279 starts an asynchronous thread consisting of blocks 2014 and 2016 so that Fig. 2F processing performance is not impacted. In a further embodiment, block 279 can be further enhanced using the SPTP value to make sure that too many broadcasts are not made. The SPTP (Source Periodicity Time Period) could be observed for getting as close as possible to broadcasting whereabouts in accordance with SPTP (e.g. worst case there are not enough broadcasts).

Fig. 21 depicts a flowchart for describing a preferred embodiment of MS whereabouts collection processing. Fig. 21 processing describes a process 1912 worker thread, and is of PIP code 6. Thread(s) 1912 purpose is for the MS of Fig. 21 processing (e.g. a second, or receiving, MS) to collect potentially useful WDR information from other MSs (e.g. at least a first, or sending, MS) in the vicinity for determining whereabouts of the receiving (second) MS. It is recommended that validity criteria set at block 1444 for 1912-Max be set as high as possible (e.g. 10) relative performance considerations of architecture 1900, with at least one thread per channel that WDR information may be received on by the receiving MS. Multiple channels for receiving data fed to queue 26 should be isolated to modular receive processing (feeding a queue 26).

In an alternative embodiment having multiple receiving transmission channels visible to process 1912 (e.g. thread(s) 1912 receiving directly), there can be a worker thread 1912 per channel to handle receiving on multiple channels simultaneously. If thread(s) 1912 do not receive directly from the channel, the preferred embodiment of Fig.

21 would not need to convey channel information to thread(s) 1912 waiting on queue 26 anyway. Embodiments could allow specification/configuration of many thread(s) 1912 per channel.

5 Processing begins at block 2102, continues to block 2104 where the process worker thread count 1912-Ct is accessed and incremented by 1 (using appropriate semaphore access (e.g. 1912-Sem)), and continues to block 2106 for interim housekeeping of pruning the WDR queue by invoking a Prune Queues procedure of Fig. 27. Block 2104 may also check the 1912-Ct value, and signal the process 1912 parent thread that all worker threads are running when 1912-Ct reaches 1912-Max. Block 2106
10 may not be required since block 2130 can cause queue 22 pruning (block 292).

Thereafter, block 2108 retrieves from queue 26 a WDR (using interface 1914), perhaps a special termination request entry, or a WDR received in data 1302 (CK 1304) or data 1312 (CK 1314), and only continues to block 2110 when a WDR has been retrieved. Block 2108 stays blocked on retrieving from queue 26 until any WDR is retrieved. If block
15 2110 determines that a special WDR indicating to terminate was not found in queue 26, processing continues to block 2112. Block 2112 adjusts date/time stamp field 1100b if necessary depending on NTP use in the LN-expanse and adjusts the confidence field 1100d accordingly. In a preferred embodiment, fields 1100b and 1100d for the WDR in process is set as follows for certain conditions:

- 20 • Fields 1100b, 1100n and 1100p all NTP indicated: keep fields 1100b and 1100d as is; or
- Fields 1100b and 1100n are NTP indicated, 1100p is not: Is correlation (field 1100m) present?: No, then set confidence (field 1100d) to 0 (for filtering out at block 2114) / Yes, then set field 1100b to 1100p (in time terms of this MS)
25 and adjust confidence lower based on differences between fields 1100b, 1100n and 1100p; or
- Fields 1100b and 1100p are NTP indicated, 1100n is not: Is correlation present?: No, then set confidence to 0 (for filtering out at block 2114) / Yes, then set field 1100b to 1100p (in time terms of this MS) and adjust
30 confidence lower based on differences between fields 1100b, 1100n and 1100p; or

- Fields 1100b NTP indicated, 1100n and 1100p not: Is correlation present?: No, then set confidence to 0 (for filtering out at block 2114) / Yes, then set field 1100b to 1100p (in time terms of this MS) and adjust confidence lower based on differences between fields 1100b, 1100n and 1100p; or
- 5 • Field 1100b not NTP indicated, 1100n and 1100p are: Is correlation present?: No, then set confidence to 0 (for filtering out at block 2114) / Yes, then set field 1100b to 1100p (in time terms of this MS) and adjust confidence lower based on differences between fields 1100b, 1100n and 1100p; or
- 10 • Fields 1100b and 1100p are not NTP indicated, 1100n is: Is correlation present?: No, then set confidence to 0 (for filtering out at block 2114) / Yes, then set field 1100b to 1100p (in time terms of this MS) and adjust confidence lower based on differences between fields 1100b, 1100n and 1100p; or
- 15 • Fields 1100b and 1100n are not NTP indicated, 1100p is: Is correlation present?: No, then set confidence to 0 (for filtering out at block 2114) / Yes, then set field 1100b to 1100p (in time terms of this MS) and adjust confidence lower based on differences between fields 1100b, 1100n and 1100p; or
- 20 • Fields 1100b, 1100n and 1100p not NTP indicated: Is correlation present?: No, then set confidence to 0 (for filtering out at block 2114) / Yes, then set field 1100b to 1100p (in time terms of this MS) and adjust confidence lower based on differences between fields 1100b, 1100n and 1100p.

25 NTP ensures maintaining a high confidence in the LN-expanse, but absence of NTP is still useful. Confidence values should be adjusted with the knowledge of the trailing time periods used for searches when sharing whereabouts (e.g. thread(s) 1942 searches). Block 2112 continues to block 2114.

30 If at block 2114, the WDR confidence field 1100d is not greater than the confidence floor value, then processing continues back to block 2106. If block 2114 determines that the WDR field 1100d is satisfactory, then block 2116 initializes a TDOA_FINAL variable to

False, and block 2118 checks if the WDR from block 2108 contains correlation (field 1100m).

If block 2118 determines the WDR does not contain correlation, then block 2120 accesses the ILMV, block 2122 determines the source (ILM or DLM) of the WDR using the originator indicator of field 1100e, and block 2124 checks suitability for collection of the WDR. While processes 19xx running are generally reflective of the ILMV roles configured, it is possible that the more descriptive nature of ILMV role(s) not be one to one in relationship to 19xx processes, in particular depending on the subset of architecture 1900 in use. Block 2124 is redundant anyway because of block 274. If block 2124 determines the ILMV role is disabled for collecting this WDR, then processing continues back to block 2106. If block 2124 determines the ILMV role is enabled for collecting this WDR, then processing continues to block 2126.

If block 2126 determines both the first (sending) and second (receiving) MS are NTP enabled (i.e. Fields 1100b, 1100n and 1100p are NTP indicated) OR if TDOA_FINAL is set to True (as arrived to via block 2150), then block 2128 completes the WDR for queue 22 insertion, block 2130 prepares parameters for Fig. 2F processing and block 2132 invokes Fig. 2F processing (interface 1916). Parameters set at block 2130 are: WDRREF = a reference or pointer to the WDR completed at block 2128; DELETEQ = Fig. 21 location queue discard processing; and SUPER = Fig. 21 supervisory notification processing. Block 2128 calculates a TDOA measurement whenever possible and inserts to field 1100f. See Fig 11A descriptions. Fields are set to the following upon exit from block 2128:

MS ID field 1100a is preferably set with: Field 1100a from queue 26.

DATE/TIME STAMP field 1100b is preferably set with: Preferred embodiment discussed for block 2112.

LOCATION field 1100c is preferably set with: Field 1100c from queue 26.

CONFIDENCE field 1100d is preferably set with: Confidence at equal to or less than field 1100d received from queue 26 (see preferred embodiment for block 2112).

LOCATION TECHNOLOGY field 1100e is preferably set with: Field 1100e from queue 26.

5 *LOCATION REFERENCE INFO field 1100f is preferably set with:* All available measurements from receive processing (e.g. AOA, heading, yaw, pitch, roll, signal strength, wave spectrum, particular communications interface 70, etc), and TDOA measurement(s) as determined in Fig. 21 (blocks 2128 and 2148).

10 *COMMUNICATIONS REFERENCE INFO field 1100g is preferably set with:* Field 1100g from queue 26.

SPEED field 1100h is preferably set with: Field 1100h from queue 26.

15 *HEADING field 1100i is preferably set with:* Field 1100i from queue 26.

ELEVATION field 1100j is preferably set with: Field 1100j from queue 26.

20 *APPLICATION FIELDS field 1100k is preferably set with:* Field 1100k from queue 26. An alternate embodiment will add, alter, or discard data (with or without date/time stamps) here at the time of block 2128 processing.

CORRELATION FIELD 1100m is preferably set with: Not Applicable (i.e. not maintained to queue 22). Was used by Fig. 21 processing.

25 *SENT DATE/TIME STAMP field 1100n is preferably set with:* Not Applicable (i.e. not maintained to queue 22). Was used by Fig. 21 processing.

30 *RECEIVED DATE/TIME STAMP field 1100p is preferably set with:* Not Applicable (i.e. not maintained to queue 22). Was used by Fig. 21 processing.

Block 2132 continues to block 2134 where a record 2400 is built (i.e. field 2400a = 1952 and field 2400b is set to null (e.g. -1)) and then block 2136 inserts the record 2400 to

TR queue 1980 (using interface 1918) so that a thread 1952 will perform processing. Blocks 2134 and 2136 may be replaced with an alternative embodiment for starting a thread 1952. Block 2136 continues back to block 2106.

5 Referring now back to block 2126, if it is determined that a TDOA measurement cannot be made (i.e. (field 1100n or 1100p not NTP indicated) OR if TDOA_FINAL is set to False), then block 2138 checks if the WDR contains a MS ID (or pseudo MS ID). If block 2138 determines there is none, then processing continues back to block 2106 because there is no way to distinguish one MS from another with respect to the WDR retrieved at block 2108 for directing bidirectional correlation. An alternate embodiment will use a provided correlation field 1100m received at block 2108, instead of a field 1100a, for 10 knowing how to target the originating MS for TDOA measurement processing initiated by a thread 1932. If block 2138 determines there is a usable MS ID (or correlation field), then block 2140 builds a record 2400 (field 2400a = 1932, field 2400b = the MS ID (or pseudo MS ID, or correlation) and particular communications interface from field 1100f (if 15 available) of the WDR of block 2108, and block 2142 inserts the record 2400 to queue 1980 (interface 1918) for starting a thread 1932. Block 2142 continues back to block 2106. An alternate embodiment causes block 2126 to continue directly to block 2140 (no block 2138) for a No condition from block 2126. Regardless of whether the originating MS ID can be targeted, a correlation (in lieu of an MS ID) may be used when the MS responds with a broadcast. The WDR request made by thread 1932 can be a broadcast rather than 20 a targeted request. Thread(s) 1932 can handle sending targeted WDR requests (to a known MS ID) and broadcast WDR requests.

Referring back to block 2118, if it is determined the WDR does contain correlation (field 1100m), block 2144 peeks the CR queue 1990 (using interface 1920) for a record 25 2450 containing a match (i.e. field 1100m matched to field 2450b). Thereafter, if block 2146 determines no correlation was found on queue 1990 (e.g. response took too long and entry was pruned), then processing continues to block 2120 already described. If block 2146 determines the correlation entry was found (i.e. thread 1912 received a response from an earlier request (e.g. from a thread 1922 or 1932), then block 2148 uses 30 date/time stamp field 2450a (from block 2144) with field 1100p (e.g. from block 2108) to calculate a TDOA measurement in time scale of the MS of Fig. 21 processing, and sets field 1100f appropriately in the WDR. Note that correlation field 2450b is valid across all

available MS communications interfaces (e.g. all supported active wave spectrums). The TDOA measurement considers duration of time between the earlier sent date/time of record 2450 and the later time of received date/time field 1100p. The TDOA measurement may further be altered at block 2148 processing time to a distance knowing the velocity of the wave spectrum used as received to queue 26. Block 2148 continues to block 2150 where the TDOA_FINAL variable is set to True, then to block 2120 for processing already described.

Referring back to block 2110, if a WDR for a worker thread termination request was found at queue 26, then block 2152 decrements the worker thread count by 1 (using appropriate semaphore access (e.g. 1912-Sem)), and thread 1912 processing terminates at block 2154. Block 2152 may also check the 1912-Ct value, and signal the process 1912 parent thread that all worker threads are terminated when 1912-Ct equals zero (0).

In the embodiment wherein usual MS communications data 1302 of the MS is altered to contain CK 1304 or 1314 for listening MSs in the vicinity, receive processing feeding queue 26 will place WDR information to queue 26 as CK 1304 or 1314 is detected for being present in usual communication data 1302 or 1304. As normal communications are conducted, transmitted data 1302 or 1312 contains new data CK 1304 or 1314 to be ignored by receiving MS other character 32 processing, but to be found by listening MSs within the vicinity which anticipate presence of CK 1304 or 1314. Otherwise, when LN-Expanse deployments have not introduced CK 1304 (or 1314) to usual data 1302 (or 1312) communicated on a receivable signal by MSs in the vicinity, Fig. 21 receives new data 1302 (or 1312) sent. In any case, field 1100p should be as accurate as possible for when data 1302 (or 1312) was actually received. Critical regions of code and/or anticipated execution timing may be used to affect a best setting of field 1100p.

So, Fig. 21 is responsible for maintaining whereabouts of others to queue 22 with data useful for triangulating itself.

Fig. 22 depicts a flowchart for describing a preferred embodiment of MS whereabouts supervisor processing, for example to ensure the MS of Fig. 22 processing (e.g. first MS) is maintaining timely whereabouts information for itself. Fig. 22 processing describes a process 1922 worker thread, and is of PIP code 6. Thread(s) 1922 purpose is for the MS of Fig. 22 processing (e.g. a first, or sending, MS), after determining its

whereabouts are stale, to periodically transmit requests for whereabouts information from MSs in the vicinity (e.g. from at least a second, or receiving, MS), and/or to start a thread 1952 for immediately determining whereabouts. Alternative embodiments to Fig. 22 will implement processing of blocks 2218 through 2224, or processing of blocks 2226 through 2228, or both as depicted in Fig. 22. It is recommended that validity criteria set at block 1444 for 1922-Max be fixed at one (1) in the preferred embodiment. Multiple channels for broadcast at block 2224 should be isolated to modular send processing feeding from a queue 24.

In an alternative embodiment having multiple transmission channels visible to process 1922, there can be a worker thread 1922 per channel to handle broadcasting on multiple channels. If thread(s) 1922 (block 2224) do not transmit directly over the channel, this embodiment would provide means for communicating the channel for broadcast to send processing when interfacing to queue 24 (e.g. incorporate a channel qualifier field with WDR request inserted to queue 24). This embodiment could allow specification of one (1) thread per channel, however multiple worker threads configurable for process 1922 as determined by the number of channels configurable for broadcast.

Processing begins at block 2202, continues to block 2204 where the process worker thread count 1922-Ct is accessed and incremented by 1 (using appropriate semaphore access (e.g. 1922-Sem)), and continues to block 2206 for interim housekeeping of pruning the CR queue by invoking a Prune Queues procedure of Fig. 27. Block 2204 may also check the 1922-Ct value, and signal the process 1922 parent thread that all worker threads are running when 1922-Ct reaches 1922-Max. Block 2206 continues to block 2208 for peeking WDR queue 22 (using interface 1924) for a special termination request entry. Thereafter, if block 2210 determines that a worker thread termination request was not found in queue 22, processing continues to block 2212. Block 2212 peeks the WDR queue 22 (using interface 1924) for the most recent highest confidence entry for this MS whereabouts by searching queue 22 for: the MS ID field 1100a matching the MS ID of Fig. 22 processing, and a confidence field 1100d greater than or equal to the confidence floor value, and a most recent date/time stamp field 1100b within a prescribed trailing period of time of block 2212 search processing using a function of the WTV (i.e. $f(WTV)$ = short-hand for "function of WTV") for the period. For example, block 2212 peeks the queue (i.e. makes a copy for use if an entry found for subsequent

processing, but does not remove the entry from queue) for a WDR of the first MS which has the greatest confidence over 75 and has been most recently inserted to queue 22 in the last 3 seconds. Since the MS whereabouts accuracy may be dependent on timeliness of the WTV, it is recommended that the $f(WTV)$ be some value less than or equal to WTV, but preferably not greater than the WTV. Thread 1922 is of less value to the MS when not making sure in a timely manner the MS is maintaining timely whereabouts for itself. In an alternate embodiment, a movement tolerance (e.g. user configured or system set (e.g. 3 meters)) is incorporated at the MS, or at service(s) used to locate the MS, for knowing when the MS has significantly moved (e.g. more than 3 meters) and how long it has been (e.g. 45 seconds) since last significantly moving. In this embodiment, the MS is aware of the period of time since last significantly moving and the $f(WTV)$ is set using the amount of time since the MS significantly moved (i.e. $f(WTV)$ = as described above, or the amount of time since significantly moving, whichever is greater). This way a large number of (perhaps more confident candidates) WDRs are searched in the time period when the MS has not significantly moved. Optional blocks 278 through 284 may have been incorporated to Fig. 2F for movement tolerance processing just described, in which case the LWT is compared to the current date/time to adjust the WTV for the correct trailing period. In any case, a WDR is sought at block 2212 which will verify whether or not MS whereabouts are current.

Thereafter, if block 2214 determines a satisfactory WDR was found, then processing continues to block 2216. Block 2216 causes thread 1922 to sleep according to a $f(WTV)$ (preferably a value less than or equal to the WTV (e.g. 95% of WTV)). When the sleep time has elapsed, processing continues back to block 2206 for another loop iteration of blocks 2206 through 2214.

If block 2214 determines a current WDR was not found, then block 2218 builds a WDR request (e.g. containing record 2490 with field 2490a for the MS of Fig. 22 processing (MS ID or pseudo MS ID) so receiving MSs in the LN-expanse know who to respond to, and field 2490b with appropriate correlation for response), block 2220 builds a record 2450 (using correlation generated for the request at block 2218), block 2222 inserts the record 2450 to queue 1990 (using interface 1928), and block 2224 broadcasts the WDR request (record 2490) for responses. Absence of field 2490d indicates to send processing feeding from queue 24 to broadcast on all available comm. interfaces 70.

With reference now to Fig. 24C, depicted is an illustration for describing a preferred embodiment of a WDR request record, as communicated to queue 24 or 26. When a LN-expanse globally uses NTP, as found in thread 19xx processing described for architecture 1900, a WDR request record 2490 may, or may not, be required. TDOA calculations can be made using a single unidirectional data (1302 or 1312) packet containing a sent date/time stamp (of when the data was sent) as described above.

Records 2490 contain a MS ID field 2490a and correlation field 2490b. MS ID field 2490a contains an MS ID (e.g. a value of field 1100a). An alternate embodiment will contain a pseudo MS ID (for correlation), perhaps made by a derivative of the MS ID with a unique (suffix) portion, so that receiving MSs can directly address the MS sending the request without actually knowing the MS ID (i.e. they know the pseudo MS ID which enables the MS to recognize originated transmissions). Correlation data field 2490b contains unique correlation data (e.g. MS id with suffix of unique number) used to provide correlation for matching sent requests (data 1302) with received WDR responses (data 1302 or 1312). Upon a correlation match, a TDOA measurement is calculated using the time difference between field 2450a and a date/time stamp of when the response was received (e.g. field 1100p). Received date/time stamp field 2490c is added by receive processing feeding queue 26 when an MS received the request from another MS. Comm interface field 2490d is added by receive processing inserting to queue 26 for how to respond and target the originator. Many MSs do not have choices of communications interfaces, so field 2490d may not be required. If available it is used, otherwise a response can be a broadcast. Field 2490d may contain a wave spectrum identifier for uniquely identifying how to respond (e.g. one to one with communications interface), or any other value for indicating how to send given how the request was received.

With reference back to Fig. 22, block 2218 builds a request that receiving MSs will know is for soliciting a response with WDR information. Block 2218 generates correlation for field 2450b to be returned in responses to the WDR request broadcast at block 2224. Block 2220 also sets field 2450a to when the request was sent. Preferably, field 2450a is set as close to the broadcast as possible. In an alternative embodiment, broadcast processing feeding from queue 24 makes the record 2450 and inserts it to queue 1990

with a most accurate time of when the request was actually sent. Fields 2450a are to be as accurate as possible. Block 2224 broadcasts the WDR request data 1302 (using send interface 1926) by inserting to queue 24 so that send processing broadcasts data 1302, for example as far as radius 1306. Broadcasting preferably uses all available communications interface(s) 70 (e.g. all available wave spectrums). Therefore, the comm interface field 2490d is not set (which implies to send processing to do a broadcast).

Block 2224 continues to block 2226 where a record 2400 is built (i.e. field 2400a = 1952 and field 2400b is set to null (e.g. -1)) and then block 2228 inserts the record 2400 to TR queue 1980 (using interface 1930) so that a thread 1952 will perform processing. Blocks 2226 and 2228 may be replaced with an alternative embodiment for starting a thread 1952. Block 2228 continues back to block 2216.

Referring back to block 2210, if a worker thread termination request entry was found at queue 22, then block 2230 decrements the worker thread count by 1 (using appropriate semaphore access (e.g. 1922-Sem)), and thread 1922 processing terminates at block 2232. Block 2230 may also check the 1922-Ct value, and signal the process 1922 parent thread that all worker threads are terminated when 1922-Ct equals zero (0).

In the embodiment wherein usual MS communications data 1302 of the MS is altered to contain CK 1304 for listening MSs in the vicinity, send processing feeding from queue 24, caused by block 2224 processing, will place the request as CK 1304 embedded in usual data 1302 at the next opportune time of sending usual data 1302. This may require the alternative embodiment of adding the entry to queue 1990 being part of send processing. As the MS conducts its normal communications, transmitted data 1302 contains new data CK 1304 to be ignored by receiving MS other character 32 processing, but to be found by listening MSs within the vicinity which anticipate presence of CK 1304. Otherwise, when LN-Expanse deployments have not introduced CK 1304 to usual data 1302 communicated on a receivable signal by MSs in the vicinity, Fig. 22 sends new WDR request data 1302.

Fig. 23 depicts a flowchart for describing a preferred embodiment of MS timing determination processing. Fig. 23 processing describes a process 1932 worker thread, and is of PIP code 6. Thread(s) 1932 purpose is for the MS of Fig. 23 processing to determine TDOA measurements when needed for WDR information received. It is

recommended that validity criteria set at block 1444 for 1932-Max be set as high as possible (e.g. 12) relative performance considerations of architecture 1900, to service multiple threads 1912.

Processing begins at block 2302, continues to block 2304 where the process worker thread count 1932-Ct is accessed and incremented by 1 (using appropriate semaphore access (e.g. 1932-Sem)), and continues to block 2306 for interim housekeeping of pruning the CR queue by invoking a Prune Queues procedure of Fig. 27. Block 2304 may also check the 1932-Ct value, and signal the process 1932 parent thread that all worker threads are running when 1932-Ct reaches 1932-Max.

Thereafter, block 2308 retrieves from queue 1980 a record 2400 (using interface 1934), perhaps a special termination request entry, or a record 2400 received from thread(s) 1912, and only continues to block 2310 when a record 2400 containing field 2400a set to 1932 has been retrieved. Block 2308 stays blocked on retrieving from queue 1980 until a record 2400 with field 2400a = 1932 is retrieved. If block 2310 determines a special entry indicating to terminate was not found in queue 1980, processing continues to block 2312.

If at block 2312, the record 2400 does not contain a MS ID (or pseudo MS ID) in field 2400b, processing continues to block 2314 for building a WDR request (record 2490) to be broadcast, and then to block 2318. Broadcasting preferably uses all available communications interface(s) 70 (e.g. all available wave spectrums). If block 2312 determines the field 2400b is a valid MS ID (not null), block 2316 builds a WDR request targeted for the MS ID, and processing continues to block 2318. A targeted request is built for targeting the MS ID (and communications interface, if available) from field 2400b. Send processing is told which communications interface to use, if available (e.g. MS has multiple), otherwise send processing will target each available interface. In the unlikely case a MS ID is present in field 2400b without the communications interface applicable, then all communications interfaces 70 are used with the targeted MS ID. In MS embodiments with multiple communications interfaces 70, then 2400b is to contain the applicable communication interface for sending. Block 2318 generates appropriate correlation for a field 2450b (e.g. to be compared with a response WDR at block 2144), block 2320 sets field 2450a to the current MS date/time stamp, block 2322 inserts the record 2450 to queue 1990 (using interface 1936), and block 2324 sends/broadcasts

(using interface 1938) a WDR request (record 2490). Thereafter, processing continues back to block 2306 for another loop iteration. An alternative embodiment will only target a WDR request to a known MS ID. For example, block 2312 would continue back to block 2306 if no MS ID is found (= null), otherwise it will continue to block 2316 (i.e. no use for block 2314).

Block 2318 sets field 2450b to correlation to be returned in responses to the WDR request sent/broadcast at block 2324. Block 2320 sets field 2450a to when the request is sent. Preferably, field 2450a is set as close as possible to when a send occurred. In an alternative embodiment, send processing feeding from queue 24 makes the record 2450 and inserts it to queue 1990 with a most accurate time of when the request was actually sent. Fields 2450a are to be as accurate as possible. Block 2324 sends/broadcasts the WDR request data 1302 (using send interface 1938) by inserting to queue 24 a record 2490 (2490a = the targeted MS ID (or pseudo MS ID) OR null if arrived to from block 2314, field 2490b = correlation generated at block 2318) so that send processing sends data 1302, for example as far as radius 1306. A null MS ID may be responded to by all MSs in the vicinity. A non-null MS ID is to be responded to by a particular MS. Presence of field 2490d indicates to send processing feeding from queue 24 to target the MS ID over the specified comm. interface (e.g. when MS has a plurality of comm. interfaces 70 (e.g. cellular, Wifi, Bluetooth, etc; i.e. MS supports multiple classes of wave spectrum)).

Referring back to block 2310, if a worker thread termination request was found at queue 1980, then block 2326 decrements the worker thread count by 1 (using appropriate semaphore access (e.g. 1932-Sem)), and thread 1932 processing terminates at block 2328. Block 2326 may also check the 1932-Ct value, and signal the process 1932 parent thread that all worker threads are terminated when 1932-Ct equals zero (0).

In the embodiment wherein usual MS communications data 1302 of the MS is altered to contain CK 1304 for listening MSs in the vicinity, send processing feeding from queue 24, caused by block 2324 processing, will place the WDR request as CK 1304 embedded in usual data 1302 at the next opportune time of sending usual data 1302. As the MS conducts its normal communications, transmitted data 1302 contains new data CK 1304 to be ignored by receiving MS other character 32 processing, but to be found by listening MSs within the vicinity which anticipate presence of CK 1304. This may require the alternative embodiment of adding the entry to queue 1990 being part of send

processing. Otherwise, when LN-Expanse deployments have not introduced CK 1304 to usual data 1302 communicated on a receivable signal by MSs in the vicinity, Fig. 22 sends/broadcasts new WDR request data 1302.

5 An alternate embodiment to block 2324 can wait for a response with a reasonable timeout, thereby eliminating the need for blocks 2318 through 2322 which is used to correlate the subsequent response (to thread 1912) with the request sent at block 2324. However, this will cause a potentially unpredictable number of simultaneously executing thread(s) 1932 when many MSs are in the vicinity.

10 Thread(s) 1932 are useful when one or both parties to WDR transmission (sending and receiving MS) do not have NTP enabled. TDOA measurements are taken to triangulate the MS relative other MSs in real time.

15 Fig. 25 depicts a flowchart for describing a preferred embodiment of MS WDR request processing, for example when a remote MS requests (e.g. from Figs. 22 or 23) a WDR. Receive processing identifies targeted requests destined (e.g. Fig. 23) for the MS of Fig. 25 processing, and identifies general broadcasts (e.g. Fig. 22) for processing as well. Fig. 25 processing describes a process 1942 worker thread, and is of PIP code 6. Thread(s) 1942 purpose is for the MS of Fig. 25 processing to respond to incoming WDR requests. It is recommended that validity criteria set at block 1444 for 1942-Max be set as high as possible (e.g. 10) relative performance considerations of architecture 1900, to 20 service multiple WDR requests simultaneously. Multiple channels for receiving data fed to queue 26 should be isolated to modular receive processing.

25 In an alternative embodiment having multiple receiving transmission channels visible to process 1942, there can be a worker thread 1942 per channel to handle receiving on multiple channels simultaneously. If thread(s) 1942 do not receive directly from the channel, the preferred embodiment of Fig. 25 would not need to convey channel information to thread(s) 1942 waiting on queue 24 anyway. Embodiments could allow specification/configuration of many thread(s) 1942 per channel.

30 Processing begins at block 2502, continues to block 2504 where the process worker thread count 1942-Ct is accessed and incremented by 1 (using appropriate semaphore access (e.g. 1942-Sem)), and continues to block 2506 for retrieving from queue 26 a record 2490 (using interface 1948), perhaps a special termination request

entry, and only continues to block 2508 when a record 2490 is retrieved. Block 2506 stays blocked on retrieving from queue 26 until any record 2490 is retrieved. If block 2508 determines a special entry indicating to terminate was not found in queue 26, processing continues to block 2510. There are various embodiments for thread(s) 1912 and thread(s) 1942 to feed off a queue 26 for different record types, for example, separate queues 26A and 26B, or a thread target field with either record found at queue 26 (e.g. like field 2400a). In another embodiment, thread(s) 1912 are modified with logic of thread(s) 1942 to handle all records described for a queue 26, since thread(s) 1912 are listening for queue 26 data anyway.

Block 2510 peeks the WDR queue 22 (using interface 1944) for the most recent highest confidence entry for this MS whereabouts by searching queue 22 for: the MS ID field 1100a matching the MS ID of Fig. 25 processing, and a confidence field 1100d greater than or equal to the confidence floor value, and a most recent date/time stamp field 1100b within a prescribed trailing period of time of block 2510 search processing (e.g. 2 seconds). For example, block 2510 peeks the queue (i.e. makes a copy for use if an entry found for subsequent processing, but does not remove the entry from queue) for a WDR of the MS (of Fig. 25 processing) which has the greatest confidence over 75 and has been most recently inserted to queue 22 in the last 2 seconds. It is recommended that the trailing period of time used by block 2510 be never greater than a few seconds. Thread 1942 is of less value to the LN-expanse when it responds with outdated/invalid whereabouts of the MS to facilitate locating other MSs. In an alternate embodiment, a movement tolerance (e.g. user configured or system set (e.g. 3 meters)) is incorporated at the MS, or at service(s) used to locate the MS, for knowing when the MS has significantly moved (e.g. more than 3 meters) and how long it has been (e.g. 45 seconds) since last significantly moving. In this embodiment, the MS is aware of the period of time since last significantly moving and the trailing period of time used by block 2510 is set using the amount of time since the MS significantly moved, or the amount of time since significantly moving, whichever is greater. This way a large number of (perhaps more confident candidate) WDRs are searched in the time period when the MS has not significantly moved. Optional blocks 278 through 284 may have been incorporated to Fig. 2F for movement tolerance processing just described, in which case the LWT is compared to the current date/time to adjust the trailing period of time used by block 2510 for the correct

trailing period. In any case, a WDR is sought at block 2510 to satisfy a request helping another MS in the LN-expanse locate itself.

5 Thereafter, if block 2512 determines a useful WDR was not found, then processing continues back to block 2506 for another loop iteration of processing an inbound WDR request. If block 2512 determines a useful WDR was found, then block 2514 prepares the WDR for send processing with correlation field 1100m set from correlation field 2490b retrieved at block 2506, and block 2516 sends/broadcasts (per field 2490a) the WDR information (using send interface 1946) by inserting to queue 24 so that send processing transmits data 1302, for example as far as radius 1306, and processing continues back to
10 block 2506. At least fields 1100b, 1100c, 1100d, 1100m and 1100n are sent/broadcast. See Fig 11A descriptions. Fields are set to the following upon exit from block 2514:

MS ID field 1100a is preferably set with: Field 2490a from queue 26.

15 *DATE/TIME STAMP field 1100b is preferably set with:* Field 1100b from queue 22.

LOCATION field 1100c is preferably set with: Field 1100c from queue 22.

20 *CONFIDENCE field 1100d is preferably set with:* Field 1100d from queue 22.

LOCATION TECHNOLOGY field 1100e is preferably set with: Field 1100e from queue 22.

LOCATION REFERENCE INFO field 1100f is preferably set with: null (not set) for Broadcast by send processing, otherwise set to field 2490d for Send by send processing.

25 *COMMUNICATIONS REFERENCE INFO field 1100g is preferably set with:* null (not set).

SPEED field 1100h is preferably set with: Field 1100h from queue 22.

30 *HEADING field 1100i is preferably set with:* Field 1100i from queue 22.

ELEVATION field 1100j is preferably set with: Field 1100j from queue 22.

APPLICATION FIELDS field 1100k is preferably set with: Field 1100k from queue 22. An alternate embodiment will add, alter, or discard data (with or without date/time stamps) here at the time of block 2514 processing.

5

CORRELATION FIELD 1100m is preferably set with: Field 2490b from queue 26.

SENT DATE/TIME STAMP field 1100n is preferably set with: Sent date/time stamp as close in processing the send/broadcast of block 2516 as possible.

10

RECEIVED DATE/TIME STAMP field 1100p is preferably set with: Not Applicable (i.e. N/A for sending).

Embodiments may rely completely on the correlation field 2490b with no need for field 2490a. Referring back to block 2508, if a worker thread termination request was found at queue 26, then block 2518 decrements the worker thread count by 1 (using appropriate semaphore access (e.g. 1942-Sem)), and thread 1942 processing terminates at block 2520. Block 2518 may also check the 1942-Ct value, and signal the process 1942 parent thread that all worker threads are terminated when 1942-Ct equals zero (0).

Block 2516 causes sending/broadcasting data 1302 containing CK 1304, depending on the type of MS, wherein CK 1304 contains WDR information prepared as described above for block 2514. Alternative embodiments of block 2510 may not search a specified confidence value, and broadcast the best entry available anyway so that listeners in the vicinity will decide what to do with it. A semaphore protected data access (instead of a queue peek) may be used in embodiments where there is always one WDR current entry maintained for the MS.

In the embodiment wherein usual MS communications data 1302 of the MS is altered to contain CK 1304 for listening MSs in the vicinity, send processing feeding from queue 24, caused by block 2516 processing, will place WDR information as CK 1304 embedded in usual data 1302 at the next opportune time of sending usual data 1302. If an opportune time is not timely, send processing should discard the send request of block 2516 to avoid broadcasting outdated whereabouts information (unless using a movement

30

tolerance and time since last significant movement). As the MS conducts its normal communications, transmitted data 1302 contains new data CK 1304 to be ignored by receiving MS other character 32 processing, but to be found by listening MSs within the vicinity which anticipate presence of CK 1304. Otherwise, when LN-Expanse deployments have not introduced CK 1304 to usual data 1302 communicated on a receivable signal by MSs in the vicinity, Fig. 25 sends/broadcasts new WDR response data 1302. In any case, field 1100n should be as accurate as possible for when data 1302 is actually sent. Critical regions of code (i.e. prevent thread preemption) and/or anticipated execution timing may be used to affect a best setting of field 1100n.

In an alternate embodiment, records 2490 contain a sent date/time stamp field 2490e of when the request was sent by a remote MS, and the received date/time stamp field 2490c is processed at the MS in Fig. 25 processing. This would enable block 2514 to calculate a TDOA measurement for returning in field 1100f of the WDR sent/broadcast at block 2516.

Fig. 26A depicts a flowchart for describing a preferred embodiment of MS whereabouts determination processing. Fig. 26A processing describes a process 1952 worker thread, and is of PIP code 6. Thread(s) 1952 purpose is for the MS of Fig. 26A processing to determine its own whereabouts with useful WDRs from other MSs. It is recommended that validity criteria set at block 1444 for 1952-Max be set as high as possible (e.g. 10) relative performance considerations of architecture 1900, to service multiple threads 1912. 1952-Max may also be set depending on what DLM capability exists for the MS of Fig. 26A processing. In an alternate embodiment, thread(s) 19xx are automatically throttled up or down (e.g. 1952-Max) per unique requirements of the MS as it travels.

Processing begins at block 2602, continues to block 2604 where the process worker thread count 1952-Ct is accessed and incremented by 1 (using appropriate semaphore access (e.g. 1952-Sem)), and continues to block 2606 for interim housekeeping of pruning the WDR queue by invoking a Prune Queues procedure of Fig. 27. Block 2604 may also check the 1952-Ct value, and signal the process 1952 parent thread that all worker threads are running when 1952-Ct reaches 1952-Max. Block 2606

may not be necessary since pruning may be accomplished at block 2620 when invoking Fig. 2F (block 292).

Thereafter, block 2608 retrieves from queue 1980 a record 2400 (using interface 1958), perhaps a special termination request entry, or a record 2400 received from thread(s) 1912, and only continues to block 2610 when a record 2400 containing field 2400a set to 1952 has been retrieved. Block 2608 stays blocked on retrieving from queue 1980 until a record 2400 with field 2400a = 1952 is retrieved. If block 2610 determines a special entry indicating to terminate was not found in queue 1980, processing continues to block 2612.

Block 2612 peeks the WDR queue 22 (using interface 1954) for the most recent highest confidence entry for this MS whereabouts by searching queue 22 for: the MS ID field 1100a matching the MS ID of Fig. 26A processing, and a confidence field 1100d greater than or equal to the confidence floor value, and a most recent date/time stamp field 1100b within a prescribed trailing period of time of block 2612 search processing using a $f(WTV)$ for the period. For example, block 2612 peeks the queue (i.e. makes a copy for use if an entry found for subsequent processing, but does not remove the entry from queue) for a WDR of the MS (of Fig. 26A processing) which has the greatest confidence over 75 and has been most recently inserted to queue 22 in the last 2 seconds. Since MS whereabouts accuracy may be dependent on timeliness of the WTV, it is recommended that the $f(WTV)$ be some value less than or equal to WTV. In an alternate embodiment, a movement tolerance (e.g. user configured or system set (e.g. 3 meters)) is incorporated at the MS, or at service(s) used to locate the MS, for knowing when the MS has significantly moved (e.g. more than 3 meters) and how long it has been (e.g. 45 seconds) since last significantly moving. In this embodiment, the MS is aware of the period of time since last significantly moving and the $f(WTV)$ is set using the amount of time since the MS significantly moved (i.e. $f(WTV)$ = as described above, or the amount of time since significantly moving, whichever is greater). This way a large number of (perhaps more confident candidate) WDRs are searched in the time period when the MS has not significantly moved. Optional blocks 278 through 284 may have been incorporated to Fig. 2F for movement tolerance processing just described, in which case the LWT is compared to the current date/time to adjust the WTV for the correct trailing period.

5 Thereafter, if block 2614 determines a timely whereabouts for this MS already exists to queue 22 (current WDR found), then processing continues back to block 2606 for another loop iteration of processing. If 2614 determines a satisfactory WDR does not already exist in queue 22, then block 2600 determines a new highest confidence WDR for this MS (Fig. 26B processing) using queue 22.

10 Thereafter, if block 2616 determines a WDR was not created (BESTWDR variable = null) for the MS of Fig. 26A processing (by block 2600), then processing continues back to block 2606. If block 2616 determines a WDR was created (BESTWDR = WDR created by Fig. 26B) for the MS of Fig. 26A processing by block 2600, then processing continues to block 2618 for preparing Fig. 2F parameters and Fig. 2F processing is invoked with the new WDR at block 2620 (for interface 1956) before continuing back to block 2606. Parameters set at block 2618 are: WDRREF = a reference or pointer to the WDR completed at block 2600; DELETEQ = Fig. 26A location queue discard processing; and SUPER = Fig. 26A supervisory notification processing.

15 Referring back to block 2610, if a worker thread termination request was found at queue 1980, then block 2622 decrements the worker thread count by 1 (using appropriate semaphore access (e.g. 1952-Sem)), and thread 1952 processing terminates at block 2624. Block 2622 may also check the 1952-Ct value, and signal the process 1952 parent thread that all worker threads are terminated when 1952-Ct equals zero (0).

20 Alternate embodiments to Fig. 26A will have a pool of thread(s) 1952 per location technology (WDR field 1100e) for specific WDR field(s) selective processing. Fig. 26A processing is shown to be generic with handling all WDRs at block 2600.

25 Fig. 26B depicts a flowchart for describing a preferred embodiment of processing for determining a highest possible confidence whereabouts, for example in ILM processing, such as processing of Fig. 26A block 2600. Processing starts at block 2630, and continues to block 2632 where variables are initialized (BESTWDR = null, THIS_MS = null, REMOTE_MS = null). BESTWDR will reference the highest confidence WDR for whereabouts of the MS of Fig. 26B processing (i.e. this MS) upon return to Fig. 26A when whereabouts determination is successful, otherwise BESTWDR is set to null (none found). THIS_MS points to an appropriately sorted list of WDRs which were originated by this MS and are DLM originated (i.e. inserted by the DLM of Fig. 26B processing). REMOTE_MS

points to an appropriately sorted list of WDRs which were originated by other MSs (i.e. from DLMs and/or ILMs and collected by the ILM of Fig. 26B processing).

5 Thereafter, block 2634 peeks the WDR queue 22 (using interface 1954) for most recent WDRs by searching queue 22 for: confidence field 1100d greater than or equal to the confidence floor value, and a most recent date/time stamp field 1100b within a prescribed trailing period of time of block 2634 search processing using a f(WTV) for the period. For example, block 2634 peeks the queue (i.e. makes a copy of all WDRs to a result list for use if any found for subsequent processing, but does not remove the entry(s) from queue) for all WDRs which have confidence over 75 and has been most recently
10 inserted to queue 22 in the last 2 seconds. It is recommended that the f(WTV) used here be some value less than or equal to the WTV (want to be ahead of curve, so may use a percentage (e.g. 90%)), but preferably not greater than a couple/few seconds (depends on MS, MS applications, MS environment, whereabouts determination related variables, etc).

15 In an alternative embodiment, thread(s) 1952 coordinate with each other to know successes, failures or progress of their sister threads for automatically adjusting the trailing f(WTV) period of time appropriately. See "Alternative IPC Embodiments" below.

20 Thread 1952 is of less value to the MS when whereabouts are calculated using stale WDRs, or when not enough useful WDRs are considered. In an alternate embodiment, a movement tolerance (e.g. user configured or system set (e.g. 3 meters)) is incorporated at the MS, or at service(s) used to locate the MS, for knowing when the MS has significantly moved (e.g. more than 3 meters) and how long it has been (e.g. 45 seconds) since last significantly moving. In this embodiment, the MS is aware of the period of time since last significantly moving and the f(WTV) is set using the amount of time since the MS significantly moved (i.e. f(WTV) = as described above, or the amount of
25 time since significantly moving, whichever is greater). This way a large number of (perhaps more confident candidates) WDRs are searched in the time period when the MS has not significantly moved. Optional blocks 278 through 284 may have been incorporated to Fig. 2F for movement tolerance processing just described, in which case the LWT is compared to the current date/time to adjust the WTV for the correct trailing period. In any
30 case, all useful WDRs are sought at block 2634 and placed into a list upon exit from block 2634.

5 Thereafter, block 2636 sets THIS_MS list and REMOTE_MS list sort keys to be used at blocks 2644 and 2654. Blocks 2638 through 2654 will prioritize WDRs found at block 2634 depending on the sort keys made at block 2636. A number of variables may be used to determine the best sort keys, such as the time period used to peek at block 2634 and/or the number of entries in the WDR list returned by block 2634, and/or other variables. When the time period of search is small (e.g. less than a couple seconds), lists (THIS_MS and REMOTE_MS) should be prioritized primarily by confidence (fields 1100d) since any WDRs are valuable for determining whereabouts. This is the preferred embodiment.

10 When the time period is great, careful measure must be taken to ensure stale WDRs are not used (e.g. > few seconds, and not considering movement tolerance). Depending on decision embodiments, there will be preferred priority order sort keys created at exit from block 2636, for example “key1/key2/key3” implies that “key1” is a primary key, “key2” is a second order key, and “key3” is a third order key. A key such as
15 “field-1100b/field-1100d/field-1100f:signal-strength” would sort WDRs first by using date/time stamp fields 1100b, then by confidence value fields 1100d (sorted within matching date/time stamp WDRs), then by signal-strength field 1100f sub-field values (sorted within matching WDR confidences; no signal strength present = lowest priority). Another sort key may be “field-1100d/field-1100b” for sorting WDRs first by using
20 confidence values, then by date/time stamps (sorted within matching WDR confidences). The same or different sort keys can be used for lists THIS_MS and REMOTE_MS. Any WDR data (fields or subfields) can be sorted with a key, and sort keys can be of N order dimension such that “key1/key2/.../keyN”. Whatever sort keys are used, block 2686 will have to consider confidence versus being stale, relative to the WTV. In the preferred
25 embodiment, the REMOTE_MS and THIS_MS lists are set with the same sort keys of “field-1100d/field-1100b” (i.e. peek time period used at block 2634 is less than 2 seconds) so that confidence is primary.

30 Thereafter, block 2638 gets the first (if any) WDR in the list returned at block 2634 (also processes next WDR in list when encountered again in loop of blocks 2638 through 2654), and block 2640 checks to see if all WDRs have already been processed. If block 2640 finds that all WDRs have not been processed, then block 2642 checks the WDR origination. If block 2642 determines the WDR is one that originated from a remote MS

(i.e. MS ID does not match the MS of Fig. 26B processing), then block 2644 inserts the WDR into the REMOTE_MS list using the desired sort key (confidence primary, time secondary) from block 2636, and processing continues to block 2638 for another loop iteration. If block 2642 determines the WDR is one that originated from this MS (MS ID field 1100a matches the MS of Fig. 26B processing (e.g. this MS being a DLM at the time of WDR creation (this MS ID = field 1100a) or this MS being an ILM at the time of WDR creation (previous processing of Fig. 26A)), then processing continues to block 2646 to determine how to process the WDR which was inserted by “this MS” for its own whereabouts.

Block 2646 accesses field 1100f for data found there (e.g. Figs. 2D and 2E may have inserted useful TDOA measurements, even though DLM processing occurred; or Fig. 3C may have inserted useful TDOA and/or AOA measurements with reference station(s) whereabouts; or receive processing may have inserted AOA and related measurements). Thereafter, if block 2648 determines presence of TDOA and/or AOA data, block 2650 checks if reference whereabouts (e.g. Fig. 3C selected stationary reference location(s)) is also stored in field 1100f. If block 2650 determines whereabouts information is also stored to field 1100f, then block 2652 makes new WDR(s) from the whereabouts information containing at least the WDR Core and field 1100f containing the AOA and/or TDOA information as though it were from a remote DLM or ILM. Block 2652 also performs the expected result of inserting the WDR of loop processing into the THIS_MS list using the desired sort key from block 2636. Processing then continues to block 2644 where the newly made WDR(s) is inserted into the REMOTE_MS list using the desired sort key (confidence primary, time secondary) from block 2636. Block 2644 continues back to block 2638.

Referring back to block 2650, if it is determined that whereabouts information was not present with the AOA and/or TDOA information of field 1100f, then processing continues to block 2644 for inserting into the REMOTE_MS list (appropriately with sort key from block 2636) the currently looped WDR from block 2634. In-range location technology associates the MS with the antenna (or cell tower) location, so that field 1100c already contains the antenna (or cell tower) whereabouts, and the TDOA information was stored to determine how close the MS was to the antenna (or cell tower) at the time. The WDR will be more useful in the REMOTE_MS list, then if added to the THIS_MS list (see loop of

blocks 2660 through 2680). Referring back to block 2648, if it is determined that no AOA and/or TDOA information was in field 1100f, then processing continues to block 2654 for inserting the WDR into the THIS_MS list (appropriately with sort key (confidence primary, time secondary) from block 2636).

5 Block 2654 handles WDRs that originated from the MS of Fig. 26B (this MS), such as described in Figs. 2A through 9B, or results from previous Fig. 26A processing. Block 2644 maintains remote DLMS and/or ILMs (their whereabouts) to the REMOTE_MS list in hope WDRs contain useful field 1100f information for determining the whereabouts of the MS of Fig. 26B processing. Block 2652 handles WDRs that originated from the MS of Fig. 26B processing (this MS), but also processes fields from stationary references used (e.g. Fig. 3C) by this MS which can be helpful as though the WDR was originated by a remote ILM or DLM. Thus, block 2652 causes inserting to both lists (THIS_MS and REMOTE_MS) when the WDR contains useful information for both. Blocks 2652, 2654 and 2644 cause the iterative loop of blocks 2660 through 2680 to perform ADLT using DLMS and/or ILMs. Alternate embodiments of blocks 2638 through 2654 may use peek methodologies to sort from queue 22 for the REMOTE_MS and THIS_MS lists.

 Referring back to block 2640, if it is determined that all WDRs in the list from block 2634 have been processed, then block 2656 initializes a DISTANCE list and ANGLE list each to null, block 2658 sets a loop iteration pointer to the first entry of the prioritized REMOTE_MS list (e.g. first entry higher priority than last entry in accordance with sort key used), and block 2660 starts the loop for working with ordered WDRs of the REMOTE_MS list. Exit from block 2640 to block 2656 occurs when the REMOTE_MS and THIS_MS lists are in the desired priority order for subsequent processing. Block 2660 gets the next (or first) REMOTE_MS list entry for processing before continuing to block 2662. If block 2662 determines all WDRs have not yet been processed from the REMOTE_MS list, then processing continues to block 2664.

 Blocks 2664 and 2670 direct collection of all useful ILM triangulation measurements for TDOA, AOA, and/or MPT triangulation of this MS relative known whereabouts (e.g. other MSs). It is interesting to note that TDOA and AOA measurements (field 1100f) may have been made from different communications interfaces 70 (e.g. different wave spectrums), depending on interfaces the MS has available (i.e. all can participate). For example, a MS with blue-tooth, WiFi and cellular phone connectivity (different class wave

spectrums supported) can be triangulated using the best available information (i.e. heterogeneous location technique). Examination of fields 1100f in Fig. 17 can show wave spectrums (and/or particular communications interfaces 70) inserted by receive processing for what the MS supports. If block 2664 determines an AOA measurement is present (field 1100f sub-field), then block 2666 appends the WDR to the ANGLE list, and processing continues to block 2668. If block 2664 determines an AOA measurement is not present, then processing continues to block 2670. If block 2670 determines a TDOA measurement is present (field 1100f sub-field), then block 2672 appends the WDR to the DISTANCE list, and processing continues to block 2674. Block 2674 uses WDRs for providing at least an in-range whereabouts of this MS by inserting to the THIS_MS list in sorted confidence priority order (e.g. highest confidence first in list, lowest confidence at end of list). Block 2674 continues to block 2668. Block 2674 may cause duplicate WDR(s) inserted to the THIS_MS list, but this will have no negative effect on selected outcome.

Block 2668 compares the ANGLE and DISTANCE lists constructed thus far from loop processing (blocks 2660 through 2682) with minimum triangulation requirements (e.g. see “Missing Part Triangulation (MPT)” above). Three (3) sides, three (3) angles and a side, and other known triangular solution guides will also be compared. Thereafter, if block 2676 determines there is still not enough data to triangulate whereabouts of this MS, then processing continues back to block 2660 for the next REMOTE_MS list entry, otherwise block 2678 maximizes diversity of WDRs to use for triangulating. Thereafter, block 2680 uses the diversified DISTANCE and ANGLE lists to perform triangulation of this MS, block 2682 inserts the newly determined WDR into the THIS_MS list in sort key order, and continues back to block 2660. Block 2680 will use heterogeneous (MPT), TDOA and/or AOA triangulation on ANGLE and DISTANCE lists for determining whereabouts.

Block 2682 preferably keeps track of (or checks THIS_MS for) what it has thus far determined whereabouts for in this Fig. 26B thread processing to prevent inserting the same WDR to THIS_MS using the same REMOTE_MS data. Repeated iterations of blocks 2676 through 2682 will see the same data from previous iterations and will use the best of breed data in conjunction with each other at each iteration (in current thread context). While inserting duplicates to THIS_MS at block 2682 does not cause failure, it may be avoided for performance reasons. Duplicate insertions are preferably avoided at block 2674 for performance reasons as well, but they are again not harmful. Block 2678

preferably keeps track of previous diversity order in this Fig. 26B thread processing to promote using new ANGLE and DISTANCE data in whereabouts determination at block 2680 (since each iteration is a superset of a previous iteration (in current thread context)). Block 2678 promotes using WDRs from different MSs (different MS IDs), and from MSs located at significantly different whereabouts (e.g. to maximize surrounded-ness), preferably around the MS of Fig. 26B processing. Block 2678 preferably uses sorted diversity pointer lists so as to not affect actual ANGLE and DISTANCE list order. The sorted pointer lists provide pointers to entries in the ANGLE and DISTANCE lists for a unique sorted order governing optimal processing at block 2680 to maximize unique MSs and surrounded-ness, without affecting the lists themselves (like a SQL database index). Different embodiments of blocks 2678 through 2682 should minimize inserting duplicate WDRs (for performance reasons) to THIS_MS which were determined using identical REMOTE_MS list data. Block 2682 causes using ADLT at blocks 2684 through 2688 which uses the best of breed whereabouts, either as originated by this MS maintained in THIS_MS list up to the thread processing point of block 2686, or as originated by remote MSs (DLMs and/or ILMs) processed by blocks 2656 through the start of block 2684.

Referring back to block 2662, if it is determined that all WDRs in the REMOTE_MS list have been processed, then block 2684 sets the BESTWDR reference to the head of THIS_MS (i.e. BESTWDR references first WDR in THIS_MS list which is so far the best candidate WDR (highest confidence) for this MS whereabouts, or null if the list is empty). It is possible that there are other WDRs with matching confidence adjacent to the highest confidence entry in the THIS_MS list. Block 2684 continues to block 2686 for comparing matching confidence WDRs, and if there are matches, then breaking a tie between WDRs with matching confidence by consulting any other WDR field(s) (e.g. field 1100f signal strength, or location technology field 1100e, etc). If there is still a tie between a plurality of WDRs, then block 2686 may average whereabouts to the BESTWDR WDR using the matching WDRs. Thereafter processing continues to block 2688 where the BESTWDR is completed, and processing terminates at block 2690. Block 2688 also frees resources (if any) allocated by Fig. 26B processing (e.g. lists). Blocks 2686 through 2688 result in setting BESTWDR to the highest priority WDR (i.e. the best possible whereabouts determined). It is possible that Fig. 26B processing causes a duplicate WDR inserted to queue 22 (at block 2620) for this MS whereabouts determination, but that is no issue

except for impacting performance to queue 22. An alternate embodiment to queue 22 may define a unique index for erring out when inserting a duplicate to prevent frivolous duplicate entries, or block 2688 will incorporate processing to eliminate the chance of inserting a WDR of less use than what is already contained at queue 22. Therefore, block 2688 may include processing for ensuring a duplicate will not be inserted (e.g. null the BESTWDR reference) prior to returning to Fig. 26A at block 2690.

Averaging whereabouts at block 2686 occurs only when there are WDRs at the head of the list with a matching highest confidence value and still tie in other WDR fields consulted, yet whereabouts information is different. In this case, all matching highest confidence whereabouts are averaged to the BESTWDR to come up with whereabouts in light of all matching WDRs. Block 2686 performs ADLT when finalizing a single whereabouts (WDR) using any of the whereabouts found in THIS_MS (which may contain at this point DLM whereabouts originated by this MS and/or whereabouts originated by remote DLMs and/or ILMs). Block 2686 must be cognizant of sort keys used at blocks 2652 and 2654 in case confidence is not the primary key (time may be primary).

If no WDRs were found at block 2634, or no THIS_MS list WDRs were found at blocks 2652 and 2654, and no REMOTE_MS list entries were found at block 2644; or no THIS_MS list WDRs were found at blocks 2652 and 2654, and no REMOTE_MS list entries were found useful at blocks 2664 and/or 2670; then block 2684 may be setting BESTWDR to a null reference (i.e. none in list) in which case block 2686 does nothing. Hopefully, at least one good WDR is determined for MS whereabouts and a new WDR is inserted for this MS to queue 22, otherwise a null BESTWDR reference will be returned (checked at block 2616). See Fig 11A descriptions. If BESTWDR is not null, then fields are set to the following upon exit from block 2688:

MS ID field 1100a is preferably set with: MS ID of MS of Fig. 26B processing.

DATE/TIME STAMP field 1100b is preferably set with: Date/time stamp of block 2688 processing.

LOCATION field 1100c is preferably set with: Resulting whereabouts after block 2688 completion.

CONFIDENCE field 1100d is preferably set with: WDR Confidence at THIS_MS list head.

5 *LOCATION TECHNOLOGY field 1100e is preferably set with: “ILM TDOA Triangulation”, “ILM AOA Triangulation”, “ILM MPT Triangulation” or “ILM in-range”, as determined by the WDRs inserted to MS_LIST at blocks 2674 and 2682. The originator indicator is set to ILM.*

10 *LOCATION REFERENCE INFO field 1100f is preferably set with: null (not set), but may be set with contributing data for analysis of queue 22 provided it is marked for being overlooked by future processing of blocks 2646 and 2648 (e.g. for debug purpose).*

COMMUNICATIONS REFERENCE INFO field 1100g is preferably set with: null (not set).

15 *SPEED field 1100h is preferably set with: Block 2688 may compare prioritized entries and their order of time (field 1100b) in THIS_MS list for properly setting this field, if possible.*

20 *HEADING field 1100i is preferably set with: null (not set). Block 2688 may compare prioritized entries and their order of time (field 1100b) in THIS_MS list for properly setting this field, if possible.*

ELEVATION field 1100j is preferably set with: Field 1100j of BESTWDR (may be averaged if WDR tie(s)), if available.

25 *APPLICATION FIELDS field 1100k is preferably set with: Field(s) 1100k from BESTWDR or tie(s) thereof from THIS_MS. An alternate embodiment will add, alter, or discard data (with or without date/time stamps) here at the time of block 2688 processing.*

30 *CORRELATION FIELD 1100m is preferably set with: Not Applicable (i.e. not maintained to queue 22).*

SENT DATE/TIME STAMP field 1100n is preferably set with: Not Applicable (i.e. not maintained to queue 22).

RECEIVED DATE/TIME STAMP field 1100p is preferably set with: Not Applicable (i.e. not maintained to queue 22).

Block 2680 determines whereabouts using preferred guidelines, such as whereabouts determined never results in a confidence value exceeding any confidence value used to determine whereabouts. Some embodiments will use the mean (average) of confidence values used, some will use the highest, and some the lowest of the WDRs used. Preferred embodiments tend to properly skew confidence values to lower values as the LN-Expanse grows away from region 1022. Blocks 2668 through 2680 may consult any of the WDR fields (e.g. field 1100f sub-fields yaw, pitch, roll; speed, heading, etc) to deduce the most useful WDR inputs for determining an optimal WDR for this MS whereabouts.

Alternative IPC embodiments

Thread(s) 1952 are started for every WDR collected from remote MSs. Therefore, it is possible that identical new WDRs are inserted to queue 22 using the same WDR information at blocks 2634 of simultaneously executing threads 1952, but this will not cause a problem since at least one will be found when needed, and duplicates will be pruned together when appropriate. Alternative embodiments provide IPC (Interprocess Communications Processing) coordination between 1952 threads for higher performance processing, for example:

- As mentioned above, thread(s) 1952 can coordinate with each other to know successes, failures or progress of their sister 1952 thread(s) for automatically adjusting the trailing f(WTV) period of time appropriately. The f(WTV) period of time used at block 2634 would be semaphore accessed and modified (e.g. increased) for another 1952 thread when a previous 1952 thread was unsuccessful in determining whereabouts (via semaphore accessed thread outcome indicator). After a successful determination, the f(WTV) period of time could be reset back to the smaller window. One

embodiment of increasing may start with 10% of the WTV, then 20% at the next thread, 30% at the next thread, up to 90%, until a successful whereabouts is determined. After successful whereabouts determination, a reset to its original starting value is made.

- 5 • A semaphore accessed thread 1952 busy flag is used for indicating a certain thread is busy to prevent another 1952 thread from doing the same or similar work. Furthermore, other semaphore protected data for what work is actually being performed by a thread can be informative to ensure that no thread 1952 starts for doing duplicated effort.
- 10 • Useful data of statistics 14 may be appropriately accessed by thread(s) 1952 for dynamically controlling key variables of Fig. 26B processing, such as the search f(WTV) time period, sort keys used, when to quit loop processing (e.g. on first successful whereabouts determination at block 2680), surrounded-ness preferences, etc. This can dynamically change the Fig. 26B
15 logic from one thread to another for desired results.

Fig. 26B continues processing through every WDR retrieved at block 2634. An alternative embodiment will terminate processing after finding the first (which is highest priority data supported) successful triangulation at block 2682.

20 Fig. 27 depicts a flowchart for describing a preferred embodiment of queue prune processing. Queue pruning is best done on an interim basis by threads which may insert to the queue being pruned. In an alternate embodiment, a background asynchronous thread will invoke Fig. 27 for periodic queue pruning to ensure no queue which can grow becomes too large. The Prune Queues procedure starts at block 2702 and continues to
25 block 2704 where parameters passed by a caller for which queue(s) (WDR and/or CR) to prune are determined. Thereafter, if block 2706 determines that the caller wanted to prune the WDR queue 22, block 2708 appropriately prunes the queue, for example discarding old entries using field 1100b, and processing continues to block 2710. If block 2706
30 determines that the caller did not want to prune the WDR queue 22, then processing continues to block 2710. If block 2710 determines that the caller wanted to prune the CR queue 1990, block 2712 appropriately prunes the queue, for example discarding old

entries using field 2450a, and processing continues to block 2714. If block 2710 determines that the caller did not want to prune the CR queue 1990, then processing continues to block 2714. Block 2714 appropriately returns to the caller.

The current design for queue 1980 does not require Fig. 27 to prune it. Alternative embodiments may add additional queues for similar processing. Alternate embodiments may use Fig. 27 like processing to prune queues 24, 26, or any other queue under certain system circumstances. Parameters received at block 2704 may also include how to prune the queue, for example when using different constraints for what indicates entry(s) for discard.

Fig. 28 depicts a flowchart for describing a preferred embodiment of MS termination processing. Depending on the MS, there are many embodiments of processing when the MS is powered off, restarted, rebooted, reactivated, disabled, or the like. Fig. 28 describes the blocks of processing relevant to the present disclosure as part of that termination processing. Termination processing starts at block 2802 and continues to block 2804 for checking any DLM roles enabled and appropriately terminating if any are found (for example as determined from persistent storage variable DLMV). Block 2804 may cause the termination of thread(s) associated with enabled DLM role(s) for DLM processing above (e.g. Figs. 2A through 9B). Block 2804 may invoke API(s), disable flag(s), or terminate as is appropriate for DLM processing described above. Such terminations are well known in the art of prior art DLM capabilities described above. Block 2804 continues to block 2806.

Blocks 2806 through 2816 handle termination of all processes/threads associated with the ILMV roles so there is no explicit ILMV check required. Block 2806 initializes an enumerated process name array for convenient processing reference of associated process specific variables described in Fig. 19, and continues to block 2808 where the first member of the set is accessed for subsequent processing. The enumerated set of process names has a prescribed termination order for MS architecture 1900. Thereafter, if block 2810 determines the process identifier (i.e. 19xx-PID such that 19xx is 1902, 1912, 1922, 1932, 1942, 1952 in a loop iteration of blocks 2808 through 2816) is greater than 0 (e.g. this first iteration of 1912-PID > 0 implies it is to be terminated here; also implies process 1912 is enabled as used in Figs. 14A, 28, 29A and 29B), then block 2812

prepares parameters for Fig. 29B invocation, and block 2814 invokes (calls) the procedure of Fig. 29B to terminate the process (of this current loop iteration (19xx)). Block 2812 prepares the second parameter in accordance with the type of 19xx process. If the process (19xx) is one that is slave to a queue for dictating its processing (i.e. blocked on queue until queue entry present), then the second parameter (process type) is set to 0 (directing Fig. 29A processing to insert a special termination queue entry to be seen by worker thread(s) for terminating). If the process (19xx) is one that is slave to a timer for dictating its processing (i.e. sleeps until it is time to process), then the second parameter (process type) is set to the associated 19xx-PID value (directing Fig. 29B to use in killing/terminating the PID in case the worker thread(s) are currently sleeping). Block 2814 passes the process name and process type as parameters to Fig. 29B processing. Upon return from Fig. 29B, block 2814 continues to block 2816. If block 2810 determines that the 19xx process is not enabled, then processing continues to block 2816. Upon return from Fig. 29B processing, the process is terminated and the associated 19xx-PID variable is already set to 0 (see blocks 2966, 2970, 2976 and 2922).

Block 2816 checks to see if all process names of the enumerated set (19xx) have been processed (iterated) by blocks 2808 through 2816. If block 2816 determines that not all process names in the set have been processed (iterated), then processing continues back to block 2808 for handling the next process name in the set. If block 2816 determines that all process names of the enumerated set were processed, then block 2816 continues to block 2818.

Block 2818 destroys semaphore(s) created at block 1220. Thereafter, block 2820 destroys queue(s) created at block 1218 (may have to remove all entries first in some embodiments), block 2822 saves persistent variables to persistent storage (for example to persistent storage 60), block 2824 destroys shared memory created at block 1212, and block 2826 checks the NTP use variable (saved prior to destroying shared memory at block 2824).

If block 2826 determines NTP is enabled, then block 2828 terminates NTP appropriately (also see block 1612) and processing continues to block 2830. If block 2826 determines NTP was not enabled, then processing continues to block 2830. Block 2828 embodiments are well known in the art of NTP implementations. Block 2828 may cause terminating of thread(s) associated with NTP use.

Block 2830 completes LBX character termination, then block 2832 completes other character 32 termination processing, and Fig. 28 processing terminates thereafter at block 2834. Depending on what threads were started at block 1240, block 2830 may terminate the listen/receive threads for feeding queue 26 and the send threads for sending data inserted to queue 24. Depending on what threads were started at block 1206, block 2832 may terminate the listen/receive threads for feeding queue 26 and the send threads for sending data inserted to queue 24 (i.e. other character 32 threads altered to cause embedded CK processing). Upon encounter of block 2834, the MS is appropriately terminated for reasons at set forth above for invoking Fig. 28.

With reference now to Fig. 29B, depicted is a flowchart for describing a preferred embodiment of a procedure for terminating a process started by Fig. 29A. When invoked by a caller, the procedure starts at block 2952 and continues to block 2954 where parameters passed are determined. There are two parameters: the process name to terminate, and the type of process to terminate. The type of process is set to 0 for a process which has worker threads which are a slave to a queue. The type of process is set to a valid O/S PID when the process worker threads are slave to a timer.

Thereafter, if block 2956 determines the process type is 0, then block 2958 initializes a loop variable J to 0, and block 2960 inserts a special termination request queue entry to the appropriate queue for the process worker thread to terminate. See Fig. 19 discussions for the queue inserted for which 19xx process name.

Thereafter, block 2962 increments the loop variable by 1 and block 2964 checks if all process prescribed worker threads have been terminated. Block 2964 accesses the 19xx-Max (e.g. 1952-Max) variable from shared memory using a semaphore for determining the maximum number of threads to terminate in the process worker thread pool. If block 2964 determines all worker threads have been terminated, processing continues to block 2966 for waiting until the 19xx-PID variable is set to disabled (e.g. set to 0 by block 2922), and then to block 2978 which causes return to the caller. Block 2966 uses a preferred choice of waiting described for blocks 2918 and 2920. The 19xx process (e.g. 1952) will have its 19xx-PID (e.g. 1952-PID) variable set at 0 (block 2922) when the process terminates. In some embodiments, the waiting methodology used at block 2966

may use the 19xx-PID variable, or may be signaled by the last terminating worker thread, or by block 2922.

If block 2964 determines that not all worker threads have been terminated yet, then processing continues back to block 2960 to insert another special termination request queue entry to the appropriate queue for the next process worker thread to terminate. Blocks 2960 through 2964 insert the proper number of termination queue entries to the same queue so that all of the 19xx process worker threads terminate.

Referring back to block 2956, if it is determined the process type is not 0 (i.e. is a valid O/S PID), then block 2968 inserts a special WDR queue 22 entry enabling a queue peek for worker thread termination. The reader will notice that the process termination order of block 2806 ensures processes which were slaves to the WDR queue 22 have already been terminated. This allows processes which are slaves to a timer to see the special termination queue entry inserted at block 2968 since no threads (which are slaves to queue) will remove it from queue 22. Thereafter, block 2970 waits until the 19xx process name (parameter) worker threads have been terminated using a preferred choice of waiting described for blocks 2918 and 2920. The 19xx process (e.g. 1902) will have its 19xx-PID (e.g. 1902-PID) variable set at 0 (block 2922) when the process terminates. In some embodiments, the waiting methodology used at block 2970 may use the 19xx-PID variable, or may be signaled by the last terminating worker thread, or by block 2922. Block 2970 also preferably waits for a reasonable timeout period in anticipation of known sleep time of the 19xx process being terminated, for cases where anticipated sleep times are excessive and the user should not have to wait for lengthy Fig. 28 termination processing. If the timeout occurs before the process is indicated to be terminated, then block 2970 will continue to block 2972. Block 2970 also continues to block 2972 when the process has successfully terminated.

If block 2972 determines the 19xx process did terminate, the caller is returned to at block 2978 (i.e. 19xx-PID already set to disabled (0)). If block 2972 determines the 19xx process termination timed out, then block 2974 forces an appropriate O/S kill to the PID thereby forcing process termination, and block 2976 sets the 19xx-PID variable for disabled (i.e. process 19xx was terminated). Thereafter, block 2978 causes return to the caller.

There are many embodiments for setting certain queue entry field(s) identifying a special queue termination entry inserted at blocks 2960 and 2968. Some suggestions: In the case of terminating thread(s) 1912, queue 26 insertion of a WDR preferably sets the MS ID field with a value that will never appear in any other case except a termination request (e.g. -100). In the case of terminating thread(s) 1902, 1922 and 1952, queue 22 insertion of a WDR preferably sets the MS ID field with a value that will never appear in any other case except a termination request (e.g. -100). In the case of terminating thread(s) 1942, queue 26 insertion of a WDR request preferably sets the MS ID field with a value that will never appear in any other case except a termination request (e.g. -100). In the case of terminating thread(s) 1932, queue 1980 insertion of a thread request queue record 2400 preferably sets field 2400a with a value that will never appear in any other case except a termination request (e.g. -100). Of course, any available field(s) can be used to indicate termination to particular thread(s)).

Terminating threads of processing in Fig. 29B has been presented from a software perspective, but there are hardware/firmware thread embodiments which may be terminated appropriately to accomplish the same functionality. If the MS operating system does not have an interface for killing the PID at block 2974, then blocks 2972 through 2976 can be eliminated for relying on a Fig. 28 invocation timeout (incorporated for block 2814) to appropriately rob power from remaining thread(s) of processing.

An ILM has many methods and systems for knowing its own location. LBX depends on MSs maintaining their own whereabouts. No service is required to maintain the whereabouts of MSs in order to accomplish novel functionality.

OTHER EMBODIMENTS

As mentioned above, architecture 1900 provides a set of processes which can be started or terminated for desired functionality. Thus, architecture 1900 provides a palette from which to choose desired deployment methods for an LN expanse.

In some embodiments, all whereabouts information can be pushed to expand the LN-expanse. In such embodiments, the palette of processes to choose from includes at least process 1902, process 1912 and process 1952. Additionally, process 1932 would be

required in anticipation of LN-expanse participating data processing systems having NTP disabled or unavailable. Additionally, process 1922 could be used for ensuring whereabouts are timely (e.g. specifically using all blocks except 2218 through 2224). Depending on DLM capability of MSs in the LN-expanse, a further subset of processes 1902, 1912, 1952 and 1932 may apply. Thread(s) 1902 beacon whereabouts information, regardless of the MS being an affirmifier or pacifier.

In some embodiments, all whereabouts information can be pulled to expand the LN-expanse. In such embodiments, the palette of processes to choose from includes at least process 1922 (e.g. specifically using all blocks except 2226 and 2228), process 1912, process 1952 and process 1942. Additionally, process 1932 would be required in anticipation of LN-expanse participating data processing systems having NTP disabled or unavailable. Depending on DLM capability of MSs in the LN-expanse, a further subset of processes 1922, 1912, 1952, 1942 and 1932 may apply.

There are many embodiments derived from architecture 1900. Essential components are disclosed for deployment varieties. In communications protocols which acknowledge a transmission, processes 1932 may not be required even in absence of NTP use. A sending MS appends a sent date/time stamp (e.g. field 1100n) on its time scale to outbound data 1302 and an acknowledging MS (or service) responds with the sent date/time stamp so that when the sending MS receives it (receives data 1302 or 1312), the sending MS (now a receiving MS) calculates a TDOA measurement by comparing when the acknowledgement was received and when it was originally sent. Appropriate correlation outside of process 1932 deployment enables the sending MS to know which response went with which data 1302 was originally sent. A MS can make use of 19xx processes as is appropriate for functionality desired.

In push embodiments disclosed above, useful summary observations are made. Service(s) associated with antennas periodically broadcast (beacon) their reference whereabouts (e.g. WDR information) for being received by MSs in the vicinity. When such services are NTP enabled, the broadcasts include a sent date/time stamp (e.g. field 1100n). Upon receipt by a NTP enabled MS in the vicinity, the MS uses the date/time stamp of MS receipt (e.g. 1100p) with the date/time stamp of when sent (e.g. field 1100n) to calculate a TDOA measurement. Known wave spectrum velocity can translate to a

distance. Upon receipt of a plurality of these types of broadcasts from different reference antennas, the MS can triangulate itself for determining its whereabouts relative known whereabouts of the reference antennas. Similarly, reference antennas are replaced by other NTP enabled MSs which similarly broadcast their whereabouts. A MS can be triangulated relative a mixture of reference antennas and other NTP enabled MSs, or all NTP enabled MSs. Stationary antenna triangulation is accomplished the same way as triangulating from other MSs. NTP use allows determining MS whereabouts using triangulation achievable in a single unidirectional broadcast of data (1302 or 1312). Furthermore, reference antennas (service(s)) need not communicate new data 1312, and MSs need not communicate new data 1302. Usual communications data 1312 are altered with a CK 1314 as described above. Usual communications data 1302 are altered with a CK 1304 as described above. This enables a MS with not only knowing there are nearby hotspots, but also where all parties are located (including the MS). Beacons hotspots, or other broadcasters, do not need to know who you are (the MS ID), and you do not need to know who they are in order to be located. Various bidirectional correlation embodiments can always be used for TDOA measurements.

In pull embodiments disclosed above, data processing systems wanting to determine their own whereabouts (requestors) broadcast their requests (e.g. record 2490). Service(s) or MSs (responders) in the vicinity respond. When responders are NTP enabled, the responses include a sent date/time stamp (e.g. field 1100n) that by itself can be used to calculate a TDOA measurement if the requestor is NTP enabled. Upon receipt by a requestor with no NTP, the requestor uses the date/time stamp of a correlated receipt (e.g. 1100p) with the date/time stamp of when sent (e.g. fields 1100n or 2450a) to calculate a time duration (TDOA) for whereabouts determination, as described above. New data or usual communications data applies as described above.

If NTP is available to a data processing system, it should be used whenever communicating date/time information (e.g. NTP bit of field 1100b, 1100n or 1100p) so that by chance a receiving data processing is also NTP enabled, a TDOA measurement can immediately be taken. In cases, where either the sending (first) data processing system or receiving (second) data processing system is not NTP enabled, then the calculating data processing system wanting a TDOA measurement will need to calculate a sent and received time in consistent time scale terms. This includes a correlated bidirectional

communications data flow to properly determine duration in time terms of the calculating data processing system. In a send initiated embodiment, a first (sending) data processing system incorporates a sent date/time stamp (e.g. fields 1100n or 2450a) and determines when a correlated response is received to calculate the TDOA measurement (both times in terms of the first (sending) data processing system). In another embodiment, a second (receiving) data processing system receives a sent date/time stamp (e.g. field 1100n) and then becomes a first (sending) data processing as described in the send initiated embodiment. Whatever embodiment is used, it is beneficial in the LN-expanse to minimize communications traffic.

The NTP bit in date/time stamps enables optimal elegance in the LN-expanse for taking advantage of NTP when available, and using correlated transmissions when it is not. A NTP enabled MS is somewhat of a chameleon in using unidirectional data (1302 or 1312 received) to determine whereabouts relative NTP enabled MS(s) and/or service(s), and then using bidirectional data (1302/1302 or 1302/1312) relative MS(s) and/or service(s) without NTP. A MS is also a chameleon when considering it may go in and out of a DLM or ILM identity/role, depending on what whereabouts technology is available at the time.

The MS ID (or pseudo MS ID) in transmissions is useful for a receiving data processing system to target a response by addressing the response back to the MS ID. Targeted transmissions target a specific MS ID (or group of MS IDs), while broadcasting is suited for reaching as many MS IDs as possible. Alternatively, just a correlation is enough to target a data source.

In some embodiments where a MS is located relative another MS, this is applicable to something as simple as locating one data processing system using the location of another data processing system. For example, the whereabouts of a cell phone (first data processing system) is used to locate an in-range automotive installed (second) data processing system for providing new locational applications to the second data processing system (or visa-versa). In fact, the second data processing may be designed for using the nearby first data processing system for determining its whereabouts. Thus, as an MS roams, in the know of its own whereabouts, the MS whereabouts is shared with nearby data processing systems for new functionality made available to those nearby data

processing systems when they know their own whereabouts (by associating to the MS whereabouts). Data processing systems incapable of being located are now capable of being located, for example locating a data processing equipped shopping cart with the location of an MS, or plurality of MSs.

5

Architecture 1900 presents a preferred embodiment for IPC (Interprocess Communications Processing), but there are other embodiments for starting/terminating threads, signaling between processes, semaphore controls, and carrying out present disclosure processing without departing from the spirit and scope of the disclosure. In some embodiments, threads are automatically throttled up or down (e.g. 1952-Max) per unique requirements of the MS as determined by how often threads loop back to find an entry already waiting in a queue. If thread(s) spend less time blocked on queue, they can be automatically throttled up. If thread(s) spend more time blocked on queue, they can be automatically throttled down. Timers can be associated with queue retrieval to keep track of time a thread is blocked.

15

LBX history 30 preferably maintains history information of key points in processing where history information may prove useful at a future time. Some of the useful points of interest may include:

20

- Interim snapshots of permissions 10 (for documenting who had what permissions at what time) at block 1478;
- Interim snapshots of charters 12 (for documenting charters in effect at what times) at block 1482;
- Interim snapshots of statistics 14 (for documenting useful statistics worthy of later browse) at block 1486;
- Interim snapshots of service propagation data of block 1474;
- Interim snapshots of service informant settings of block 1490;
- Interim snapshots of LBX history maintenance/configurations of block 1494;
- Interim snapshots of a subset of WDR queue 22 using a configured search criteria;

25

30

- Interim snapshots of a subset of Send queue 24 using a configured search criteria;
- Interim snapshots of a subset of Receive queue 26 using a configured search criteria;
- 5 • Interim snapshots of a subset of PIP data 8;
- Interim snapshots of a subset of data 20;
- Interim snapshots of a subset of data 36;
- Interim snapshots of other resources 38;
- 10 • Trace, debug, and/or dump of any execution path subset of processing flowcharts described; and/or
- Copies of data at any block of processing in any flowchart heretofore described.

Entries in LBX history 30 preferably have entry qualifying information including at least a
15 date/time stamp of when added to history, and preferably an O/S PID and O/S TID
(Thread Identifier) associated with the logged entry, and perhaps applicable applications
involved (e.g. see fields 1100k). History 30 may also be captured in such a way there are
conditions set up in advance (at block 1494), and when those conditions are met,
applicable data is captured to history 30. Conditions can include terms that are MS system
20 wide, and when the conditions are met, the data for capture is copied to history. In these
cases, history 30 entries preferably include the conditions which were met to copy the
entry to history. Depending on what is being kept to history 30, this can become a large
amount of information. Therefore, Fig. 27 can include new blocks for pruning history 30
appropriately. In another embodiment, a separate thread of processing has a sleeper loop
25 which when awake will prune the history 30 appropriately, either in its own processing or
by invoking new Fig. 27 blocks for history 30. A parameter passed to processing by block
2704 may include how to prune the history, including what data to prune, how old of data
to prune, and any other criteria appropriate for maintaining history 30. In fact, any pruning
30 by Fig. 27 may include any reasonable parameters for how to prune particular data of the
present disclosure.

Location applications can use the WDR queue for retrieving the most recent highest confidence entry, or can access the single instance WDR maintained (or most recent WDR of block 289 discussed above). Optimally, applications are provided with an API that hides what actually occurs in ongoing product builds, and for ensuring appropriate semaphore access to multi-threaded accessed data.

Correlation processing does not have to cause a WDR returned. There are embodiments for minimal exchanges of correlated sent date/time stamps and/or received date/time stamps so that exchanges are very efficient using small data exchanges. Correlation of this disclosure was provided to show at least one solution, with keeping in mind that there are many embodiments to accomplish relating time scales between data processing systems.

Architecture 1900 provides not only the foundation for keeping an MS abreast of its whereabouts, but also the foundation upon which to build LBX nearby functionality. Whereabouts of MSs in the vicinity are maintained to queue 22. Permissions 10 and charters 12 can be used for governing which MSs to maintain to queue 22, how to maintain them, and what processing should be performed. For example, MS user Joe wants to alert MS user Sandy when he is in her vicinity, or user Sandy wants to be alerted when Joe is in her vicinity. Joe configures permissions enabling Sandy to be alerted with him being nearby, or Sandy configured permissions for being alerted. Sandy accepts the configuration Joe made, or Joe accepts the configuration Sandy made. Sandy's queue 22 processing will ensure Joe's WDRs are processed uniquely for desired functionality.

Fig. 8C was presented in the context of a DLM, however architecture 1900 should be applied for enabling a user to manually request to be located with ILM processing if necessary. Blocks 862 through 870 are easily modified to accomplish a WDR request (like blocks 2218 through 2224). In keeping with current block descriptions, block 872 would become a new series of blocks for handling the case when DLM functionality was unsuccessful. New block 872-A would broadcast a WDR request soliciting response (see blocks 2218 through 2224). Thereafter, a block 872-B would wait for a brief time, and subsequently a block 872-C would check to see if whereabouts have been determined

(e.g. check queue 22). Thereafter, if a block 872-D determines whereabouts were not determined, an error could be provided to the user, otherwise the MS whereabouts were successfully determined and processing continues to block 874. Applications that may need whereabouts can now be used. There are certainly emergency situations where a user may need to rely on other MSs in the vicinity for being located.

To maintain modularity in interfaces to queues 24 and 26, parameters may be passed rather than having the modular send/receive processing access fields of application records. When WDRs are “sent”, the WDR will be targeted (e.g. field 1100a), perhaps also with field 1100f indicating which communications interface to send on (e.g. MS has plurality of comm. interfaces 70). When WDRs are “broadcast” (e.g. null MS ID), the WDR is preferably outbound on all available comm. interfaces 70), unless field 1100f indicates to target a comm. interface. Analogously, when WDR requests are “sent”, the request will be targeted (e.g. field 2490a), perhaps also with field 2490d indicating which communications interface to send on (e.g. MS has plurality of comm. interfaces 70). When WDR requests are “broadcast” (e.g. null MS ID), the WDR is preferably outbound on all available comm. interfaces 70), unless field 1100f indicates to target a comm. interface.

Fields 1100m, 1100n, 1100p, 2490b and 2490c are also of interest to the transport layer. Any subset, or all, of transport related fields may be passed as parameters to send processing, or received as parameters from receiving processing to ensure send and receive processing is adaptable using pluggable transmission/reception technologies.

An alternate embodiment to the BESTWDR WDR returned by Fig. 26B processing may be set with useful data for reuse toward a future Fig. 26B processing thread whereabouts determination. Field 1100f (see pg. 168) can be set with useful data for that WDR to be in turn used at a subsequent whereabouts determination of Fig. 26B. This is referred to as Recursive Whereabouts Determination (RWD) wherein ILMs determine WDRs for their whereabouts and use them again for calculating future whereabouts (by populating useful TDOA, AOA, MPT and/or whereabouts information to field 1100f).

An alternate embodiment may store remote MS movement tolerances (if they use one) to WDR field 1100f so the receiving MS can determine how stale are other WDRs in

queue 22 from the same MS, for example when gathering all useful WDRs to start with in determining whereabouts of Fig. 26B processing (e.g. block 2634). Having movement tolerances in effect may prove useful for maximizing useful WDRs used in determining a whereabouts (Fig. 26B processing).

5

While various embodiments of the present disclosure have been described above, it should be understood that they have been presented by way of example only, and not limitation. Thus, the breadth and scope of the present disclosure should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

10

WHAT IS CLAIMED IS:

1. A method by a sending data processing system, the method comprising:
- accessing, by the sending data processing system, identity information for describing an originator identity associated with the sending data processing system;
 - 5 accessing, by the sending data processing system, application information for an application in use at the sending data processing system;
 - accessing, by the sending data processing system, location information associated with the sending data processing system;
 - accessing, by the sending data processing system, reference information for further
10 describing the location information associated with the sending data processing system;
 - preparing, by the sending data processing system, a broadcast unidirectional wireless data record including:
 - the identity information for describing the originator identity associated with the sending data processing system,
 - 15 the application information for the application in use at the sending data processing system,
 - the location information associated with the sending data processing system, and
 - the reference information for further describing the location
20 information associated with the sending data processing system;
 - maintaining, by the sending data processing system, a configuration for when to perform beaconing of the broadcast unidirectional wireless data record; and
 - transmitting, by the sending data processing system, the broadcast unidirectional
25 wireless data record for receipt by a plurality of receiving mobile data processing systems in a wireless vicinity of the sending data processing system wherein the broadcast unidirectional wireless data record is beaconed by the sending data processing system in accordance with the configuration for when to perform beaconing, and wherein the broadcast unidirectional wireless data record includes at least:
 - 30 the identity information for describing the originator identity associated with the sending data processing system wherein the identity information is for an alert determined by each receiving mobile data processing system of

the plurality of receiving mobile data processing systems that the each receiving mobile data processing system is in the wireless vicinity of the sending data processing system,

5

the application information for the application in use at the sending data processing system,

the location information associated with the sending data processing system to be used by the each receiving mobile data processing system for determining their own location relative to the location information, and

10

the reference information for further describing the location information associated with the sending data processing system for describing to the each receiving mobile data processing system useful information associated with the sending data processing system.

15

2. The method of claim 1 wherein the broadcast unidirectional wireless data record includes web site information associated with the sending data processing system.

20

3. The method of claim 1 wherein the broadcast unidirectional wireless data record includes environmental condition information associated with the sending data processing system.

4. The method of claim 1 wherein the broadcast unidirectional wireless data record includes information for at least one service associated with the sending data processing system.

25

5. The method of claim 1 wherein the broadcast unidirectional wireless data record includes information for at least one transaction associated with the sending data processing system.

30

6. The method of claim 1 wherein the broadcast unidirectional wireless data record includes information for one or more data processing systems remote to the sending data processing system.

7. The method of claim 1 wherein the broadcast unidirectional wireless data record includes information for distinguishing an elevation or altitude.

5 8. The method of claim 1 wherein the broadcast unidirectional wireless data record includes confidence information for describing a reliability of data in the broadcast unidirectional wireless data record.

9. The method of claim 1 wherein the broadcast unidirectional wireless data record includes information that is presented to a user interface of the each receiving mobile data processing system.
10

10. The method of claim 1 wherein the broadcast unidirectional wireless data record includes information that is processed by the each receiving mobile data processing system for determining by the each receiving mobile data processing system what to present to a user interface.
15

11. The method of claim 1 wherein the broadcast unidirectional wireless data record includes at least one of:

20 information for a location technology used to locate the sending data processing system,

information for a triangulation measurement associated with the sending data processing system,

information for a time difference of arrival measurement associated with the sending data processing system,

25 information for a time of arrival measurement associated with the sending data processing system,

information for an angle of arrival measurement associated with the sending data processing system,

30 information for a yaw measurement associated with the sending data processing system,

information for a pitch measurement associated with the sending data processing system,

information for a roll measurement associated with the sending data processing system,

information for an accelerometer measurement associated with the sending data processing system,

5 information for a communications signal strength of a transmission associated with the sending data processing system,

information for a communications wave spectrum characteristic of a transmission associated with the sending data processing system,

10 information for a communications wave spectrum class of a transmission associated with the sending data processing system,

information for a communications wave spectrum frequency of a transmission associated with the sending data processing system,

information associated with a wireless data record received by the sending data processing system from a particular data processing system,

15 information maintained by an application associated with the sending data processing system,

information for an application in use at the sending data processing system,

information for an application context of an application associated with the sending data processing system,

20 information for a navigation Application Programming Interface associated with the sending data processing system,

information for a situational location associated with the sending data processing system,

information for a speed associated with the sending data processing system,

25 information for a heading associated with the sending data processing system,

time information associated with the sending data processing system,

information for a service condition associated with the sending data processing system,

30 information for a physical address associated with the sending data processing system,

information for a logical address associated with the sending data processing system,

information for a user configuration associated with the sending data processing system,

information for monitoring movement of the sending data processing system,

information for an identifier associated with the sending data processing system, or

5 information in accordance with one or more permissions configured by a user associated with the sending data processing system.

12. The method of claim 1 wherein the broadcast unidirectional wireless data record includes information that can be processed according to a user configured permission maintained at the each receiving mobile data processing system.

13. The method of claim 12 wherein the user configured permission is configured by a user of the sending data processing system for providing permission to an identity of at least one of the plurality of receiving mobile data processing systems.

14. The method of claim 12 wherein the user configured permission is configured by a user of at least one of the plurality of receiving mobile data processing systems for providing permission to an identity associated with the sending data processing system.

15. The method of claim 12 wherein the user configured permission enables providing an alert for who is nearby.

16. The method of claim 1 wherein the identity information is a dependable and recognizable derivative of the originator identity associated with the sending data processing system.

17. The method of claim 1 wherein the location information associated with the sending data processing system is determined by the sending data processing system with a direct location method, or an indirect location method, or with information communicated to the sending data processing system by a remote data processing system.

18. The method of claim 1 wherein the transmitting, by the sending data processing system, the broadcast unidirectional wireless data record for receipt by the plurality of receiving mobile data processing systems in the wireless vicinity of the sending data processing system includes transmitting the broadcast unidirectional wireless data record
5 by a plurality of distinctly different radio communication interfaces of the sending data processing system.

19. The method of claim 1 including:
searching, by the sending data processing system, a plurality of data records in a
10 historical collection; and
retrieving, by the sending data processing system, one of the plurality of data records for the preparing, by the sending data processing system, the broadcast unidirectional wireless data record.

20. The method of claim 1 including presenting information for the broadcast unidirectional wireless data record to a user interface for a user to manage the information for the broadcast unidirectional wireless data record by at least one of: view the information for the broadcast unidirectional wireless data record, delete the information for the broadcast unidirectional wireless data record, modify the information for the broadcast
20 unidirectional wireless data record, or add to the information for the broadcast unidirectional wireless data record.

21. A sending data processing system, comprising:
one or more processors; and
25 at least one memory coupled to the one or more processors, wherein the at least one memory includes executable instructions, which when executed by the one or more processors, results in the system:
accessing, by the sending data processing system, identity information for describing an originator identity associated with the sending data processing
30 system;
accessing, by the sending data processing system, application information for an application in use at the sending data processing system;

accessing, by the sending data processing system, location information associated with the sending data processing system;

accessing, by the sending data processing system, reference information for further describing the location information associated with the sending data processing system;

preparing, by the sending data processing system, a broadcast unidirectional wireless data record including:

the identity information for describing the originator identity associated with the sending data processing system,

the application information for the application in use at the sending data processing system,

the location information associated with the sending data processing system, and

the reference information for further describing the location information associated with the sending data processing system;

maintaining, by the sending data processing system, a configuration for when to perform beaconing of the broadcast unidirectional wireless data record; and

transmitting, by the sending data processing system, the broadcast unidirectional wireless data record for receipt by a plurality of receiving mobile data processing systems in a wireless vicinity of the sending data processing system wherein the broadcast unidirectional wireless data record is beacons by the sending data processing system in accordance with the configuration for when to perform beaconing, and wherein the broadcast unidirectional wireless data record includes at least:

the identity information for describing the originator identity associated with the sending data processing system wherein the identity information is for an alert determined by each receiving mobile data processing system of the plurality of receiving mobile data processing systems that the each receiving mobile data processing system is in the wireless vicinity of the sending data processing system,

the application information for the application in use at the sending data processing system,

5

the location information associated with the sending data processing system to be used by the each receiving mobile data processing system for determining their own location relative to the location information, and

10

the reference information for further describing the location information associated with the sending data processing system for describing to the each receiving mobile data processing system useful information associated with the sending data processing system.

ABSTRACT

Provided is a distributed system and method for enabling new and useful location dependent features and functionality to mobile data processing systems. Mobile data processing systems interact with each other as peers in communications and interoperability. A mobile data processing system may dynamically take on roles, depending on the environment and capabilities available at a particular time. Reference whereabouts data is appropriately shared between mobile data processing systems to carry out automatic location techniques ensuring mobile data processing systems are kept up to date with their own whereabouts and whereabouts of others, regardless of the freely moving travels of any of the mobile data processing systems involved, and the location technologies that may or may not be available when needed. A confidence is associated to whereabouts data shared for facilitating selection of the best candidate data used in determining new whereabouts information.

1/70

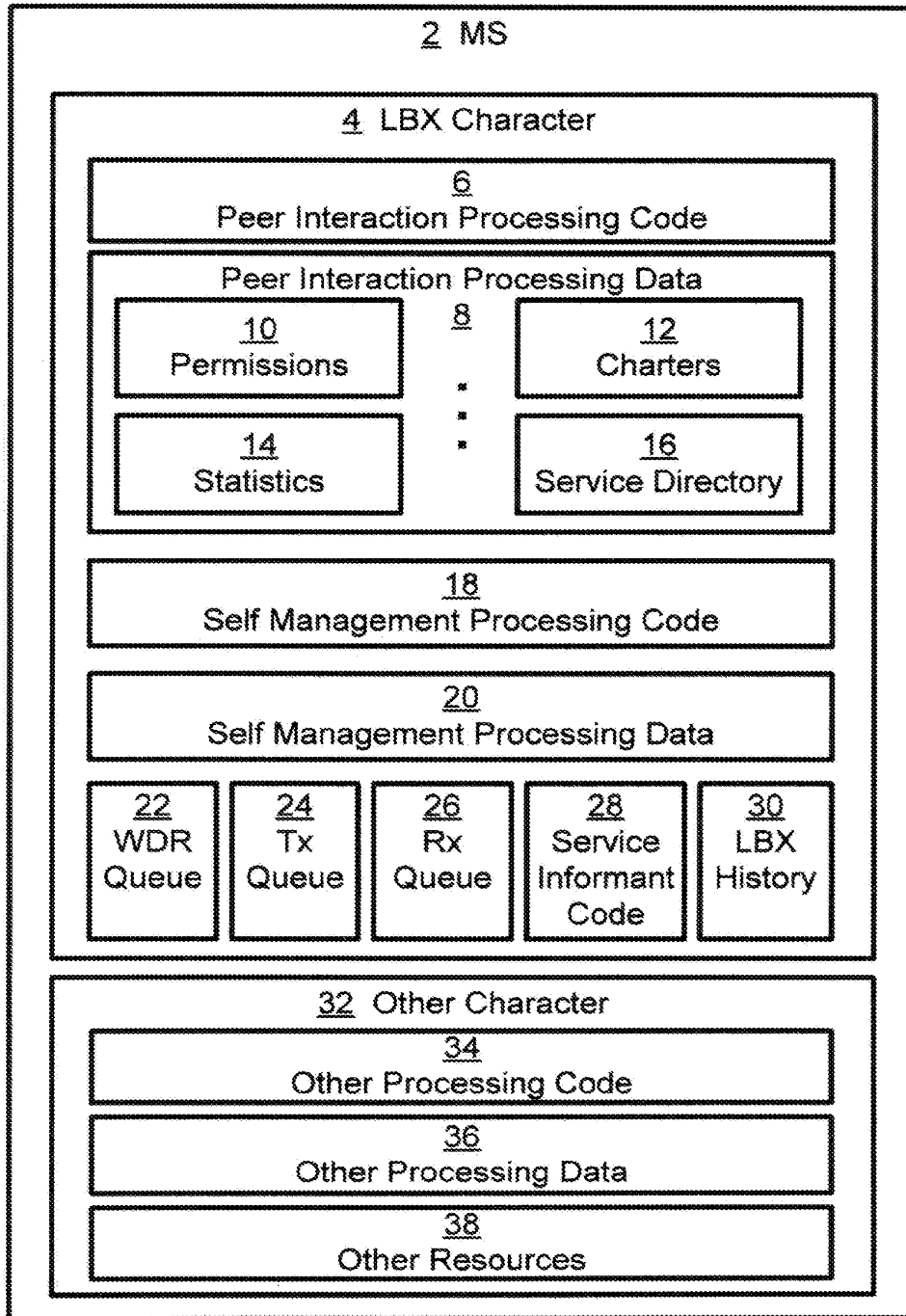


Fig. 1A

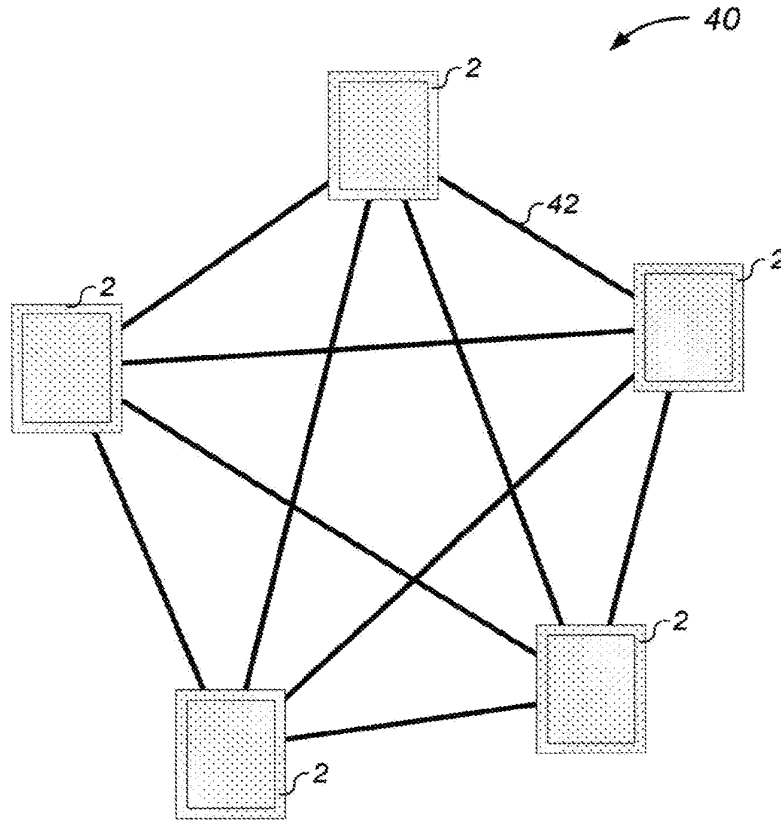


Fig. 1B

3/70

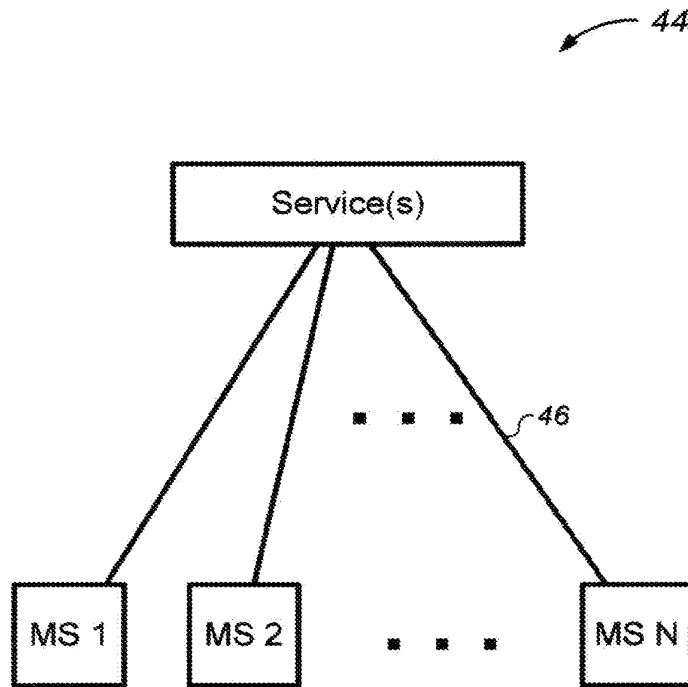


Fig. 1C

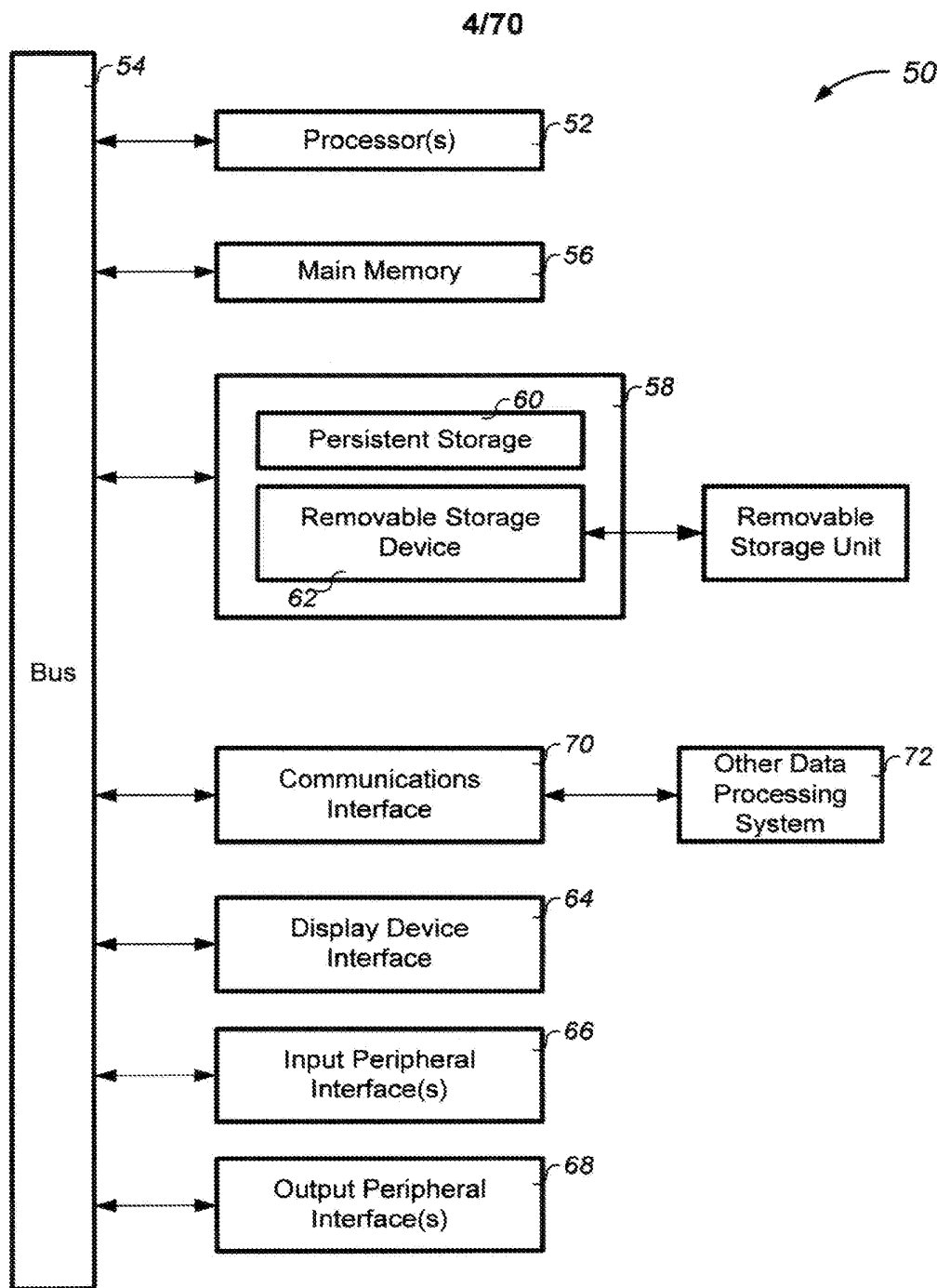


Fig. 1D

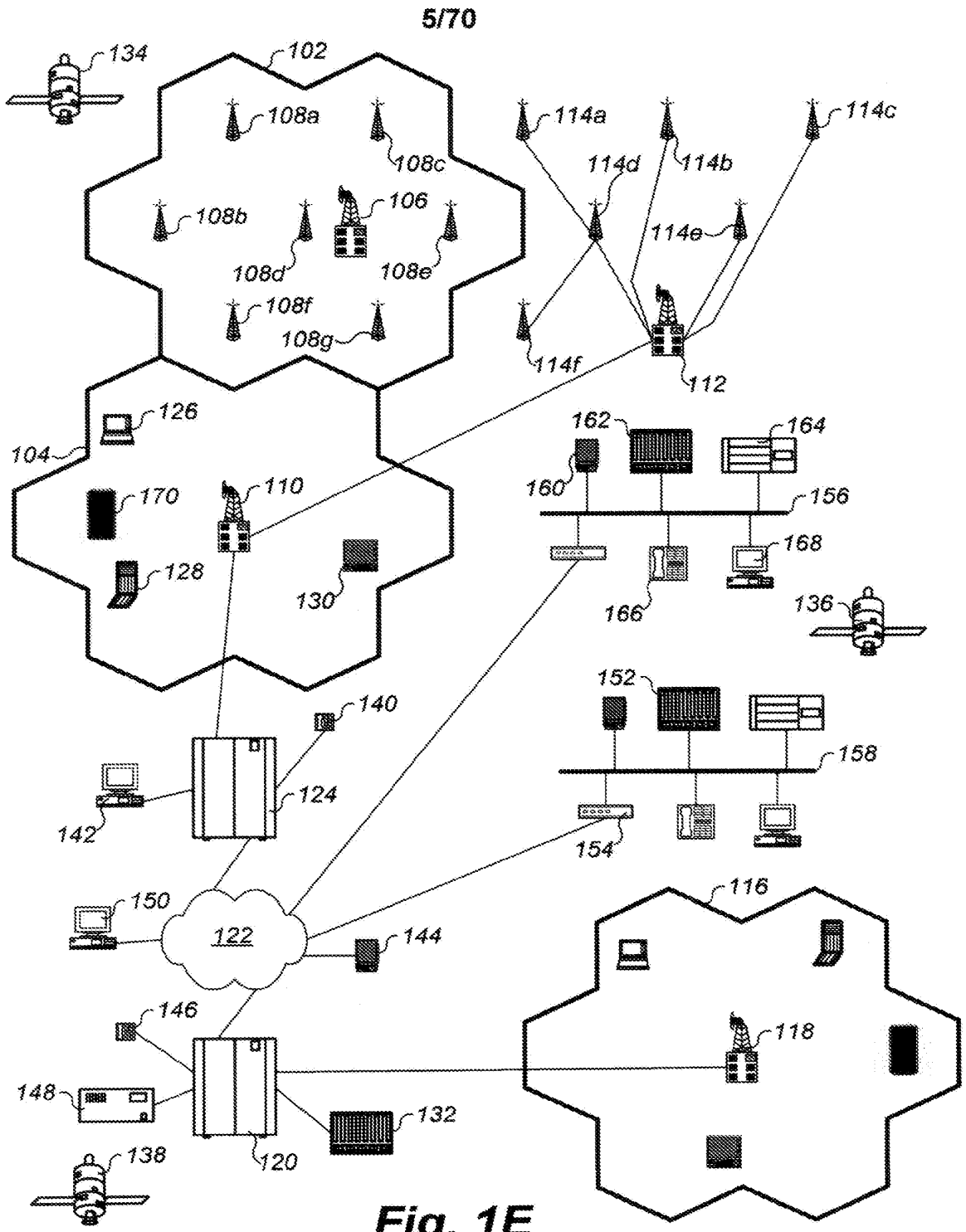


Fig. 1E

6/70

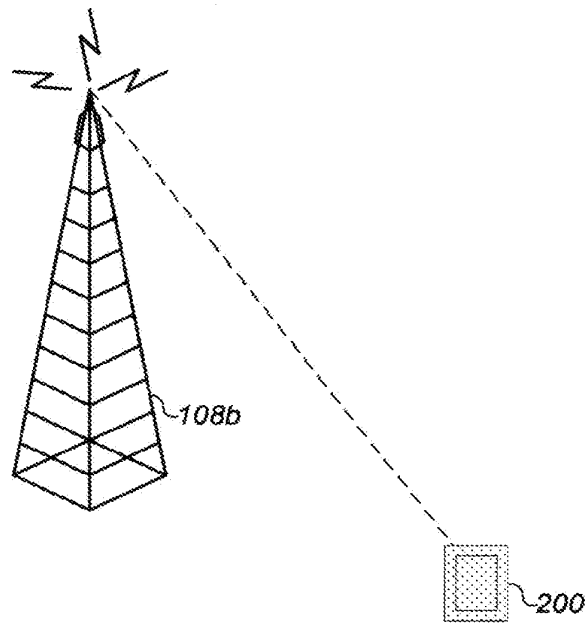


Fig. 2A

7170

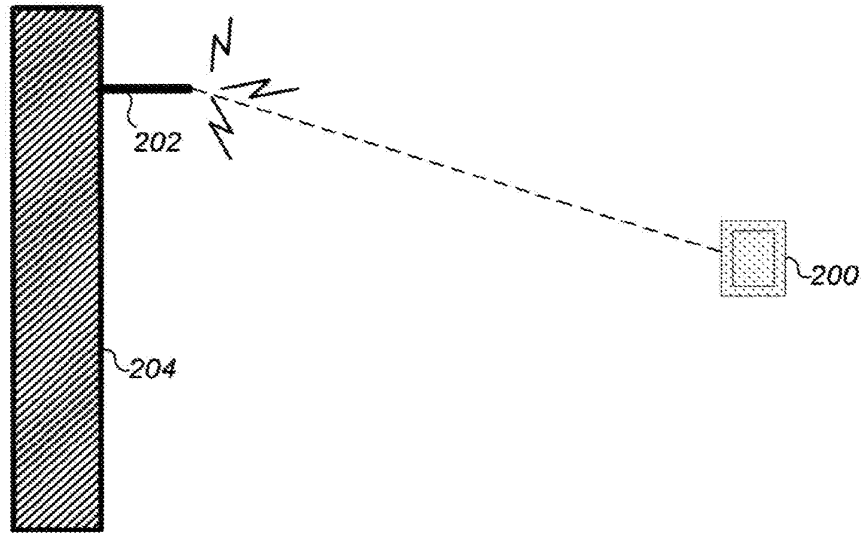


Fig. 2B

8/70

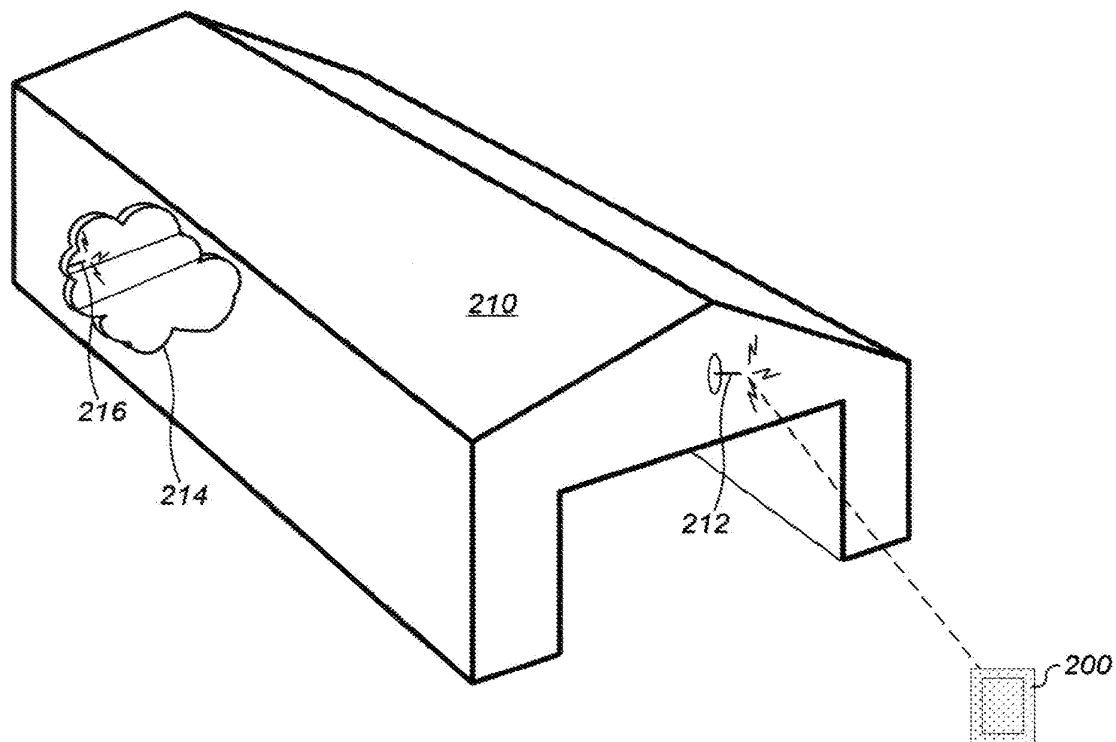


Fig. 2C

9/70

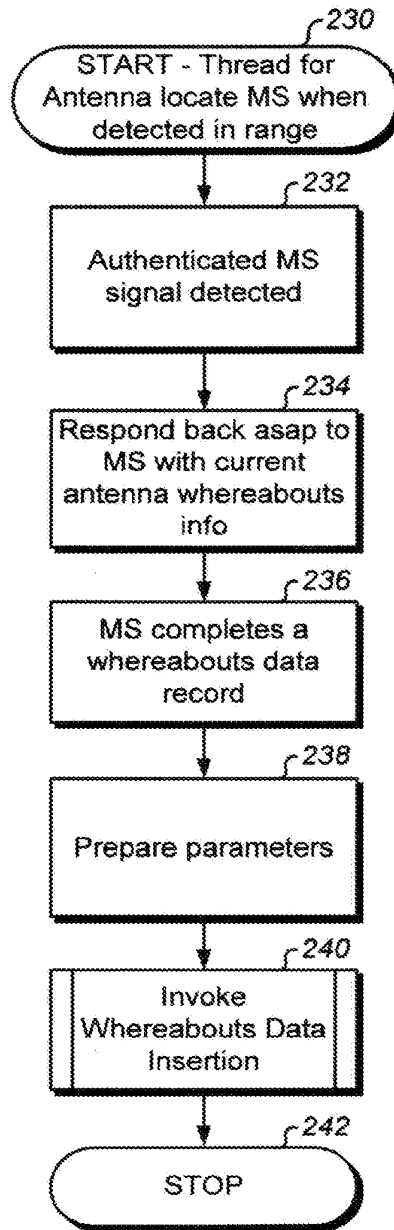


Fig. 2D

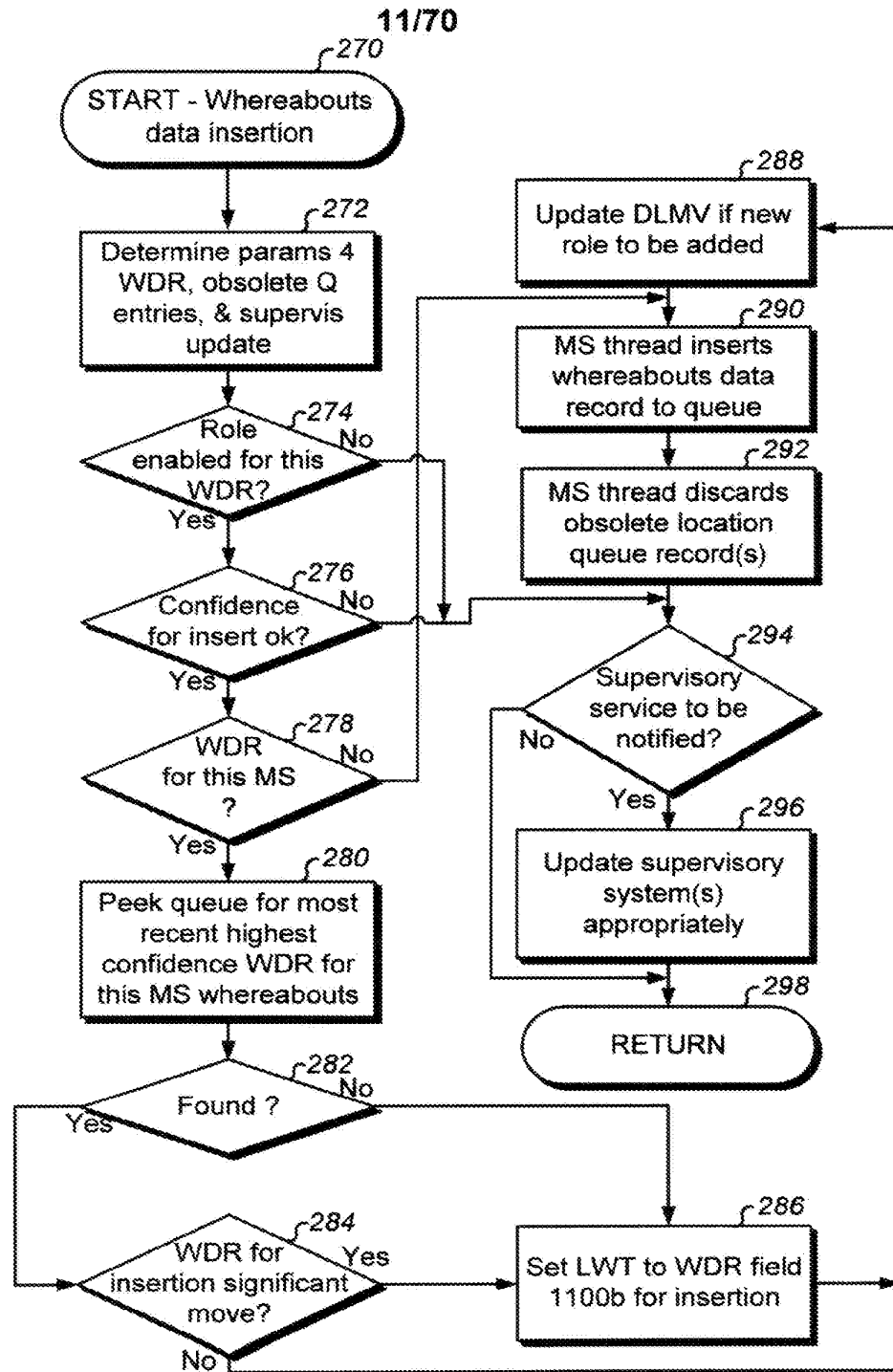


Fig. 2F

12/70

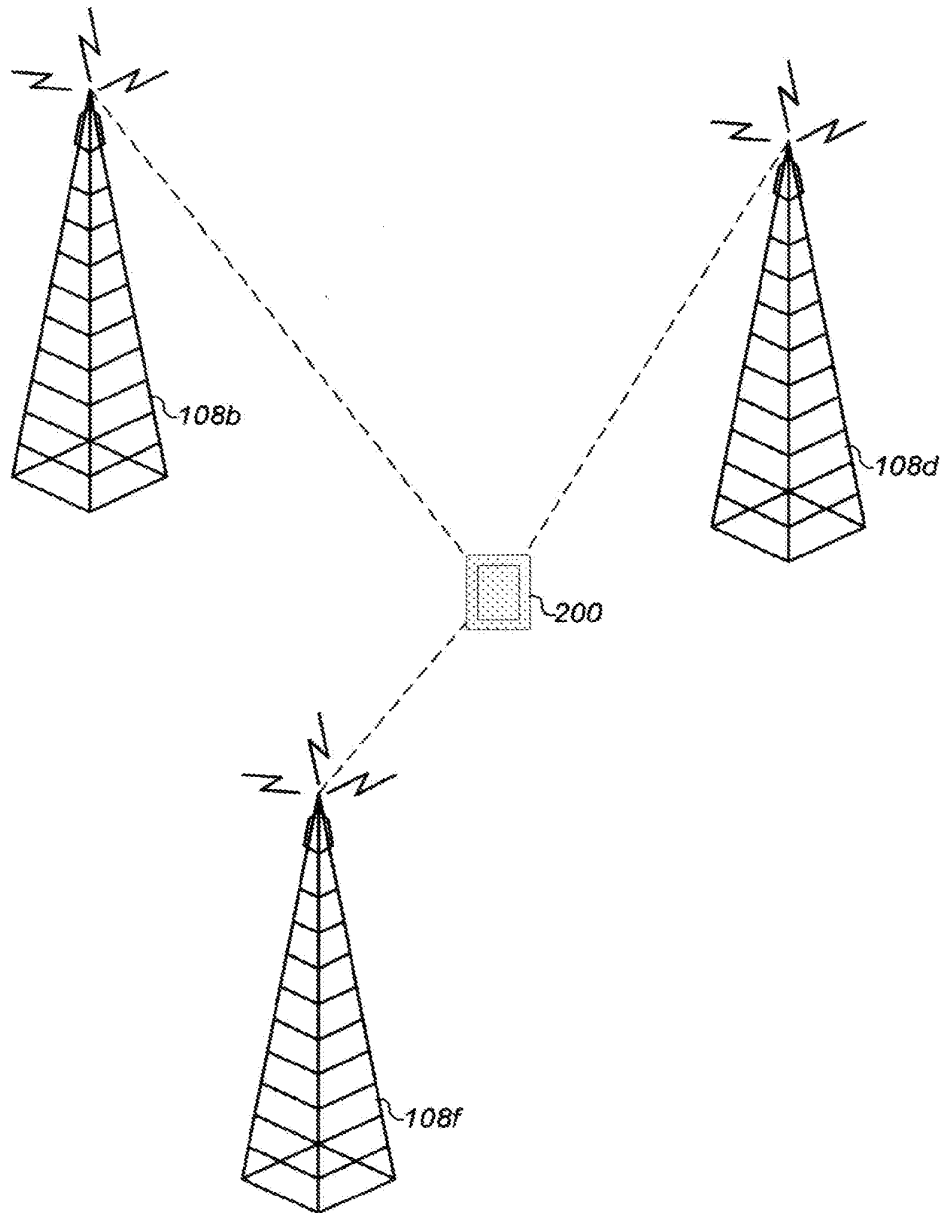


Fig. 3A

13/70

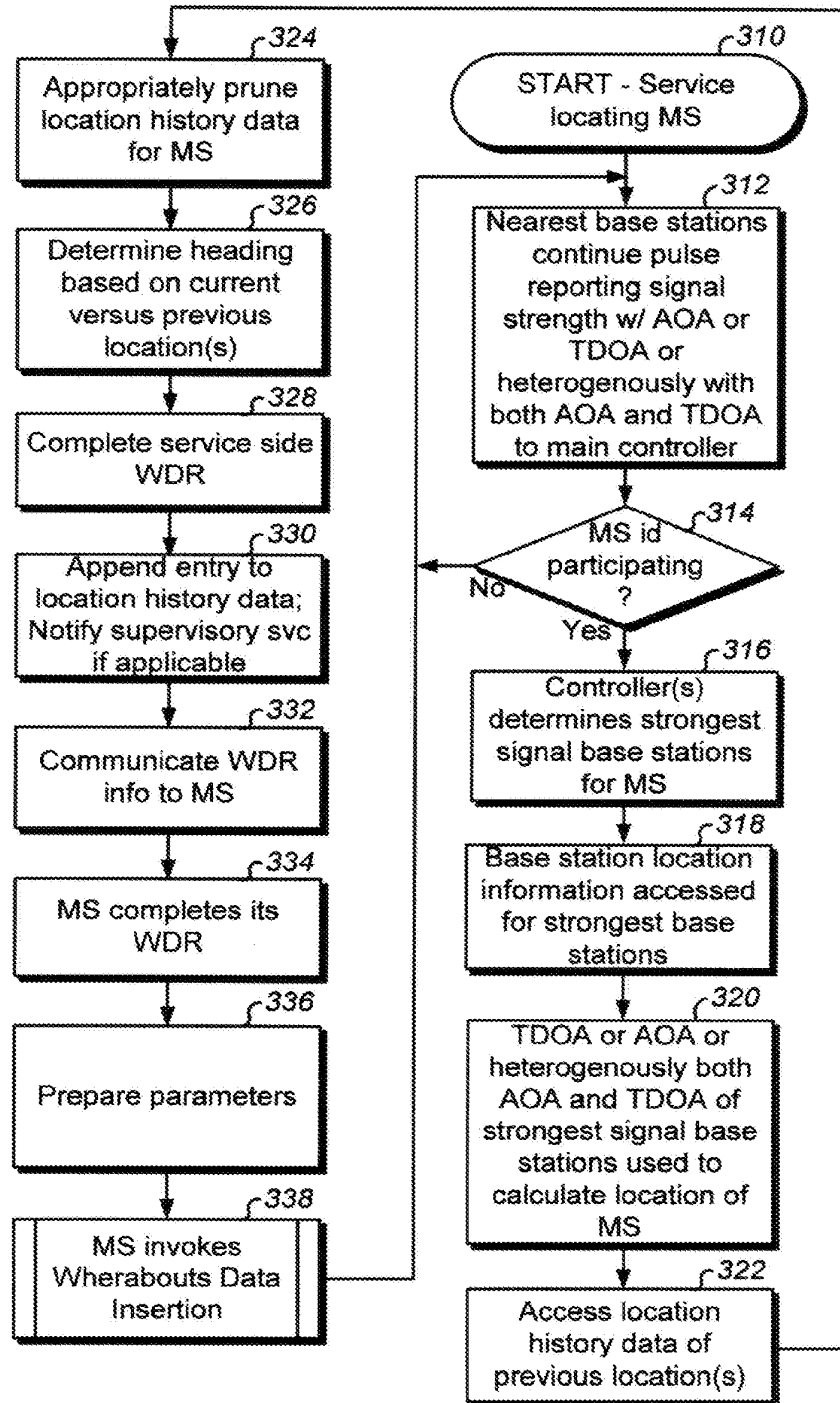


Fig. 3B

14/70

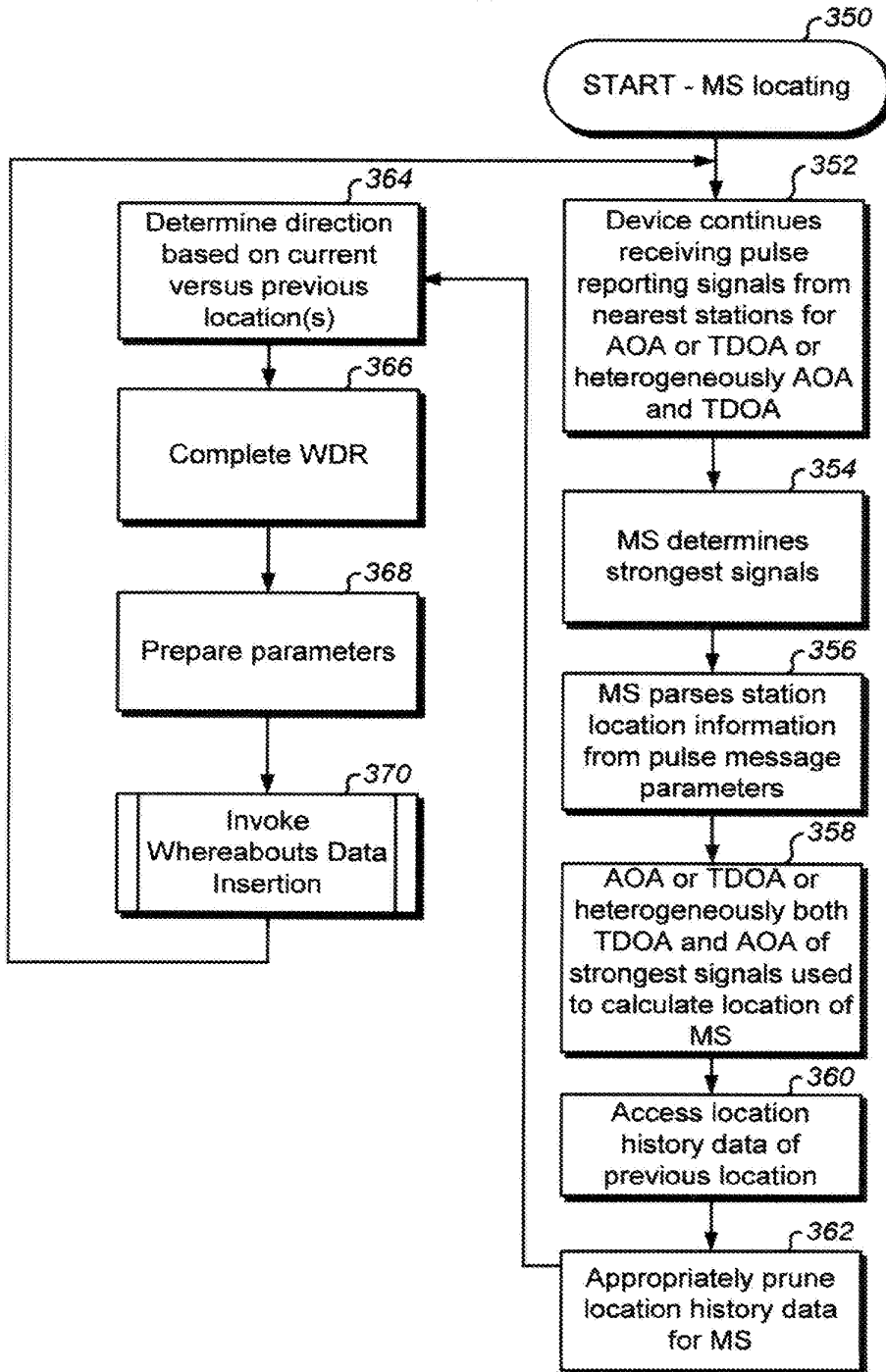


Fig. 3C

15/70

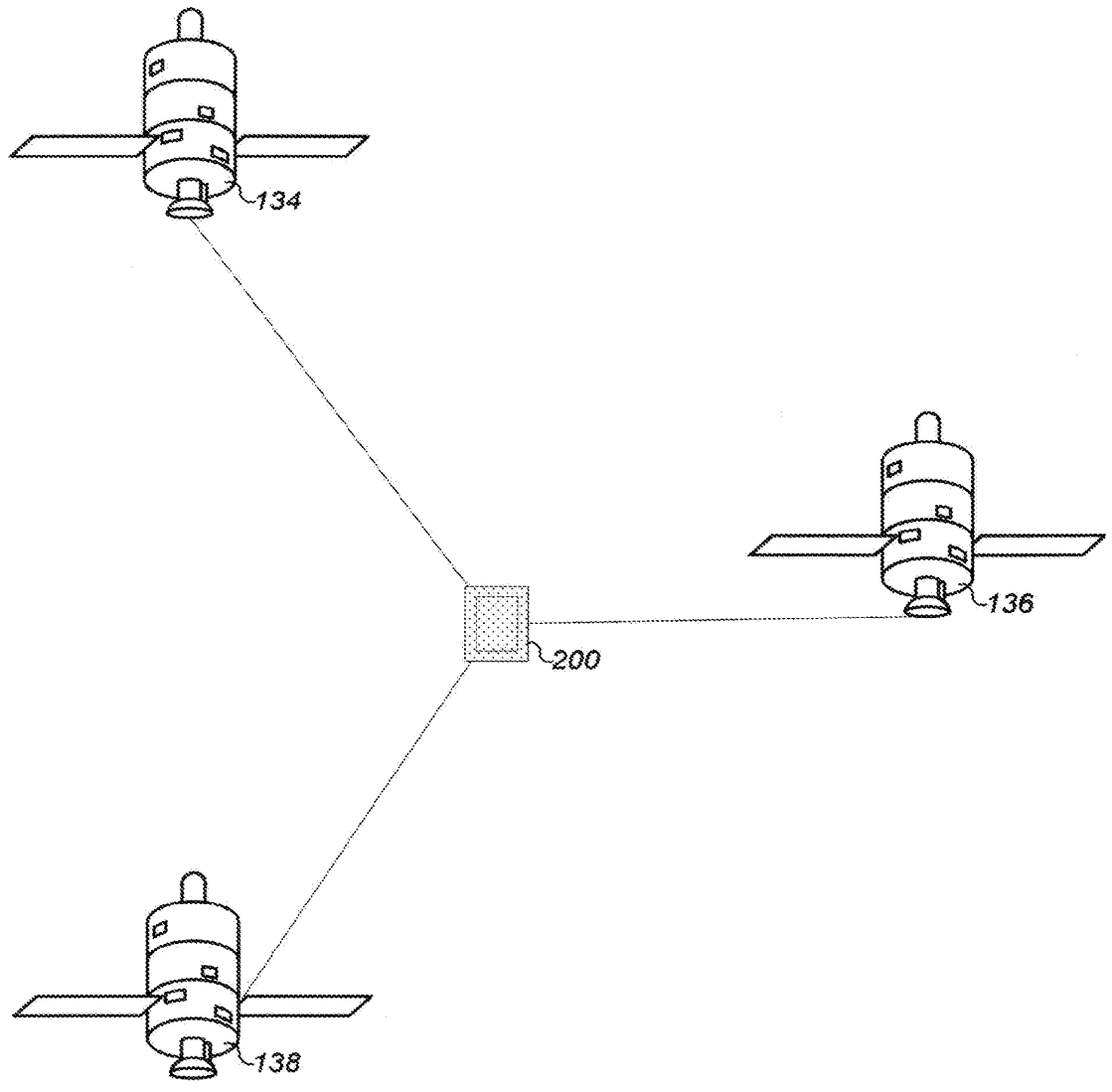


Fig. 4A

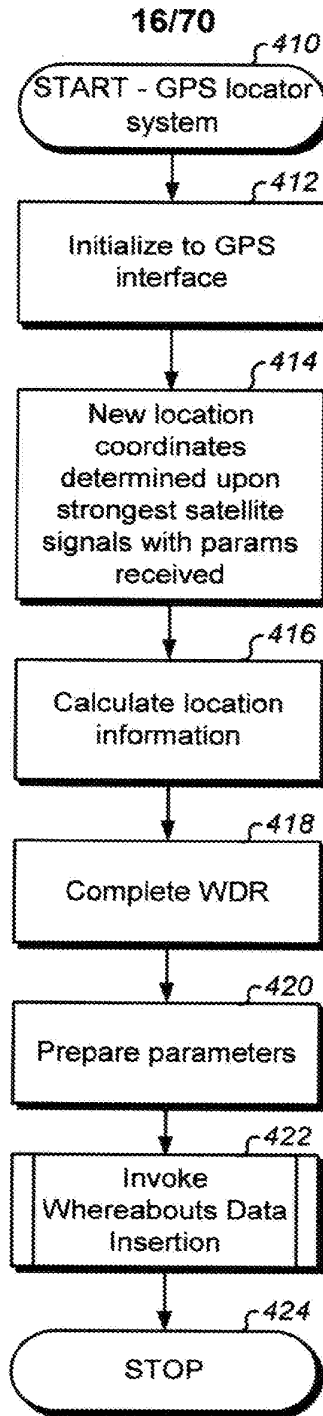


Fig. 4B

17/70

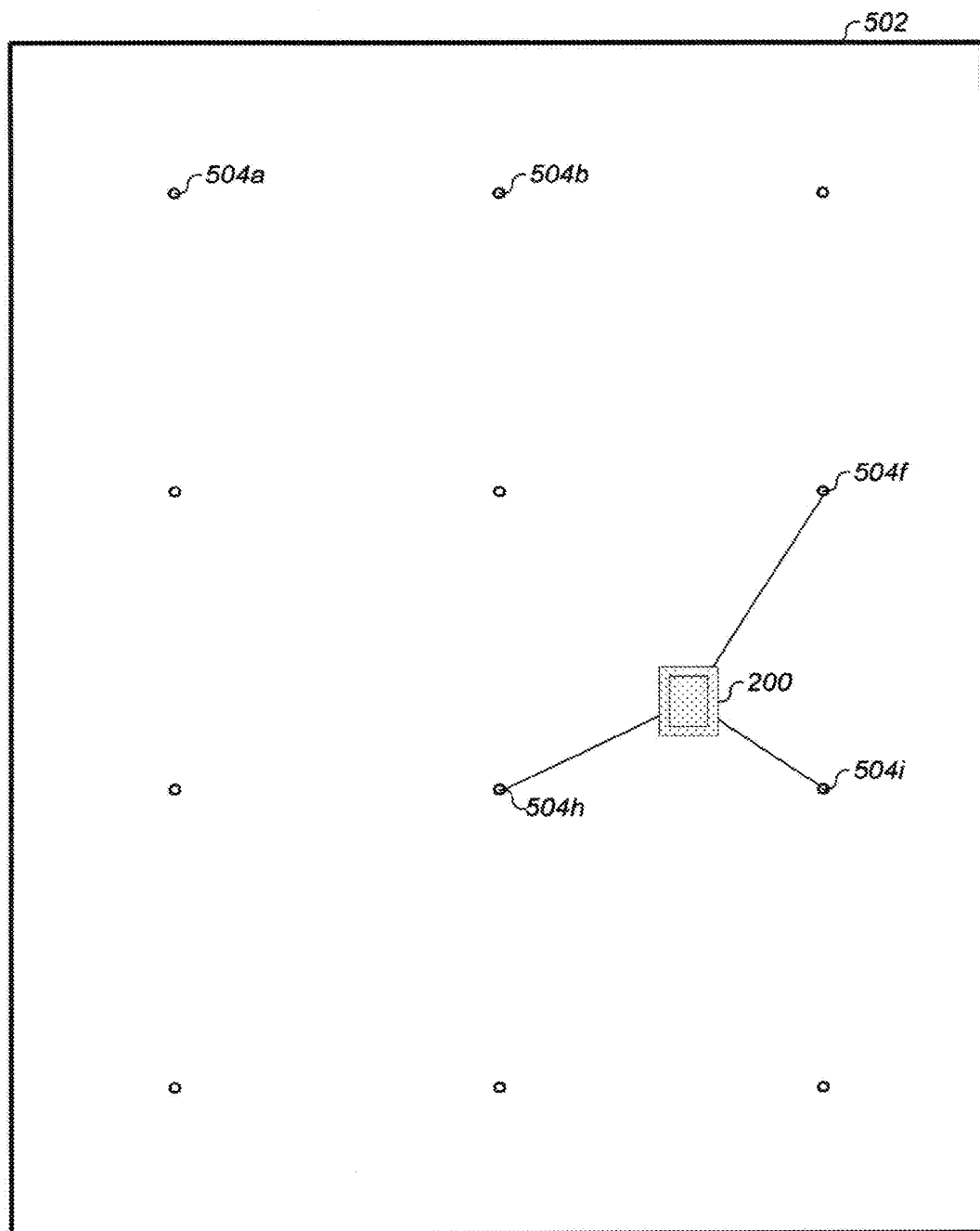


Fig. 5A

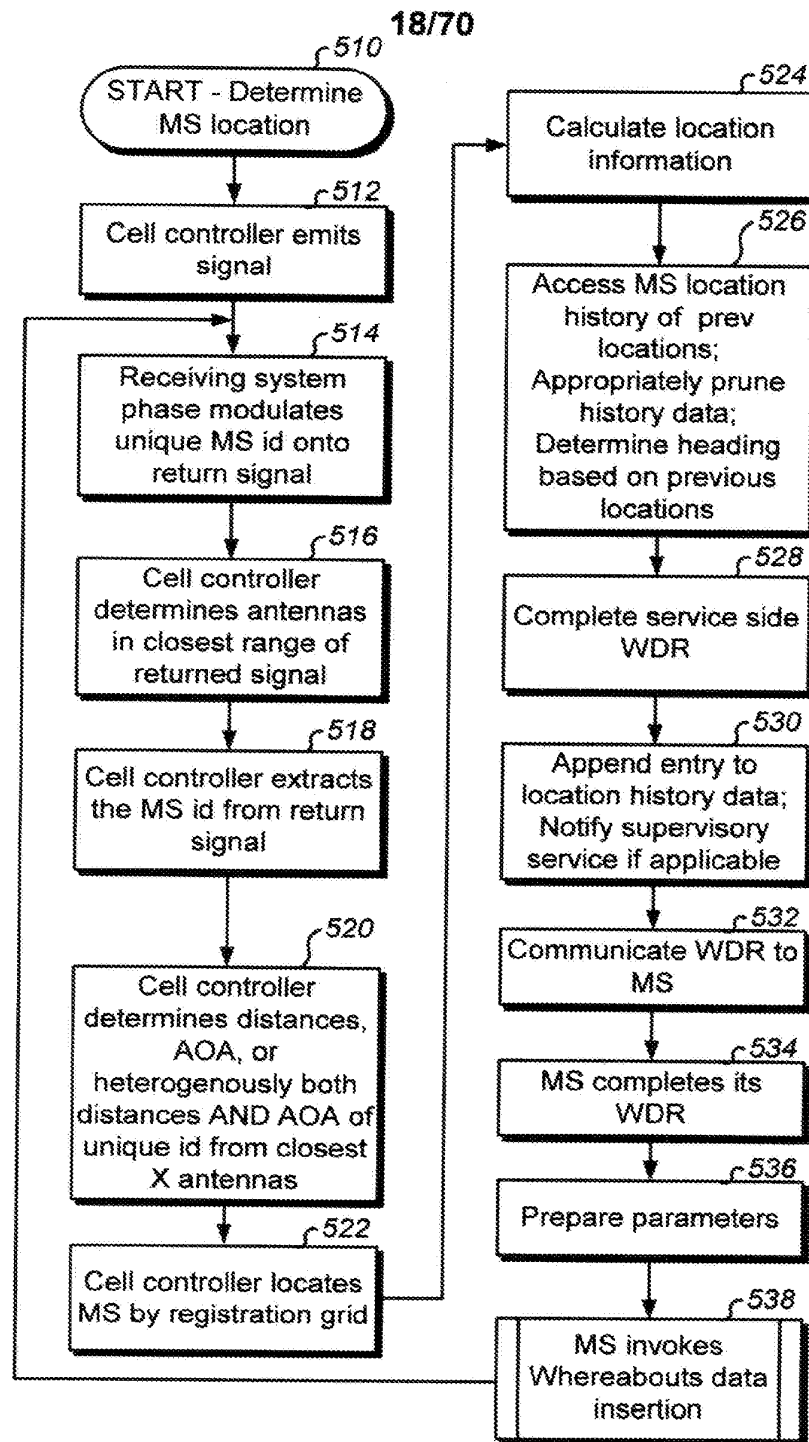


Fig. 5B

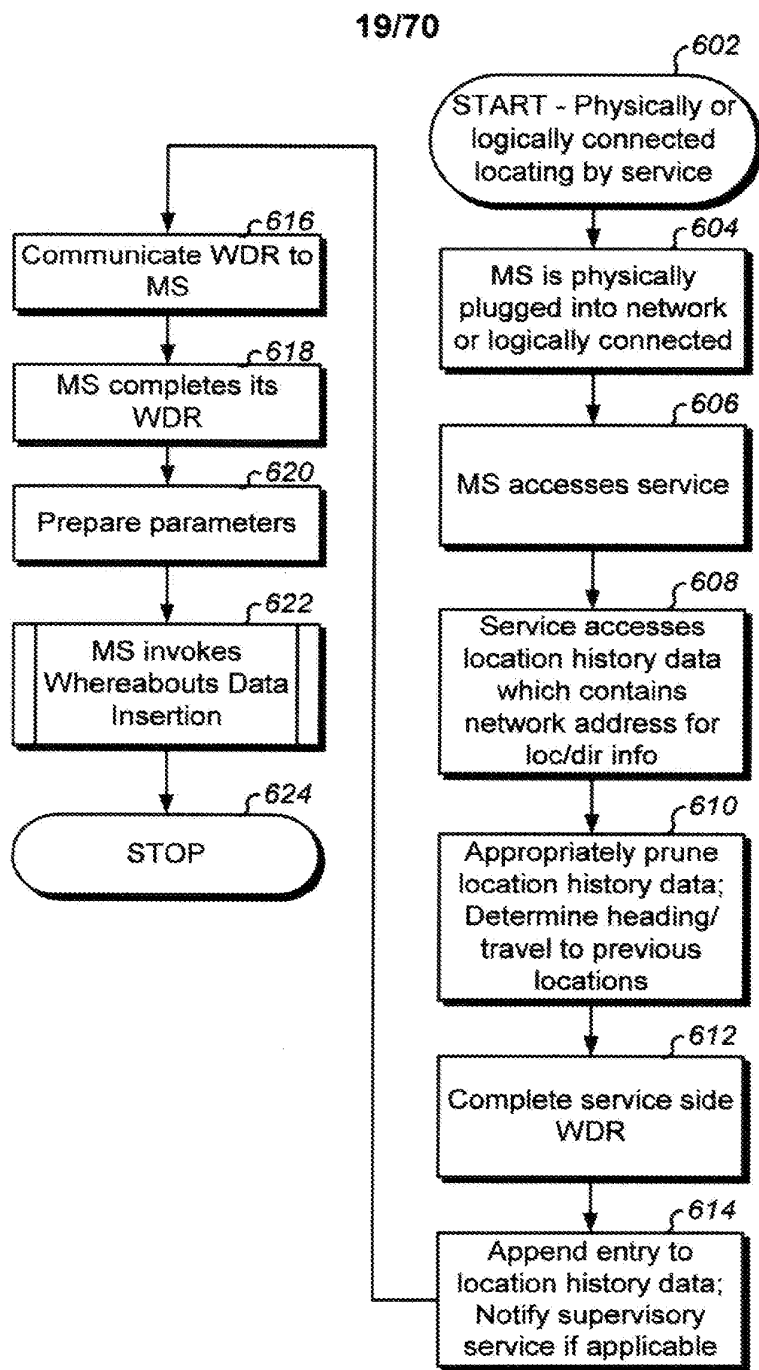


Fig. 6A

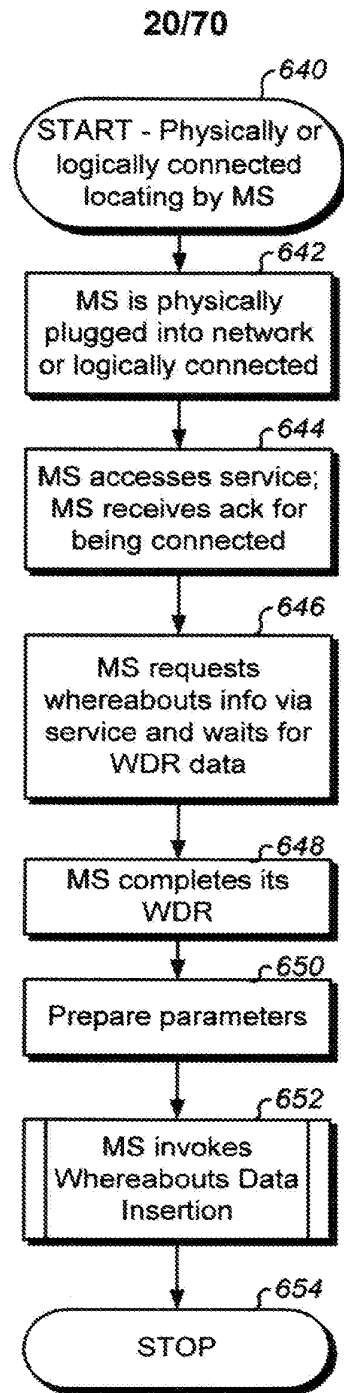


Fig. 6B

21/70

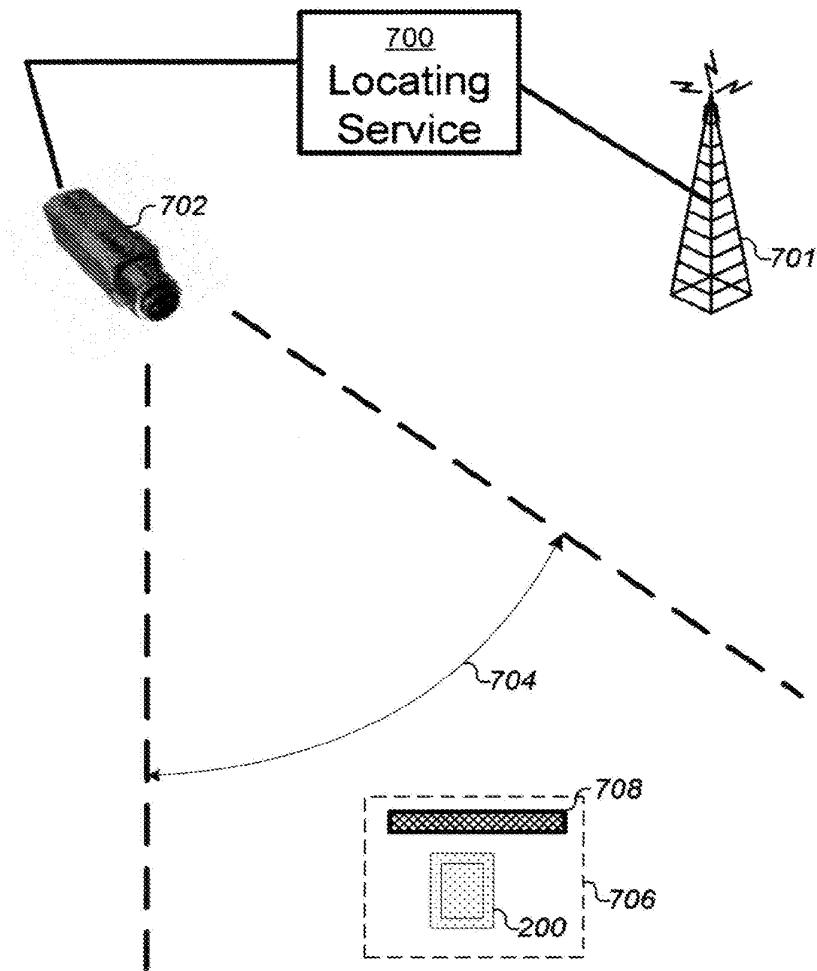


Fig. 7A

22/70

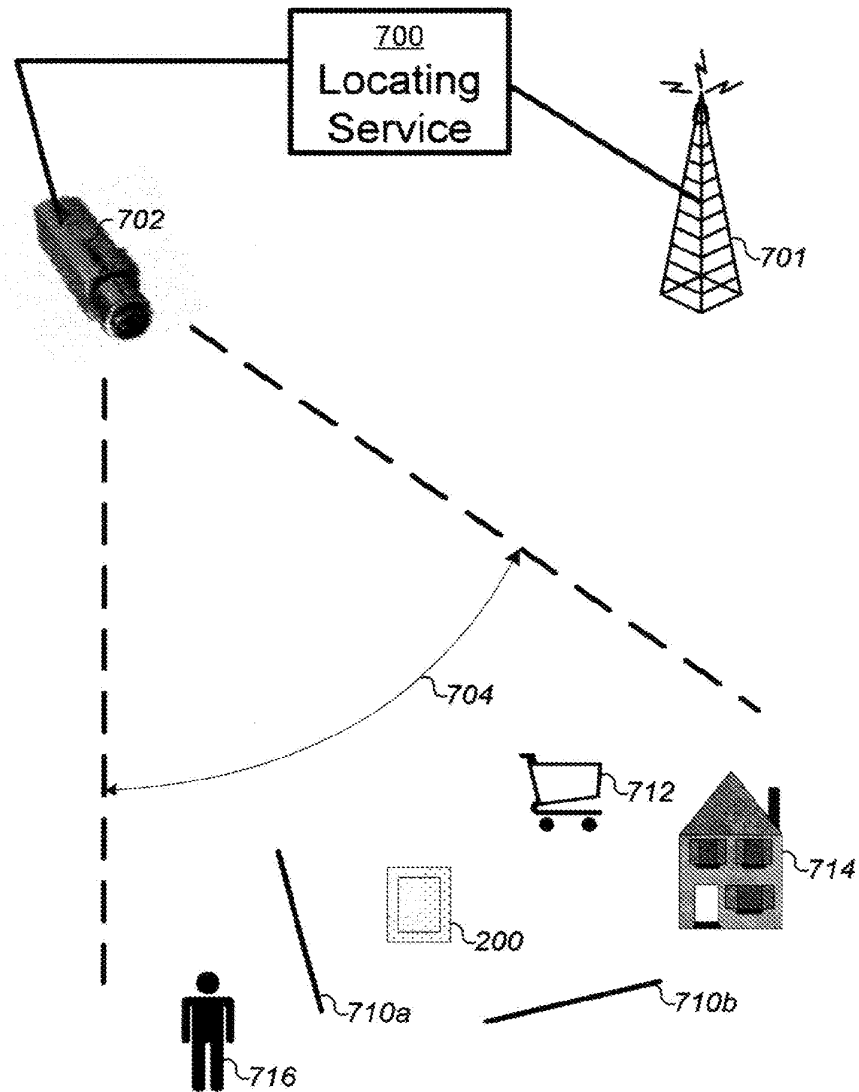


Fig. 7B

23/70

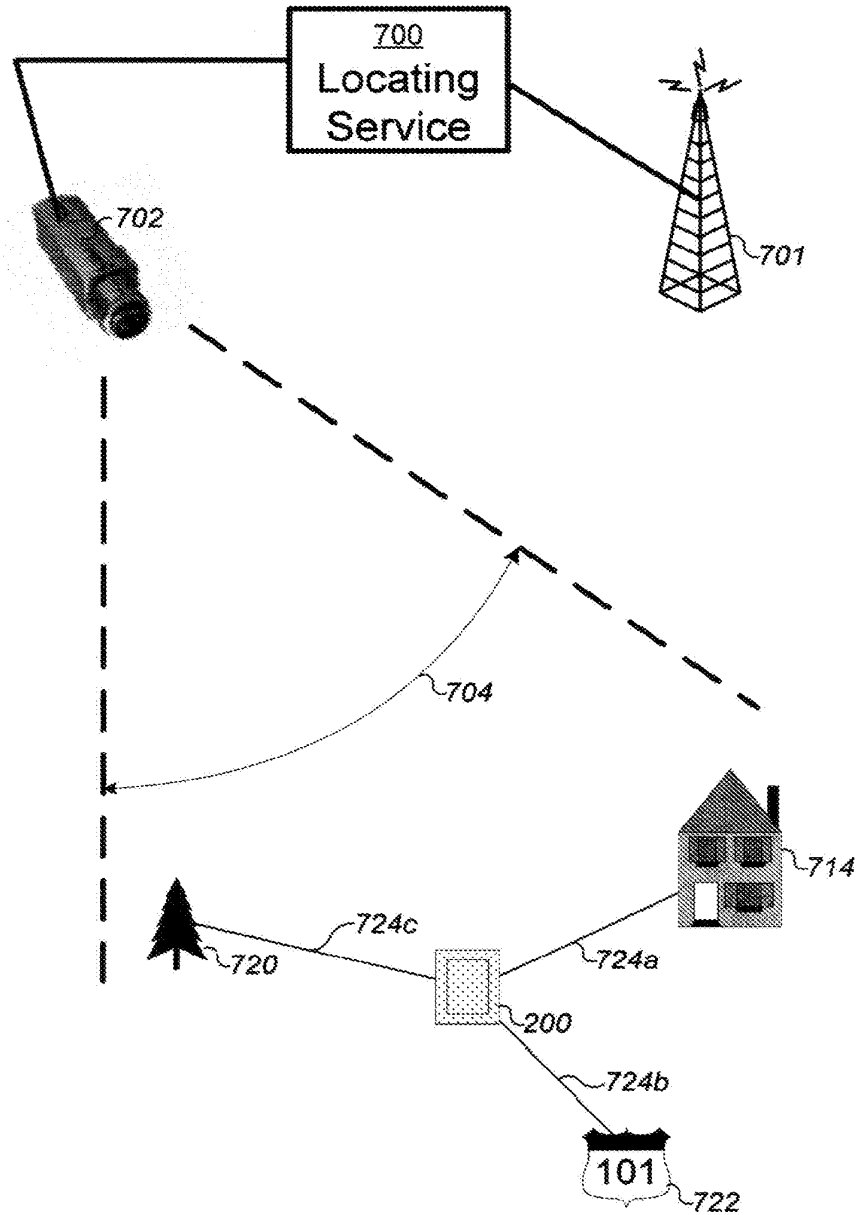


Fig. 7C

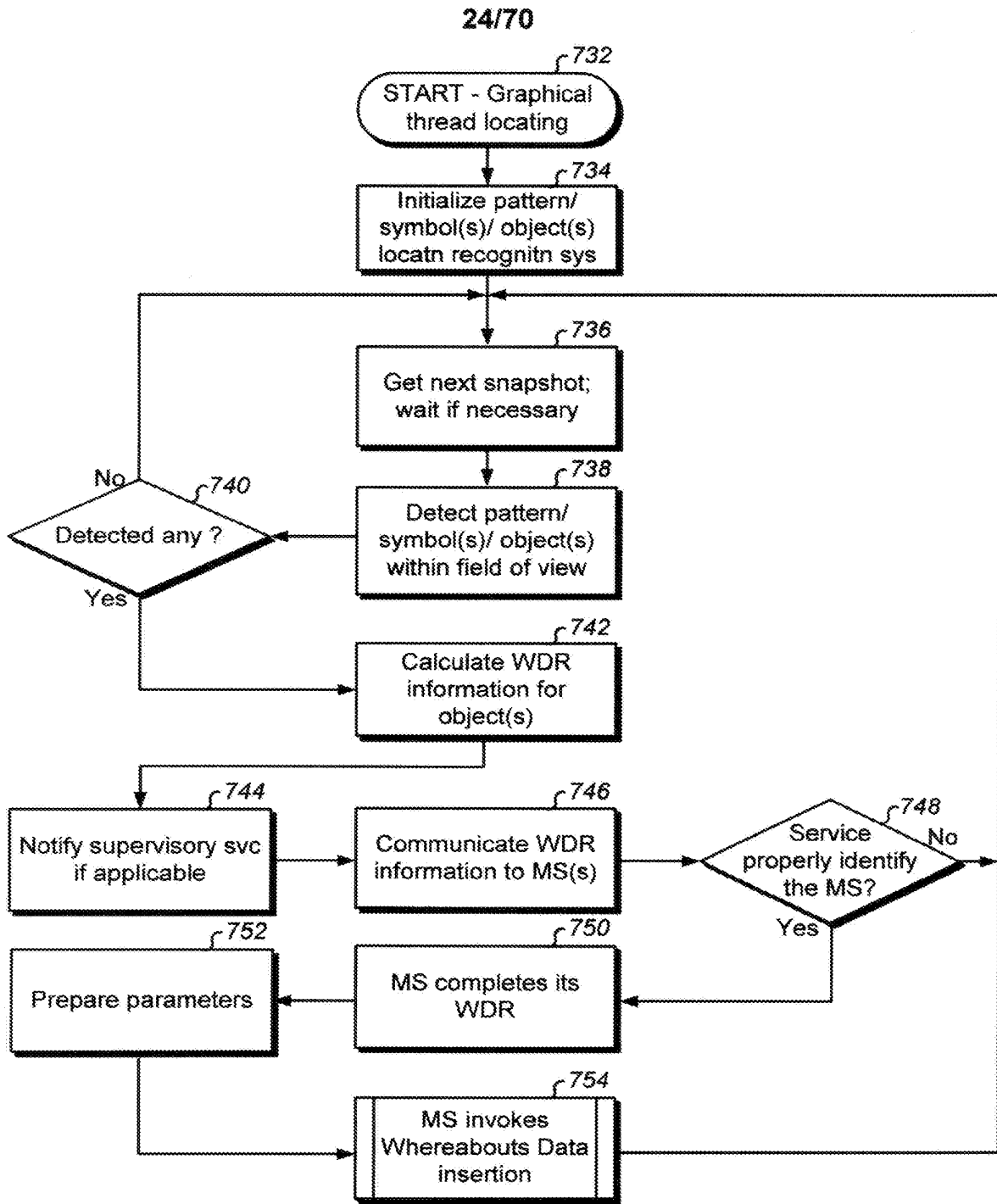


Fig. 7D

25/70

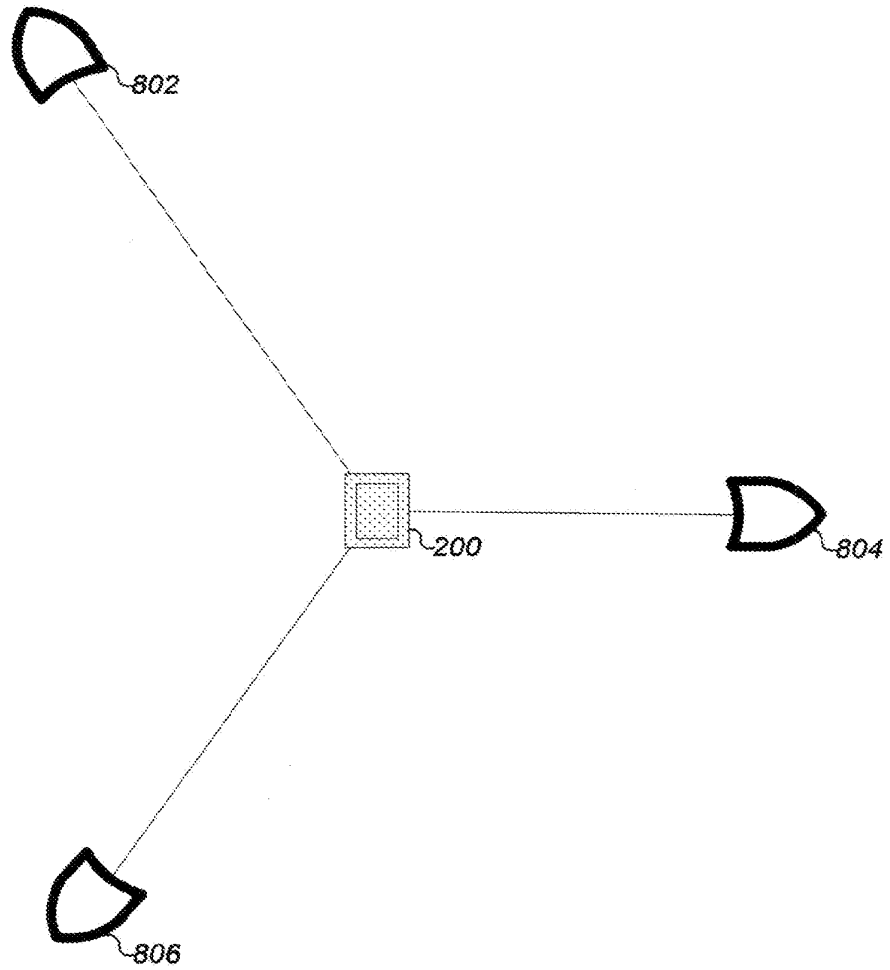


Fig. 8A

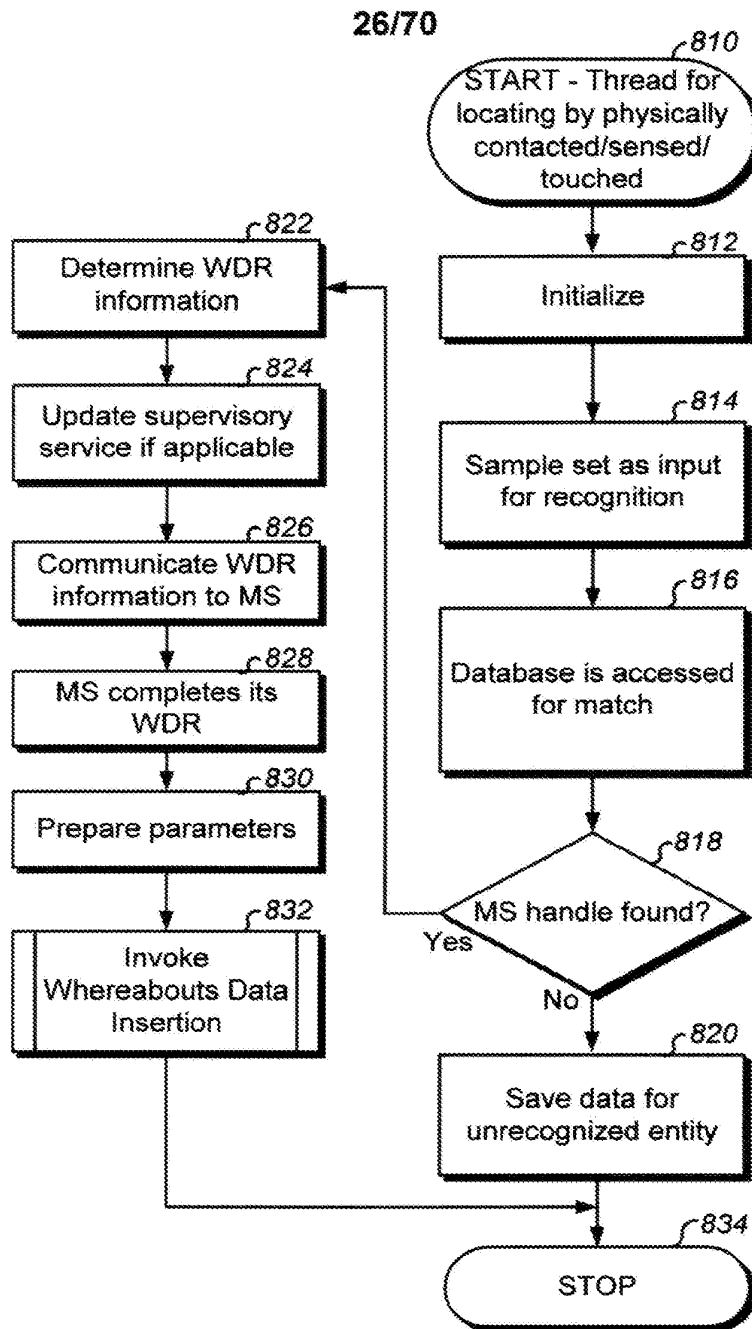


Fig. 8B

27/70

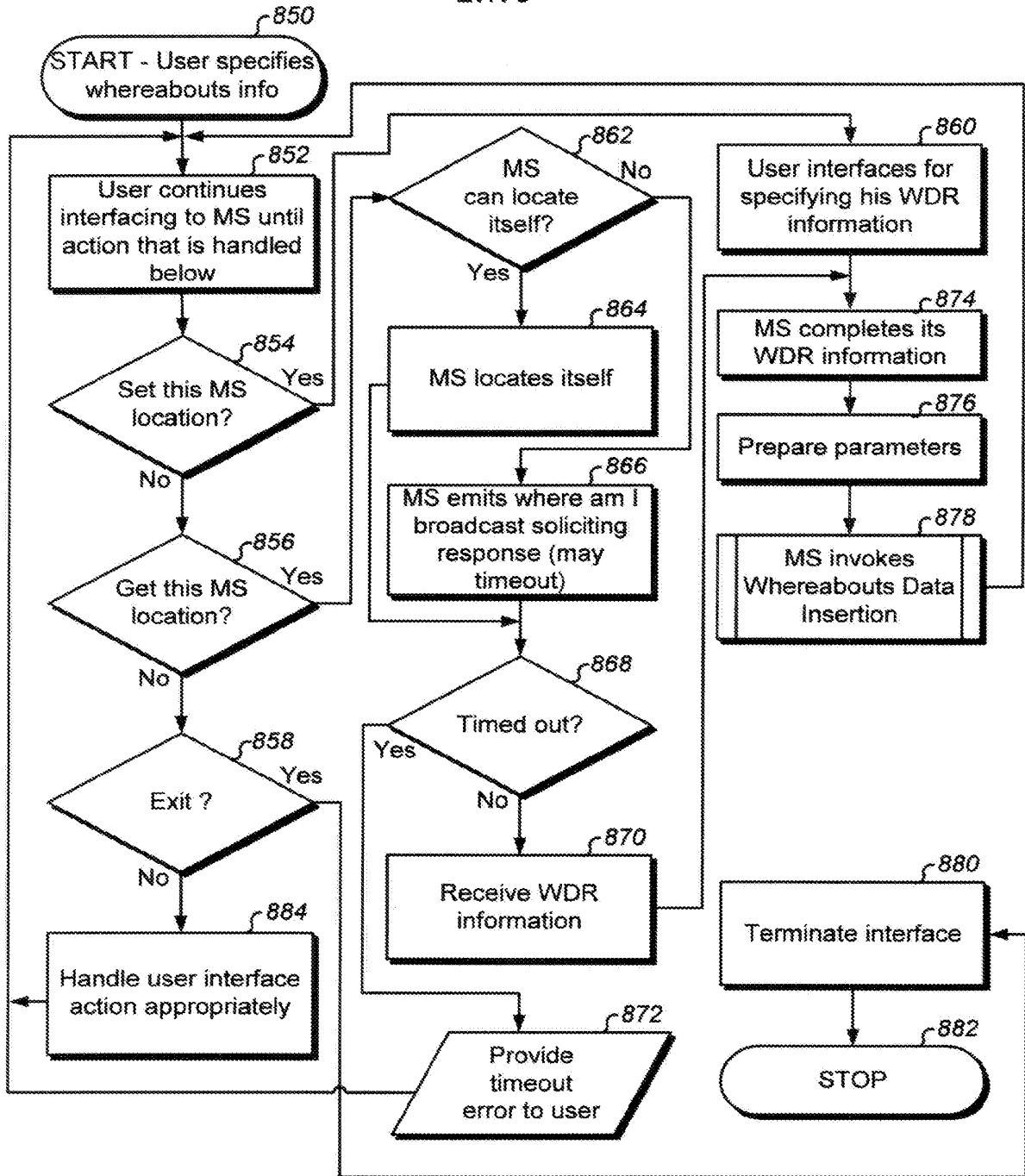


Fig. 8C

28/70

		MS (id 0A12:43EF:985B:012F)
GPS	C	X
A-GPS	C	
D-GPS	C	
Graphic-Pattern(s)	C	
Graphic-Distances	C	
Graphic-Triangulate	C	
Artificial Intelligence	C	
Cell Range	C	X
Cell AOA	C	
Cell TDOA	C	X
Cell MPT	C	X
Antenna Range	C	X
Antenna AOA	C	X
Antenna TDOA	C	X
Antenna MPT	C	X
LIDAR/optics	C	
Manual	C	
Contact	C	X
MPT	C	X
Client Logical Connect	C	
Server Logical Connect	C	
Client Physical Connect	C	
Server Physical Connect	C	
Sound/Acoustics	C	
Microdot/ RFI	C	
Transponder	C	
Others	C	
...	C	

Fig. 9A

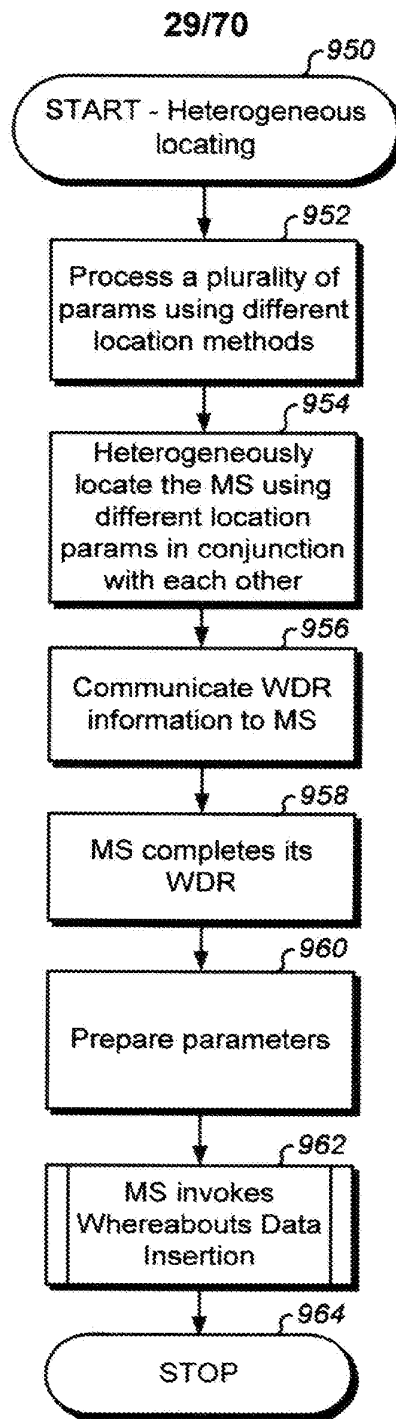


Fig. 9B

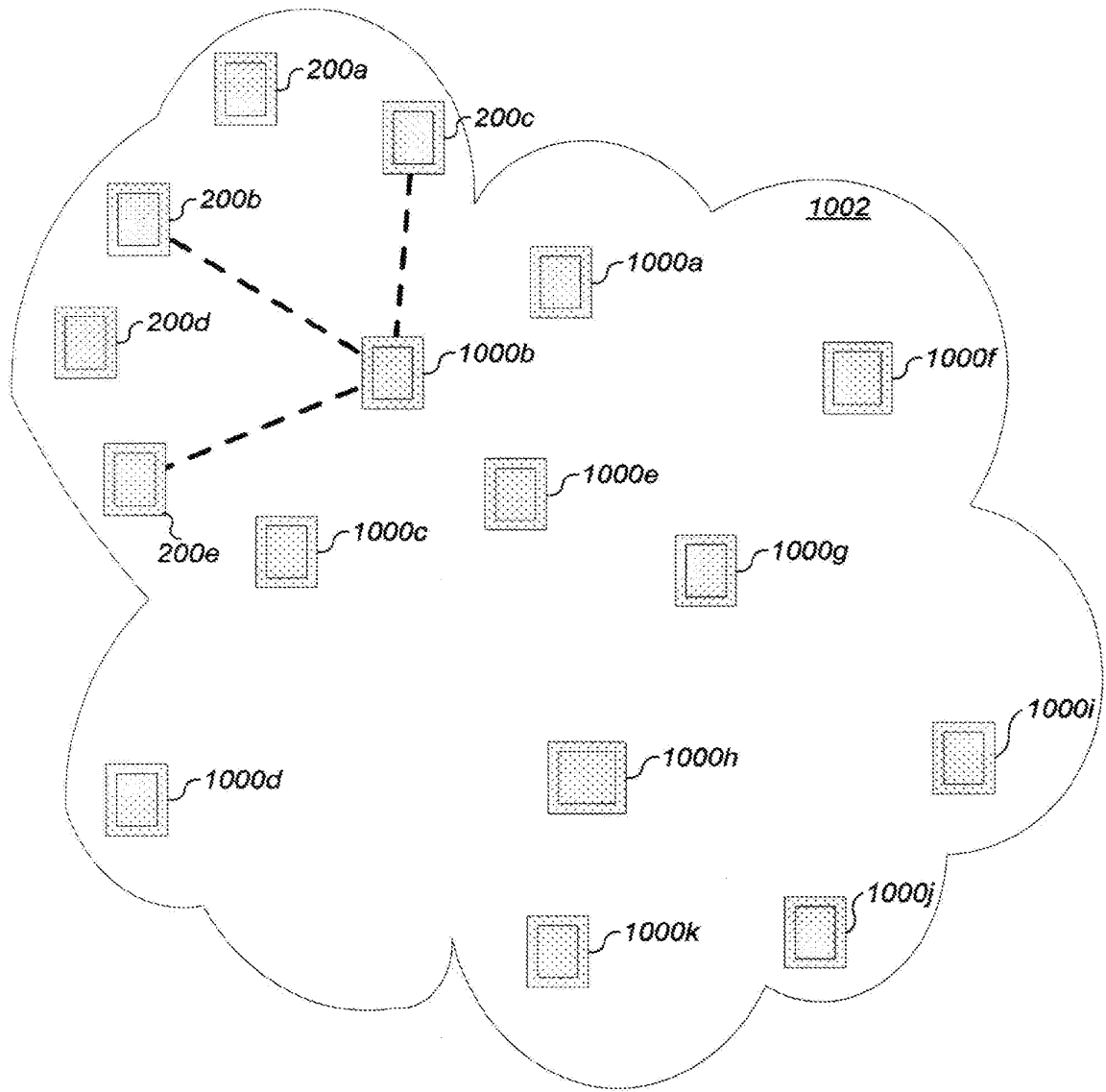


Fig. 10A

31/70

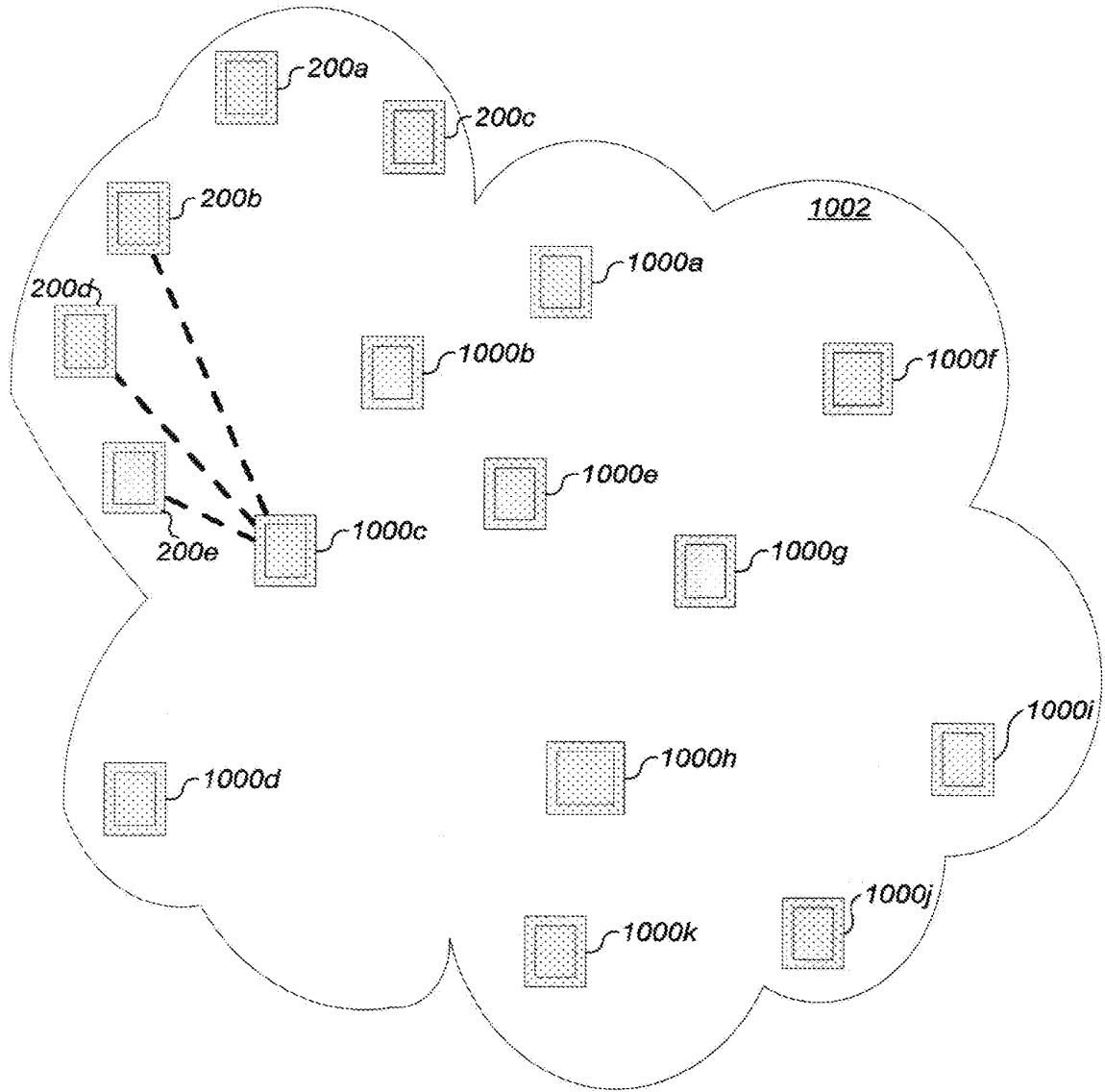


Fig. 10B

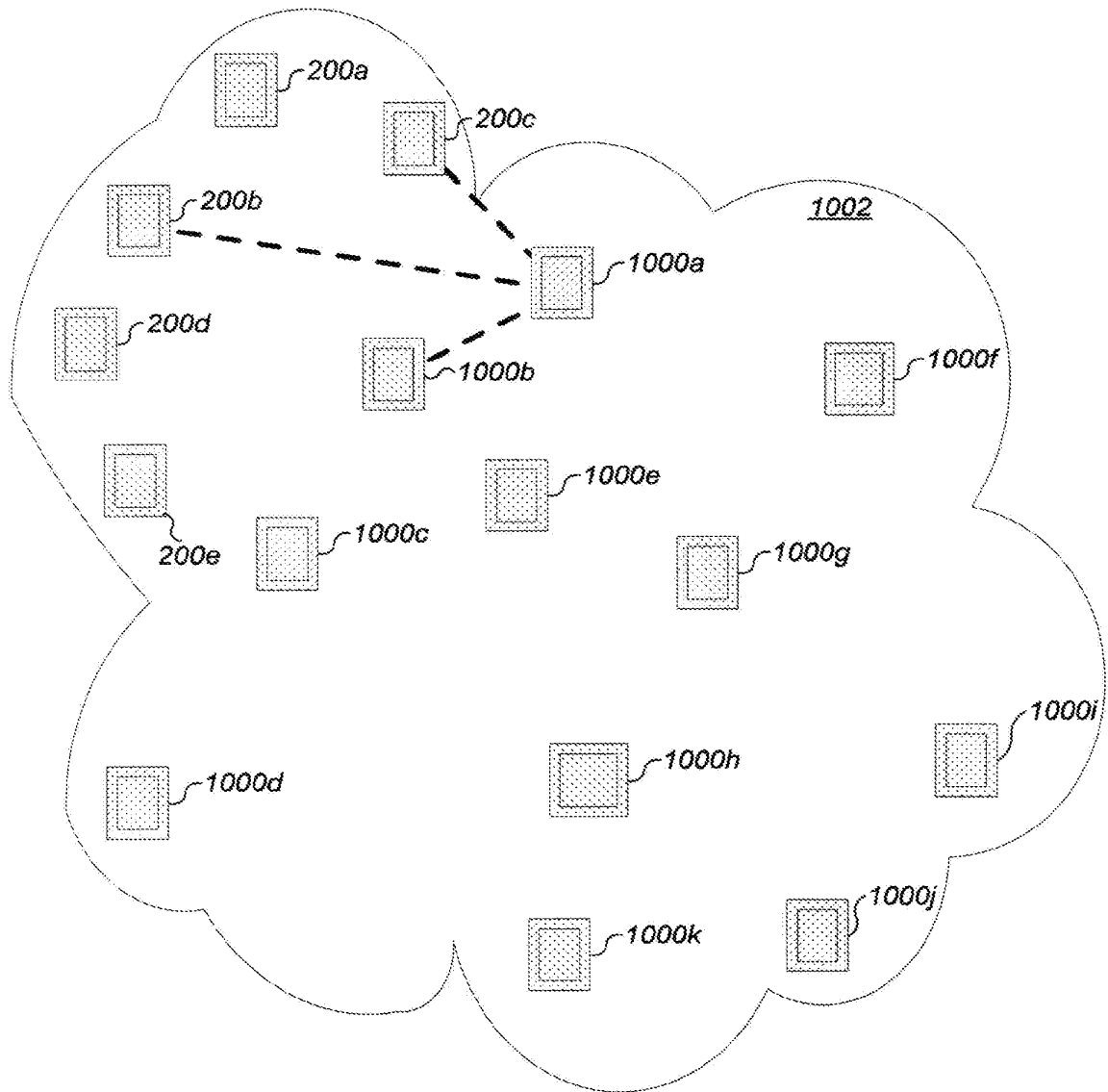


Fig. 10C

33/70

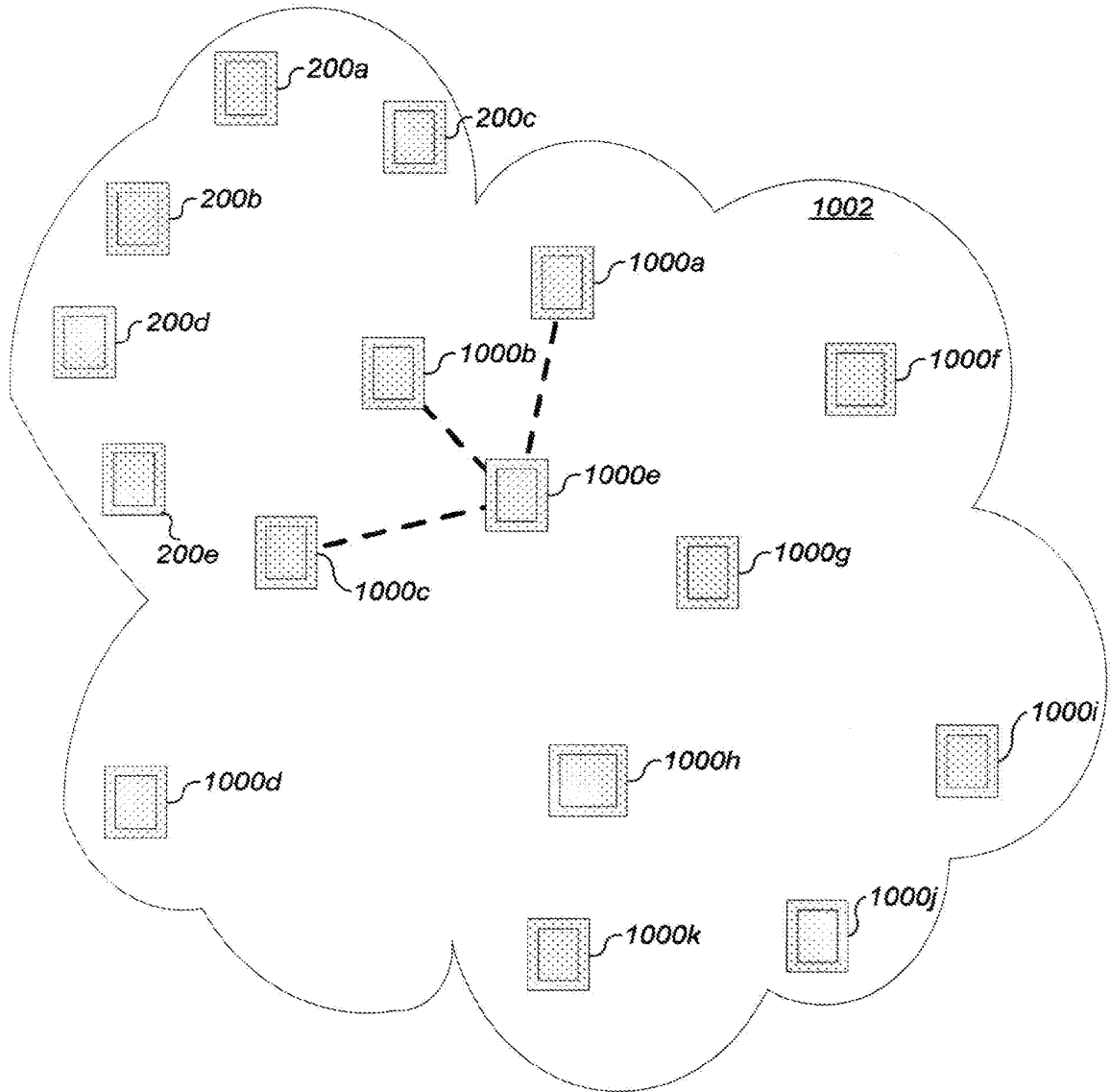


Fig. 10D

34/70

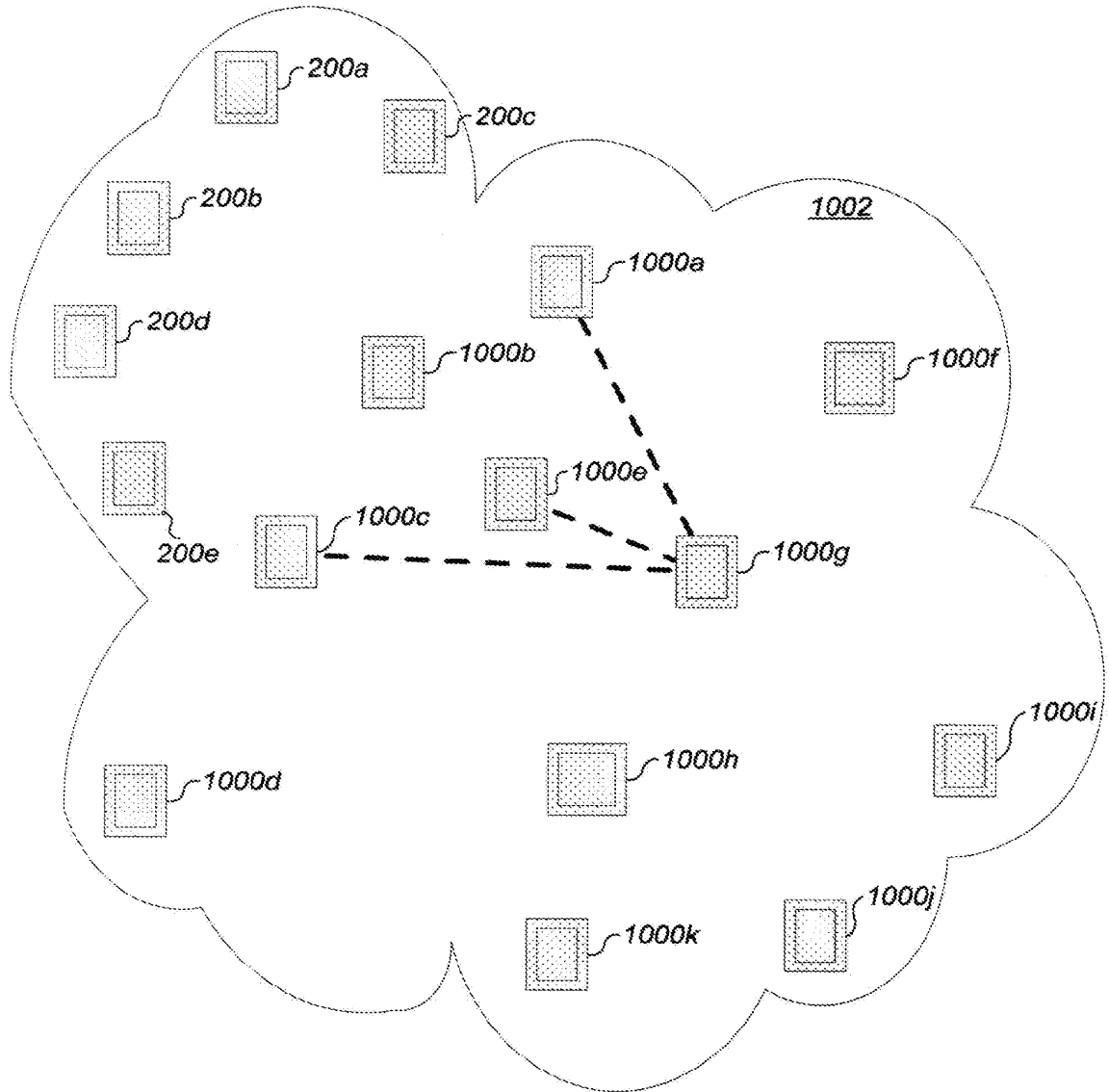


Fig. 10E

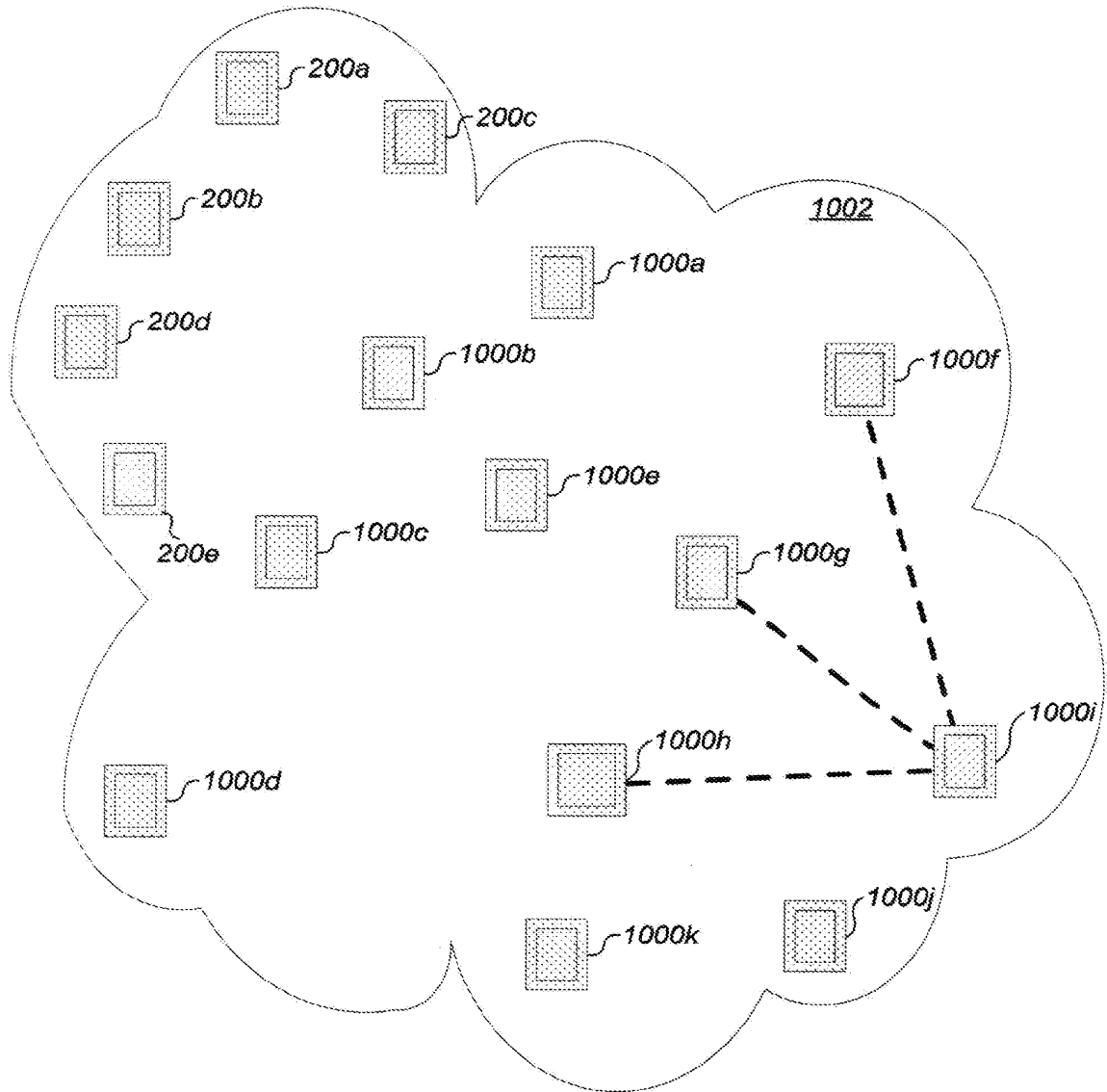


Fig. 10F

36/70

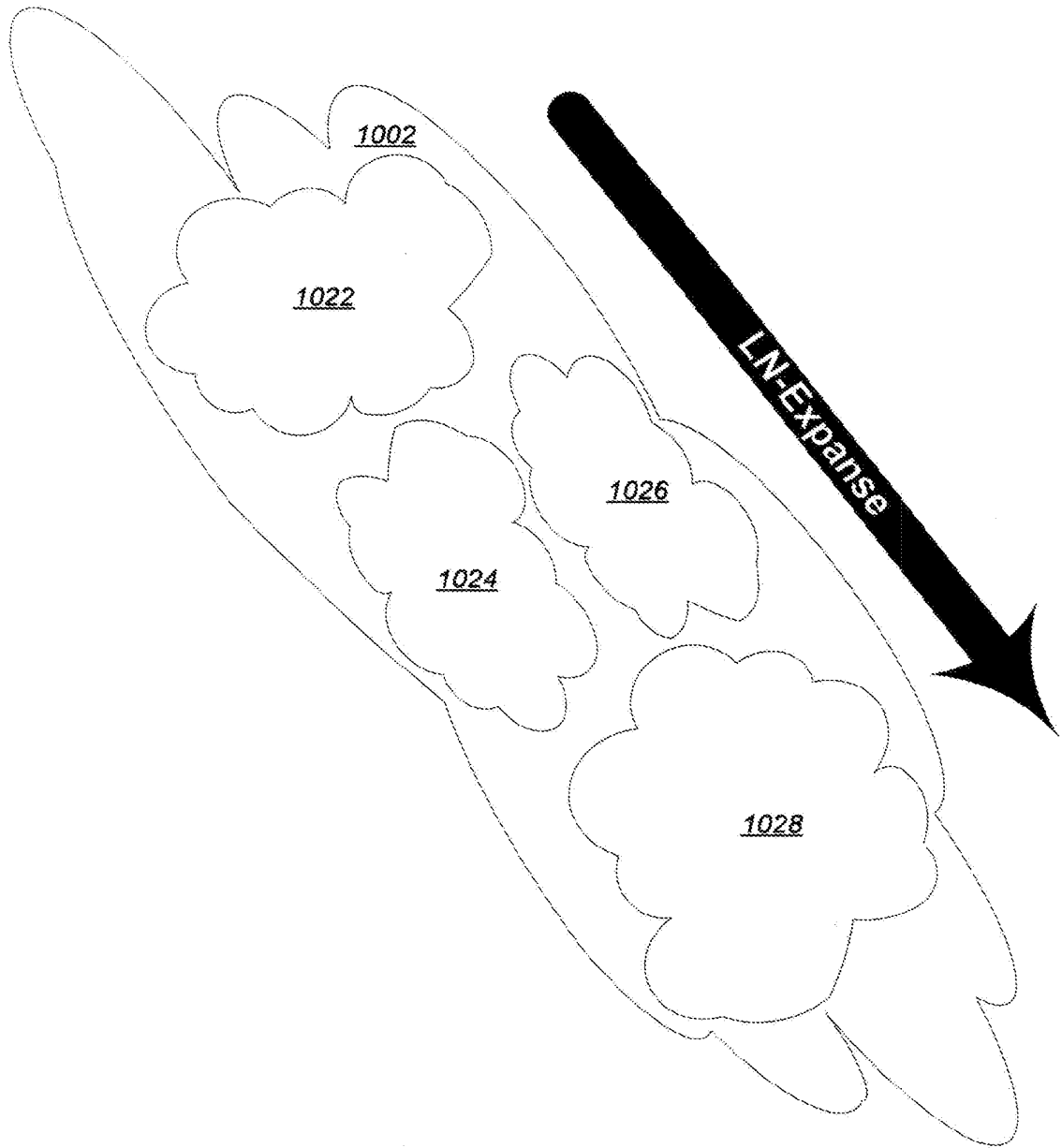


Fig. 10G

37/70

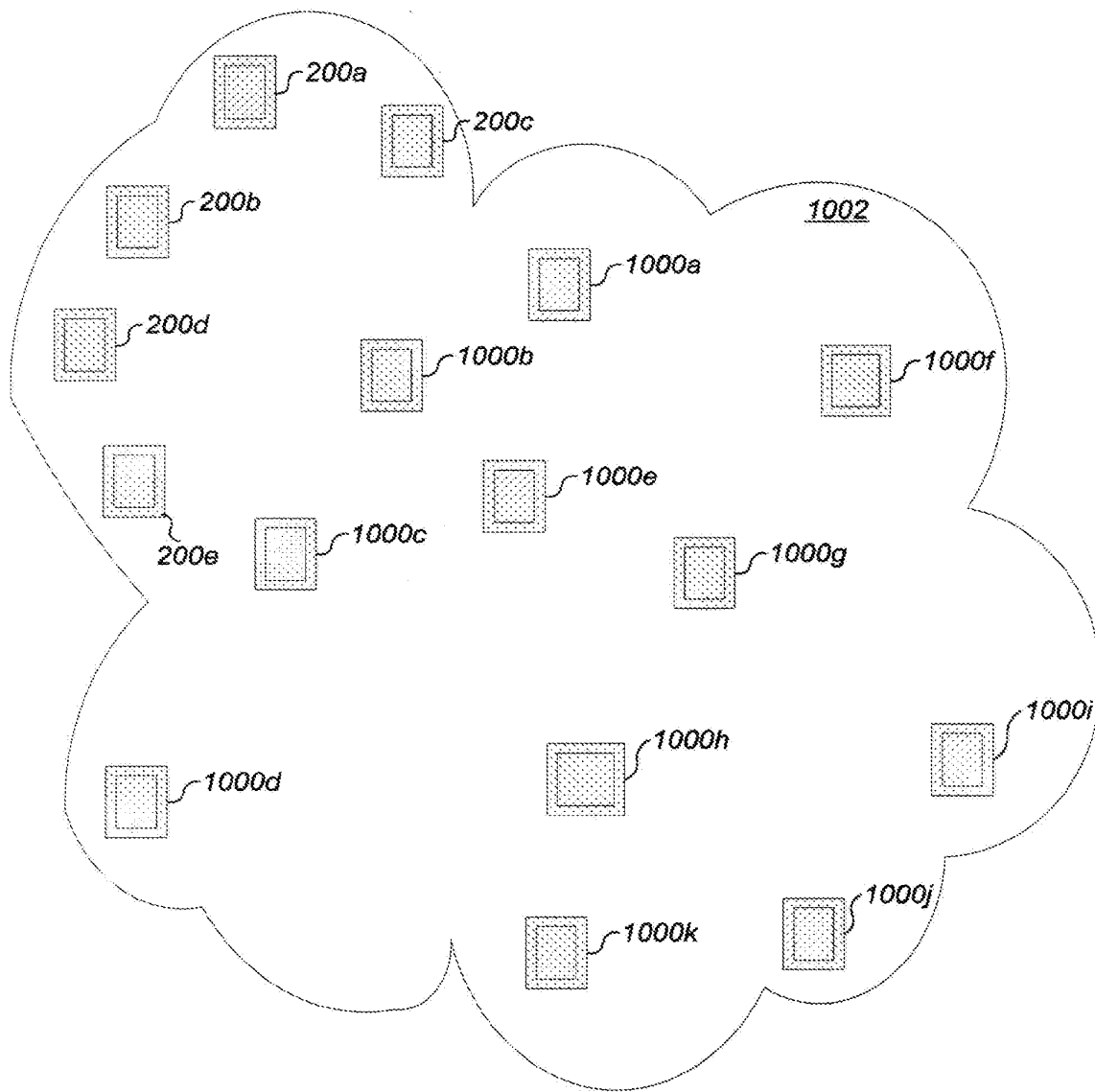


Fig. 10H

38/70

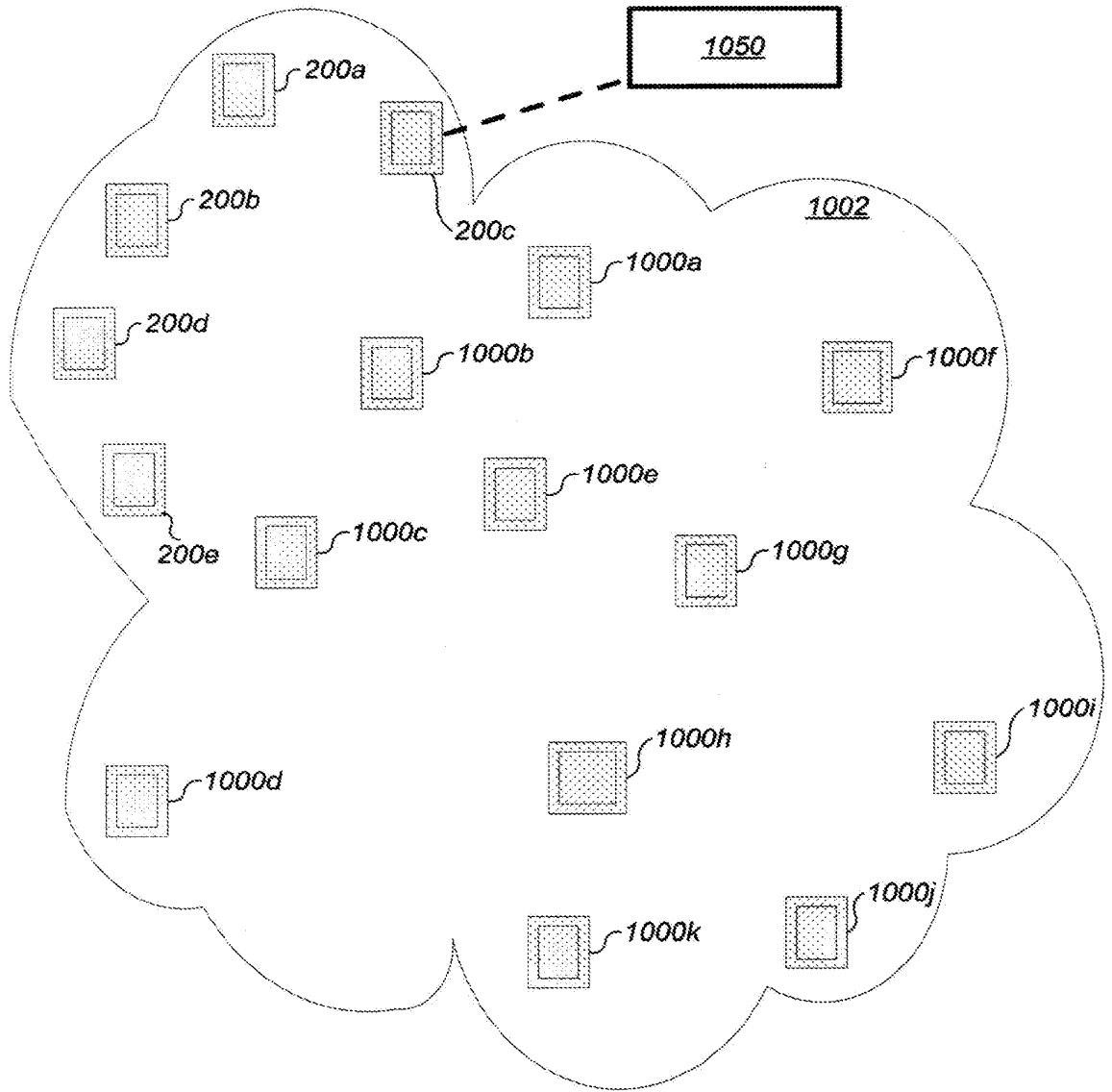


Fig. 10I

39/70

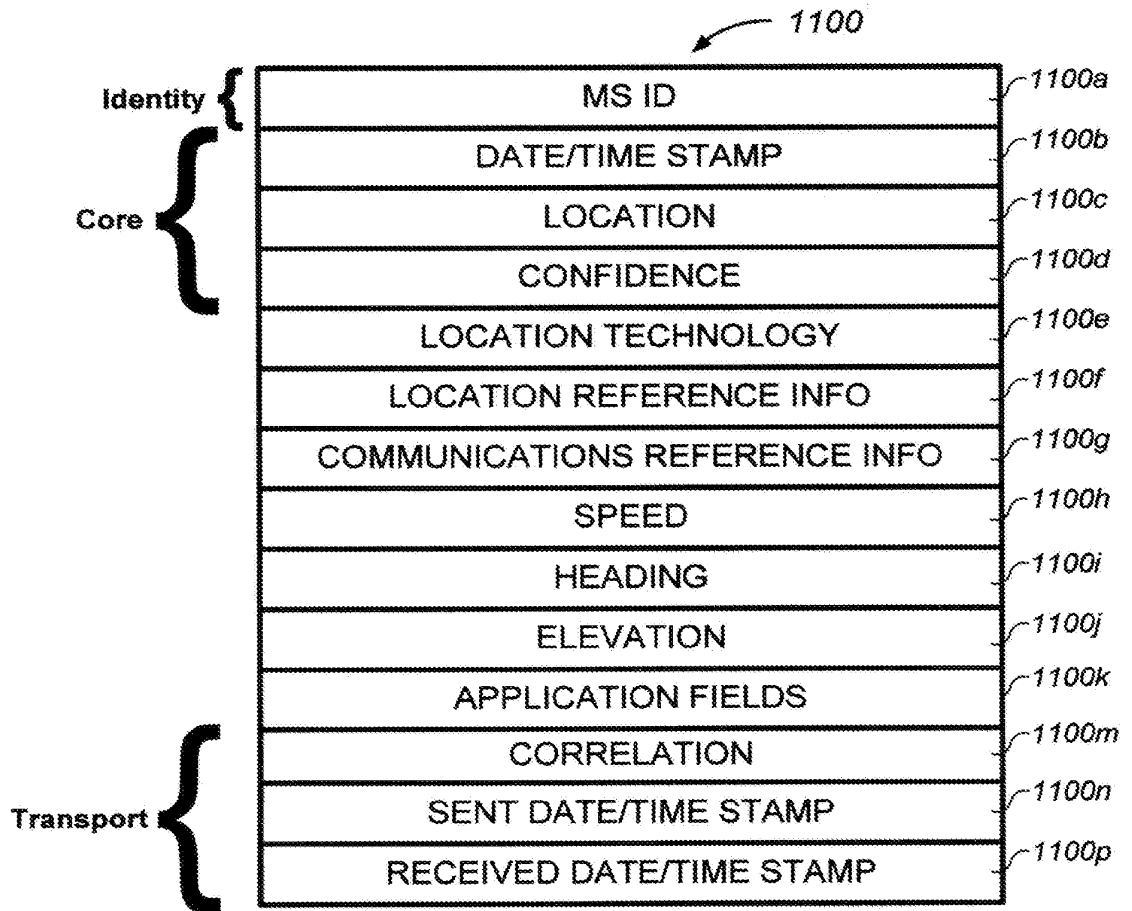


Fig. 11A

40/70

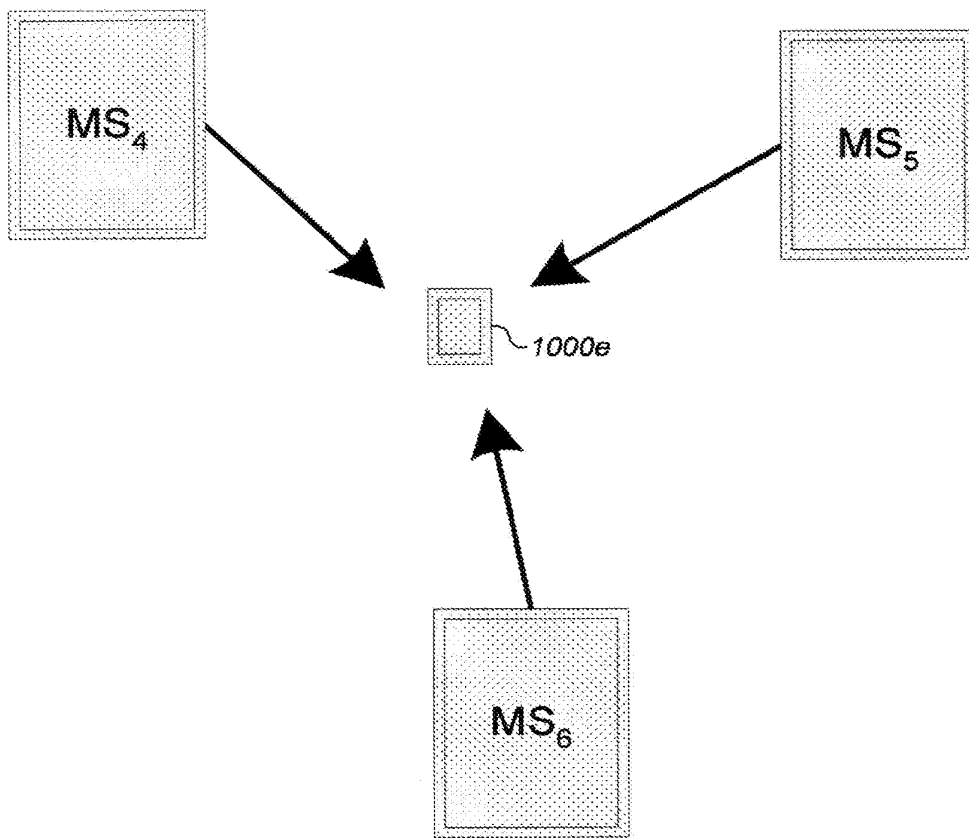


Fig. 11B

41/70

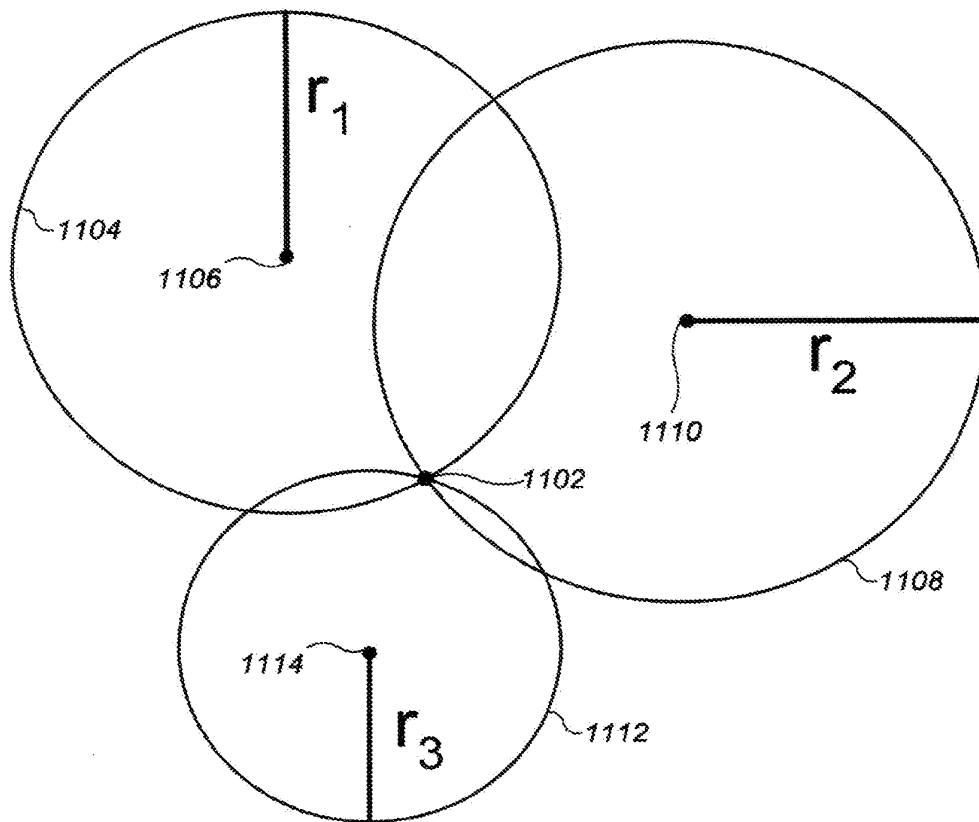


Fig. 11C

42/70

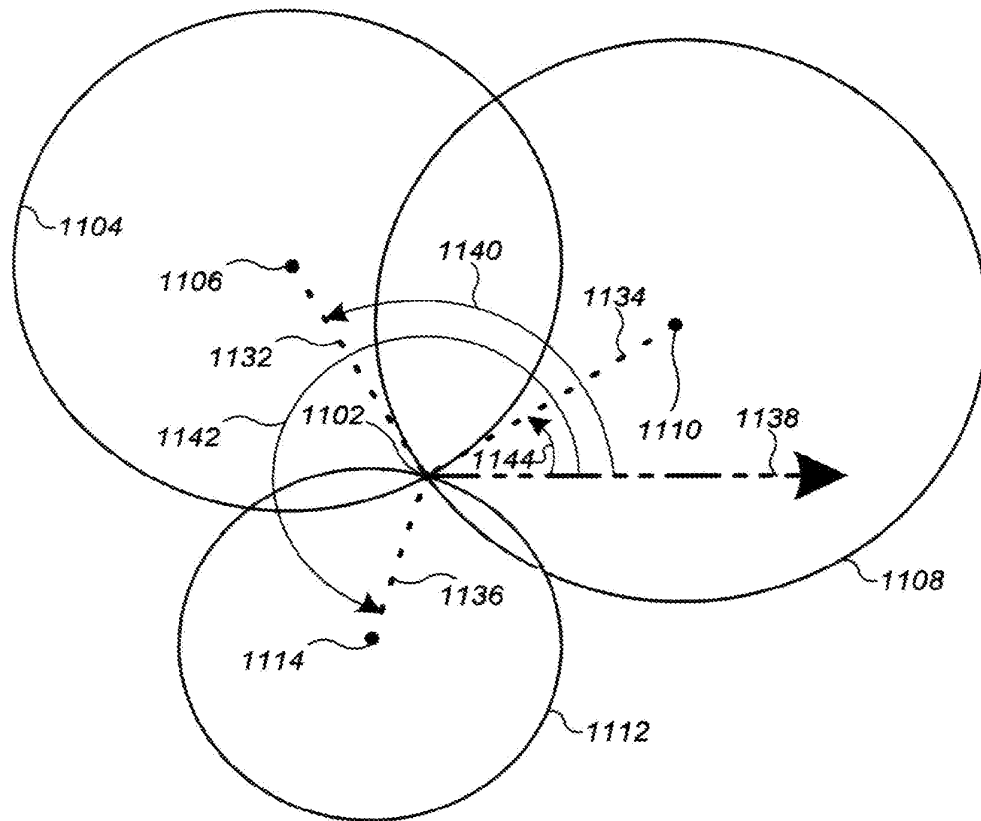


Fig. 11D

43/70

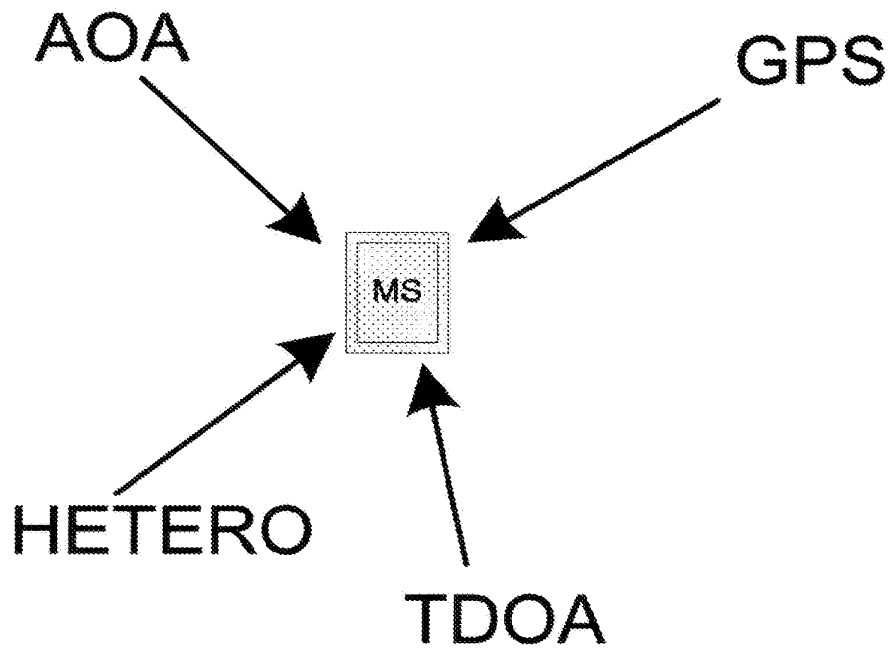


Fig. 11E

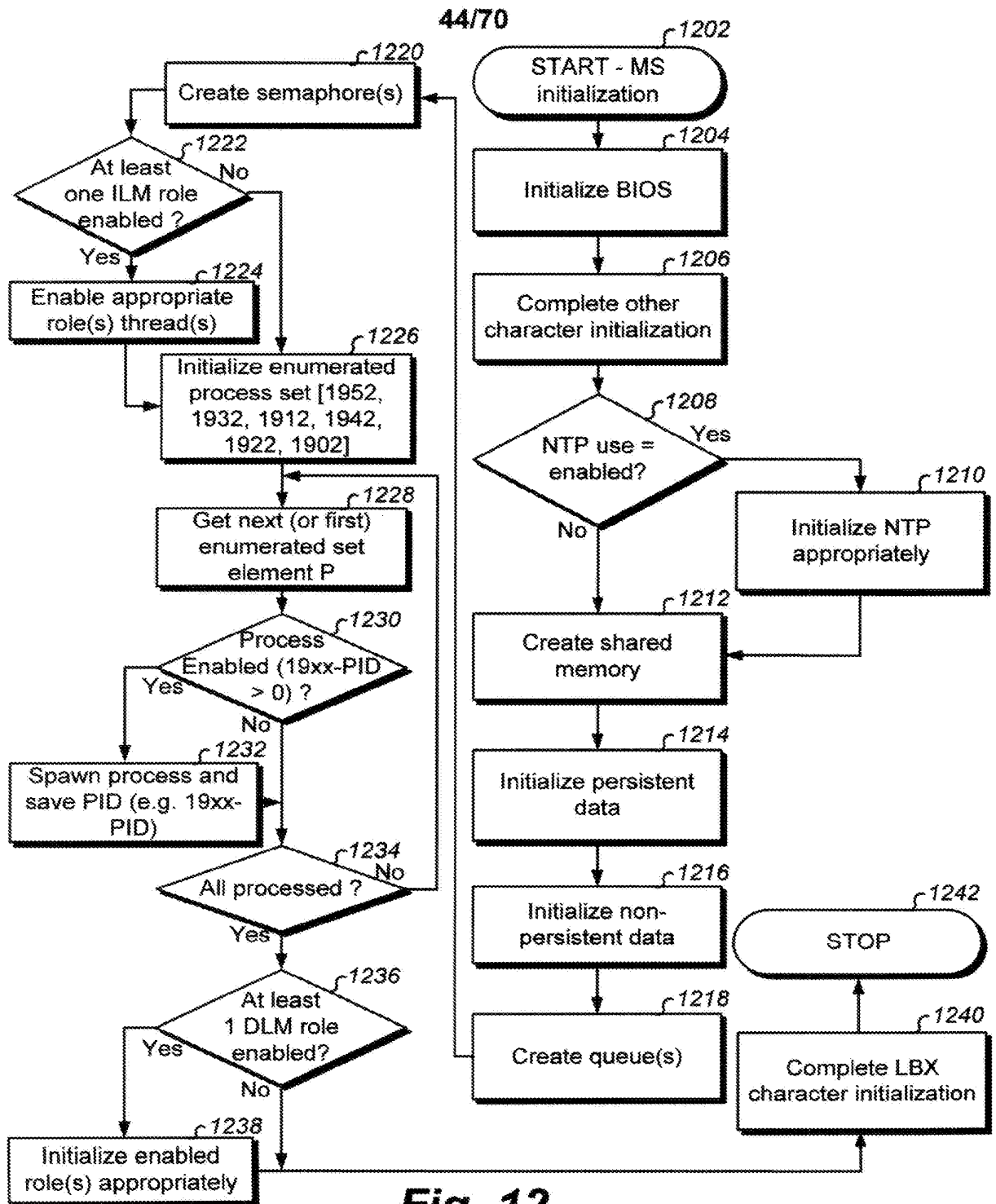


Fig. 12

45/70

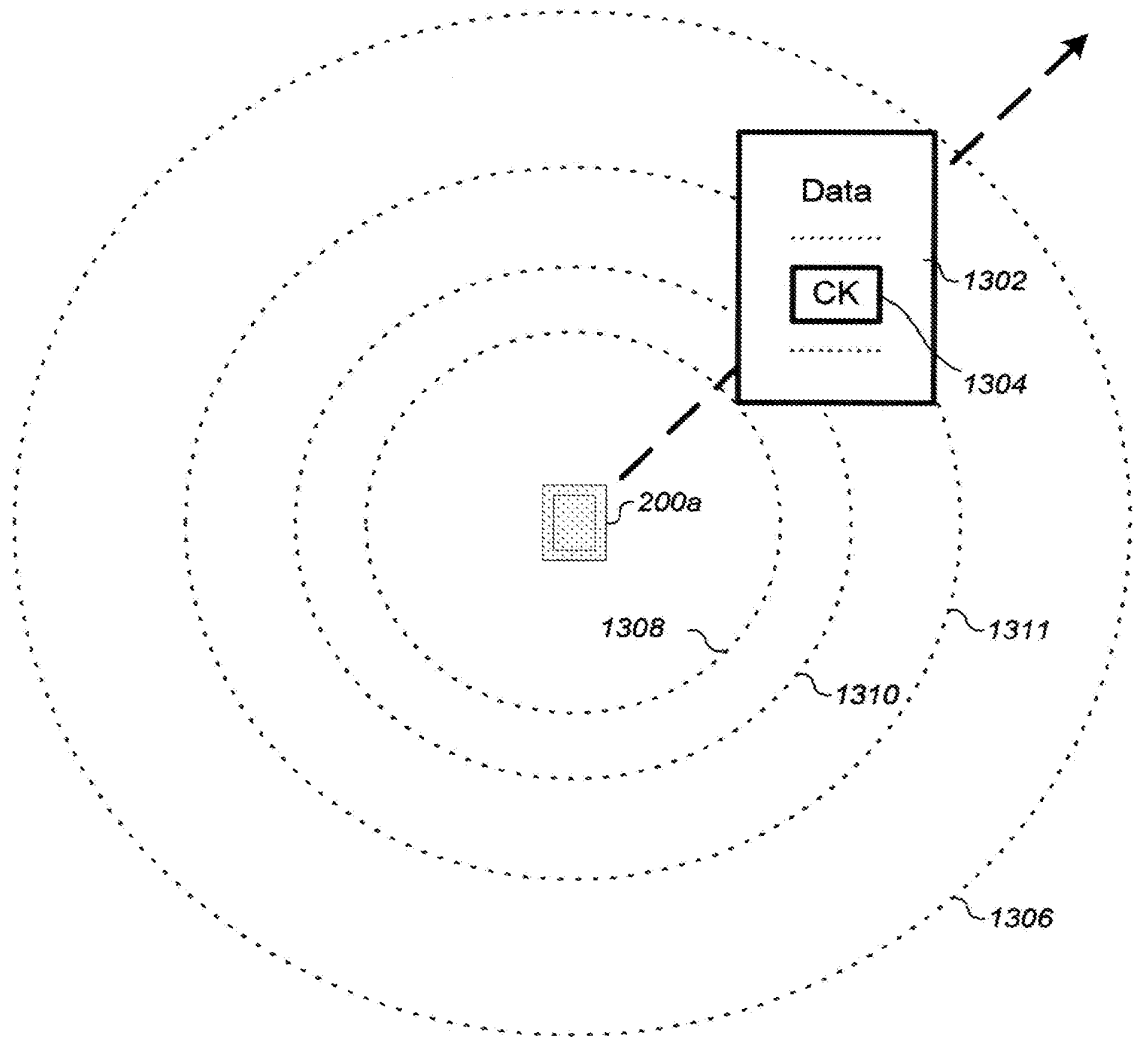


Fig. 13A

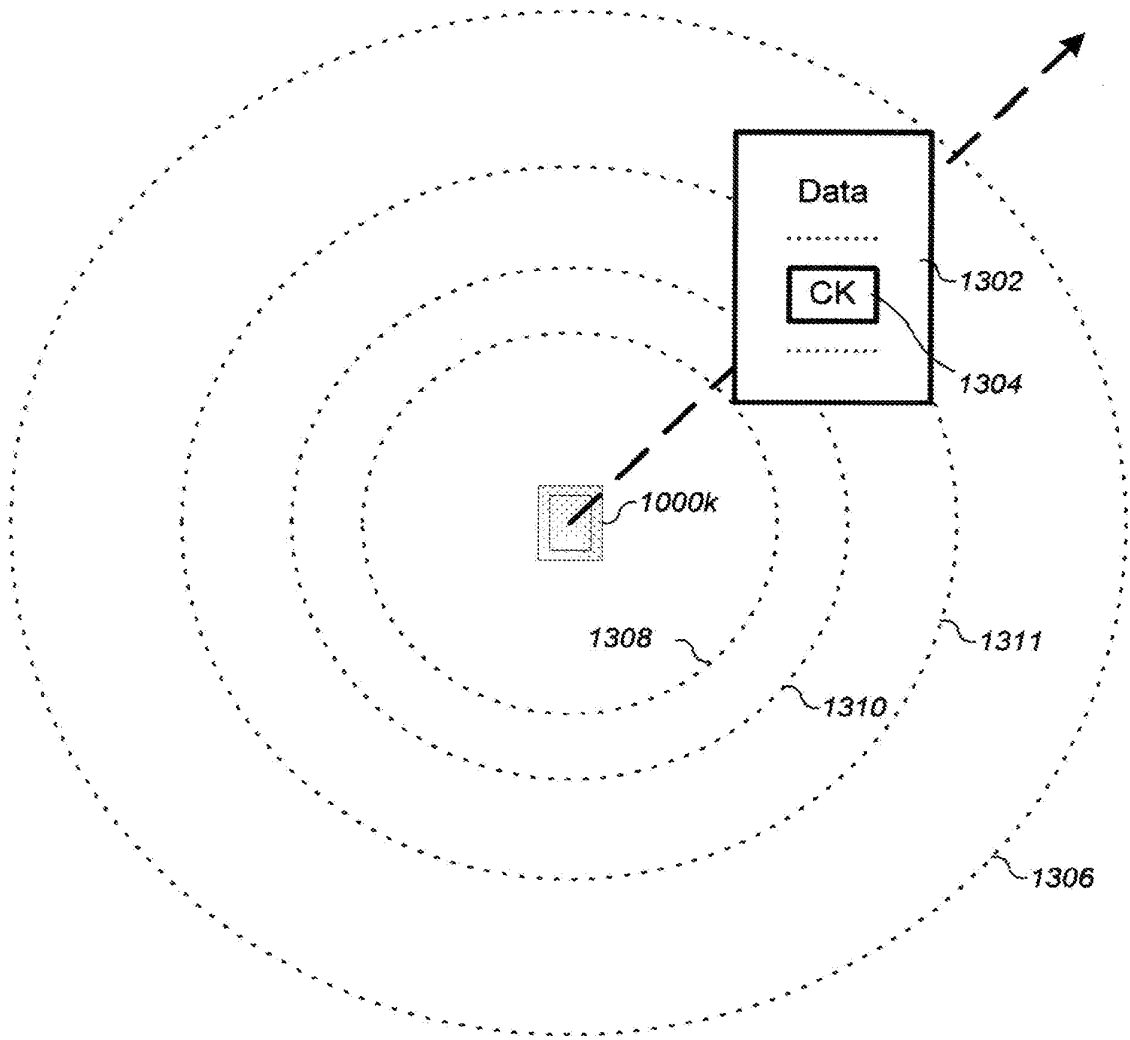


Fig. 13B

47/70

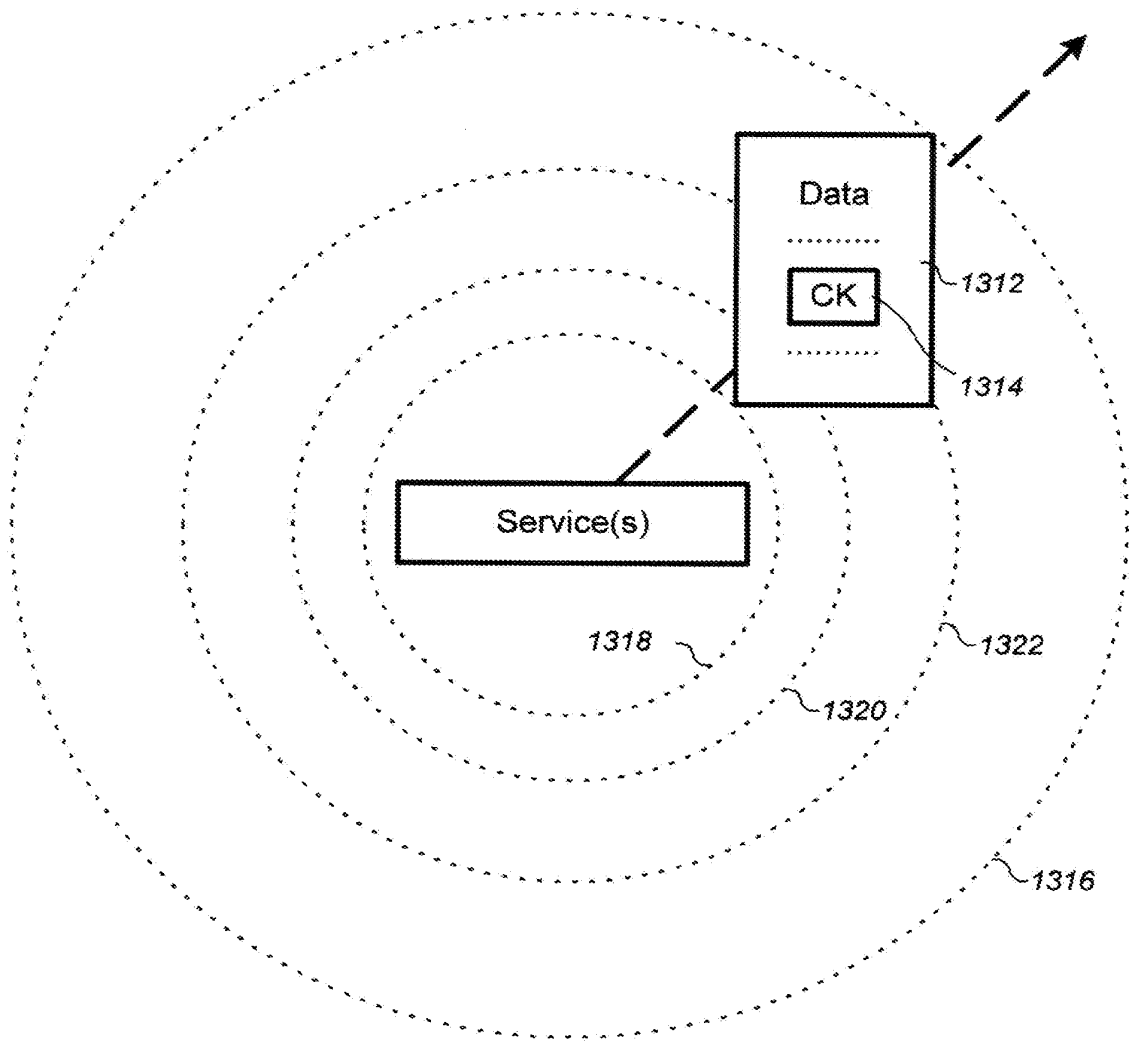


Fig. 13C

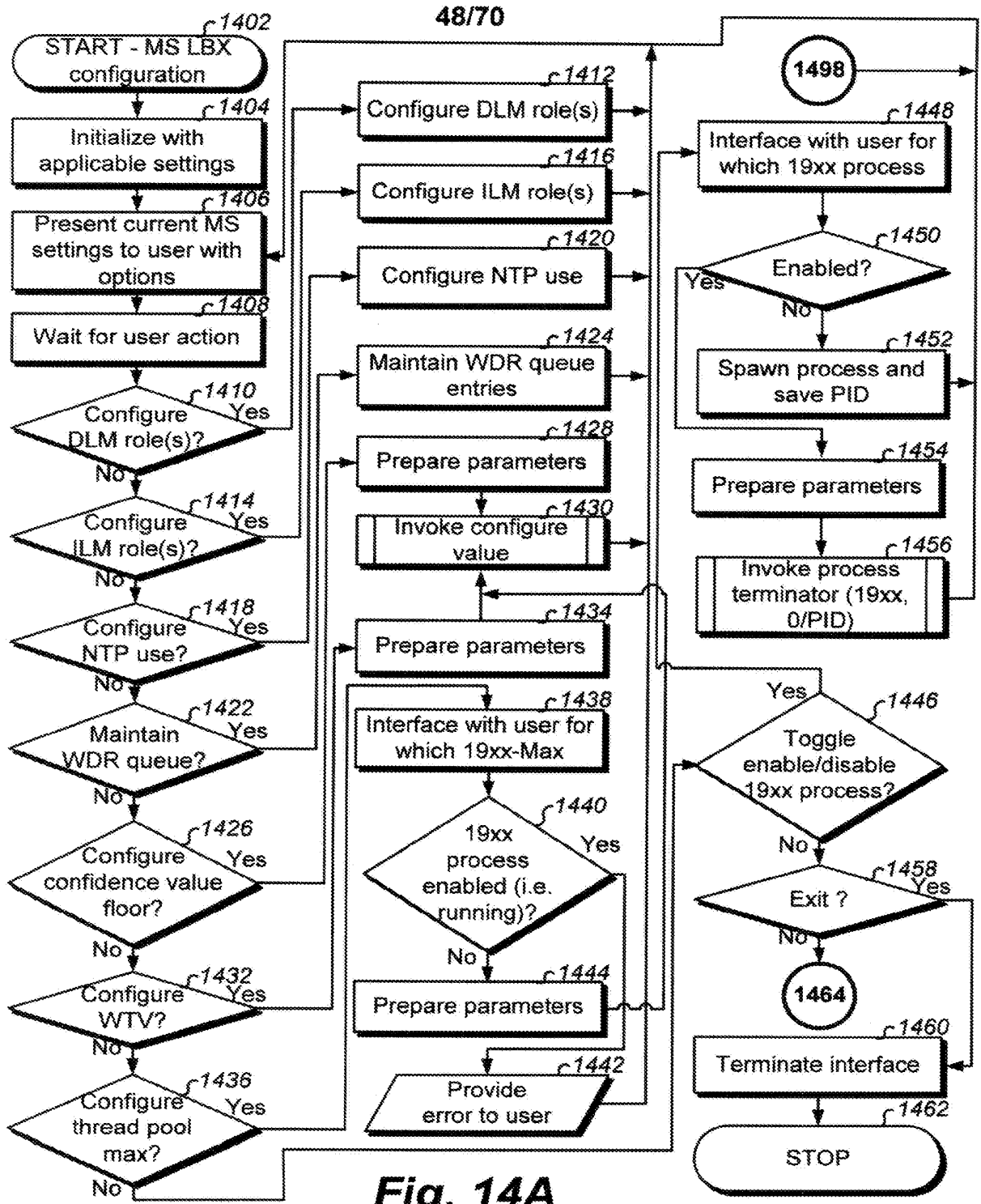


Fig. 14A

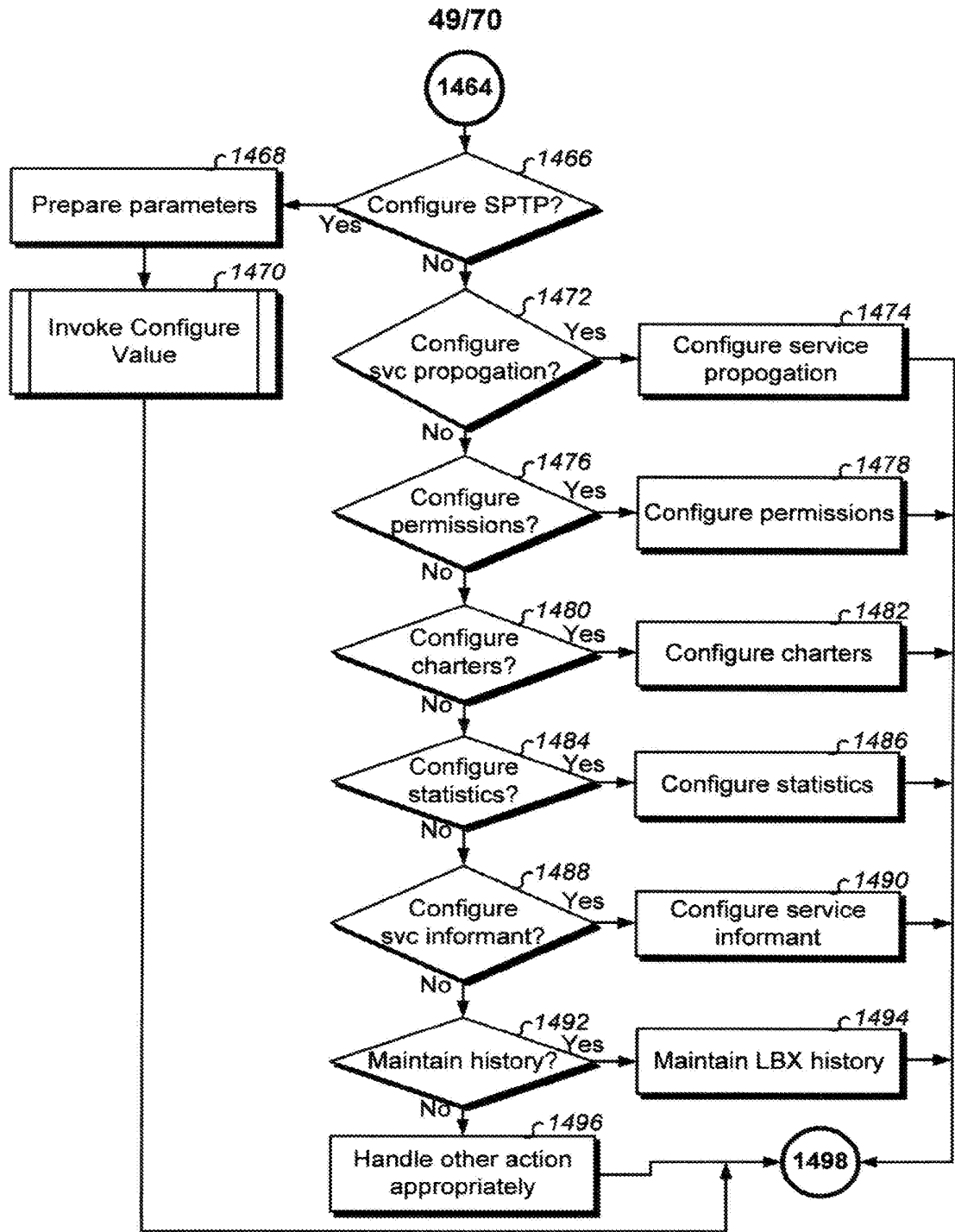


Fig. 14B

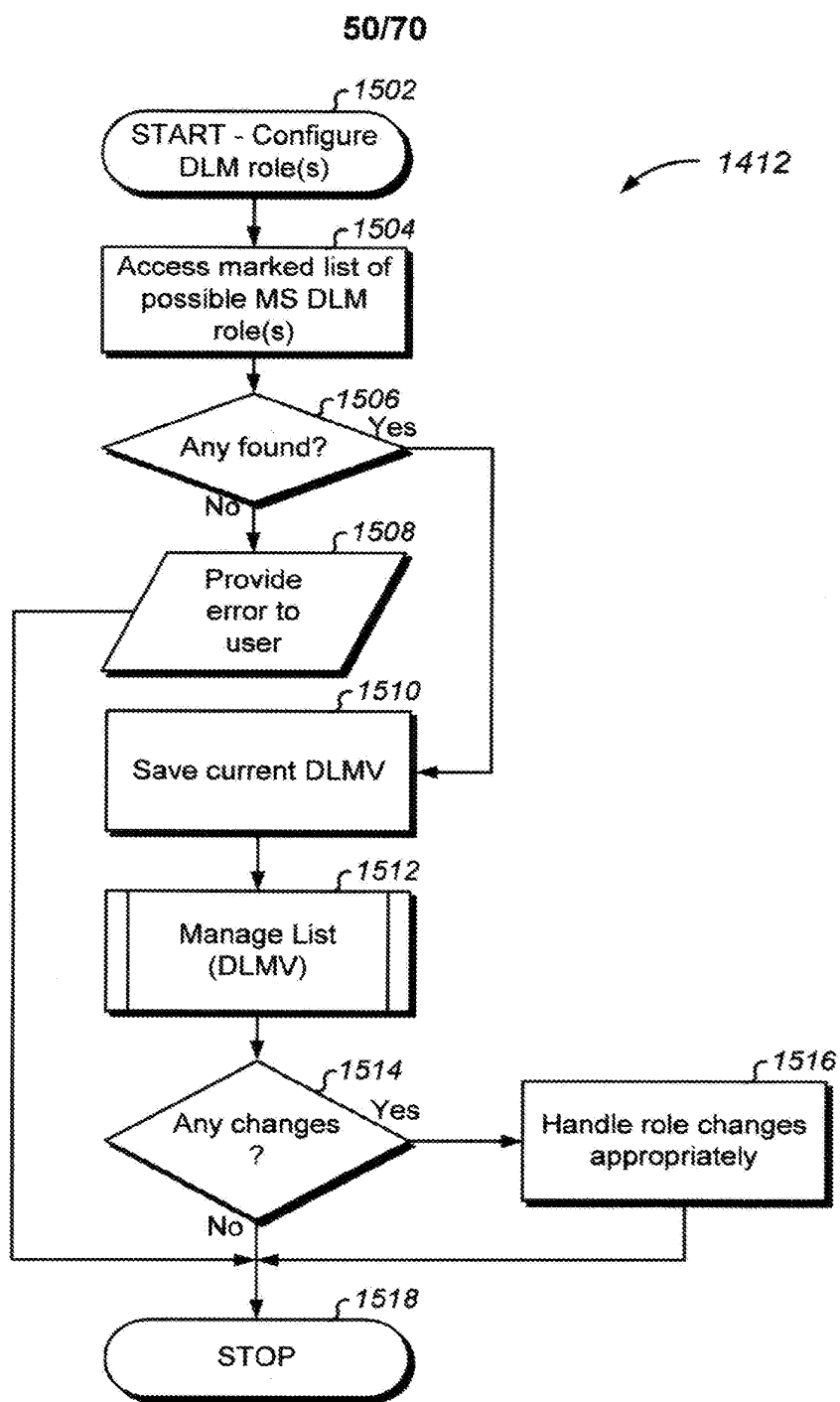


Fig. 15A

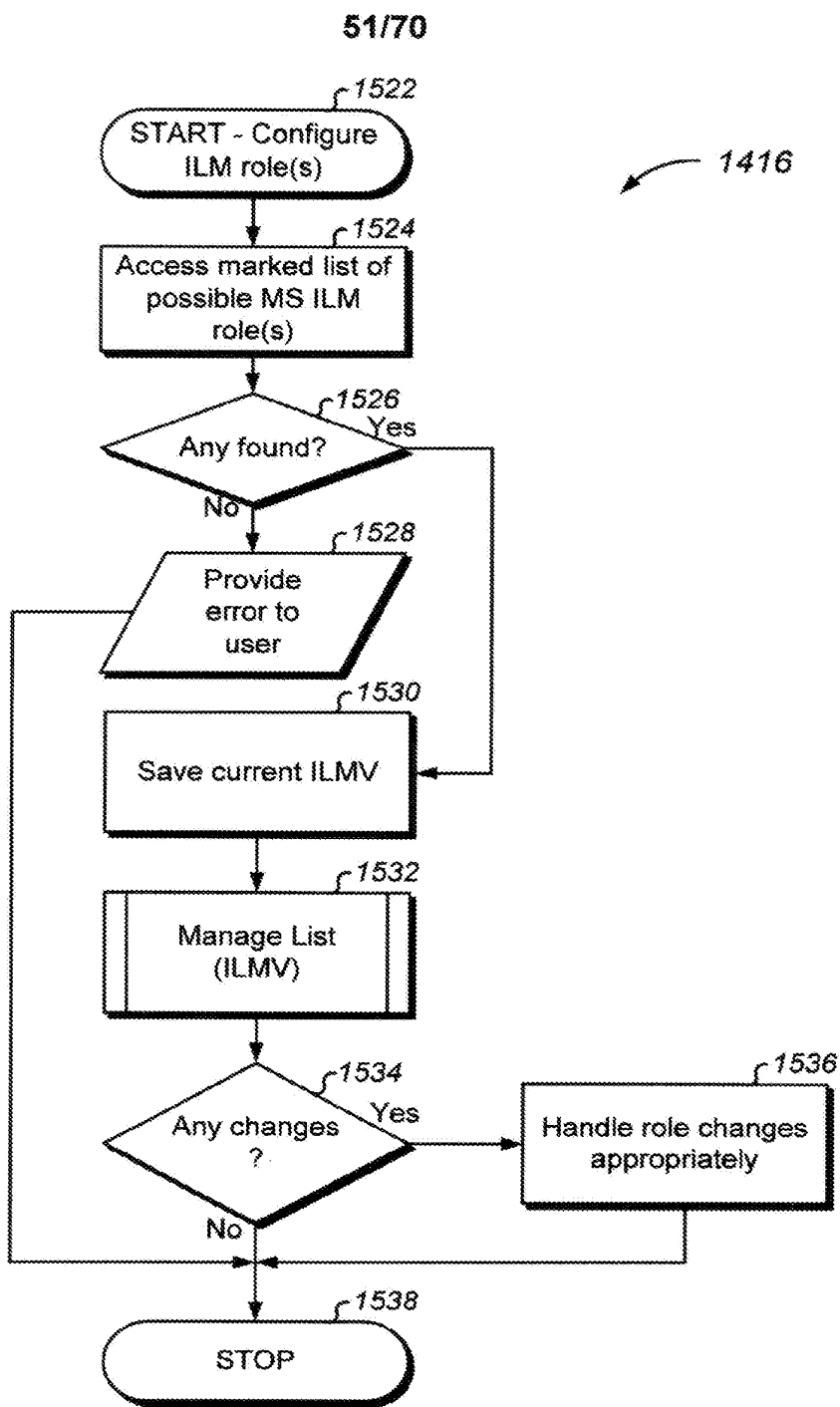


Fig. 15B

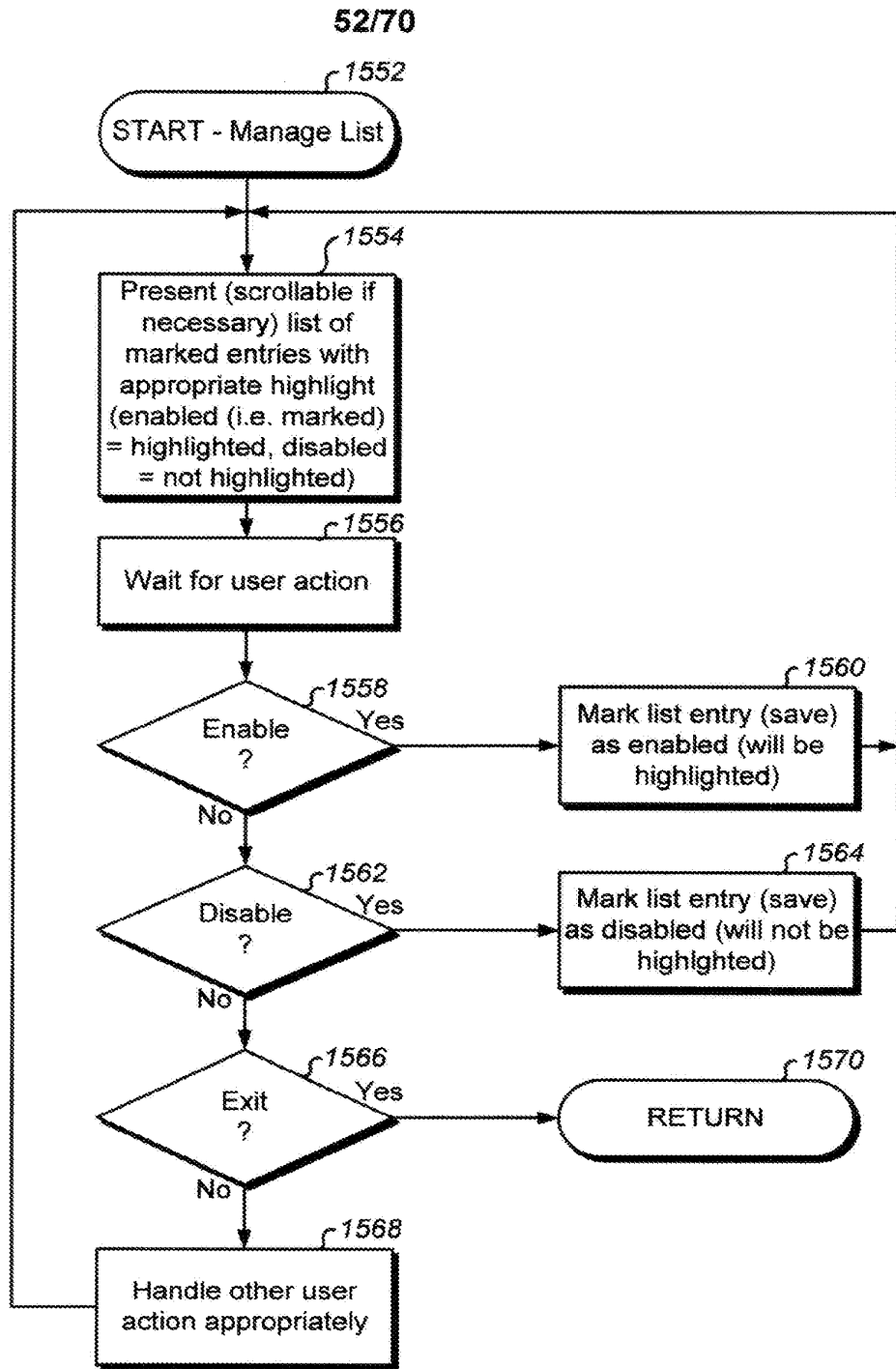


Fig. 15C

53/70

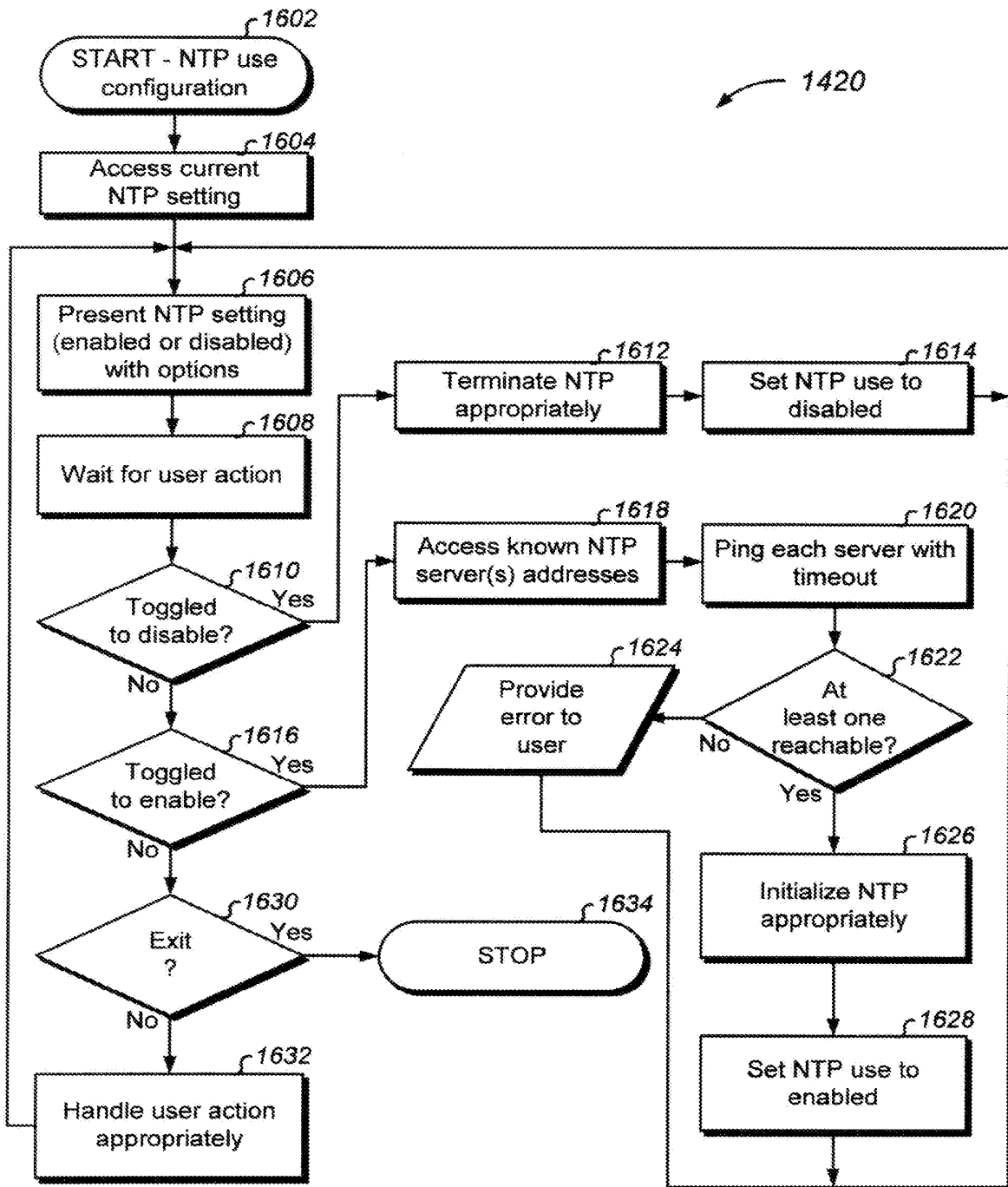


Fig. 16

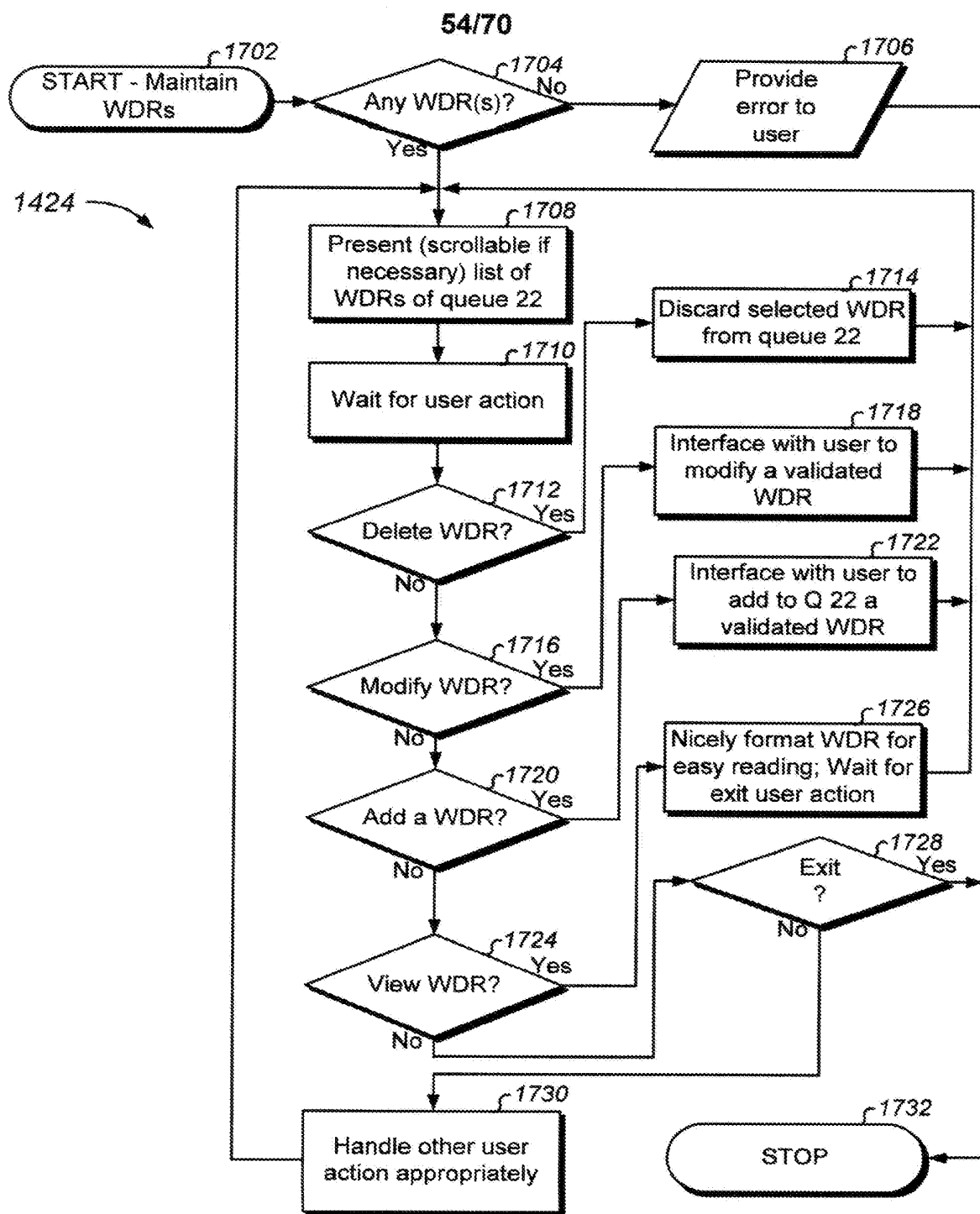


Fig. 17

55/70

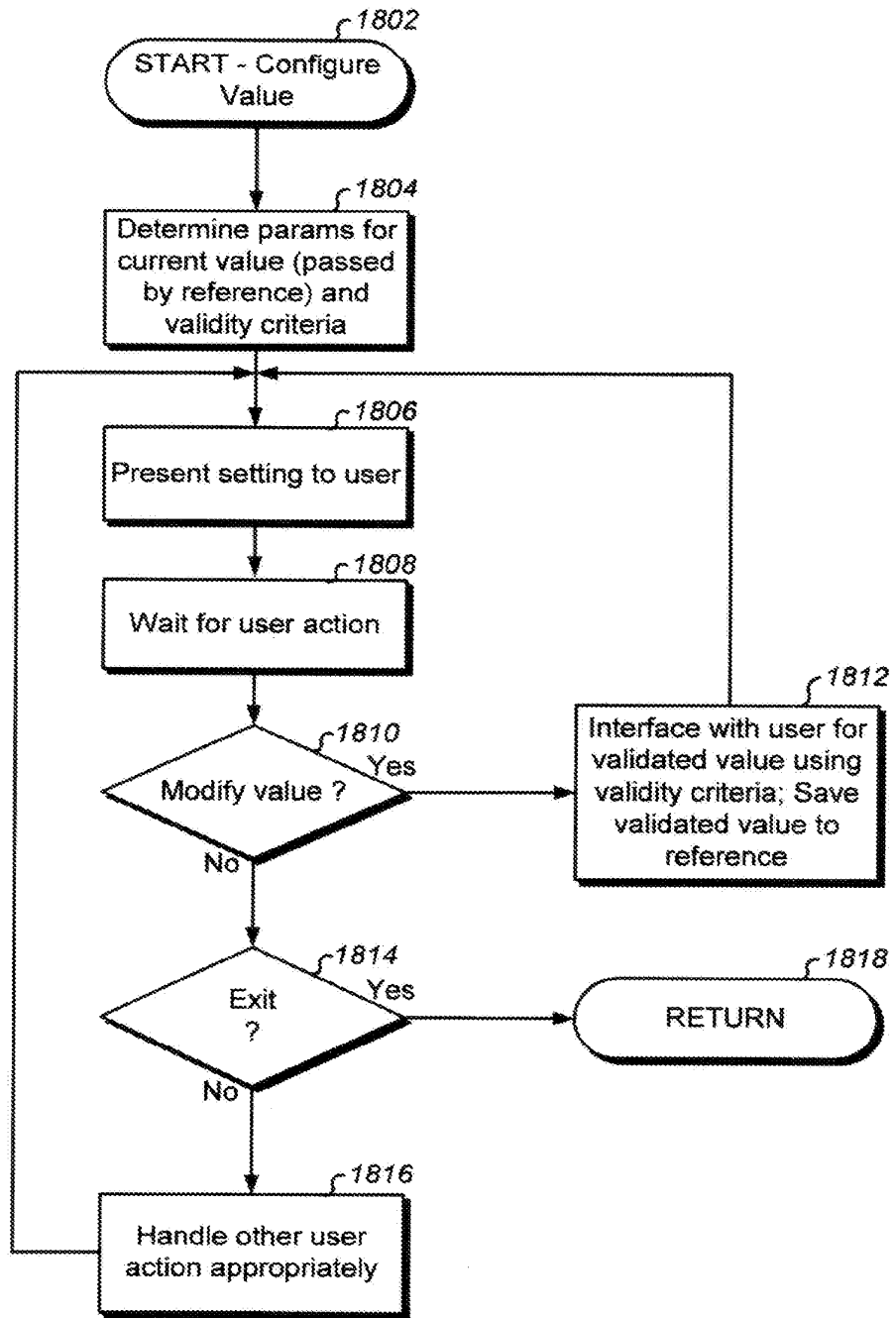


Fig. 18

56/70

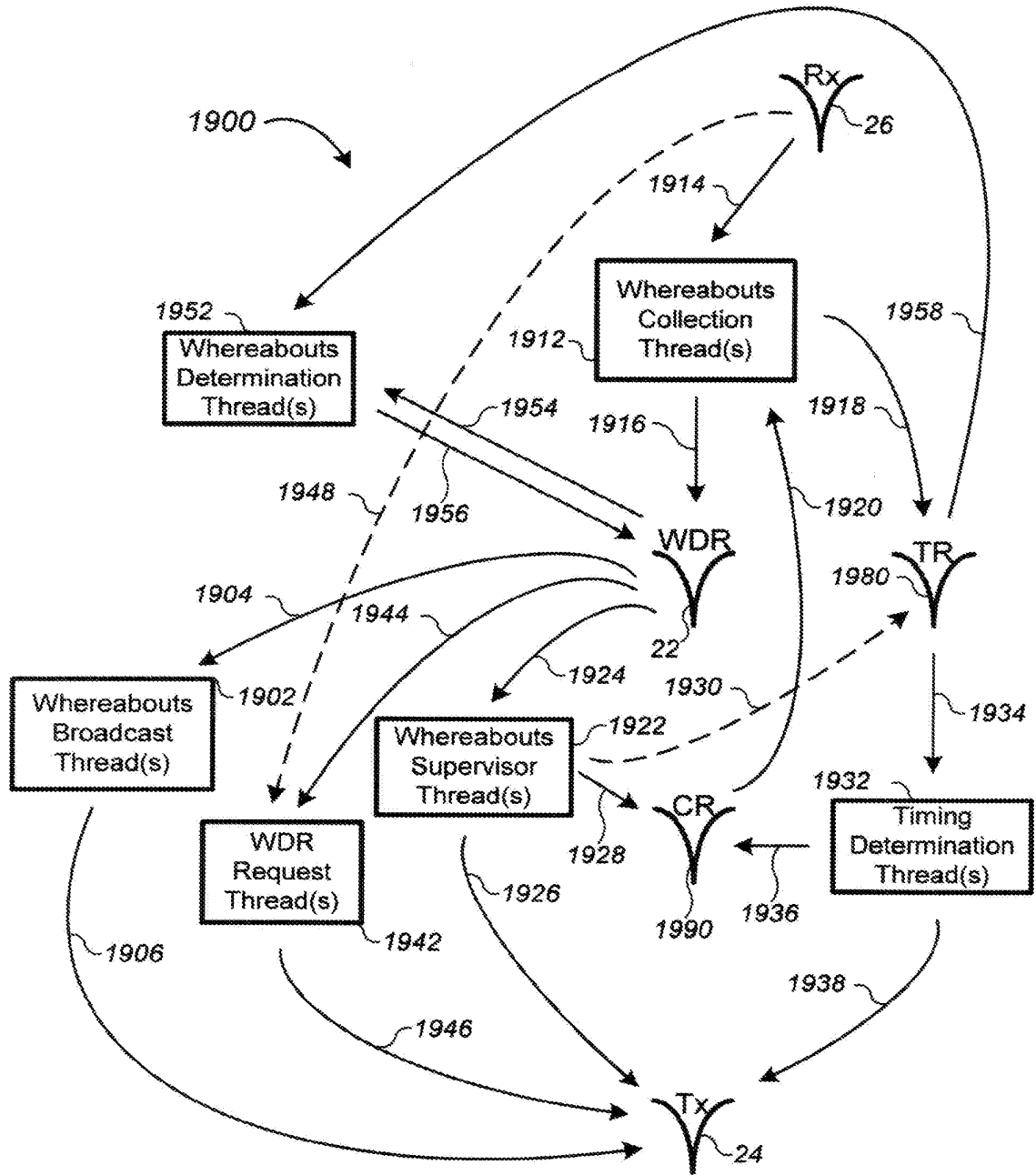


Fig. 19

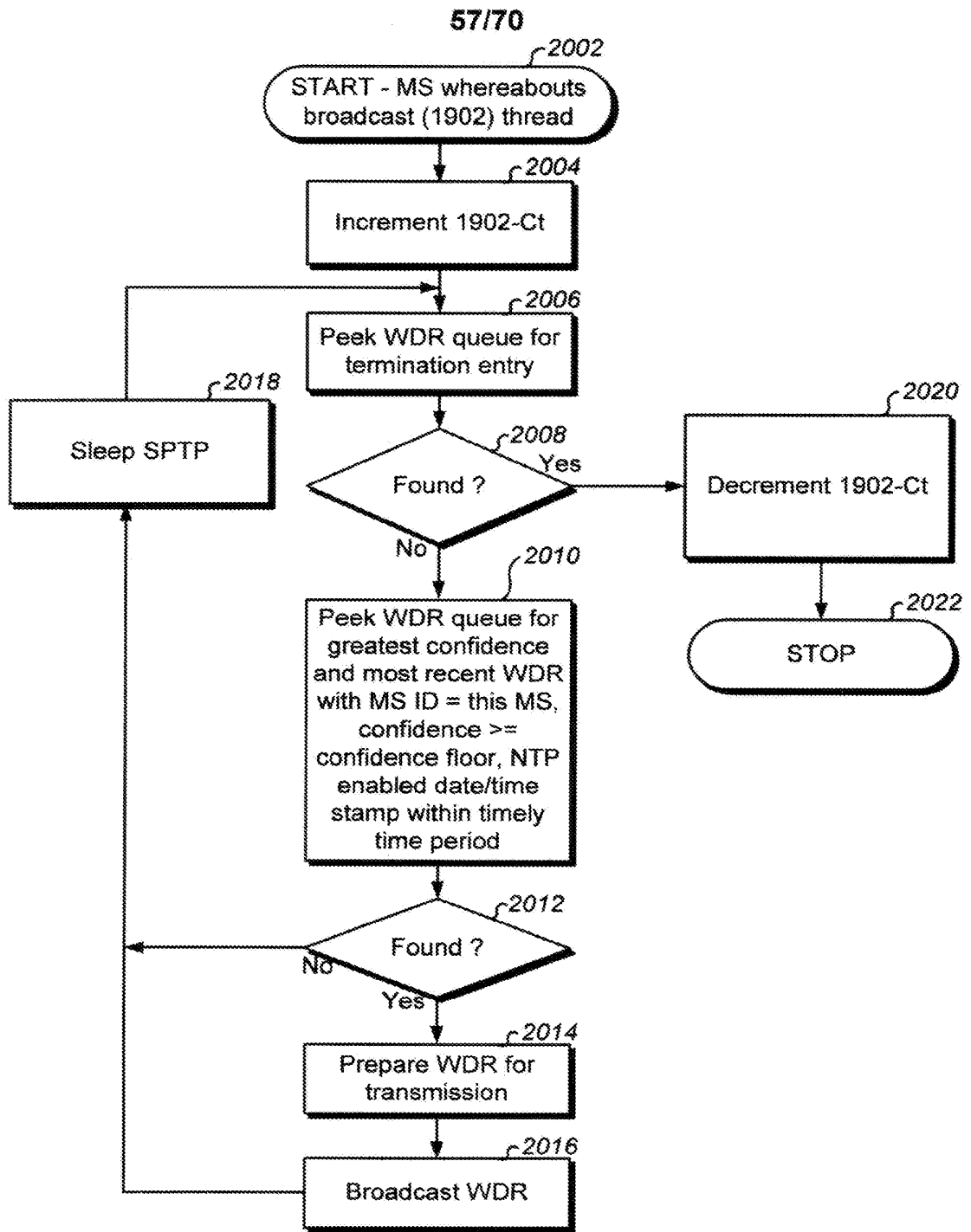
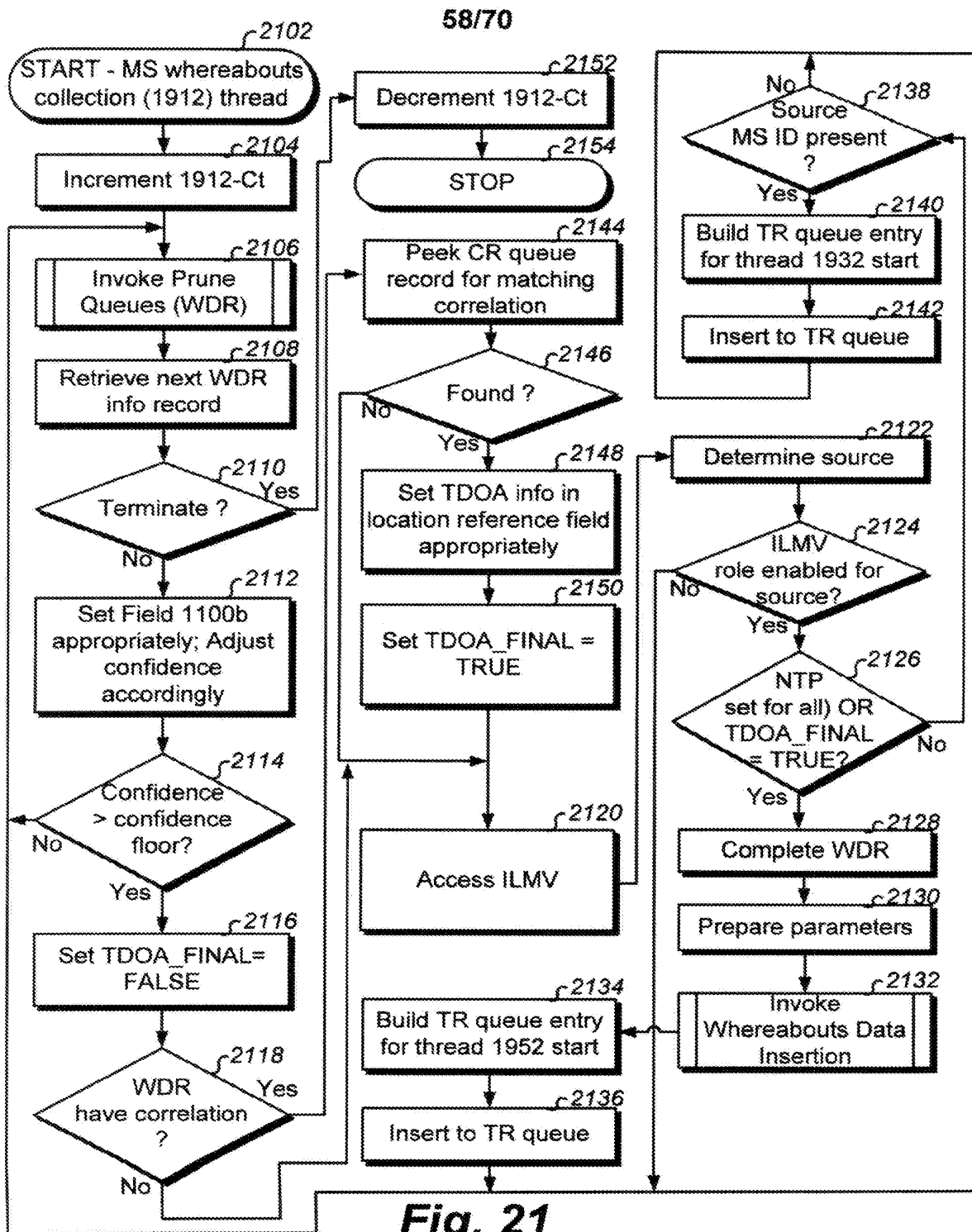


Fig. 20



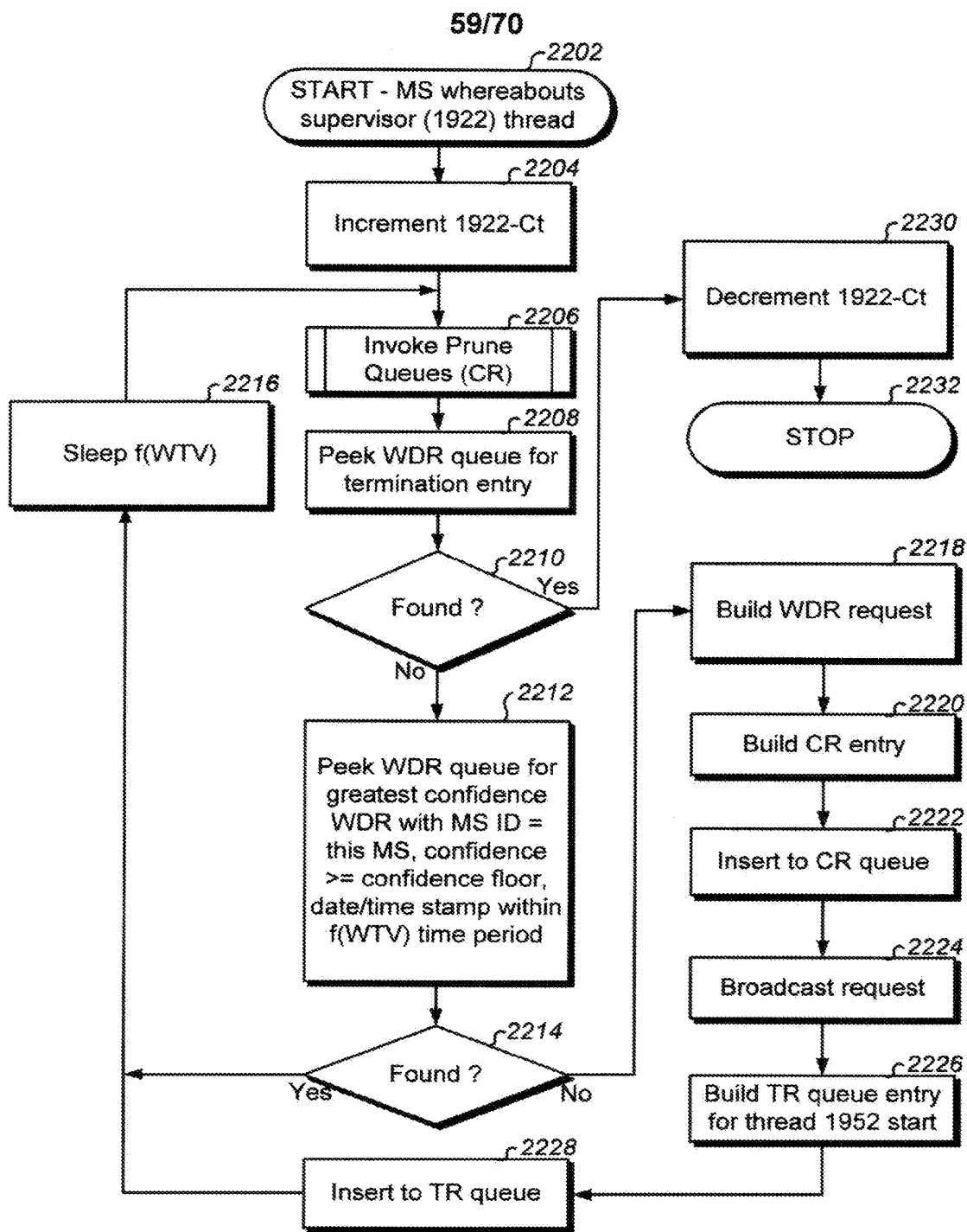


Fig. 22

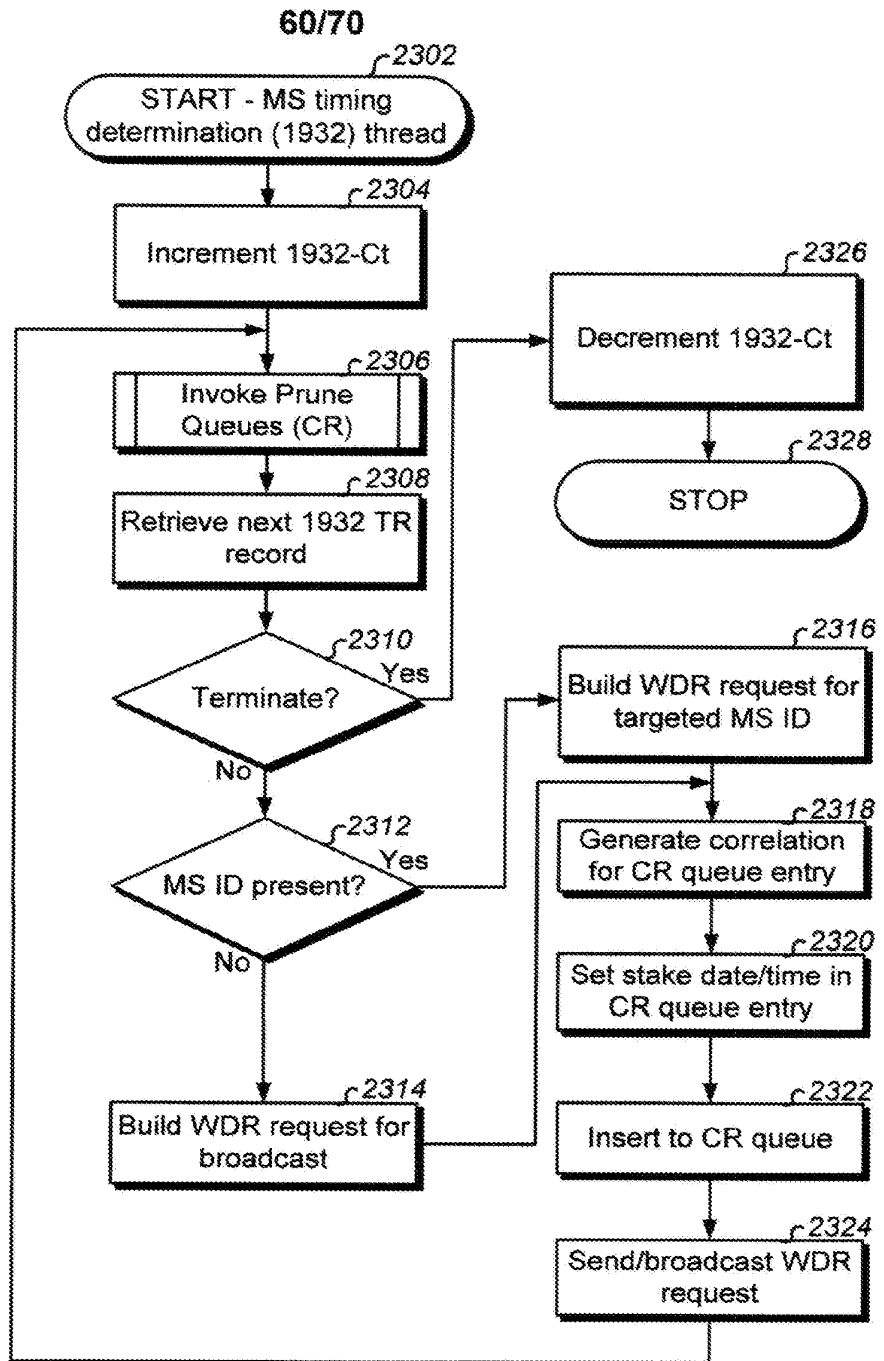


Fig. 23

61/70

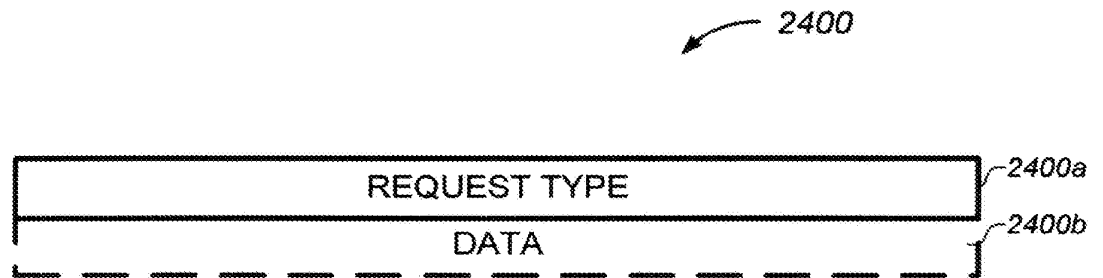


Fig. 24A

62/70

2450

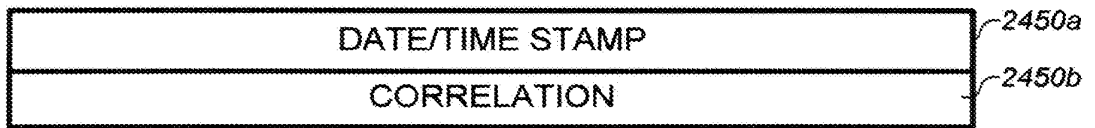



Fig. 24B

63/70

2490

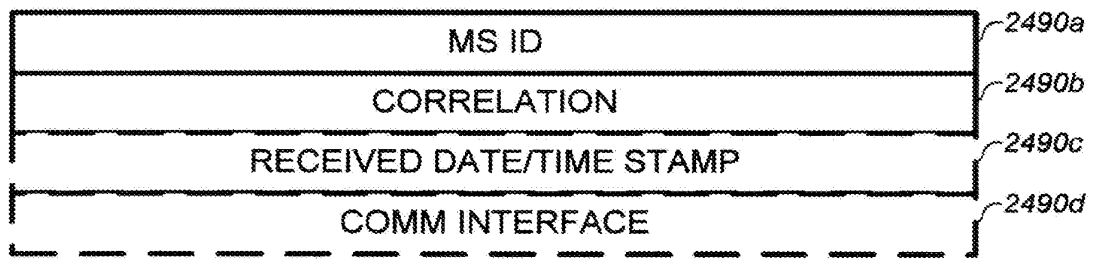


Fig. 24C

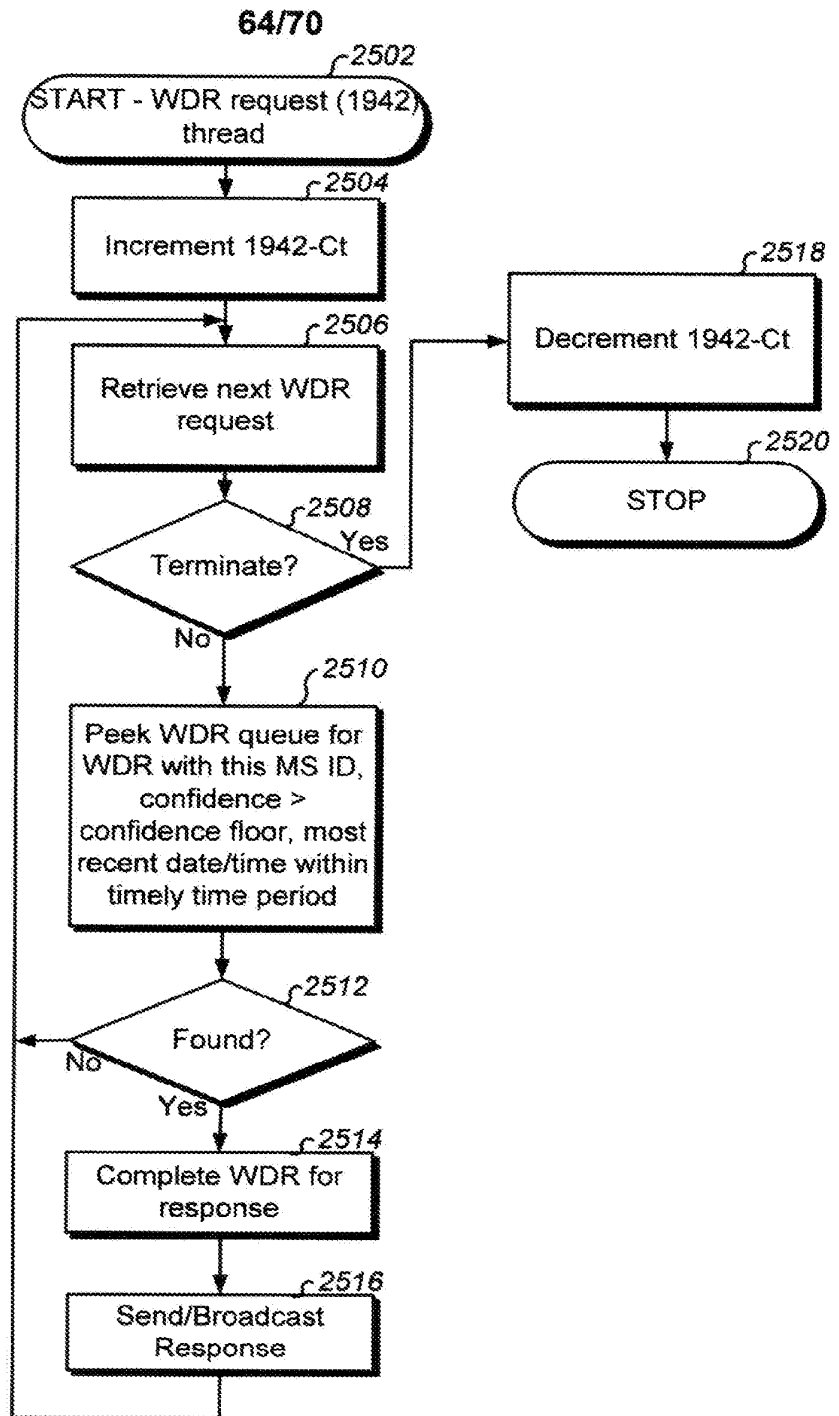


Fig. 25

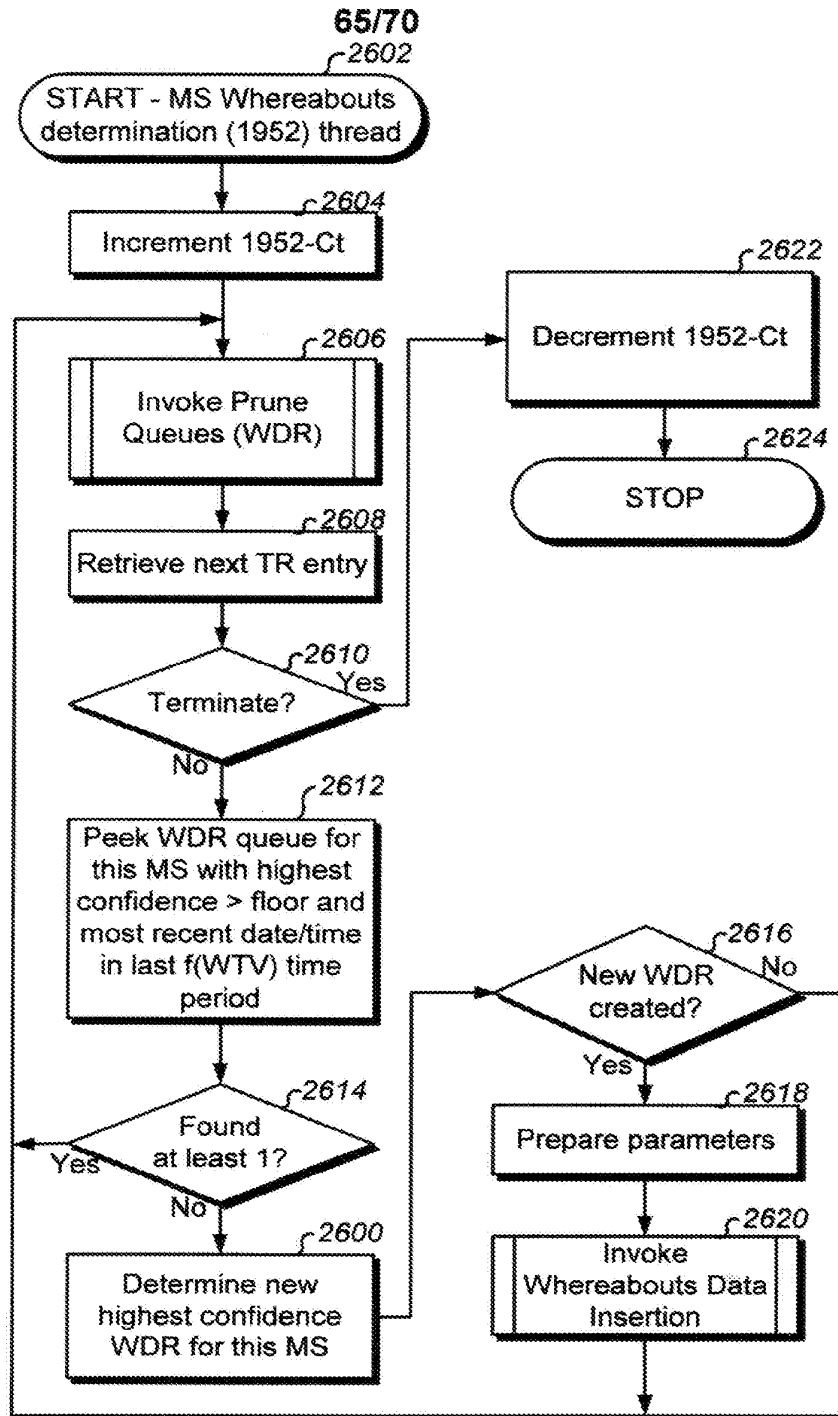


Fig. 26A

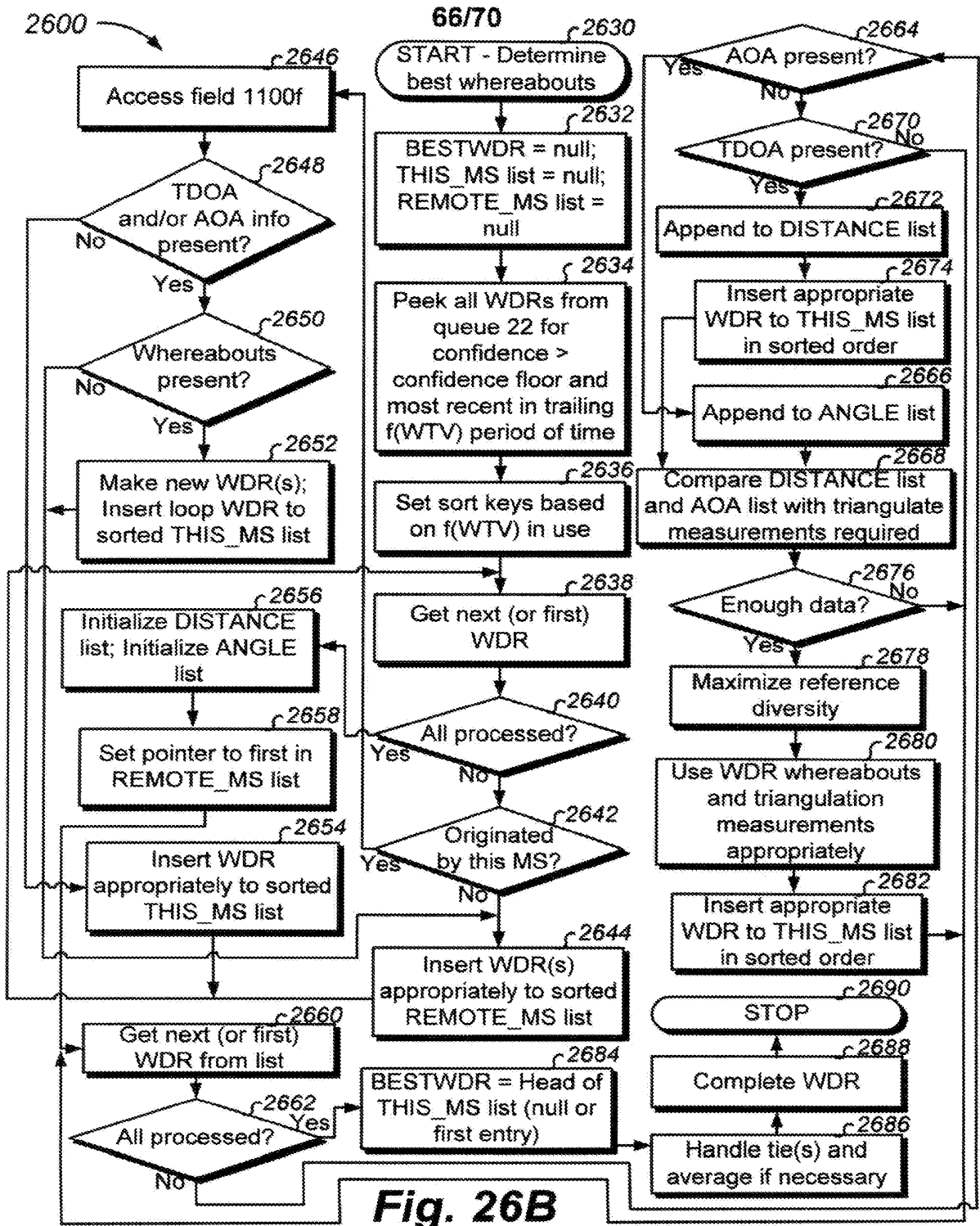


Fig. 26B

67/70

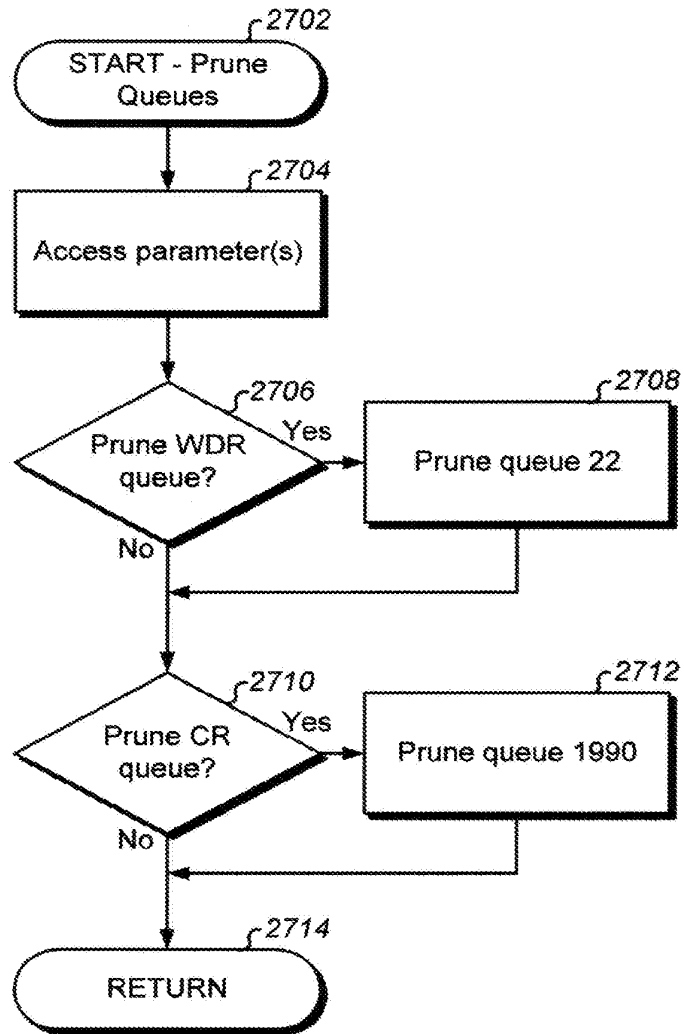


Fig. 27

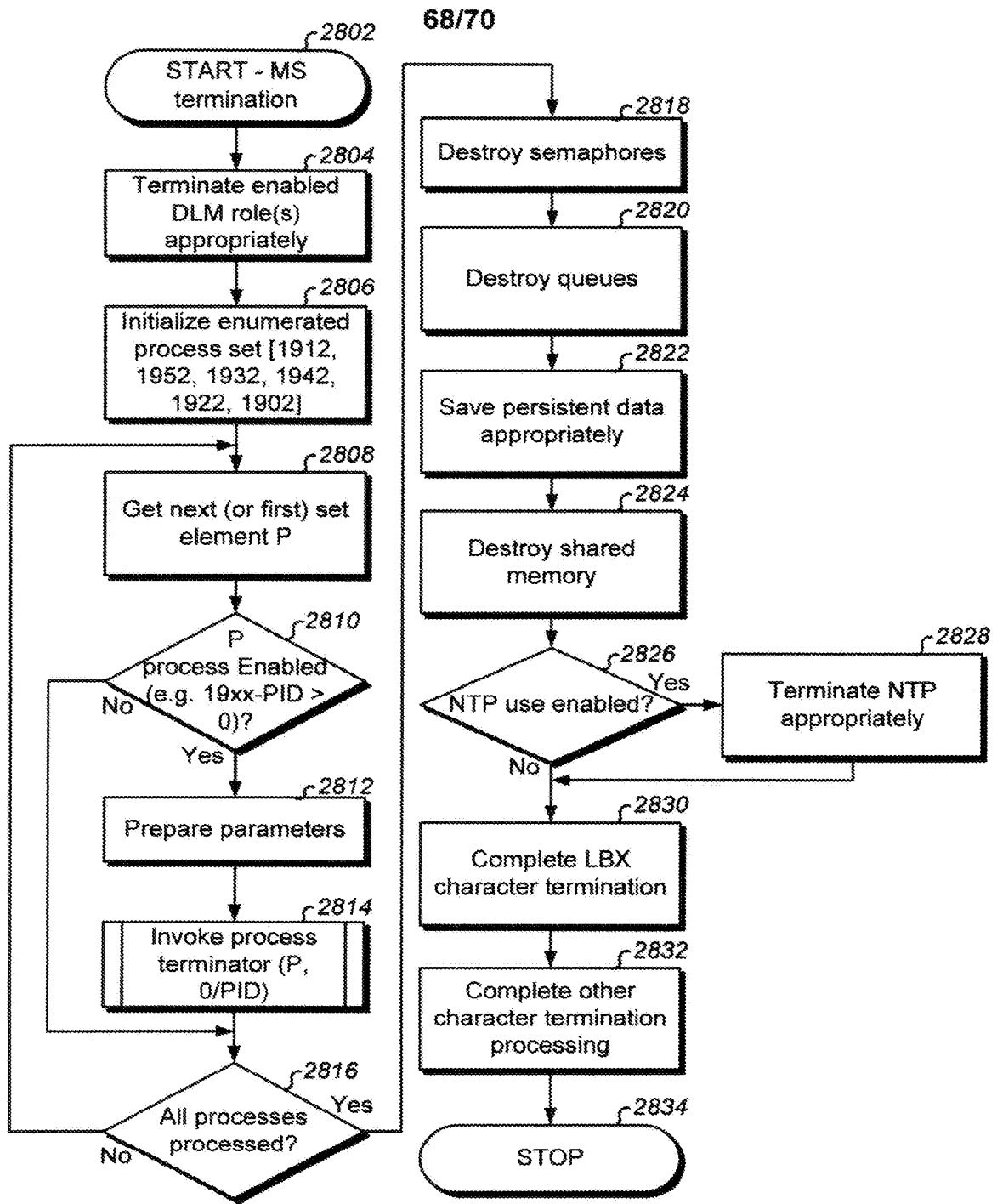


Fig. 28

69/70

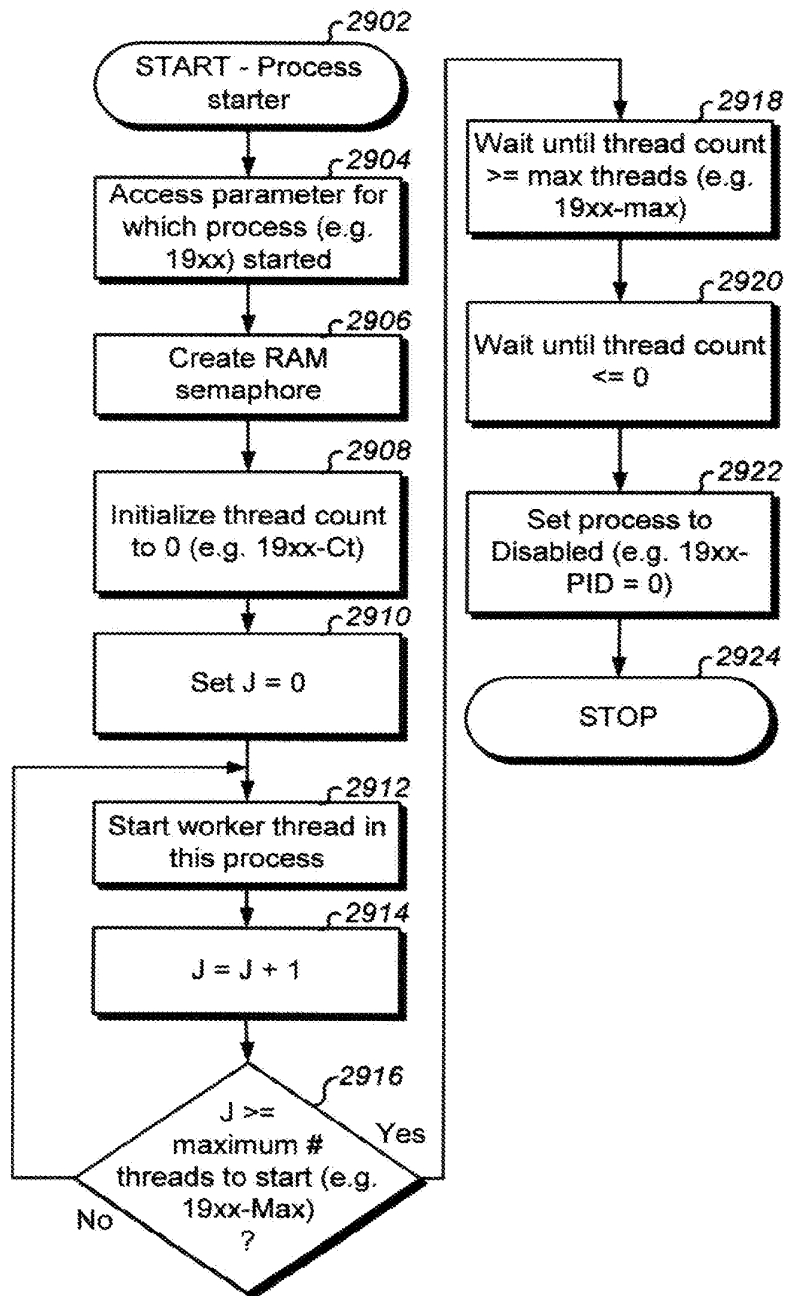


Fig. 29A

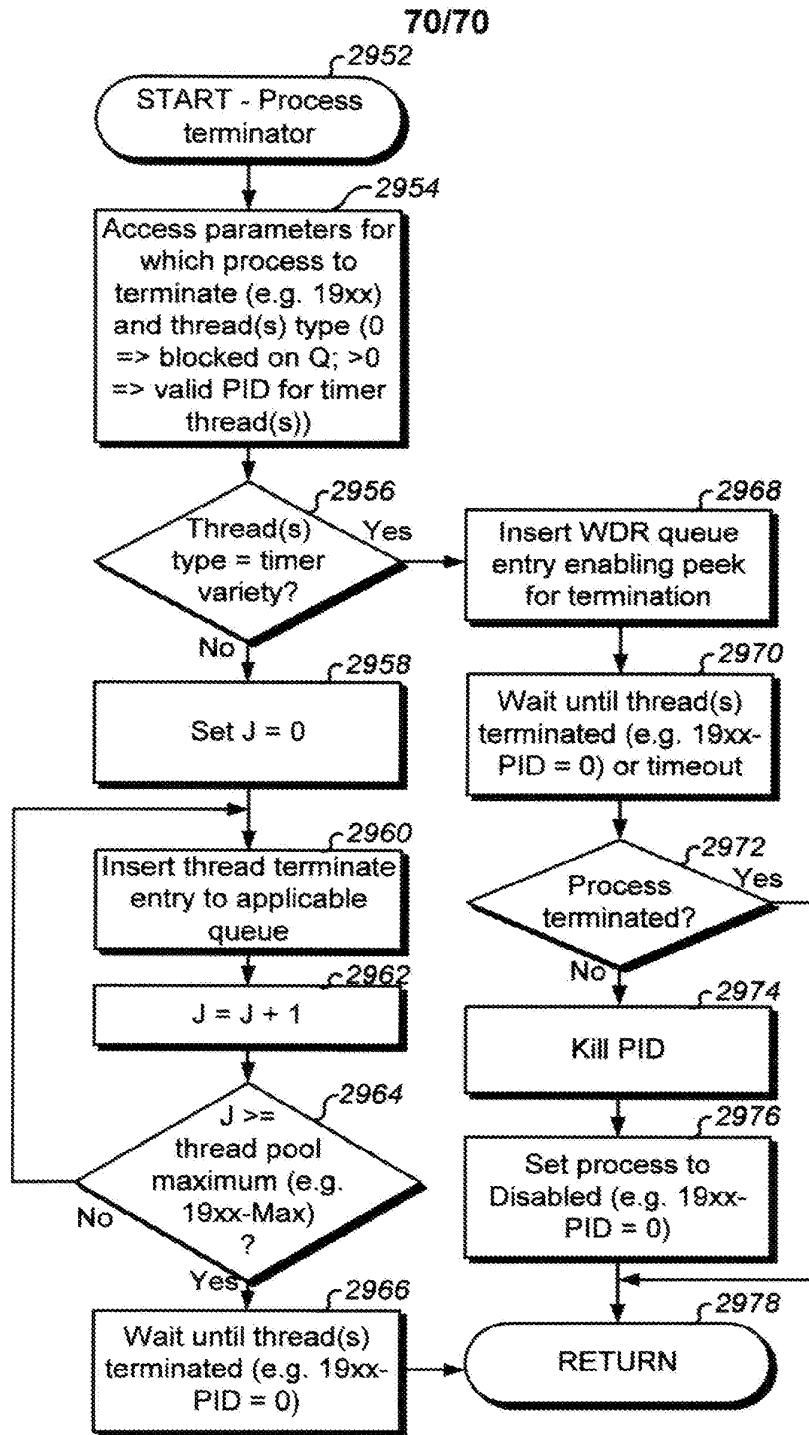


Fig. 29B

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications
---------------------------	--

As the below named inventor(s), I/we declare that:

This declaration is directed to: The attached application, or
 United States application or PCT International application number _____
 filed on _____
 As amended on _____ (if applicable);

I/we believe that I/we am/are the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought;

I/we have reviewed and understand the contents of the above-identified application, including the claims, as amended by any amendment specifically referred to above;

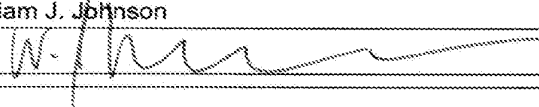
I/we acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me/us to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application. The above-identified application was made or authorized to be made by me/us.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

All statements made herein of my/our own knowledge are true, all statements made herein on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and may jeopardize the validity of the application or any patent issuing thereon. I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) or both.

FULL NAME OF INVENTOR(S)

Inventor one: William J. Johnson Date: 9/11/13
 Signature:  Citizen of: US
 Inventor two: _____ Date: _____
 Signature: _____ Citizen of: _____

Additional inventors or a legal representative are being named on _____ additional form(s) attached hereto.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
 If you need assistance in completing this form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal

Application Number:				
Filing Date:				
Title of Invention:	System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications			
First Named Inventor/Applicant Name:	William J. Johnson			
Filer:	Craig Jeffrey Yudell/Shenise Ramdeen			
Attorney Docket Number:	JOHNS-001US3			
Filed as Small Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	2202	1	40	40
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				40

Electronic Acknowledgement Receipt

EFS ID:	16921846
Application Number:	14033540
International Application Number:	
Confirmation Number:	1470
Title of Invention:	System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications
First Named Inventor/Applicant Name:	William J. Johnson
Customer Number:	42640
Filer:	Craig Jeffrey Yudell/Shenise Ramdeen
Filer Authorized By:	Craig Jeffrey Yudell
Attorney Docket Number:	JOHNS-001US3
Receipt Date:	23-SEP-2013
Filing Date:	
Time Stamp:	09:11:19
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$40
RAM confirmation Number	11479
Deposit Account	503083
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	JOHNS-001US3_ADS09-23-13.pdf	1396268	no	5
			408f9d47da6fa9b6afdeb06d476395fe78906431		
Warnings:					
Information:					
2		JOHNS-001US3_Applicationasfilepkg09-23-13.pdf	990814	yes	192
			bb3d9ab8e9c1f9b2ccf0a0092a662c8d26dd4d2		
Multipart Description/PDF files in .zip description					
Document Description			Start	End	
Specification			1	183	
Claims			184	191	
Abstract			192	192	
Warnings:					
Information:					
3	Drawings-only black and white line drawings	JOHNS-001US3_FiledDrawings09-23-13.pdf	14798355	no	70
			a097687982911104a154e44fd9d2f0e45855d148		
Warnings:					
Information:					
4	Oath or Declaration filed	JOHNS-001US3_Declaration09-23-13.pdf	430132	no	1
			d7a943fa43969816cd4c47eb87f71cc3c27dd1ae		
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	29830	no	2
			1ae69455e8de596e393f3f070e89fb35f85e521		
Warnings:					
Information:					
Total Files Size (in bytes):			17645399		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Patent Application Fee Transmittal

Application Number:	14033540
Filing Date:	
Title of Invention:	System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications
First Named Inventor/Applicant Name:	William J. Johnson
Filer:	Craig Jeffrey Yudell/Shenise Ramdeen
Attorney Docket Number:	JOHNS-001US3

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360

Pages:

Claims:

Miscellaneous-Filing:

Petition:

Patent-Appeals-and-Interference:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				730

Electronic Acknowledgement Receipt

EFS ID:	16926380
Application Number:	14033540
International Application Number:	
Confirmation Number:	1470
Title of Invention:	System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications
First Named Inventor/Applicant Name:	William J. Johnson
Customer Number:	42640
Filer:	Craig Jeffrey Yudell/Shenise Ramdeen
Filer Authorized By:	Craig Jeffrey Yudell
Attorney Docket Number:	JOHNS-001US3
Receipt Date:	23-SEP-2013
Filing Date:	
Time Stamp:	14:46:58
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$730
RAM confirmation Number	1302
Deposit Account	503083
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)
 Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)
 Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Fee Worksheet (SB06)	fee-info.pdf	35050 b3a7e0f174041e411f1c6c741f9f9fd366bbb915	no	2

Warnings:

Information:

Total Files Size (in bytes): 35050

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 10/08/2013

CCETIN SALE #00000002 Mailroom Dt: 09/23/2013 503083 14033540
01 FC : 2081 400.00 DA

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number
14/033,540

APPLICATION AS FILED - PART I

(Column 1)		(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	21 minus 20 = *	1	x 40 =	40	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 = *		x 210 =	0.00	OR		
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			400			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	1170		TOTAL	

APPLICATION AS AMENDED - PART II

AMENDMENT A	(Column 1)	(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
Total (37 CFR 1.16(i))	*	Minus **	=	x	=	OR	x	=
Independent (37 CFR 1.16(h))	*	Minus ***	=	x	=	OR	x	=
Application Size Fee (37 CFR 1.16(s))						OR		
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR		
				TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
AMENDMENT B	(Column 1)	(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
Total (37 CFR 1.16(i))	*	Minus **	=	x	=	OR	x	=
Independent (37 CFR 1.16(h))	*	Minus ***	=	x	=	OR	x	=
Application Size Fee (37 CFR 1.16(s))						OR		
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR		
				TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
 The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY. DOCKET NO, TOT CLAIMS, IND CLAIMS. Row 1: 14/033,540, 09/23/2013, 2668, 1170, JOHNS-001US3, 21, 2

CONFIRMATION NO. 1470

FILING RECEIPT



42640
Yudell Isidore Ng Russell PLLC
8911 N. Capital of Texas Hwy.,
Suite 2110
Austin, TX 78759

Date Mailed: 10/16/2013

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Inventor(s) William J. Johnson, Flower Mound, TX;
Applicant(s) William J. Johnson, Flower Mound, TX;

Power of Attorney: None

Domestic Priority data as claimed by applicant
This application is a CON of 12/077,041 03/14/2008

Foreign Applications for which priority is claimed (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access - A proper Authorization to Permit Access to Application by Participating Offices (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 10/08/2013

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is US 14/033,540

Projected Publication Date: 01/23/2014

Non-Publication Request: No

Early Publication Request: No

** SMALL ENTITY **

Title

System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications

Preliminary Class

382

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	3636421		1972-03-26	Barker et al.	
	2	4021780		1977-05-01	Narey et al.	
	3	4445118		1984-04-01	Taylor et al.	
	4	4757267		1988-07-01	Riskin	
	5	4841560		1989-06-01	Chan et al.	
	6	4922516		1990-05-01	Butler et al.	
	7	4977399		1990-12-01	Price et al.	
	8	5095532		1992-03-10	Mardus	
	9	5122795		1992-06-01	Cubley et al.	
	10	5185857		1993-02-09	Rozmanith et al	
	11	5223844		1993-06-29	Mansell et al.	
	12	5243652		1993-09-07	Teare et al.	
	13	5303393		1994-04-12	Noreen et al.	
	14	5321242		1994-06-14	Heath, Jr.	
	15	5365516		1994-11-15	Jandrell	
	16	5371794		1994-12-06	Diffie et al.	
	17	5390237		1995-02-12	Hoffman et al.	
	18	5404505		1995-04-04	Levinson	
	19	5432841		1995-07-11	Rimer	
	20	5444444		1995-08-22	Ross	
	21	5451757		1995-09-19	Heath, Jr.	
	22	5461627		1995-10-24	Rypinski	
	23	5264822		1993-11-23	Vogelman et al.	
	24	5475735		1995-12-10	Williams et al.	
	25	5485163		1996-01-16	Singer et al.	
	26	5487103		1996-01-23	Richardson	
	27	5493309		1996-02-20	Bjornholt et al.	
	28	5497414		1996-03-01	Bartholomew	
	29	5504482		1996-04-02	Schreder	
	30	5511111		1996-04-01	Serbetcioğlu et al.	
	31	5511233		1996-04-23	Otten	
	32	5512908		1996-04-01	Herrick	
	33	5513263		1996-04-30	White et al.	
	34	5528248		1996-06-18	Steiner et al.	
	35	5544354		1996-08-06	May et al.	
	36	5559520		1996-09-24	Barzegar et al.	
	37	5566235		1996-10-15	Hetz	
	38	5870555		1999-02-09	Pruett et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	39	5581479		1996-12-03	McLaughlin	
	40	5588042		1996-12-24	Comer	
	41	5590398		1996-12-31	Matthews	
	42	5596625		1997-01-21	LeBlanc	
	43	5602843		1997-02-11	Gray	
	44	5610973		1997-03-11	Comer	
	45	5625364		1997-04-29	Herrick et al.	
	46	5627549		1997-05-06	Park	
	47	5636245		1997-06-03	Ernst et al.	
	48	5646632		1997-07-08	Khan et al.	
	49	5654959		1997-08-05	Baker et al.	
	50	5657375		1997-08-22	Connolly et al.	
	51	5661492		1997-08-26	Shoap et al.	
	52	5663734		1997-09-02	Krasner	
	53	5664948		1997-09-09	Dimitriadis et al.	
	54	5666481		1997-09-09	Lewis	
	55	5687212		1997-11-11	Kinser, Jr. et al	
	56	5689431		1997-11-18	Rudow et al.	
	57	5694453		1997-12-02	Fuller et al.	
	58	5701301		1997-12-23	Weisser, Jr.	
	59	5712899		1998-01-27	Pace, II, Harold	
	60	5713075		1998-01-27	Threadgill et al.	
	61	5714948		1998-02-03	Farmakis et al.	
	62	5717688		1998-02-10	Belanger et al.	
	63	5720033		1998-02-17	Deo	
	64	5724521		1998-03-03	Dedrick	
	65	5727057		1998-03-10	Emery et al.	
	66	5729680		1998-03-17	Belanger et al.	
	67	5771283		1998-06-23	Chang et al.	
	68	5774534		1998-06-30	Mayer	
	69	5778304		1998-07-07	Grube et al.	
	70	5790974		1998-08-04	Tognazzini, Bruce	
	71	5794210		1998-08-11	Goldhaber et al.	
	72	5796727		1998-08-18	Harrison et al.	
	73	5798733		1998-08-25	Ethridge	
	74	5806018		1998-09-08	Smith et al.	
	75	5812763		1998-09-22	Teng	
	76	5819155		1998-10-06	Worthey et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	77	5835061		1998-11-10	Stewart	
	78	5838774		1998-11-17	Weisser, Jr.	
	79	5842010		1998-11-24	Jain et al.	
	80	5845211		1998-12-01	Roach	
	81	5852775		1998-12-22	Hidary, Murray	
	82	5855007		1998-12-29	Jovicic et al.	
	83	5870724		1999-02-09	Lawlor et al.	
	84	5875186		1999-02-23	Belanger et al.	
	85	5875401		1999-02-23	Rochkind	
	86	5878126		1999-03-02	Velamuri et al.	
	87	5880958		1999-03-09	Helms et al.	
	88	5881131		1999-03-09	Farris et al.	
	89	5884284		1999-03-16	Peters et al.	
	90	5889953		1999-03-30	Thebaut et al.	
	91	5896440		1999-04-20	Reed et al.	
	92	5897640		1999-04-27	Veghte et al.	
	93	5903636		1999-05-11	Malik	
	94	5907544		1999-05-25	Rypinski	
	95	5920846		1999-07-06	Storch et al.	
	96	5922040		1999-07-13	Prabhakaran	
	97	5923702		1999-07-13	Brenner et al.	
	98	5933420		1999-08-03	Jaszewski et al.	
	99	5938721		1999-08-17	Dussell et al.	
	100	5949867		1999-09-07	Sonnenberg	
	101	5950130		1999-09-07	Coursey	
	102	5961593		1999-10-05	Gabber et al.	
	103	5963866		1999-10-05	Palamara et al.	
	104	5963913		1999-10-05	Henneuse et al.	
	105	5968176		1999-10-19	Nessett et al.	
	106	5969678		1999-10-19	Stewart	
	107	5982867		1999-11-09	Urban et al.	
	108	5983091		1999-11-09	Rodriguez	
	109	5987381		1999-11-16	Oshizawa	
	110	5991287		1999-11-23	Diepstraten et al.	
	111	5995015		1999-11-30	De Temple et al.	
	112	6006090		1999-12-21	Coleman et al.	
	113	6009398		1999-12-28	Mueller et al.	
	114	6011975		2000-01-04	Emery et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	115	6026151		2000-02-15	Bauer et al.	
	116	6028921		2000-02-22	Malik et al.	
	117	6047327		2000-04-04	Tso et al.	
	118	6055637		2000-04-25	Hudson et al.	
	119	6058106		2000-05-02	Cudak et al.	
	120	6067297		2000-05-23	Beach	
	121	6076080		2000-06-13	Morscheck et al.	
	122	6085086		2000-07-04	La Porta et al.	
	123	6091956		2000-07-18	Hollenberg	
	124	6101381		2000-08-08	Tajima et al.	
	125	6101443		2000-08-08	Kato et al.	
	126	6112186		2000-08-29	Bergh et al.	
	127	6115669		2000-09-05	Watanabe et al.	
	128	6122520		2000-09-19	Want et al.	
	129	6133853		2000-10-17	Obradovich et al.	
	130	6138003		2000-10-24	Kingdon et al.	
	131	6138119		2000-10-24	Hall et al.	
	132	6141609		2000-10-31	Herdeg et al.	
	133	6144645		2000-11-07	Struhsaker et al.	
	134	6154152		2000-11-28	Ito	
	135	6154637		2000-11-28	Wright et al.	
	136	6157829		2000-12-05	Grube et al.	
	137	6163274		2000-12-19	Lindgren, Gary L.	
	138	6167255		2000-12-26	Kennedy, III et al.	
	139	6182226		2001-01-30	Reid et al.	
	140	6184829		2001-02-06	Stilp	
	141	6185426		2001-02-06	Alperovich et al.	
	142	6185484		2001-02-06	Rhinehart	
	143	6192314		2001-02-20	Khavakh et al.	
	144	6202054		2001-03-13	Lawlor et al.	
	145	6205478		2001-03-20	Sugano et al.	
	146	6208854		2001-03-27	Roberts et al.	
	147	6208866		2001-03-27	Rouhollahzadeh et al.	
	148	6226277		2001-05-01	Chuah	
	149	6229477		2001-05-08	Chang et al.	
	150	6229810		2001-05-08	Gerszberg et al.	
	151	6233329		2001-05-15	Urban et al.	
	152	6233452		2001-05-15	Nishino	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	153	6236360		2001-05-22	Rudow et al.	
	154	6236940		2001-05-22	Rudow et al.	
	155	6246361		2001-06-12	Weill et al.	
	156	6259405		2001-07-10	Stewart et al.	
	157	6263209		2001-07-17	Reed et al.	
	158	6278938		2001-08-21	Alumbaugh	
	159	6285665		2001-09-04	Chuah et al.	
	180	6285931		2001-09-04	Hattori et al.	
	181	6298234		2001-10-02	Brunner	
	182	6308273		2001-10-23	Goertzel et al.	
	183	6311069		2001-10-30	Havinis et al.	
	184	6317718		2001-11-13	Fano	
	185	6321092		2001-11-20	Fitch et al.	
	186	6324396		2001-11-27	Vasa et al.	
	187	6326918		2001-12-04	Stewart	
	188	6327254		2001-12-04	Chuah	
	189	6327357		2001-12-04	Meek et al.	
	190	6332127		2001-12-18	Bandera et al.	
	191	6332163		2001-12-21	Bowman-Amuah	
	192	6343290		2002-01-29	Cossins et al.	
	193	6353664		2002-03-05	Cannon et al.	
	194	6359880		2002-03-19	Curry et al.	
	195	6360101		2002-03-19	Irvin	
	196	6366561		2002-04-02	Bender	
	197	6377548		2002-04-23	Chuah et al.	
	198	6377810		2002-04-23	Geiger et al.	
	199	6377982		2002-04-23	Rai et al.	
	200	6385531		2002-05-07	Bates et al.	
	201	6385591		2002-05-07	Mankoff	
	202	6389426		2002-05-14	Turnbull et al.	
	203	6393482		2002-05-21	Rai et al.	
	204	6400722		2002-06-04	Chuah et al.	
	205	6414950		2002-07-02	Rai et al.	
	206	6415019		2002-07-02	Savaglio et al.	
	207	6418308		2002-07-09	Heinonen et al.	
	208	6421441		2002-07-16	Dzuban	
	209	6421714		2002-07-16	Rai et al.	
	210	6427073		2002-07-30	Kortelsalmi et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	211	6427119		2002-07-30	Stefan et al.	
	212	6430276		2002-08-06	Bouvier et al.	
	213	6430562		2002-08-06	Kardos et al.	
	214	6442391		2002-08-27	Johansson et al.	
	215	6442687		2002-08-27	Savage, Colin	
	216	6449272		2002-09-10	Chuah et al.	
	217	6449497		2002-09-10	Kirbas et al.	
	218	6463533		2002-10-08	Calamera et al.	
	219	6470378		2002-10-22	Tracton et al.	
	220	6470447		2002-10-22	Lambert et al.	
	221	6473626		2002-10-29	Nevoux et al.	
	222	6477382		2002-11-05	Mansfield et al.	
	223	6477526		2002-11-05	Hayashi et al.	
	224	6484029		2002-11-19	Hughes et al.	
	225	6484092		2002-11-19	Seibel	
	226	6484148		2002-11-19	Boyd	
	227	6490291		2002-12-03	Lee et al.	
	228	6496491		2002-12-17	Chuah et al.	
	229	6496931		2002-12-17	Rajchel et al.	
	230	6505046		2003-01-07	Baker	
	231	6505048		2003-01-07	Moles et al.	
	232	6505049		2003-01-07	Dorenbosch	
	233	6505120		2003-01-07	Yamashita et al.	
	234	6505163		2003-01-07	Zhang et al.	
	235	6512754		2003-01-28	Feder et al.	
	236	6516055		2003-02-04	Bedeski et al.	
	237	6516416		2003-02-04	Gregg et al.	
	238	6519252		2003-02-11	Sallberg	
	239	6519458		2003-02-11	Oh et al.	
	240	6522876		2003-02-18	Weiland et al.	
	241	6526275		2003-02-25	Calvert	
	242	6526349		2003-02-25	Bullock et al.	
	243	6532418		2003-03-11	Chun et al.	
	244	6545596		2003-04-08	Moon	
	245	6546257		2003-04-08	Stewart	
	246	6560442		2003-05-06	Yost et al.	
	247	6560461		2003-05-06	Fomukong et al.	
	248	6577643		2003-06-10	Rai et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	249	6577644		2003-06-10	Chuah et al.	
	250	6594482		2003-07-15	Findikli et al.	
	251	6618474		2003-09-09	Reese, Morris	
	252	6618593		2003-09-09	Drutman et al.	
	253	6622016		2003-09-16	Sladek et al.	
	254	6628627		2003-09-30	Zendle et al.	
	255	6628928		2003-09-30	Crosby et al.	
	256	6628938		2003-09-30	Rachabathuni et al.	
	257	6633633		2003-10-14	Bedingfield	
	258	6640184		2003-10-28	Rabe, Duane Carl	
	259	6647257		2003-11-11	Owensby, Craig A.	
	260	6647269		2003-11-11	Hendrey et al.	
	261	6650901		2003-11-18	Schuster et al.	
	262	6654610		2003-11-25	Chen et al.	
	263	6662014		2003-12-09	Walsh	
	264	6665536		2003-12-16	Mahany	
	265	6665718		2003-12-16	Chuah et al.	
	266	6671272		2003-12-30	Vaziri et al.	
	267	6675017		2004-01-06	Zellner et al.	
	268	6675208		2004-01-06	Rai et al.	
	269	6677894		2004-01-13	Sheynblat et al.	
	270	6697783		2004-02-24	Brinkman et al.	
	271	6701160		2004-03-02	Pinder et al.	
	272	6701251		2004-03-02	Stefan et al.	
	273	6704311		2004-03-09	Chuah et al.	
	274	6716101		2004-04-06	Meadows et al.	
	275	6721406		2004-04-13	Contractor	
	276	6725048		2004-04-20	Mao et al.	
	277	6732080		2004-05-04	Blants	
	278	6732101		2004-05-04	Cook	
	279	6732176		2004-05-04	Stewart et al.	
	280	6738808		2004-05-18	Zellner et al.	
	281	6754504		2004-06-22	Reed	
	282	6754582		2004-06-22	Smith et al.	
	283	6772064		2004-08-03	Smith et al.	
	284	6799049		2004-09-28	Zellner et al.	
	285	6801509		2004-10-05	Chuah et al.	
	286	6816720		2004-11-09	Hussain et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	287	6819929		2004-11-16	Antonucci et al.	
	288	6829475		2004-12-07	Lee et al.	
	289	6850758		2005-02-01	Paul et al.	
	290	6867733		2005-03-15	Sandhu et al.	
	291	6868074		2005-03-15	Hanson, Joel	
	292	6874011		2005-03-29	Spielman	
	293	6876858		2005-04-15	Duvall et al.	
	294	6898569		2005-05-24	Bansal et al.	
	295	6937869		2005-08-30	Rayburn	
	296	6954147		2005-10-11	Cromer et al.	
	297	6985747		2006-01-10	Chithambaram	
	298	6999572		2006-02-04	Shaffer et al.	
	299	7005985		2006-02-28	Steeves	
	300	7023995		2006-04-04	Olsson	
	301	7043231		2006-05-09	Bhatia et al.	
	302	7069319		2006-06-27	Zellner et al.	
	303	7085555		2006-08-01	Zellner et al.	
	304	7103368		2006-09-05	Teshima	
	305	7103476		2006-09-05	Smith et al.	
	306	7106843		2006-09-12	Gainsboro et al.	
	307	7110749		2006-09-19	Zellner et al.	
	308	7116977		2006-10-03	Moton et al.	
	309	7124101		2006-10-17	Mikurak	
	310	7130631		2006-10-31	Enzmann et al.	
	311	7139722		2006-11-21	Perrella et al.	
	312	7181225		2007-02-20	Moton et al.	
	313	7181529		2007-02-20	Bhatia et al.	
	314	7188027		2007-03-06	Smith et al.	
	315	7190960		2007-03-13	Wilson et al.	
	316	7203502		2007-04-10	Wilson et al.	
	317	7212829		2007-05-01	Lau et al.	
	318	7224978		2007-05-29	Zellner et al.	
	319	7236799		2007-06-26	Wilson et al.	
	320	7245925		2007-07-17	Zellner	
	321	7260378		2007-08-21	Holland et al.	
	322	7272493		2007-09-18	Hamrick et al.	
	323	7292939		2007-11-06	Smith et al.	
	324	7295924		2007-11-13	Smith et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	325	7362851		2008-04-22	Contractor	
	326	7383052		2008-06-03	Moton et al.	
	327	RE39717		2007-07-03	Yates et al.	
	328	5363377		1994-11-08	Sharpe	
	329	5625668		1997-04-29	Loomis	
	330	5455807		1995-10-03	Nepple	
	331	5586254		1996-12-07	Kondo et al.	
	332	5089814		1992-02-18	DeLuca et al.	
	333	5265070		1993-11-23	Minowa	
	334	5131020		1992-07-14	Liebesny et al.	
	335	5245608		1993-09-14	Deaton et al.	
	336	5583864		1996-12-10	Lightfoot et al.	
	337	5590196		1996-12-13	Moreau	
	338	5594779		1997-01-14	Goodman	
	339	5592470		1997-01-07	Rudrapatna et al.	
	340	5664948		1997-09-09	Dimitriadis et al.	
	341	5677905		1997-10-14	Bigham	
	342	5704049		1997-12-30	Briechle	
	342	5887259		1999-03-23	Zicker et al.	
	343	6067082		2000-05-23	Enmei	
	344	6157946		2000-12-05	Itakura et al.	
	345	7155199		2006-12-26	Zalewski et al.	
	346	5121126		1992-06-09	Clagett	
	347	5608854		1997-03-04	Labedz et al.	
	348	5561704		1996-10-01	Samilando	
	349	5892454		1999-04-06	Schipper et al.	
	350	6340958		2002-01-22	Cantu et al.	
	351	5347632		1994-09-13	Filepp et al.	
	352	6018293		2000-01-25	Smith et al.	
	353	5539395		1996-07-23	Buss et al.	
	354	5214793		1993-05-25	Conway et al.	
	355	5826195		1998-10-20	Westerlage et al.	
	356	6820062		2004-11-05	Gupta et al.	
	357	6937998		2005-08-30	Swartz et al.	
	358	6759960		2004-07-06	Stewart et al.	
	359	6697018		2004-02-24	Stewart et al.	
	360	7058594		2006-06-06	Stewart et al.	
	361	7009556		2006-03-07	Stewart et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	362	4255619		1981-03-10	Saito	
	363	4536647		1985-08-20	Atalla et al.	
	364	4845504		1989-07-04	Roberts, et al.	
	365	4973952		1990-11-27	Malec et al.	
	366	4974170		1990-11-27	Bouve et al.	
	367	5363245		1997-06-03	Ernst et al.	
	368	5870724		1999-02-09	Lawlor et al.	
	369	6407673		2002-06-18	Lane	
	370	6408307		2002-06-18	Semple et al.	
	371	6414635		2002-07-02	Stewart et al.	
	372	6442479		2002-08-27	Barton	
	373	6452498		2002-09-17	Stewart	
	374	6615131		2003-09-02	Rennard et al.	
	375	6405123		2002-06-11	Rennard et al.	
	376	626615		2001-07-24	Jin	
	377	4644351		1987-02-17	Zabarsky et al.	
	378	5337044		1944-08-09	Folger et al.	
	379	5469362		1995-11-23	Hunt et al.	
	380	5758049		1998-11-10	Johnson et al.	
	381	5835061		1998-11-10	Stewart	
	382	5969678		1998-10-19	Stewart	
	383	6073062		2000-06-06	Hoshino et al.	
	384	6236362		2001-05-22	Leblanc et al.	
	385	6326918		2001-12-04	Stewart	
	386	6259405		2001-07-10	Stewart et al.	
	387	6252544		2001-06-26	Hoffberg	
	388	6414635		2002-07-02	Stewart et al.	
	389	6452498		2002-09-17	Stewart	
	390	6697018		2004-02-24	Stewart	
	391	6731238		2004-05-04	Johnson	
	392	6759960		2004-07-06	Stewart	
	393	7009556		2006-03-07	Stewart	
	394	5196031		1993-03-16	Ordish	
	395	6345288		2002-02-05	Reed et al.	
	396	6571279		2003-05-27	Herz et al.	
	397	6456234		2002-09-24	Johnson	
	398	6246948		2001-06-12	Thakker	
	399	7386396		2008-06-10	Johnson	

Substitute for form 1449/PTO				Complete if Known		
				Application Number	14/033,540	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	400	7177651		2007-02-13	Almassy	
	401	7787887		2010-08-31	Gupta et al.	
	402	6427115		2002-07-30	Sekiyama	
	403	6370389		2002-04-09	Isomursu et al.	
	404	6381311		2002-04-30	Joyce et al.	
	405	6389055		2002-05-14	August et al.	

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Complete if Known	
	Application Number	14/033,540
	Filing Date	2013-09-23
	First Named Inventor	William J. Johnson
	Examiner Name	Not yet assigned
	Art Unit	2668
Attorney Docket No.	JOHNS-001US3	

U.S. PATENT APPLICATION PUBLICATIONS

Examiner Initials	Cite No.	Publication Number	Kind Code	Publication Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	2001/0021646		2001-09-13	Antonucci et al.	
	2	2001/0034709		2001-10-25	Stoifo et al.	
	3	2001/0049275		2001-12-06	Pierry et al.	
	4	2001/0051911		2001-12-13	Marks et al.	
	5	2002/0037709		2002-03-28	Bhatia et al.	
	6	2002/0037722		2002-03-28	Hussain et al.	
	7	2002/0037731		2002-03-28	Mao et al.	
	8	2002/0037744		2002-03-28	Bhatia et al.	
	9	2002/0037750		2002-03-28	Hussain et al.	
	10	2002/0038362		2002-03-28	Bhatia et al.	
	11	2002/0038384		2002-03-28	Khan et al.	
	12	2002/0038386		2002-03-28	Bhatia et al.	
	13	2002/0052781		2002-05-02	Aufricht et al.	
	14	2002/0077083		2002-06-20	Zellner et al.	
	15	2002/0077084		2002-06-20	Zellner et al.	
	16	2002/0077118		2002-06-20	Zellner et al.	
	17	2002/0077130		2002-06-20	Owensby	
	18	2002/0077897		2002-06-20	Zellner et al.	
	19	2002/0087335		2002-07-01	Meyers et al.	
	20	2002/0090932		2002-07-04	Bhatia et al.	
	21	2002/0095312		2002-07-18	Wheat	
	22	2002/0102993		2002-08-01	Hendrey et al.	
	23	2002/0107027		2002-08-08	O'Neil	
	24	2002/0120713		2002-08-29	Gupta et al.	
	25	2002/0161637		2002-10-31	Sugaya	
	26	2002/0174147		2002-11-21	Wang et al.	
	27	2003/0016233		2003-01-23	Charpentier	
	28	2003/0140088		2003-07-24	Robinson et al.	
	29	2003/0169151		2003-09-11	Ebling et al.	
	30	2004/0002329		2004-01-01	Bhatia et al.	
	31	2004/0097243		2004-05-20	Zellner et al.	
	32	2004/0111269		2004-06-10	Koch	
	33	2004/0164898		2004-08-26	Stewart	
	34	2004/0203903		2004-10-14	Wilson et al.	
	35	2004/0205198		2004-10-14	Zellner et al.	
	36	2004/0266453		2004-12-30	Maanoja et al.	
	37	2005/0043036		2005-02-24	loppe et al.	
	38	2005/0060365		2005-03-17	Robinson et al.	
	39	2005/0096067		2005-05-05	Martin, Dannie E.	
	40	2005/0114777		2005-05-26	Szeto	
	41	2005/0151655		2005-07-14	Hamrick et al.	
	42	2005/0246097		2005-11-03	Hamrick et al.	
	43	2005/0272445		2005-12-08	Zellner, Samuel	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENT APPLICATION PUBLICATIONS						
Examiner Initials	Cite No.	Publication Number	Kind Code	Publication Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	44	2006/0030335		2006-02-09	Zellner et al.	
	45	2006/0030339		2006-02-09	Zhovnirovsky et al.	
	46	2006/0059043		2006-03-16	Chan et al.	
	47	2006/0089134		2006-04-27	Moton et al.	
	48	2006/0094447		2006-05-04	Zellner, Samuel	
	49	2006/0099966		2006-05-11	Moton et al.	
	50	2006/0105784		2006-05-18	Zellner et al.	
	51	2006/0106537		2006-05-18	Hamrick et al.	
	52	2006/0167986		2006-07-27	Trzyna et al.	
	53	2006/0189327		2006-08-24	Zellner et al.	
	54	2006/0189332		2006-08-24	Benco et al.	
	55	2006/0195570		2006-08-31	Zellner et al.	
	56	2006/0253252		2006-11-09	Hamrick et al.	
	57	2007/0010260		2007-01-11	Zellner et al.	
	58	2007/0042789		2007-02-22	Moton et al.	
	59	2007/0105565		2007-05-10	Enzmann et al.	
	60	2007/0124721		2007-05-31	Cowing et al.	
	61	2007/0136603		2007-06-14	Kuecuekyan	
	62	2007/0250920		2007-10-25	Lindsay	
	63	2008/0096529		2008-04-24	Zellner	
	64	2005/0017068		2005-01-27	Zalewski et al.	
	65	2001/0028301		2001-10-11	Geiger et al.	
	66	2001/0007450		2001-07-12	Begum	
	67	2004/0186902		2004-09-23	Stewart et al.	
	68	2006/0164302		2006-07-27	Stewart et al.	
	69	2006/0183467		2006-08-17	Stewart et al.	
	70	2006/0059043		2006-03-16	Stewart et al.	
	71	2002/0035474		2002-03-31	Alpdemir	
	72	2001/0001239		2001-05-17	Stewart	
	73	2002/0046090		2002-04-18	Stewart	
	74	2003/0003990		2003-01-02	Von Kohorn	
	75	2003/0018527		2003-01-23	Filepp et al.	
	76	2002/0035493		2002-03-21	Mozayeny et al.	
	77	2002/0046069		2002-04-18	Mozayeny et al.	
	78	2002/0046077		2002-04-18	Mozayeny et al.	
	79	2002/0091991		2002-07-11	Castro	
	80	2005/0004838		2005-01-06	Perkowski et al.	
	81	2005/0002419		2005-01-06	Doviak et al.	
	82	2004/0264442		2004-12-30	Kubler et al.	
	83	2004/0246940		2004-12-09	Kubler et al.	
	84	2004/0228330		2004-11-18	Kubler et al.	
	85	2004/0151151		2004-08-05	Kubler et al.	
	86	2004/0252051		2004-12-16	Johnson	
	87	2007/0005188		2007-01-04	Johnson	
	88	2007/0233387		2007-10-04	Johnson	

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Complete if Known	
	Application Number	14/033,540
	Filing Date	2013-09-23
	First Named Inventor	William J. Johnson
	Examiner Name	Not yet assigned
	Art Unit	2668
Attorney Docket No.	JOHNS-001US3	

U.S. PATENT APPLICATION PUBLICATIONS

Examiner Initials	Cite No.	Publication Number	Kind Code	Publication Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	89	2007/0276587		2007-11-29	Johnson	
	90	2007/0232326		2007-10-04	Johnson	
	91	2008/0030308		2008-02-07	Johnson	
	92	2006/0022048		2006-02-02	Johnson	
	93	2009/0233622		2009-09-17	Johnson	
	94	2009/0233633		2009-09-17	Johnson	
	95	2010/0069035		2010-03-18	Johnson	
	96	2010/0227595		2010-09-09	Johnson	
	97	2006/0010202		2006-01-12	Blackstock et al.	
	98	2004/0201459		2004-10-14	Rich et al.	
	99	2006/0136544		2006-06-22	Atsmon et al.	
	100	2007/0281716		2007-12-06	Altman et al.	
	101	2006/0240828		2006-10-26	Jain et al.	
	102	2007/0275730		2007-11-29	Bienas et al.	
	103	2006/0194589		2006-08-31	Sankisa	
	104	2007/0287473		2007-12-13	Dupray	
	105	2008/0071761		2008-03-20	Singh et al.	
	106	2004/0116131		2004-06-17	Hochrainer et al.	
	107	2007/0275730		2007-11-29	Bienas et al.	
	108	2007/0244633		2007-10-18	Phillips et al.	
	109	2008/0170679		2008-07-17	Sheha et al.	
	110	2005/0050227		2005-03-03	Michelman	
	111	2003/0030731		2003-02-13	Colby	
	112	2006/0009190		2006-01-12	Laliberte	
	113	2006/0198359		2006-09-07	Fok et al.	
	114	2001/0005864		2001-06-28	Mousseau et al.	
	115	2010/0146160		2010-06-10	Piekarski	
	116	2005/0283833		2005-12-22	Lalonde et al.	
	117	2010/0159946		2010-06-24	Cheung et al.	
	118	2002/0095454		2002-07-18	Reed et al.	
	119	2006/0252465		2006-11-09	Karstens et al.	
	120	2008/0301561		2008-12-04	Bain	
	121	2009/0067593		2009-03-12	Ahlin	
	122	2009/0167524		2009-07-02	Chesnutt et al.	
	123	2009/0190734		2009-07-16	White et al.	
	124	2009/0054077		2009-02-26	Gauthier et al.	
	125	2006/0194589		2006-08-31	Sankisa	
	126	2011/0021145		2011-01-27	Johnson et al.	
	127	2010/0235748		2010-09-16	Johnson et al.	
	128	2009/0233623		2009-09-17	Johnson et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
FOREIGN PATENT DOCUMENTS						
Examiner Initial	Cite No.	Foreign Patent Document Number	Kind Code	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	WO 00/076249		2000-12-14	Telefonaktiebolaget LM Ericsson	
	2	EP 779752		2004-06-16	AT&T Corp.	
	3	EP 838933		2008-04-29	IBM Corporation	
	4	EP 915590		1999-05-12	Unwired Planet, Inc.	
	5	EP 917320		1999-05-19	Lucent Technologies, Inc.	
	6	EP 924914		2003-04-23	Nokia Corporation	
	7	EP 935364		1999-08-11	AT&T Corp.	
	8	WO 99/16263		1999-04-01	Nokia Telecommunications	
	9	WO 99/51005		1999-10-07	Transaccess Corp.	
	10	EP 0712227		1996-05-01	Harris Corporation	
	11	EP 1435749		2004-07-01	Evolium S.A.S.	
	12	EP 1445923		2004-08-01	NEC Corporation	
	13	GB 2396779		2004-06-01	Samsung Electronics Co., Ltd	
	14	JP 11-168478		1999-06-01	Pronet Tracking System, Inc.	
	15	JP 01-194628		1989-08-01	NEC Corporation	
	16	JP 03-128540		1991-05-01	Hitachi Comm. Syst., Inc.	
	17	JP 07-234789		1995-09-01	Hitachi Ltd	
	18	JP 07-288514		1995-10-01	Mita Ind. Co., Ltd	
	19	JP 07-319706		1995-12-01	Hitachi Ltd	
	20	JP 08-44568		1996-02-01	Hitachi Zosen Group	
	21	JP 08-87296		1996-04-01	Hamagami et al.	
	22	WO 00/02365		2000-01-01	Bell South Int. Prop. Corp.	
	23	WO 02/11407		2002-02-01	Bell South Int. Prop. Corp.	
	24	WO 04/80092		2004-09-01	Siemens Aktiengesellschaft	
	25	WO 98/19484		1998-05-01	Siemens Aktiengesellschaft	
	26	WO 99/27716		1999-06-01	Ericsson, Inc.	
	27	WO 99/55012		1999-10-01	Netline Communications Technologies LTD	

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Complete if Known	
	Application Number	14/033,540
	Filing Date	2013-09-23
	First Named Inventor	William J. Johnson
	Examiner Name	Not yet assigned
	Art Unit	2668
Attorney Docket No.	JOHNS-001US3	

NON PATENT LITERATURE

Examiner Initial	Cite No.	Include name of author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.
	1	Bill N. Schilit and Marvin M. Theimer, Disseminating Active Map Information Mobile Hosts, IEEE Network, September/October 1994.
	2	Andy Harter and Andy Hooper, A Distributed Location system for the Active Office, IEEE Network, January/February 1994.
	3	Max J. Egenhofer, Spatial SQL: A Query and Presentation Language, IEEE Network, February 1994.
	4	Mike Spreitzer and Marvin Theimer, Providing Location Information in a Ubiquitous Computing Environment, Proceedings of the Fourteenth ACM Symposium on Operating Systems Principles, December 1993.
	5	George W. Fitzmaurice, Situated Information Spaces and Spatially Aware Palmtop Computers, Communication of the ACM, July 1993.
	6	Ronald Azuma, Tracking Requirements for Augmented Reality, Communications of the ACM, Vol. 36 No. 1, January 1992.
	7	Roy Want, et al., The Active Badge Location System, ACM Transactions on Information Systems, Vol. 10, No. 1, January 1992.
	8	Marvin White, Emerging Requirements for Digital Maps for In-Vehicle Pathfinding and Other Traveller Assistance, Vehicular Navigation and Information Systems Conference Proceedings, Part 1, October 1991.
	9	Fred Phail, The Power of a Personal Computer for Car Information and Communications Systems, Vehicular Navigation and Information Systems Conference Proceedings, Part 1, October 1991.
	10	Thomas A. Dingus, et al., Human Factors Engineering the TravTek Driver Interface, Vehicular Navigation and Information Systems Conference Proceedings, Part II, October 1991.
	11	Michael Muffat et al., European Cooperation on Dual Mode Route Guidance Perspectives for Advanced Research Partners, Vehicular Navigation and Information Systems Conference Proceedings, Part II, October 1991.
	12	High-Performance Wireless Access Point for the Enterprise, ORiNOCO™ AP-100 Access Point for the Enterprise, Lucent Technologies, 2000
	13	MobileStar Network, MobileStar Network First to Provide Business Travelers with High-Speed Data Access via the Internet-Wirelessly, New York, NY, June 24, 1998
	14	ORiNCO AP-1000 - Getting Started, Lucent Technologies
	15	Harry Chen, et al., "Dynamic Service Discovery for Mobile Computing: Intelligent Agents Meet Jini in the Aether," Cluster Computing, Special Issue on Internet Scalability, vol. 4, no. 4, February 2001
	16	3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; Functional Stage 2 Description of Location Services in UMTS (1999)
	17	http://www.openwave.com/us/news_room/press_releases/2001/20020320 , "Open Wave Announces Availability to End-to-End Set of Location Services for Wireless Internet".
	18	Trembly, A., "Wireless products arm road warriors," National Underwriter, Vol. 105, No. 3, pp 23-25, Dialog 02113577 67213220 (January 2001)
	19	Antonio, Interfaces and Algorithms for a Wide -Area Event Notification Service, October 1999.

Examiner:

Date Considered:

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Complete if Known		
	Application Number	14/033,540	
	Filing Date	2013-09-23	
	First Named Inventor	William J. Johnson	
	Examiner Name	Not yet assigned	
	Art Unit	2668	
Attorney Docket No.	JOHNS-001US3		
CERTIFICATION STATEMENT			
Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s): <input type="checkbox"/> That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1). OR <input type="checkbox"/> That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2). <input type="checkbox"/> See attached certification statement. <input type="checkbox"/> Fee set forth in 37 CFR 1.17 (p) has been submitted herewith. <input checked="" type="checkbox"/> None			
SIGNATURE			
A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.			
Signature	/Craig J. Yudell/	Date (YYYY-MM-DD)	2013-11-12
Name/Print	Craig J. Yudell	Registration No.	39,083
This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.			

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
14 December 2000 (14.12.2000)

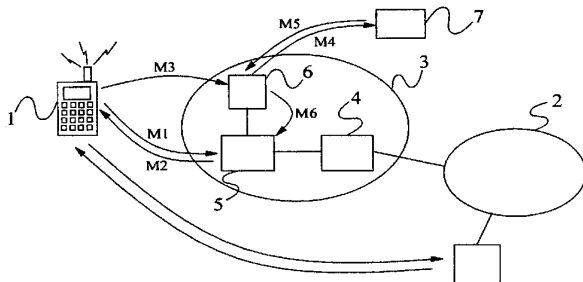
PCT

(10) International Publication Number
WO 00/76249 A1

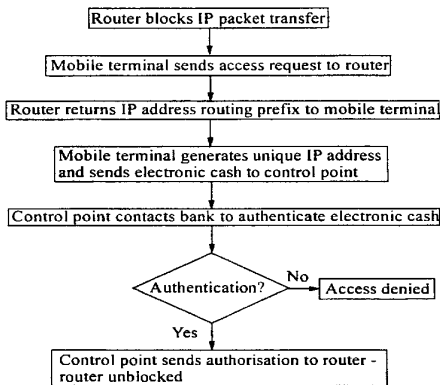
- (51) International Patent Classification?: H04Q 7/38, H04L 12/56
- (72) Inventors: VILANDER, Harri; Albergan Esplanadi 11 A 3, FIN-02600 Espoo (FI). JOKELA, Petri; Kyyhkysmäki 16 B 29, FIN-02600 Espoo (FI). VUOPIONPERÄ, Raimo; Ruusulankatu 1 C 31, FIN-00260 Helsinki (FI).
- (21) International Application Number: PCT/SE00/01136
- (74) Agent: ERICSSON RADIO SYSTEMS AB; Ericsson Research, Patent Support Unit, S-164 80 Stockholm (SE).
- (22) International Filing Date: 31 May 2000 (31.05.2000)
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.
- (25) Filing Language: English
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European
- (26) Publication Language: English
- (30) Priority Data:
9926180.2 8 June 1999 (08.06.1999) GB
9913152.6 8 June 1999 (08.06.1999) GB
- (71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE).

[Continued on next page]

(54) Title: MOBILE INTERNET ACCESS



(57) Abstract: A method of authorising an Internet Protocol (IP) enabled mobile host (1) to access the Internet (2) via a wireless LAN, GSM, or UMTS access network (3) comprises initially sending an IP access request from the mobile host (1) to an IP router (5) within the access network (3). In response to receipt of said access request at the IP router (5), an IP address routing prefix is sent from the IP router (5) to the mobile host (1). Electronic cash is then forwarded from the mobile host (1) to a control point (6) within the access network (3). The control point (6) confirms the authenticity and/or sufficiency of the electronic cash and, providing that confirmation is made, sends an authorisation message to the IP router (5). The IP router (5) blocks the transmission of IP packets between the mobile host (1) and the Internet (2) prior to receipt of the authorisation message and permits the passage of IP packets only after an authorisation message has been received.



WO 00/76249 A1



patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *With international search report.*

MOBILE INTERNET ACCESS

Field of the Invention

The present invention relates to mobile Internet access and in particular, though not necessarily, to mobile Internet access with a mobile wireless host.

Background to the Invention

With the increasing use of the Internet, interest has grown in the possibility of accessing the Internet using mobile hosts which are able to roam between access networks. These access networks may be networks to which the mobile hosts are connected via fixed lines or may be wireless networks to which the mobile hosts are connected using a radio interface. Examples of fixed line networks are Ethernet networks whilst examples of wireless networks are mobile telephone networks as well as wireless Local Area Networks (LANs).

A difficulty which must be overcome in order to fully implement mobile Internet access with roaming, is the need to authenticate and/or authorise a roaming host (or rather the subscriber using the mobile host) which uses a foreign network as its access network. It is generally envisaged that such a roaming host should belong to a subscriber of some other network, i.e. the subscriber's 'home' network, and that the foreign access network must contact this home network in order to authorise the roaming host.

One disadvantage of this proposal is that it does not enable a mobile host to access the Internet anonymously. That is to say that in order to access the Internet a roaming host must disclose its identity either to the access network or to some other home network. Another disadvantage is that a trust relationship must exist between the home network and the access network in order that the networks can confidently exchange billing information. Whilst it may be straightforward to establish a trust relationship between two telecoms operators for example, it may be more difficult where the access network is a wireless Local Area Network operated, for example, in an Internet café.

Summary of the Invention

According to a first aspect of the invention there is provided a method of authorising an Internet Protocol (IP) enabled mobile host to access the Internet via an access network, the method comprising:

negotiating an IP address between the mobile host and the access network and/or other hosts attached to the access network;

sending electronic cash or other authentication message from the mobile host to a control point within the access network; and

confirming at the control point the authenticity of said electronic cash or authentication message and, providing that confirmation is made, sending an authorisation message from the control point to an IP node,

wherein the IP node blocks the transmission of IP packets between the mobile host and the Internet prior to receipt of said authorisation message and permits the passage of IP packets only after an authorisation message has been received.

Anonymous access is possible where a mobile host has access to electronic cash which can be transferred from the mobile host to the access network. Providing that sufficient electronic cash is transferred to the access network, the access network may authorise the mobile host to access the Internet without the need to refer to some other home network of the mobile host.

It will be appreciated that the present invention is applicable in particular to IPv6.

Preferably, upon receipt of the electronic cash at the control point, the control point contacts a bank, or other electronic cash provider or node of the access network, in order to authenticate and ensure the sufficiency of the received electronic cash.

Providing that the bank (or cash provider or other node) returns a confirmation or authentication message to the control point, the control point is able to send the authorisation message to the IP node in order to allow the passage of IP data packets between the mobile host and the Internet.

Preferably, electronic cash payments are incorporated into IP packets sent from the mobile host to the control point. More preferably, the payments are incorporated into the option field of IP packets. Other payment related messages may also be incorporated into IP packets. These include; a price enquiry message sent from the mobile host to the control point, a price list message sent from the control point to the mobile host, and a request for further payment also sent from the control point to the mobile host.

As an alternative to the use of electronic cash, the mobile host may transmit a password or certificate to the control point. The authenticity of the password or certificate may then be checked with a foreign network operator or the like.

Preferably, said IP node provides routing functionality for IP data packets. This node may also provide for protocol conversion between the carrier protocol used by the access network, and that used by the Internet. However, where the carrier protocol of the access network is compatible with that of the Internet, no such conversion may be required. The control point and the IP node may be co-located. Electronic cash or said other authentication message may be sent to the control point via the router. The payments may be piggybacked onto IP datagrams. Payments or authorisation messages may be extracted by the router and forwarded to the control point.

Preferably, said step of negotiating an IP address is carried out in response to the sending of an IP access request from the mobile host to said IP node within the access network. Alternatively, the negotiation may be initiated by receipt of a network advertisement message broadcast by the access network.

The step of negotiating an IP address between the mobile host and the access network may comprise sending an IP address or part thereof from the IP node, or another network node, to the mobile host. In certain embodiments of the present invention, subsequent to receipt of the access request at the IP node, the IP node or other network node returns to the mobile host an IP address prefix. The remainder of the IP address may be provided or generated by the mobile host itself. This remaining part of the IP address may be an International Mobile Subscriber Identity (IMSI) code in the case

where the access network is a mobile telephone network and the mobile host is a mobile telephone host or the like. Where the access network is a fixed line access network, the remaining part of the IP address may be the address of the mobile host within that network, e.g. an Ethernet address in the case of an Ethernet network.

Said other network node may be a DHCP server. The control point may be incorporated into the DHCP server, so that the e-cash payments are received by the DHCP server. The DHCP server sends open and close messages to said IP node to unblock or block the flow of IP packets to and from said IP node.

The term "negotiating" used above encompasses a step of sending a Neighbour Solicitation message from the mobile host to other hosts connected to the network. In the event that there is an IP address collision, a host may respond by sending a Neighbour Advertisement message to the mobile host.

The access network may be a wireless Local Area Network (LAN) or Wide Area Network (WAN). In this case, where the IP node returns a part of an IP address, the remainder of the address may correspond to the address of the host in the access network, e.g. an Ethernet address. Alternatively, the access network may be a mobile telecommunications network such as a GSM network or a UMTS network.

Preferably, the method of the present invention comprises temporarily allocating to the mobile host a home agent located in the access network. More preferably, this allocation exists for the duration of the Internet connection. The home agent is responsible for routing datagrams to the mobile host in the event that the mobile host roams within the access network and may also remain responsible when the mobile host roams out of the access network into a new access network.

Preferably, the method comprises informing an Internet server of the IP address allocated to the mobile host, or of an IP address of an allocated home agent. The server maintains a mapping between mobile host identities and temporary IP addresses/home agent addresses for subscribing mobile hosts. A correspondent host wishing to communicate with the mobile host sends a mobile host identifier to the server. The

server may either forward the message to the mobile host or may return the temporary address to the correspondent host. In the former case, the Internet server may be a Call Control server (using the Session Initiation Protocol (SIP)), whilst in the latter case the Internet server may be a Domain Name System (DNS) server.

According to a second aspect of the present invention there is provided apparatus for use in enabling an Internet Protocol (IP) enabled mobile host to access the Internet, the apparatus comprising:

means for conducting a negotiation between the mobile host and the access network and/or other hosts attached to the access network to allocate a mobile address to the mobile host; and

a control point within the access network for receiving electronic cash or other authentication message sent from the mobile host and for confirming the authenticity of the sent electronic cash or authentication message and, providing that confirmation is made, for sending an authorisation message to an IP node,

the IP node being arranged in use to block the transfer of messages between the mobile host and the Internet prior to receipt of an authorisation message from the control point and being arranged to allow the transfer upon receipt of the authorisation message.

Brief Description of the Drawings

Figure 1 illustrates schematically a communication system for enabling a mobile IP host to access the Internet;

Figure 2 is a flow diagram illustrating an access method used in the system of Figure 1.

Figure 3a illustrates signalling between a mobile host and an Internet access network according to a first embodiment of the present invention;

Figure 3b illustrates further signalling in the embodiment of Figure 3a;

Figure 4 illustrates signalling between a mobile host and an Internet access network according to a second embodiment of the present invention;

Figure 5 illustrates signalling between a mobile host and an Internet access network according to a third embodiment of the present invention;

Figure 6 illustrates signalling between a mobile host, an access network, and the Internet, where the mobile host is temporarily attached to the access network;
Figure 7 illustrates signalling where the mobile host of Figure 6 roams within the access network; and
Figure 8 illustrates signalling where the mobile host of Figure 6 roams into a new access network.

Detailed Description of Certain Embodiments

There is illustrated in Figure 1 a telecommunications system in which a mobile host 1 is able to communicate with the Internet 2 by making use of an access network 3. In the example to be described here, the access network 3 is a wireless Local Area Network (LAN) whilst the mobile host 1 is a mobile wireless host. More particularly, the wireless LAN 3 is an Ethernet network, with the mobile host 1 comprising an Ethernet "card" which is programmed with an Ethernet address. Typically this address is worldwide unique and is allocated by the card manufacturer. In the example given here, the LAN 3 uses the TCP/IP protocol over the Ethernet connection. As an alternative to wireless LAN, it will be appreciated that other forms of access networks may be used including Wide Area Networks and mobile telecommunications networks (e.g. UMTS and GSM networks).

The wireless LAN 3 is coupled to the Internet 2 via an IP gateway node 4. This gateway node 4 is in turn connected to a number of "primary" IP routers 5 (only one of which is shown in the Figure) within the wireless LAN 3. Each of the primary IP routers 5 provides a gateway between the Ethernet LAN and the IP "world". This function involves protocol conversions if necessary. In addition, the primary routers 5 are involved in the allocation of IP addresses to the mobile hosts, which addresses are world-wide unique.

For the purpose of this example, it is assumed that the mobile host 1 does not have a subscription with the operator of the wireless LAN 3 or with any other network (e.g. LAN, WAN, telephone network etc) with which the wireless LAN 3 has a billing relationship. That is to say that the mobile host 3 does not have a "home" network.

When the mobile host 1 is within the radio coverage area of the wireless LAN 3 and is switched on, the mobile host 1 attempts to make a normal attachment to the wireless LAN 3. It does this via radio transceiver stations which are not illustrated in Figure 1. The mobile host 1 initiates a negotiation with one of the primary routers 5 (typically the router which is physically closest to the radio transceiver station which handles the host's access), requesting in message M1 an IP address routing prefix from the router. In the case of Internet Protocol version 6 (IPv6), this prefix contains 64 bits and is returned by the router 5 as message M2 to the mobile host 1 over the radio interface. In order to generate a complete IPv6 address, the mobile host 1 adds to the routing prefix an address part which is unique to the mobile host 1. This part may be generated, for example, using the Ethernet card address of the mobile host 1.

Following the return of the IPv6 address prefix from the router 5, and the formulation of the complete IP address, the router 5 does not immediately start coupling IP data packets between the mobile host 1 and the Internet 2. Rather, the router 5 awaits authorisation of the access request from a control point 6 to which the router 5 is connected.

The authorisation process at the control point 6 is conducted as follows. Firstly, upon receipt of the IP routing prefix from the router 5, the mobile host 1 transmits an amount of electronic cash (e-cash) M3 to the control point 6 via the radio transceiver station (and possibly via the router 5). The e-cash is accompanied by the IP address now allocated to the mobile host 1. In order to verify the amount and authenticity of the e-cash, the control point 6 contacts a bank or other e-cash provider 7 which is responsible for the transmitted e-cash. This may involve sending a certificate M4, which accompanies the e-cash, to the bank or e-cash provider 7. In the event that the amount of e-cash is insufficient, or the bank or e-cash provider 7 returns a message M5 indicating that the e-cash is not authentic, the control point 6 will return a fail message M6 to the mobile host 1 (possibly via the router 5) indicating that the access request is denied. The control point 6 will then notify the responsible router 5 of this situation.

Assuming on the other hand that the amount of e-cash sent to the control point 6 is sufficient, and that the bank or e-cash provider 7 returns in message M5 confirmation

that the e-cash is authentic, the control point 6 will transmit an authorisation message in message M6 to the responsible router 5. Upon receipt of the authorisation message, the router will start to relay IP packets between the mobile host 1 and the Internet 2. The mobile host 1 is then able to exchange IP data packets with a correspondent host 8, via the Internet.

Figure 2 is a flow diagram illustrating further the authorisation process described above.

The process described above, where an IP address is generated by the mobile host 1 itself, is referred to as "stateless address allocation". Figure 3a illustrates the signalling involved in this scenario where it is assumed that the control point 6 is integrated into the router 5 (i.e. in the following discussion it is assumed that communications regarding e-cash may be exchanged between the router 5 and the control point 6). The mobile host 1 first sends a Router Solicitation message to the router 5 of the access network 3. An e-cash enquiry message is "piggybacked" onto the Router Solicitation message. The router 5 responds with a Router Advertisement message telling the mobile host 1 how it must obtain an IP address. In addition, e-cash pricing information is placed in an option field of the Router Advertisement message. The mobile host 1 learns from this message whether the charging is time-based or volume-based, the exact pricing for IP address leasing (e.g. per minute or per kilobyte), and which types of e-cash payment the access network 3 will accept.

The mobile host 1 is able to accept or reject the terms proposed by the network 3. If the terms are accepted, the received information is used to set the e-cash "module" in the mobile host 1 so that the host 1 pays the correct amount of e-cash. The mobile host 1 generates an IP address and validates the address by broadcasting a Neighbour Solicitation message. All of the other hosts connected to the access network 3 listen to this message and will issue a Neighbour Advertisement message if the generated IP address corresponds to an already allocated address (alternatively the Neighbour Advertisement message may be sent to a server in the access network which records currently allocated IP addresses). In the event that there is no reply to the Neighbour Solicitation message, the mobile host 1 starts to send data through the router 5. E-cash is paid to the network 3 by piggybacking e-cash payments onto datagrams sent through

the router 5. Typically, e-cash payments are sent at intervals, as requested by the router 5 in the Router Advertisement message.

The router 5 extracts the e-cash payment from received datagrams and checks the validity of the payment as described above (using the services of the control point 6). Assuming that the access is authorised on the basis of the received payment, the basic datagram is then forwarded to the intended correspondent host 8 over the Internet 2. It is possible that an e-cash payment may run out if the mobile host 1 has not strictly obeyed the terms provided by the router 5. In this case, the router 5 may send a notify message to the mobile host 1 just prior to the payment running out, reminding the mobile host 1 to make a further payment. The mobile host 1 should respond with a further payment. A Request for Immediate Payment message may be sent to the mobile host 1 by the router 5 in the event that a payment has already run out, notifying the mobile host 1 of this fact and that the router 5 has started to discard received datagrams sent from (or to) the mobile host 1. This scenario is illustrated in Figure 3b.

It is noted that piggybacked payment related messages, such as a price enquiry or an e-cash payments, may be included into the IPv6 extension header (e.g. the "Hop-by-Hop" option field) of an IP datagram.

Figure 4a illustrates an alternative scenario to the stateless address allocation scenario described above. This is referred to as "stateful address allocation" and uses a server (not shown in Figure 1) in the access network 3 which maintains a list of all of the IP addresses allocated by the network 3. A protocol known as Dynamic Host Configuration Protocol (DHCP) has been specified by the Internet Engineering Task Force (IETF) for negotiating stateful address allocation between the server (DHCP server) and the mobile host 1. As with the stateless address allocation scenario, the process commences with the sending of a Router Solicitation message, containing a piggybacked price enquiry, from the mobile host 1 to the Router 5. The Router 5 again replies with a Router Advertisement message, containing a piggybacked price list. The mobile host 1 learns from the Router Advertisement message that it must obtain an IP address from the DHCP server. It does this using the DHCP protocol, and thereafter e-cash payments are piggybacked on IP datagrams sent to the router 5 (from where they

are sent to the control point). **Reminder and Request for Immediate Payment messages** can be sent from the router 5 to the mobile host 1.

It will be appreciated that in the scenario described above, the DHCP server does not require any modification to implement the invention. However, in order to facilitate time-based charging, a modification may be required to the DHCP server. This takes advantage of the fact that IP addresses allocation by the DHCP server normally have a limited lifetime. After a lifetime has expired, the mobile host must renew the IP address allocation. E-cash payments in respect of IP address renewals may be piggybacked on DHCP address renewal messages.

Two new control messages are required; an Open Route message and a Close Route message. These messages are sent from the DHCP server (acting as control point for the IP router) to the router to tell the router either to accept or discard datagrams received from (or sent to) the mobile host. This scenario requires that e-cash functionality be incorporated into the DHCP server, with "opening" and "closing" route functionality being incorporated into the router. Figure 5 illustrates the modified scenario.

The system described above works satisfactorily whilst a mobile host remains within one homogeneous network. However, it does not by itself provide for "roaming" between different types of access networks or between networks operated by different operators. When a mobile host "de-registers" with one network and registers with a new network, there is no mechanism for forwarding Internet datagrams, addressed to the old network, to the new network as the communication channel between the mobile host and the old network no longer exists. It is therefore necessary to open a new communication channel between the mobile host and the new network. All datagrams addressed to the old network and not yet received by the mobile host are lost as a result of this channel change. This is obviously not feasible for applications such as voice over IP or video telephony, and may also cause real problems for other applications such as www browsers and file transfers.

A mobile Internet access protocol (IPv6) which provides for roaming is currently being standardised by the Internet Engineering Task Force (IETF). This protocol makes use of a "home agent", located in a mobile host's home network (i.e. the network to which the mobile host subscribes), to keep track of the host when it leaves the home network. A mobile host is fixedly allocated an Internet address (or name) corresponding to the home network.

When a mobile host is registered with its home network, the functionality of the network's home agent is off for that host (i.e. the host is "deregistered" with the home agent) so that the home agent does not alter the flow of datagrams from the Internet to the network's router and the mobile host. When the mobile host leaves its home network and contacts a foreign network (FN), the host is allocated a temporary IP address by the foreign network. The mobile host then transmits the received Internet address to the home network's home agent, together with a registration instruction. The home agent registers the new status of the mobile host and records the newly allocated Internet address as a "care-of-address" for the host. Whenever the mobile host registers with a new foreign network, a new care-of-address is sent to the home network's home agent to replace the previously registered care-of-address.

It will be appreciated that, as a mobile host has a fixed Internet address allocated to it, datagrams destined for the host will at least in the first instance be sent to the home network (the mobile host may subsequently issue a Binding Update notification to the Correspondent host allowing direct communication between the two hosts). If a mobile host has an active Internet connection when it passes from its home network to a foreign network, and a datagram destined for the host subsequently arrives at the home network, the home agent determines that the mobile host is registered with a foreign network and forwards the datagrams to the registered care-of-address. Similarly, if a mobile host initiates a new Internet access when registered with a foreign network, the host continues to use its allocated Internet address. The home agent has already received the care-of-address and can again forward datagrams destined for the mobile host to the foreign network for transfer to the host.

The functionality described above may be implemented in embodiments of the present invention by temporarily allocating a home agent in an access network to a mobile host, where that host has been authorised to use the access network by the payment of e-cash or the like. The allocated home agent acts like a normal home agent for the host, except that when the connection is terminated, e.g. because a payment runs out, the mobile host is deleted from the set of mobile hosts serviced by the home agent. In order to enable correspondent hosts to be able to communicate with a mobile host making use of a dynamically allocated home agent, use is made of a Domain Name System (DNS) server in the Internet which provides a "real" home for the mobile host. The DNS server is notified of the temporary addresses of mobile hosts (which subscribe to the service offered by the DNS server) and maps these to respective permanent IP names of the mobile hosts (e.g. mymobile.dnsserver.com).

With reference to Figure 6, the following four steps can be identified in establishing a connection between a mobile host (MH) and a correspondent host (CH). The mobile host attaches (step 1) to the access network via an access point (AP₁) as described above with reference to Figures 1 to 5 (where the access point is a router). The mobile host is allocated a home agent (HA) which is notified of the IP address temporarily allocated to the mobile host. The mobile host notifies (step 2) the DNS (to which it subscribes) of the temporary address which it has been allocated. The DNS maps this address to a permanent IP name of the mobile host.

A correspondent host sends (step 3) an IP address discovery message to the DNS server, the message including the mobile host's IP name (e.g. mymobile.dnsserver.com). The DNS server identifies the current temporary address of the mobile host. The DNS server then returns a message to the correspondent host advising it of the temporary IP address of the mobile host. Once the correspondent host is aware of the temporary address of the mobile host, communication (step 4) can begin between the mobile host and the correspondent host.

Two roaming scenarios which make use of the home agent are illustrated in Figures 7 and 8. In Figure 7, a mobile host moves (step 1) within the same access network. As a result of this move, the host connects (step 2) to a new access point (AP₂) and receives a

new temporary IP address. The mobile host notifies (step 3) the home agent of its new temporary address. When a correspondent host sends an IP address discovery message to the DNS server, as the DNS server has not been updated with the new temporary IP address of the mobile host, but rather still retains the original temporary IP address (allocated by AP₁), the correspondent host is notified of the old temporary IP address and thereafter communicates (step 5) directly with the home agent. The home agent handles the routing of received packets to the mobile host by mapping the old temporary address to the new temporary address. The mobile host may subsequently communicate directly (step 6) with the correspondent host in the event that the former send a Binding Update message to the latter. When a mobile host is allocated a new temporary address during an ongoing IP communication, a Binding Update message may be used to inform the correspondent host of the new address.

In the scenario of Figure 8, the mobile host roams (step 1) from a first to a second access network. Assuming that the mobile host has been authorised for such roaming by the first access network, the home agent allocated to the mobile host in the first network remains responsible for the host even after it has entered the second network. Thereafter, steps 2 to 6 for the scenario of Figure 8 are substantially the same as for the scenario of Figure 7, with datagrams from the correspondent host being routed through the home agent of the first network in the first instance. In this scenario, the mobile host may be required to make an additional payment to the new access network in order to enable it to make use of the available IP services.

It will be appreciated by the person of skill in the art that various modifications may be made to the above described embodiments without departing from the scope of the present invention. For example, whilst the above description assumes that the IP address allocation procedure is initiated by the sending of a Router Solicitation message from the mobile host to an IP router, it is possible that the process may be initiated by receipt at the mobile host of a broadcast Router Advertisement message. Rather than send a Router Solicitation message, the mobile host merely listens for Router Advertisement messages which are broadcast periodically by the access network.

Claims

1. A method of authorising an Internet Protocol (IP) enabled mobile host to access the Internet via an access network, the method comprising:
 - negotiating an IP address between the mobile host and the access network and/or other hosts attached to the access network;
 - sending electronic cash or other authentication message from the mobile host to a control point within the access network; and
 - confirming at the control point the authenticity of said electronic cash or authentication message and, providing that confirmation is made, sending an authorisation message from the control point to an IP node,
 - wherein the IP node blocks the transmission of IP packets between the mobile host and the Internet prior to receipt of said authorisation message and permits the passage of IP packets only after an authorisation message has been received.
2. A method according to claim 1, wherein said step of negotiating an IP address is carried out in response to the sending of an IP access request from the mobile host to said IP node within the access network.
3. A method according to claim 1 or 2 and comprising routing IP data packets at said IP node.
4. A method according to claim 3 and comprising carrying out a protocol conversion at the IP node between the carrier protocol used by the access network, and that used by the Internet.
5. A method according to any one of the preceding claims and comprising, upon receipt of the access request at the IP node, returning from the IP node to the mobile host an IP address prefix.

6. A method according to any one of claims 1 to 4, wherein said step of negotiating comprises carrying out a negotiation between the mobile host and a DHCP server of the access network.
7. A method according to any one of the preceding claims, wherein the access network is a wireless Local Area Network (LAN), Wide Area Network (WAN), UMTS network or GSM network.
8. A method according to any one of the preceding claims, wherein, upon receipt of electronic cash at the control point, the control point contacts a bank, or other electronic cash provider, to authenticate and ensure the sufficiency of the received electronic cash and, providing that the bank or cash provider returns a confirmation or authentication message to the control point, the control point sends the authorisation message to the IP node in order to allow the passage of IP data packets between the mobile host and the Internet.
9. A method according to any one of the preceding claims and comprising incorporating electronic cash payments into IP packets sent from the mobile host to the control point.
10. A method according to any one of the preceding claims, wherein said IP node is an IP router.
11. A method according to claim 9, wherein the IP router is co-located with the control point.
12. A method according to claim 9, wherein said control point is co-located with a DHCP server, the DHCP server allocating an IP address to the mobile host during the IP address negotiation.
13. A method according to any one of the preceding claims and comprising temporarily allocating to the mobile host a home agent located in the access network.

14. A method according to claim 13, wherein the allocation of the home agent exists for the duration of the Internet connection.

15. A method according to any one of the preceding claims and comprising informing an Internet server of the IP address allocated to the mobile host, the server maintaining a mapping between mobile host identities and temporary IP addresses for subscribing mobile hosts.

16. A method according to claim 15, wherein the Internet server is a Domain Name Server (DNS).

17. A method according to any one of claims 1 to 14 and comprising informing an Internet server of the location of the mobile host, the server maintaining a mapping between mobile host identities and locations for subscribing mobile hosts.

18. According to a second aspect of the present invention there is provided apparatus for use in enabling an Internet Protocol (IP) enabled mobile host to access the Internet, the apparatus comprising:

means for conducting a negotiation between the mobile host and the access network and/or other hosts attached to the access network to allocate a mobile address to the mobile host; and

a control point within the access network for receiving electronic cash or other authentication message sent from the mobile host and for confirming the authenticity of the sent electronic cash or authentication message and, providing that confirmation is made, for sending an authorisation message to an IP node,

the IP node being arranged in use to block the transfer of messages between the mobile host and the Internet prior to receipt of an authorisation message from the control point and being arranged to allow the transfer upon receipt of the authorisation message.

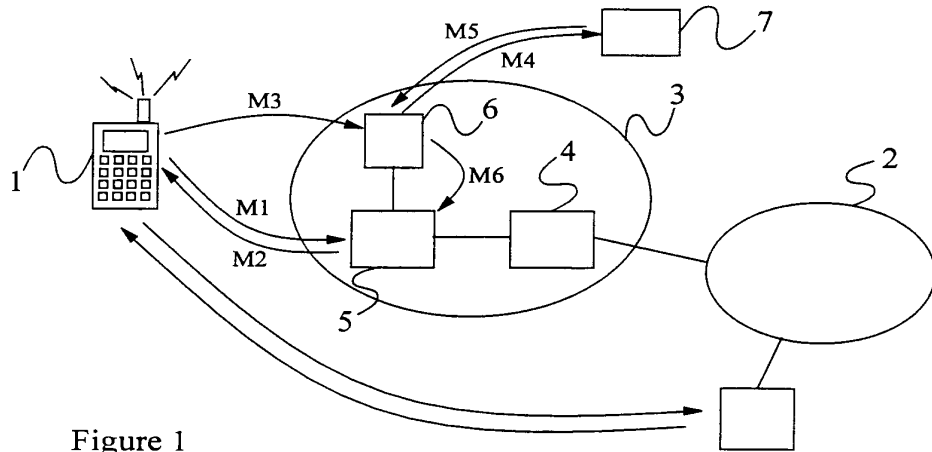


Figure 1

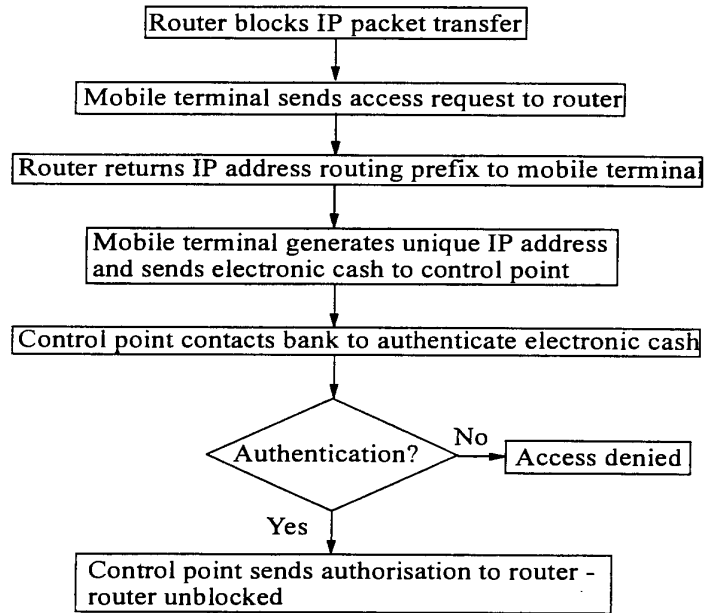


Figure 2

SUBSTITUTE SHEET (RULE 26)

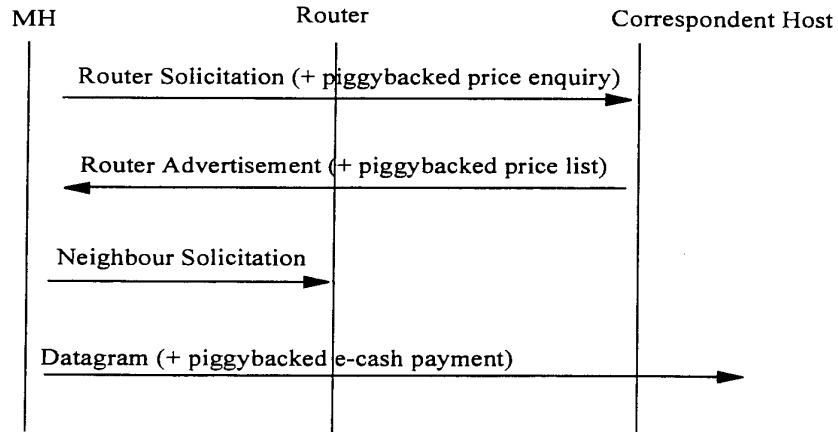


Figure 3a

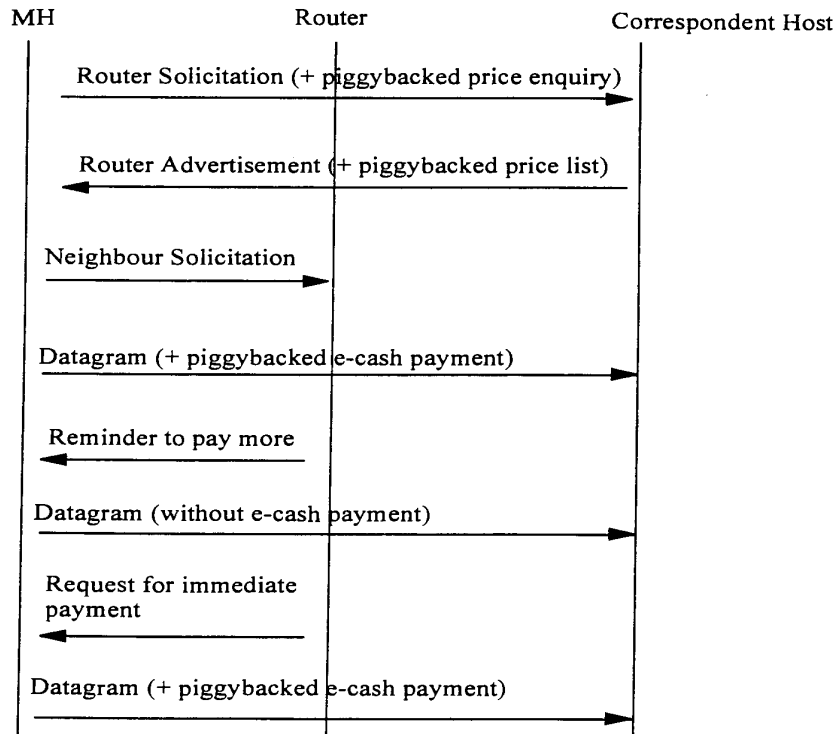


Figure 3b

SUBSTITUTE SHEET (RULE 26)

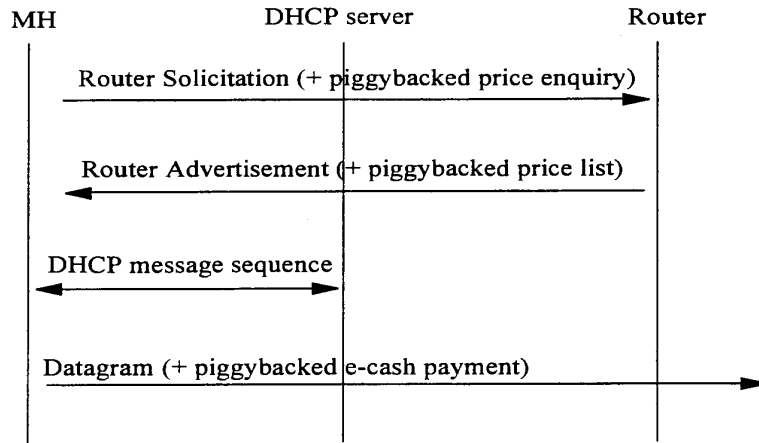


Figure 4

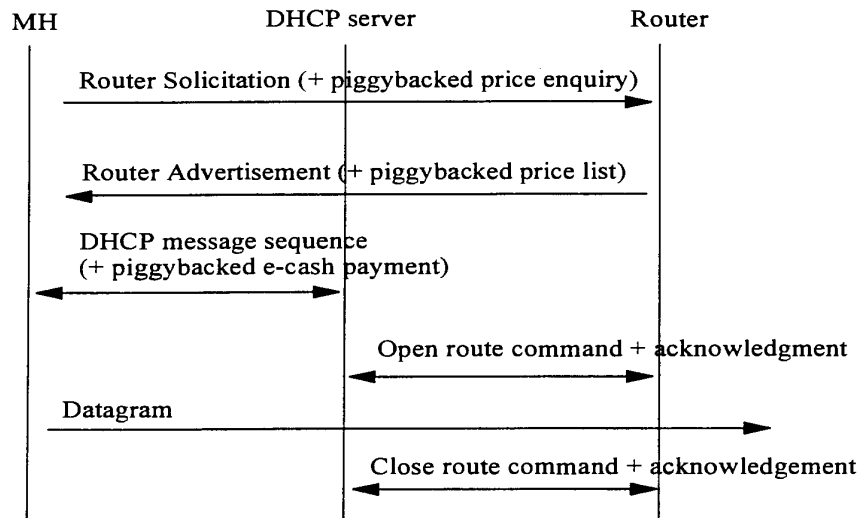


Figure 5

SUBSTITUTE SHEET (RULE 26)

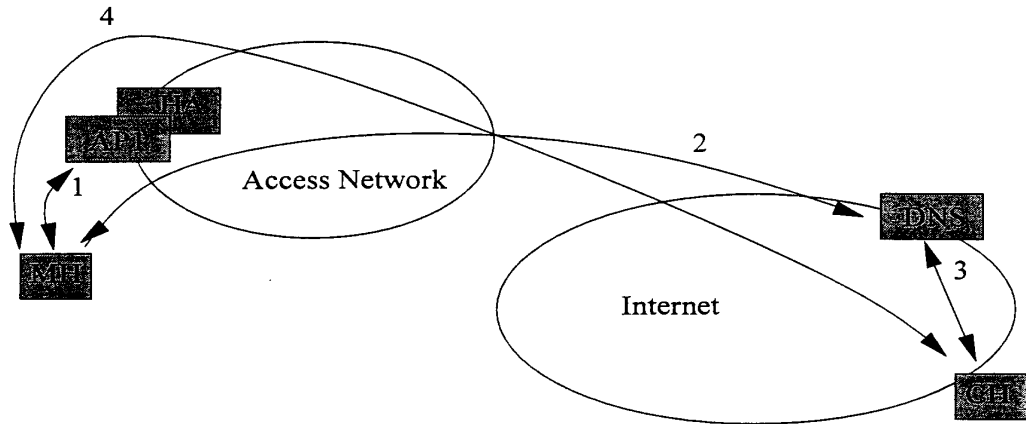


Figure 6

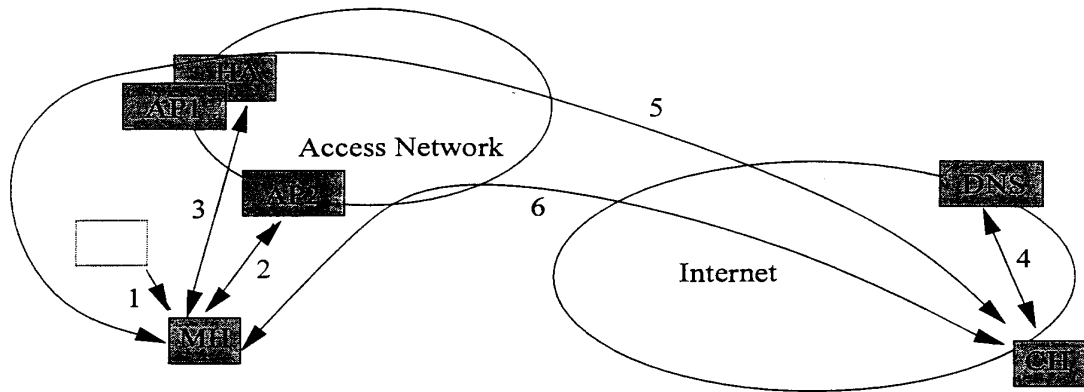


Figure 7

SUBSTITUTE SHEET (RULE 26)

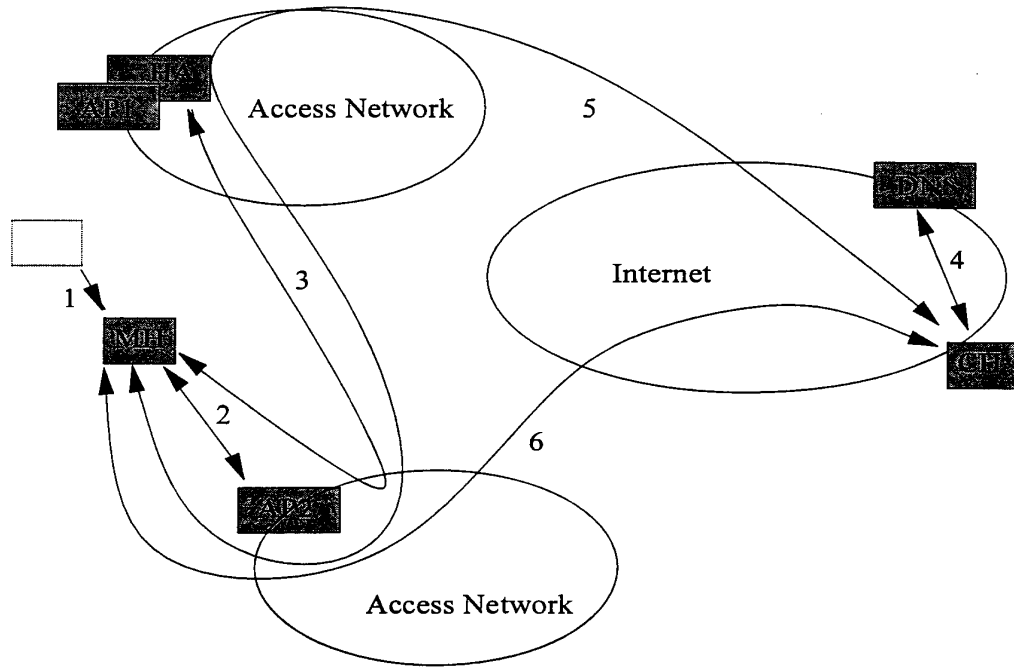


Figure 8

SUBSTITUTE SHEET (RULE 26)

INTERNATIONAL SEARCH REPORT

International application No. PCT/SE 00/01136
--

A. CLASSIFICATION OF SUBJECT MATTER		
IPC7: H04Q 7/38, H04L 12/56 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
IPC7: H04Q, H04L		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
SE,DK,FI,NO classes as above		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9832301 A1 (TELEFONAKTIEBOLAGET LM ERICSSON), 23 July 1998 (23.07.98), page 6, line 15 - line 27; page 9, line 3 - line 15; page 14, line 23 - page 16, line 4 --	1-18
A	EP 0483547 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION), 6 May 1992 (06.05.92), column 6, line 5 - column 7, line 32, abstract --	1-8
A	WO 9740615 A2 (AT & T CORP), 30 October 1997 (30.10.97), page 3, line 1 - page 4, line 25 --	1-18
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&" document member of the same patent family</p>		
Date of the actual completion of the international search		Date of mailing of the international search report
22 August 2000		12 -09- 2000
Name and mailing address of the ISA Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86		Authorized officer Nabil Ayoub/js Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No. PCT/SE 00/01136
--

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5708655 A (TOTH ET AL.), 13 January 1998 (13.01.98), column 7, line 17 - column 8, line 67, abstract -- -----	1-8

Form PCT ISA 210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

08/05/00

International application No.

PCT/SE 00/01136

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9832301 A1	23/07/98	AU 5684698 A	07/08/98
		EP 0953265 A	03/11/99
EP 0483547 A1	06/05/92	DE 69119353 D,T	07/11/96
		JP 2516291 B	24/07/96
		JP 4227149 A	17/08/92
		US 5159592 A	27/10/92
WO 9740615 A2	30/10/97	AU 2200397 A	12/11/97
		US 5905736 A	18/05/99
US 5708655 A	13/01/98	AU 3199797 A	07/01/98
		BR 9709572 A	10/08/99
		CA 2257981 A	18/12/97
		CN 1228228 A	08/09/99
		EP 0904665 A	31/03/99
		WO 9748246 A	18/12/97



Europäisches Patentamt
 European Patent Office
 Office européen des brevets



(11) EP 0 779 752 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication: 18.06.1997 Bulletin 1997/25 (51) Int. Cl.⁶: H04Q 7/22, H04Q 7/38, H04B 7/26

(21) Application number: 96120005.2

(22) Date of filing: 12.12.1996

(84) Designated Contracting States:
 DE FR GB SE

(30) Priority: 12.12.1995 US 570903

(71) Applicant: AT&T Wireless Services, Inc.
 Kirkland, Washington 98033 (US)

(72) Inventors:
 • Bamburak, Michael D.
 Columbia MD 21046 (US)

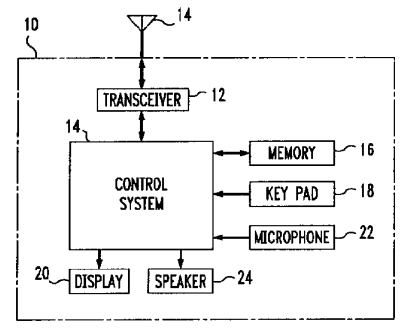
- Daly, John J.
 Neshanic Station NJ 08853 (US)
- Lawrence, Christopher Gregory
 Kirkland, Washington 98034 (US)
- Prise, Michael Edward
 Kirkland, Washington 98033 (US)
- Raffel, Michael Allen
 Redmond, Washington 98052 (US)

(74) Representative: KUHNEN, WACKER & PARTNER
 Alois-Steinecker-Strasse 22
 85354 Freising (DE)

(54) A method for selecting a wireless service provider in a multi-service provider environment using a geographic database

(57) A communication device locates a wireless service provider in a multi-service provider environment by tuning to a first frequency band and receiving a geographic identifier from the service provider operating in the first frequency band. The received geographic identifier is compared to a listing of stored geographic identifiers in order to attempt to locate a matching stored geographic identifier. Each of the stored geographic identifiers are associated with a desirable frequency band having a desirable service provider. If comparing the received geographic identifier with the matching stored geographic identifiers does not produce a match, frequency bands are examined until a second frequency band having a desirable service provider is located. The listing of stored geographic identifiers is then updated so that the second frequency band is associated with the received geographic identifier.

FIG. 3



EP 0 779 752 A2

Description**Background of the Invention****Field of the Invention**

The present invention relates to communications; more specifically, communications in a multi-service provider environment.

Description of the Related Art

FIG. 1 illustrates a portion of the radio frequency spectrum. Frequency range 10 centered around 800 MHz has historically been known as the cellular frequency range and frequency range 12 centered about 1900 MHz is a newer defined frequency range associated with personal communication services (PCS). Each range of frequencies, i.e., the cellular and PCS, are broken into two portions. In cellular frequency range 10, there is uplink portion 14 which is used for communications from a mobile communication device to a base station such as a cellular base station. Portion 16 of cellular frequency range 10 is used for downlink communications, that is, communications from a cellular base station to a mobile communication device. In a similar fashion, Portion 18 of PCS frequency range 12 is used for uplink communications, that is, communications from a mobile communication device to a base station. Portion 20 of PCS frequency range 12 is used for downlink communications, i.e., communications from a base station to a mobile communication device.

Each of the frequency ranges are broken into bands which are typically associated with different service providers. In the case of cellular frequency range 10, frequency bands 30 and 32 are designated band "a" for uplink and downlink communications, respectively. In a particular geographic area, a cellular service provider is assigned frequency band "a" in order to carry out mobile communications. Likewise, in the same geographic area another cellular service provider is assigned frequency bands 34 (uplink) and 36 (downlink) which are designated band "b". The frequency spectrums assigned to the service providers are separated so as to not interfere with each other's communications and thereby enable two separate service providers to provide service in the same geographic area. Recently, the US Government auctioned the PCS frequency spectrum to service providers. As with the cellular frequency range, the PCS frequency range is broken into several bands where a different service provider may use a particular frequency band for which it is licensed within a particular geographical area. The PCS bands are referred to as A, B, C, D, E and F. The A band includes uplink band 50 and downlink band 52. The B band includes uplink band 54 and downlink band 56. Band C includes uplink band 58 and downlink band 60. Each uplink and downlink band of the A, B and C bands are approximately 30 MHz wide. The D band includes

uplink band 62 and downlink band 64. The E band includes uplink band 66 and downlink band 68. Likewise, band F includes uplink band 70 and downlink band 72. The uplink and downlink bands of bands D, E and F are approximately 10 MHz wide each. It should be noted that with the cellular and PCS frequency bands, it is possible to have as many as eight different wireless communication service providers in a particular area.

Each of the different cellular and PCS bands consist of control channels and communication channels in both the uplink and downlink direction. In the case of analog cellular bands, there are 21 control channels for both the "a" and "b" bands. Each of the control channels include an uplink and a downlink portion. The control channels transmit information such as an SOC (System Operator Code), an SID (System Identifier Code), paging information call setup information and other overhead information such as information relating to registering with the mobile communication system. The portion of the cellular band's spectrum not occupied by the control channels is used for communication channels. Communication channels carry voice or data communications, where each channel consists of an uplink and downlink communications link. Presently there are several cellular communication standards. An analog standard known as EIA/TIA 553 was built upon the AMPS (Advanced Mobile Phone Service) standard. This standard supports 21 analog control channels (ACC) and several hundred analog voice or traffic channels (AVC). A newer standard is the EIA/TIA IS54B standard which supports dual mode operation. Dual mode operation refers to having an analog control channel, and either an analog voice/traffic channel or a digital traffic channel (DTC). The AVC or DTC are used for actual communications, and the ACC is used to transfer information relating to, for example, call set-ups, service provider identification, and the other overhead or system information.

A newer standard, the EIA/TIA IS136 standard supports communications covered by both analog and dual mode cellular, and also includes a totally digital communication scheme which was designed for the PCS frequency bands A-F and cellular frequency bands "a" and "b". This standard allows for a digital traffic channel (DTC) and a digital control channel (DCCH). In the case of the DTC, not only is the voice or data communicated, but in addition, a digital channel locator (DL) is transmitted in the DTC. The DL enables a mobile communication device that locks onto the DTC to use the information in the DL to locate a DCCH for purposes of obtaining information such as the SOC, SID, paging information, and other system overhead information carried on the digital control channel.

When a mobile communication device such as a mobile telephone attempts to register with the service provider, it locks onto a control channel and reads information such as the SOC and SID. If the SOC and/or SID correspond to a service provider with which the user

has a communication services agreement, the telephone may register with the service provider's mobile communication system via the up-link control channel.

FIG. 2 illustrates a map of the United States illustrating cities such as Seattle, Chicago and Washington, DC. For example, in Seattle frequency band A has been licensed to SOC (Service Operator Code) 001 with a SID of 43 and band C has been licensed to SOC 003 with a SID of 37. In Chicago, suppose that frequency band C has been licensed to SOC 001 with a SID equal to 57, and that band B has been licensed to SOC 003 with a SID of 51. In Washington, DC suppose that frequency band "a" has been licensed to a SOC 001 with a SID of 21, and that band A has been licensed to SOC 003 with a SID of 17. It should be noted that the same SOC may be found in several different locations although on different frequency bands. It should also be noted that the same SOC will be associated with different SIDs in each geographical area and that in the same geographic area different service providers have different SIDs. If a particular subscriber to a wireless telecommunication service has an agreement with a service provider having a SOC of 001, that subscriber would prefer to use systems with a SOC of 001 because the subscriber is likely to receive a less expensive rate. When the subscriber is in Seattle he/she would prefer to be on band A, and if in Chicago on band C, and if in Washington, DC on band "a". The above described situation presents a problem for a wireless communication service subscriber. As a subscriber moves from one area of the country to another, the telephone when turned on, searches for the "home" service provider, or the service provider with which the subscriber has a pre-arranged agreement. If for example, the subscriber travels from Seattle to Chicago, when turning the phone on in Chicago, the phone will search through the different bands of the spectrum to identify the service operator with the code 001 in order to find the desired service provider.

In order to find a particular service provider, the phone may have to search through both the "a" and "b" cellular bands, and through the eight PCS bands. It should be recalled that there are up to 21 different ACCs in each of the "a" and "b" cellular bands. It may be necessary to check 42 ACCs in order to find an ACC from which a SOC or SID may be obtained. Additionally, searching for a particular SOC or SID in PCS bands A through F is particularly time consuming. The digital control channels (DCCHs), which contain the SOC and SID, are not assigned to specific frequencies within a particular PCS band. As a result, the mobile communication device may find it necessary to search through the spectrum of each PCS band looking for a DCCH, or an active DTC that has a digital channel locator (DL) which will direct the mobile communication device to the DCCH. As illustrated above, the process of searching for a particular service provider is laborious and may require a period of time on the order of several minutes.

Summary of the Invention

An embodiment of the present invention provides a method for locating a particular or desirable communications service provider in an environment having a plurality of service providers. After power-up, a mobile communications device such as a cellular telephone, checks the most recently used control channel to determine whether an optimal service provider is available on that channel. If an optimal service provider is not available or if that channel is not available, the mobile communication device performs a search through frequency spectrum in a pre-determined order until an optimal or acceptable service provider is located.

In another embodiment of the invention, the frequency spectrum is searched in a predetermined order that changes based on information entered by a mobile communication device distributor or mobile communication device user. In yet another embodiment of the invention, the pre-determined order for searching the spectrum for service providers is updated by over the air programming. In still another embodiment of the present invention, the pre-determined order for searching is based on the mobile communication device's operational history.

In yet another embodiment of the present invention, the communication device tunes to a first frequency band and receives a geographic identifier from the service provider operating in the first frequency band. The received geographic identifier is compared to a listing of stored geographic identifiers in order to attempt to locate a matching stored geographic identifier. Each of the stored geographic identifiers are associated with a desirable frequency band having a desirable service provider. If comparing the received geographic identifier with the matching stored geographic identifiers does not produce a match, frequency bands are examined until a second frequency band having a desirable service provider is located. The listing of stored geographic identifiers is then updated so that the second frequency band is associated with the received geographic identifier.

Brief Description of the Drawings

FIG. 1 illustrates the frequency spectrum used for wireless communications;
 FIG. 2 illustrates service areas within the United States;
 FIG. 3 is a block diagram of a mobile communication device;
 FIG. 4 is a flow chart illustrating a spectrum searching routine;
 FIG. 5 is a flow chart illustrating the global spectrum search routine;
 FIG. 6 is a flow chart illustrating a periodic search routine;
 FIG. 7 is a flow chart illustrating a received signal strength search routine;
 FIG. 8 illustrates a search schedule;

FIG. 9 illustrates a prioritized list of service providers; and

FIG. 10 illustrates a list of geographic identifiers and prioritized desirable frequency bands.

Detailed Description of the Invention

FIG. 3 illustrates a block diagram of a mobile communication device such as a cellular telephone or personal communication device. Mobile communication device 10 includes transceiver 12 which sends and receives signals from antenna 14. Mobile communication device 10 is controlled by control system 14 which may include a microprocessor or a microcomputer. Control system 14 uses memory 16 for storing programs that are executed and for storing information that is entered by the user, the distributor, the communication services provider or the manufacturer. Information such as user preferences, user telephone numbers, preferred service provider lists and frequency search schedules are stored in memory 16. Memory 16 may include storage devices such as random access memory (RAM), read only memory (ROM) and/or programmable read only memory (PROM). A user communicates with control system 14 via keypad 18. Control system 14 communicates information to the user via display 20. Display 20 may be used to display information such as status information and items such as telephone numbers entered via keypad 18. Sound information to be transmitted from the mobile communication device 10 is received via microphone 22, and sound communications received by mobile communication device 10 are played to the user via speaker 24.

After initially powering-up, a mobile communication device locates a service provider and registers with the service provider. Recalling FIG. 1, service providers are located at a plurality of frequency bands across the radio spectrum. In order to find a service provider, the communication device searches the spectrum to find service providers. The communications device examines received service provider code e.g., SOC's (Service Operator Code) or SID's (System Identification Code) to determine whether the service provider is an optimal, preferred or prohibited service provider.

FIG. 4 illustrates a process or program that control system 14 executes in order to find a desirable service provider. After power-up, step 30 is executed to initialize a non-optimal flag by clearing the flag. Step 32 determines whether the last service provider, that is, the service provider used before powered down, was an optimal service provider. This is determined by checking the SOC or SID of the last service provider and determining whether that service provider's SOC or SID corresponds to the SOC or SID of an optimal service provider. The SOC or SID of the last service provider and a list of optimal and preferred service providers is stored in memory 16. If in step 32 it is determined that the prior service provider was not optimal, a global spectrum search is executed. If the last service provider

was optimal, step 34 is executed where system 14 attempts to lock onto the control signal of the service provider. If the lock is unsuccessful, which may indicate that that control channel is no longer available or out of range, the global spectrum search is executed. If a lock is successful, step 36 is executed. In step 36, it is determined whether the control channel contains the SOC or SID of an optimal service provider. Once again, this is determined by comparing the SOC or SID from the control signal with a list of optimal service provider SOC's or SID's. If the SOC or SID does not belong to that of an optimal service provider, the global spectrum search 33 is executed and the identity of the frequency band in which the non-optimal SOC or SID was located is passed to global search routine 33 so as to avoid unnecessarily searching this portion of the spectrum again. If in step 36 it is determined that an optimal service provider has been located, step 38 registers communication device 10 with the service provider. Step 40 is an idle state where control system 14 simply monitors the control channel of the service provider for communication system overhead information and for paging information that may indicate an incoming communication. While in idle state 40, a timer is activated which permits a low-duty cycle search to be performed if the phone is presently registered in a non-optimal service provider system. This situation may arise if global spectrum search 33 provides a preferred but not optimal service provider. Periodically, such as every 5 minutes, step 42 is executed to determine whether the non-optimal flag has been set, if the non-optimal flag is not set, control system 14 returns to idle step 40. If the non-optimal has been set, step 42 leads to the execution of periodic search routine 44 where a search is conducted in order to attempt to locate an optimal service provider. If periodic search routine 44 produces an optimal service provider, the non-optimal service provider flag is cleared and the mobile communication device registers with the optimal service providers while executing periodic search routine 44. The mobile communications device then enters a idle state by executing step 40. If an optimal service provider is not located in routine 44, control system 14 returns to an idle state by executing step 40.

FIG. 5 illustrates a flowchart of global spectrum search routine 33 which is executed by control system 14. At step 60 it is determined whether the last control channel used by the mobile communication device was a personal communication services related control channel, that is, a control channel in the bands A through F. If the last control channel was not a PCS control channel, step 62 is executed. In step 62 it is determined whether the mobile communication device can lock onto, or receive and decode the last ACC (Analog Control Channel) that was used. If the mobile communication device can successfully lock onto the last ACC, step 64 is executed. If the communication device cannot lock onto the last ACC, step 66 is executed. In step 66, an RSS (Received Signal Strength Scan) is performed. This step involves the mobile communication device

tuning to each of the 21 ACCs associated with the cellular band of the last used ACC, and attempting to lock onto the strongest received signal. In step 68, it is determined whether a lock has been achieved. In step 68 if a lock is not obtained, a predetermined search schedule is executed in order to find a service provider; if in step 72 a lock is obtained, step 64 is executed where the SOC or SID obtained from the control channel is compared to a list of optimal SOC's or SID's. In step 70 if the received SOC or SID is associated with an optimal service provider, step 72 is executed where the mobile communication device clears the non-optimal flags, registers with the communication service provider, and then enters an idle state by executing step 40 of FIG. 4. If, in step 70 it is determined that an optimal service provider SOC or SID was not received, step 74 is executed where the identity of the frequency band just searched is stored in memory 16. Step 78 is executed after step 74, after 68 if a lock is not obtained, or after step 60 if the last control signal was from a PCS frequency band. In step 78, a search schedule is downloaded using a master search schedule. When downloading the search schedule in step 80, frequency bands previously searched are removed from the downloaded schedule so as to avoid searching bands that have already been searched. For example, bands searched in the search routine discussed with regard to FIG. 4 and the cellular band search discussed with regard to step 74 are removed from the search schedule. After the modified search schedule has been loaded, a search pointer is initialized to point to the first band identified by the modified search schedule. The first band identified on the modified schedule is searched with regard to received signal strength (RSS) in step 79's RSS routine. In the case of bands "a" and "b", the ACC with the strongest signal is selected. In the case of the PCS bands, that is the bands A through F, 2.5 MHz sections of each band are searched in 30 kilohertz steps. The mobile communication device tunes to the strongest signal that crosses a minimum threshold, e.g., -110dBm, within the 2.5 MHz band being examined. In step 80 it is determined whether the signal is valid, that is, conforms to one of the above mentioned standards. If it is not valid, the search pointer is incremented in step 96, and if the signal is valid, step 82 is executed. In step 82 it is determined whether the signal is a ACC. If the signal is an ACC, the SOC or SID is decoded in step 90. If the signal is not an ACC, step 84 determines whether the received signal is a digital traffic channel (DTC) or a digital control channel (DCCH). If the signal is a DCCH the SOC or SID is extracted in step 90. If it is determined that the received signal is a DTC, step 86 is executed where the DL (digital channel locator) is extracted to identify the location of the DCCHs associated with the DTC that has been received. In step 88, the mobile communication device tunes to the strongest DCCH of the digital control channels identified by the DL. In step 90, the SOC or SID of the received DCCH is extracted and in step 91, it is determined whether the SOC or SID is associated

with an optimal service provider. If the SOC or SID is associated with an optimal service provider, step 92 clears the non-optimal flag and step 96 registers the mobile communication device with the service provider. After step 96, the communication device enters the idle state in step 40 of FIG. 4. If in step 92 it is determined that the SOC or SID does not belong to that of an optimal service provider, step 94 is executed where the SOC or SID is stored in memory 16 indicating whether the SOC or SID was at least a preferred rather than an undesirable or prohibited service provider with the spectral location of the SOC's or SID's control channel. In step 96 the search pointer that identifies the band being searched is advanced to identify the next band in the schedule for searching. In step 98 it is determined whether the pointer has reached the end of the search schedule. If the end of the search schedule has not been reached, step 82 is executed to perform mother received signal strength search routine as discussed above, and if the last frequency band has been searched, step 100 is executed. In step 100 the mobile communication device registers with the best stored SOC or SID, that is, an SOC or SID that has at least been associated with a preferred service provider. The best service provider can be identified by comparing the stored SOC's or SID's with a list of preferred SOC's or SID's. The list of preferred SOC's or SID's can include the optimal SOC(s) or SID(s) and a prioritized list of preferred SOC's or SID's where the higher priority will get preference for registration. The listing also includes undesirable or prohibited SOC(s) or SID(s) that are used only in emergencies (e.g., 911 calls) or if the user enters an override command. After registering with the service provider in step 100, step 102 is executed to set the non-optimal flag, and then step 40 of FIG. 4 is executed where the mobile communication device enters the idle state.

It should be noted that the searching operation of FIGs. 4 and 5 may be carried out in a simplified manner. With regard to FIG. 4, control system 14 may execute step 33 after step 30 while always skipping steps 32, 34, 36 and 38. With regard to FIG. 5, control system 14 may start the global spectrum search with step 78 while always skipping steps 60-74.

FIG. 6 illustrates a flowchart for the periodic search routine executed by control system 14. In step 120 it is determined whether the periodic search flag has been set. If the periodic search flag has not been set, step 122 is executed where periodic search flag is set and the search schedule is initialized by loading the master search schedule into the search schedule used by the periodic search routine; however, the frequency band currently being received is not included in the search schedule used for the periodic search routine. Step 122 also sets a search pointer to the first band in the search schedule. In step 124 a received signal strength search (RSS) routine is conducted. As in step 79 of the global spectrum search routine of FIG. 5, step 124 is a RSS routine of any PCS and cellular bands that are in the

search schedule. In the case of a cellular band search, the 21 ACCs are searched using a received signal strength search i.e., the transceiver tunes to the strongest ACC. In the case of a PCS frequency band search, as discussed earlier, each band is broken into segments of approximately 2.5 MHz where a search of each segment is conducted in 30 kilohertz steps. The strongest signal within the 2.5 MHz segment and above a minimum threshold, such as -110dBm, is selected. In step 126 the selected signal is examined to determine if it is valid by conforming to one of the previously referenced standards. If the signal is invalid, step 144 is executed and if the signal is valid, step 129 is executed. Step 129 determines whether the signal is an ACC. If the signal is a ACC, step 130 is executed when the SOC or SID is extracted and if the signal is not a ACC, step 132 is executed. Step 132 determines whether a DTC signal has been received. If the signal is not a DTC signal (therefore it is a DCCH signal), step 130 is executed to extract the SOC or SID from the DCCH signal. If in step 132 it is determined that a DTC has been received, step 134 is executed to extract the DL to enable tuning to a DCCH. In step 136 a received signal strength search is conducted of the DCCHs where the strongest signal is selected, and then step 130 is executed to extract an SOC or SID from the signal. In step 138 it is determined whether the SOC or SID is an optimal SOC or SID. If the SOC or SID is optimal, step 140 clears the non-optimal flag and in step 142 the mobile communication device registers with the service provider associated with the optimal SOC or SID. Step 40 of FIG. 4 is then executed to enter the idle state. If in step 138 it is determined that the SOC or SID was not an optimal service provider, step 144 is executed. In step 144 the search pointer is incremented to the next band to be searched. In step 146, it is determined whether the entire search schedule has been completed. If the schedule has not been completed, step 40 is executed so that the mobile communication device can be returned to the idle state. If in step 146 it is determined that the search schedule has been completed, step 148 clears the periodic search flag and then step 40 is executed so that the mobile communication device can enter the idle state.

FIG. 7 illustrates a flow chart of the RSS routine or received signal strength search routine which is carried out, for example, in steps 79 of FIG. 5 and 124 of FIG. 6. Step 170 determines whether the band being searched is one of the "a" or "b" cellular bands. If a cellular band is being searched, step 172 is executed where the 21 ACCs are searched to determine which is the strongest, the strongest ACC is tuned to by transceiver 12 under the control of control system 14 and then the RSS routine is exited. If in step 170 it is determined that a cellular band is not being searched, step 178 tunes transceiver 12 to the beginning of the first 2.5 MHz band in the PCS band being searched. Step 178 also clears a search scratch pad memory location in memory 16. The search scratch pad is used to record the amplitude or strength and location of a received sig-

nal. In step 180 it is determined whether the signal being received is greater than a threshold. If the signal is greater than the threshold, step 182 is executed, if the signal is not greater than the threshold, step 184 is executed. In step 182 it determined whether the received signal strength is greater than the signal strength value stored in the search scratch pad. If the received signal is not greater, then step 184 is executed. If the received signal strength is greater, step 186 is executed and the present signal strength is recorded in the search scratch pad with the received signal's location in the spectrum. In step 184, transceiver 12 is tuned to a frequency 30 kilohertz higher than the frequency at which it was tuned. Step 188 determines whether the new frequency extends beyond the 2.5 MHz band currently being searched. If the new frequency does not exceed the 2.5 MHz band, step 180 is executed to once again examine received signal strength relative to the signal strength or amplitude value stored in the search scratch pad. If in step 188 it is determined that the 30 kilohertz increment extends beyond the 2.5 MHz band being examined, step 190 is executed. In step 190, the transceiver tunes to the signal location specified in the search scratch pad. If the signal is a valid signal and can be decoded, the RSS routine is exited. If the signal is not valid or cannot be decoded, (e.g., the signal does not conform to the above-referenced standards) step 192 is executed. In step 192, the transceiver is tuned to the beginning of the next 2.5 MHz band within the PCS band being searched. Step 194 determines whether the new 2.5 MHz band extends beyond the PCS band currently being searched. If the new increment extends beyond the PCS band being searched, the periodic search routine is exited. If the 2.5 MHz increase does not result in extending beyond the PCS band being searched, step 196 is executed. In step 196, the search scratch pad containing signal strength measurements and signal location information is cleared to prepare for searching another band. After step 196, step 180 is executed as described above.

FIG. 8 illustrates a master search schedule. The master schedule is used to initialize search schedules used in the above described search routines. The master search schedule is stored in a memory such as memory 16. The master search schedule can be initially programmed by the mobile communication device's manufacturer, distributor or user. It should be noted that the first location in the search schedule is left unprogrammed. If left blank, the blank is ignored when initializing the search schedules for the search routines. It is desirable for the first location to be programmed with the band in which the user's home service provider resides. For example, if the user has a service agreement with a service provider who is licensed to operate in PCS band B within the SID or geographical area in which the user most frequently is located, band B is programmed into the first slot of the master search schedule. If, for example, band B is programmed in the first slot, the slot originally containing band B is made blank. This avoids

searching the same band twice. It should also be noted that the user can vary the master search schedule through keypad 18. Additionally, the master search schedule may be reprogrammed using signals received over the wireless communication channel. For example, the mobile communication device may be restricted to accepting new programming for the master search schedule only from a service provider transmitting the home SID and an optimal SOC. It is also possible to accept over the air programming if the service provider sends a prearranged code. It is desirable to restrict the over the air programming through the use of codes, home SIDs and/or optimal SOCs to avoid unintentional or undesirable altering of the master search schedule. Over the air programming may be implemented using for example, logical sub-channels of a digital control channel. The logical sub-channels have the capability to transmit data addressed to a particular mobile communication device and to receive data, such as confirmation data, from the mobile communications device.

When the search schedules are initialized using the master search schedule, it is also possible to precede the first location in the master search schedule with other frequency bands based on, for example, the prior history of the mobile communication device's use. For example, the first location searched may be the location where the phone was last turned off (powered down) or the location where the phone was last turned on (powered up).

FIG. 9 illustrates a table stored in memory 16 defining the optimal service provider's SOC and SIDs, and preferred service provider's SOCs and SIDs. The SOC or SID with the lowest number has the highest priority and is preferred over service providers with higher numbers and therefore a lower priority. For example, an SOC or SID with a priority level 2 would be preferred over an SOC or SID with a priority level of 5. The table may also include SOCs or SIDs that are undesirable or prohibited. In the case of SOCs or SIDs that are prohibited, it is desirable to permit connection to the prohibited SOCs or SIDs when an emergency call, such as a 911 call, is attempted or when the user enters an override command. The table in FIG. 9 may be programmed by the manufacturer, by the distributor when the phone is purchased or by the user. It is also possible to program the table of FIG. 9 over the air using restrictions similar to those used when programming the master search schedule over the air.

FIG. 10 illustrates a list of geographic identifiers with associated frequency bands that are prioritized based on the desirability of the service provider operating in the band. The listing of FIG. 10 is stored in memory 16, and is used for the selection of a frequency band containing a desirable service provider. After initially powering up, communication device 10 tunes to the first frequency band of the frequency search schedule, the last used frequency band, or the frequency band used when the device was last powered up. After tuning to the band, the communication device monitors the control

signal associated with the band to obtain a geographic identifier such as a SID. The communication device then accesses the table of FIG. 10 in order to determine which frequency band has a desirable service provider. For example, if the device received a geographic identifier such as 51, the table of FIG. 10 instructs the communication device to tune to frequency band C for the most desirable service provider. The communication device then tunes to frequency band C and attempts to register with the service provider operating on frequency band C. If for some reason the device is unsuccessful in registering with a service provider on frequency band C, the next highest priority frequency band may be used. In the case of SID 51, the next most desirable frequency band is cellular band "b". Once again, the communication device will tune to the frequency specified by the table and attempt to register with the service provider operating on that frequency band. The table of FIG. 10 offers the frequency bands in a prioritized order. The frequency bands listed to the far left are the optimal or most desirable frequency bands, i.e., the frequency bands with the optimal or most desirable service provider. Frequency bands listed further to the right decrease in desirability or priority until prohibited frequency bands are listed at the far right. Prohibited frequency bands may be used in emergency situations or when overridden by the operator of the communication device.

The table of FIG. 10 may be programmed into memory 16 of the communication device by the device manufacturer, by the distributor or by the user via the keypad. It is also possible to program the table of FIG. 10 using over the air programming in a manner similar to that which was used for programming the search schedule of FIG. 8 or the prioritized table of service providers of FIG. 9. In some cases, there may not be a geographic identifier or SID in the table of FIG. 10 for a identifier that is received from a control channel to which the communication device is tuned. In this case, the communications device executes the search algorithms discussed earlier in an effort to locate a desirable service provider. When a desirable service provider has been located, the table of FIG. 10 is updated to list the previously unlisted geographic identifier and the frequency at which a desirable service provider is located.

Claims

1. A method by which a communication device locates a wireless service provider in a multi-service provider environment, comprising the steps of:

tuning to a first frequency band;
 receiving a received geographic identifier from a service provider in the first frequency band;
 comparing the received geographic identifier to a listing of stored geographic identifiers in order to locate a matching stored geographic identifier, each of the stored geographic identifiers

- being associated with a desirable frequency band having a desirable service provider; and tuning to a first desirable frequency band, the first desirable frequency band being associated with the matching stored geographic identifier. 5
2. The method of claim 1, further comprises the steps of unsuccessfully attempting to register with a first desirable service provider in the first desirable frequency band; 10
- determining a second desirable frequency band associated with the matching stored geographic identifier, the second desirable frequency band being less desirable than the first desirable frequency band; and tuning to the second desirable frequency band. 15
3. A method by which a communication device locates a wireless service provider in a multi-service provider environment, comprising the steps of: 20
- tuning to a first frequency band; receiving a received geographic identifier from a service provider in the first frequency band; 25
- comparing the received geographic identifier to a listing of stored geographic identifiers in order to attempt to locate a matching stored geographic identifier, each of the stored geographic identifiers being associated with a desirable frequency band having a desirable service provider; 30
- examining frequency bands until a second frequency band having the desirable service provider is located, the examination being carried out if the step of comparing the received geographic identifier does not produce the matching stored geographic identifier; and 35
- updating the listing of stored geographic identifiers so that the second frequency band is associated with the received geographic identifier. 40
4. The method of claims 1 or 3 wherein the step of receiving the received geographic identifier comprises receiving a system identifier code from a wireless service provider. 45
5. The method of claims 1 or 3, further comprising the step of modifying the listing of stored geographic identifiers using information transmitted over a wireless interface. 50
6. The method of claims 1 or 3, further comprising the step of modifying the listing of stored geographic identifiers using information from a keypad. 55
7. The method of claim 3, wherein the step of examining frequency bands comprises examining a plural-
- ity of frequency bands in an order specified by a frequency band search schedule.
8. The method of claim 7, further comprising the step of modifying the frequency band search schedule using information transmitted over a wireless interface.
9. The method of claim 7, further comprising the step of modifying the frequency band search schedule using information from a keypad.

FIG. 1

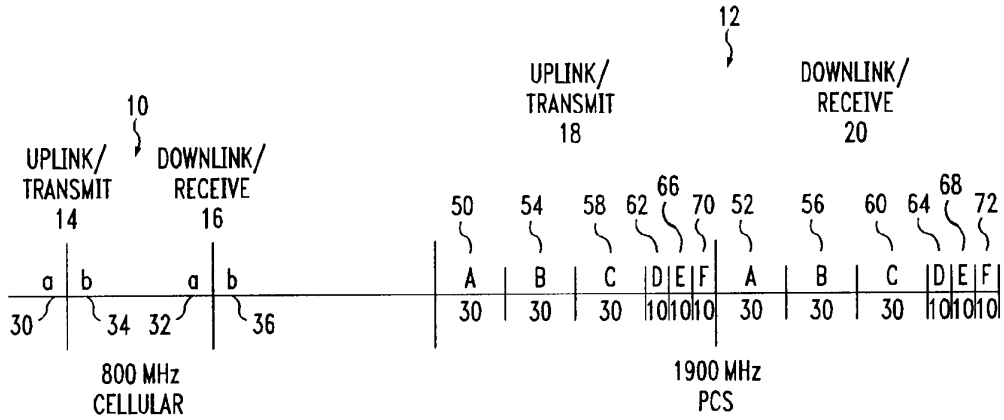


FIG. 2

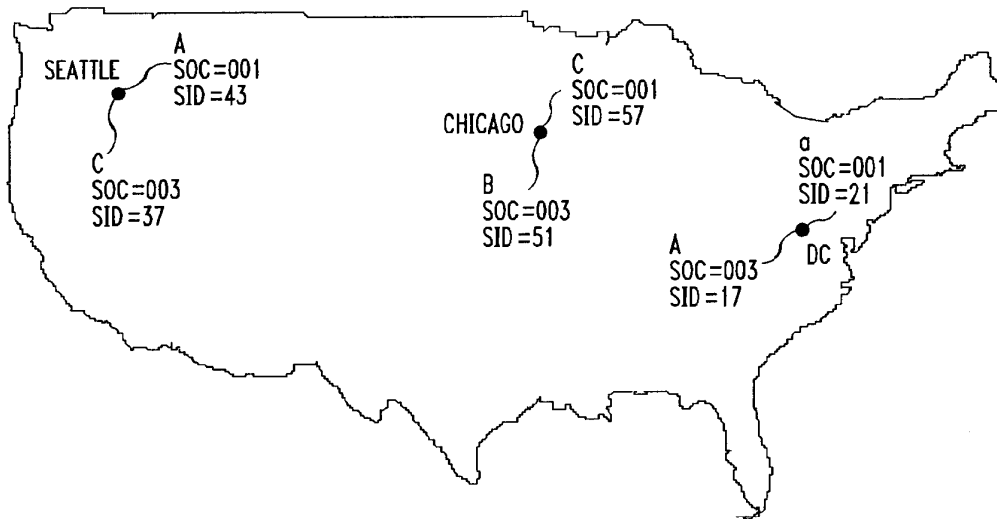


FIG. 3

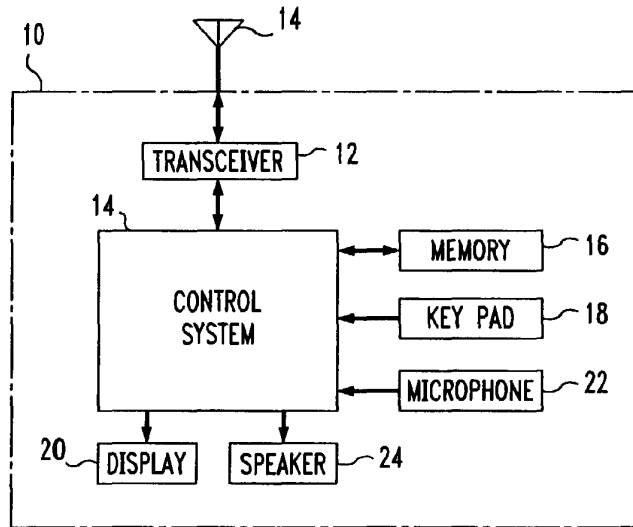


FIG. 4

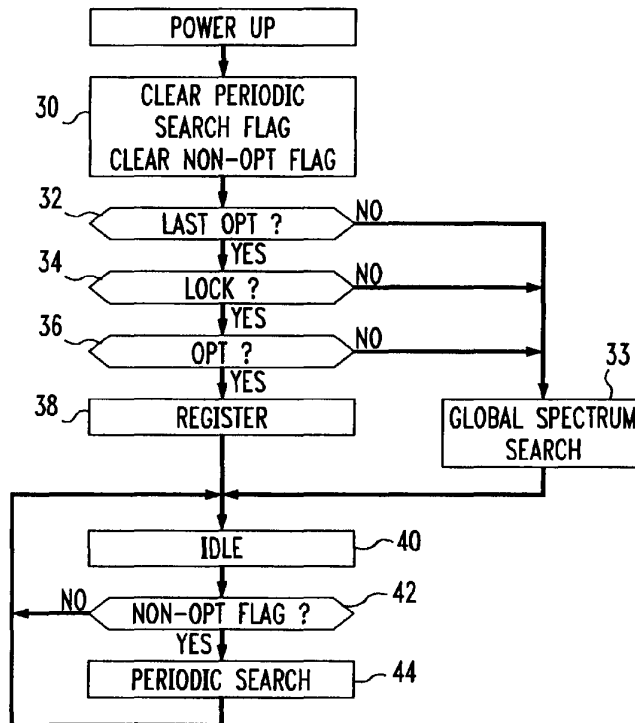


FIG. 5

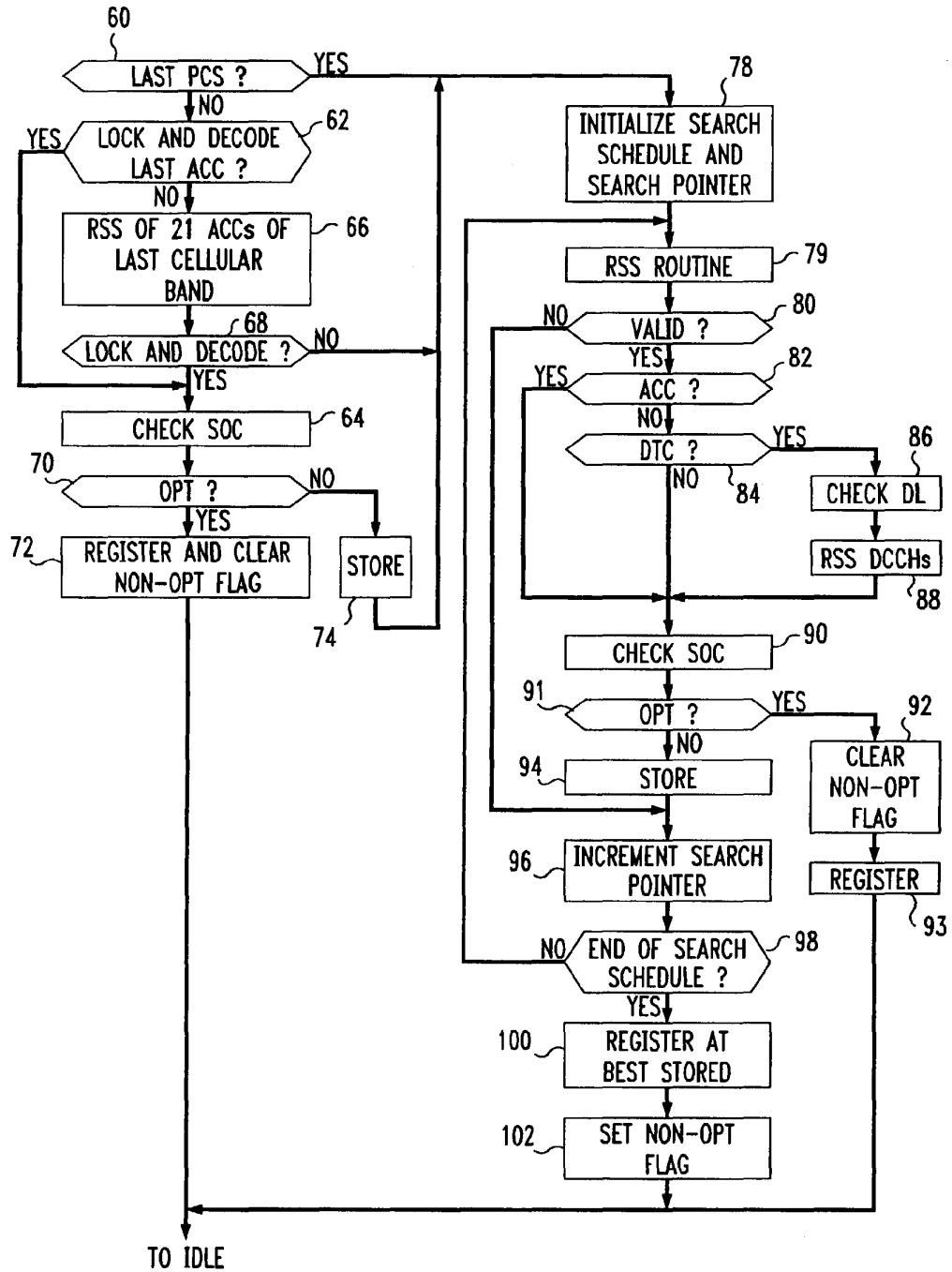


FIG. 6

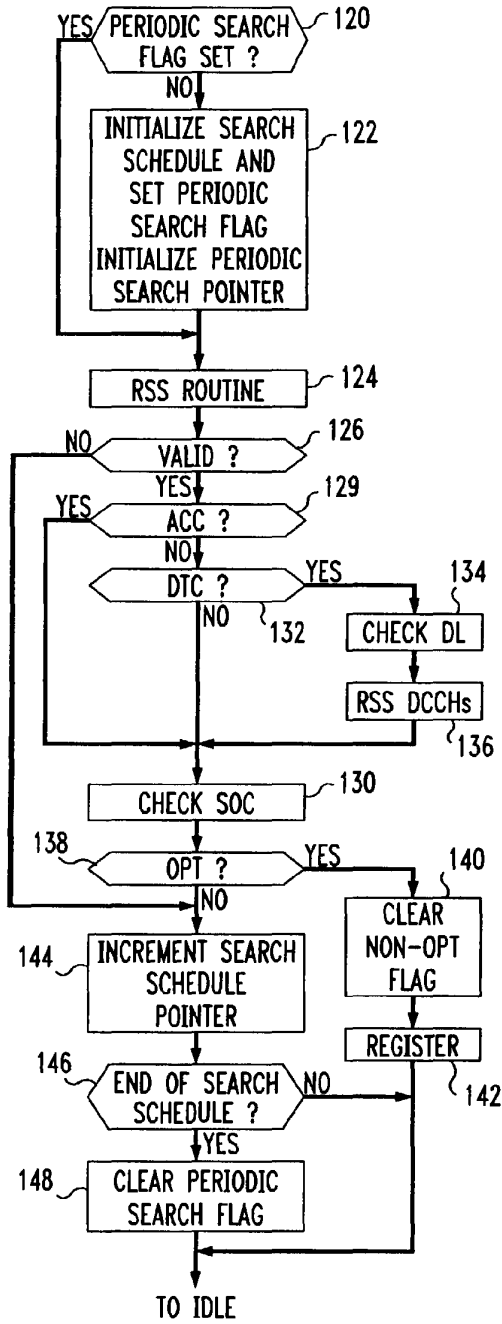


FIG. 7

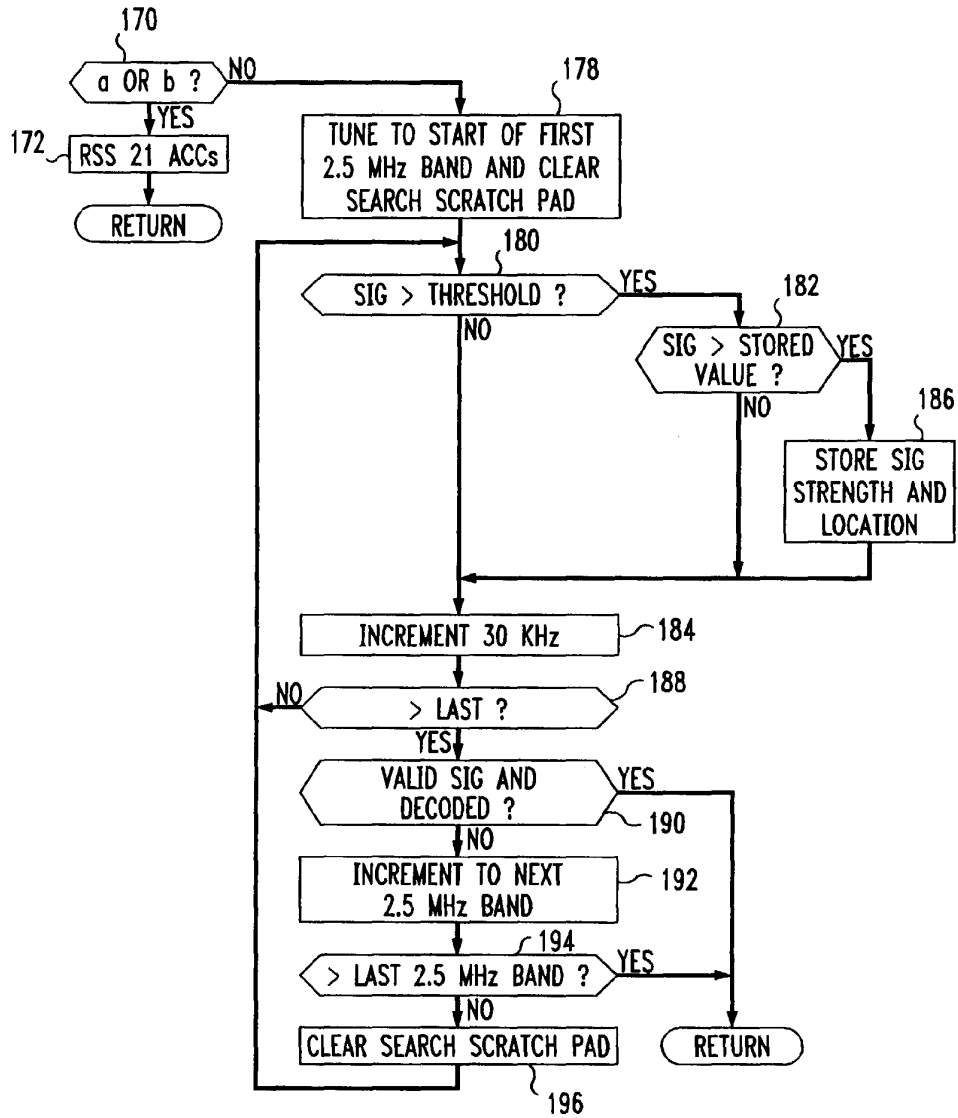


FIG. 8

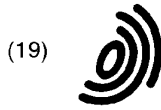
1	2	3	4	5	6	7	8	9
	A	a	C	B	b	D	F	E

FIG. 9

PRIORITY	SOC	SID	SID		SID	SID
OPT	001	43	57	...	21	62
1	011	42	28	...	52	68
2	100	45	23	...	54	77
⋮	⋮	⋮	⋮		⋮	⋮
n	111	49	24	...	58	70
PROHIBIT	101	52	27	...	50	75

FIG. 10

SID	FREQ	FREQ		FREQ	PROHIBIT
43	A	D	...	a	E
37	A	D	...	a	E
57	C	b	...	D	a
51	C	b	...	D	a
21	a	c	...	E	b
17	a	c	...	E	b
⋮	⋮	⋮		⋮	⋮



Europäisches Patentamt
 European Patent Office
 Office européen des brevets



(11) EP 0 838 933 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
 29.04.1998 Bulletin 1998/18

(51) Int Cl. 6: H04L 29/06

(21) Application number: 97480072.4

(22) Date of filing: 16.10.1997

(84) Designated Contracting States:
 AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
 NL PT SE
 Designated Extension States:
 AL LT LV RO SI

(72) Inventor: Doreen, Revis R.
 Durham, NC 27713 (US)

(74) Representative: Therias, Philippe
 Compagnie IBM FRANCE,
 Département de Propriété Intellectuelle
 06610 La Gaude (FR)

(30) Priority: 24.10.1996 US 740062

(71) Applicant: INTERNATIONAL BUSINESS
 MACHINES CORPORATION
 Armonk, NY 10504 (US)

(54) Method and apparatus for access level control in a metropolitan area network

(57) Apparatus and method for using an access level portion of an address to control the level of access for subscribers in a metropolitan area network. The address is assigned to the subscriber terminal either dynamically by the network head-end, or is permanently assigned. The network head-end controls which of various services are offered to subscribers based on the

access level portion of the address. If a subscriber's identity mandates a different level of access than dictated by the access level portion, an address filter is installed by the network head-end. The invention lends itself to use in an internet protocol based metropolitan area network of the type that makes use of the cable TV system.

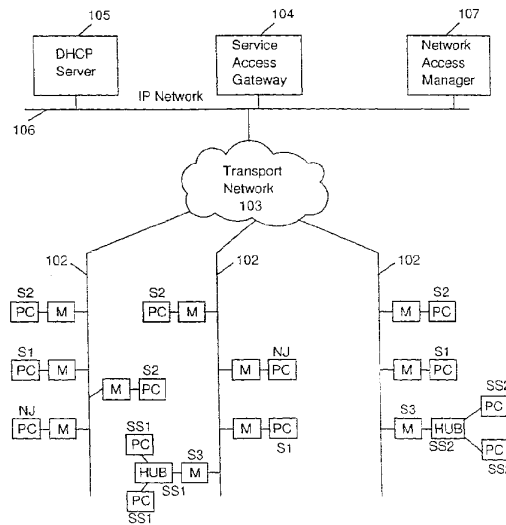


FIG. 1

EP 0 838 933 A1

Description**Background****Field of the Invention**

This invention relates to control of the level of access of multiple subscribers in a network, without depending on network topology for such control. The invention can be used in any of a variety of types of networks; however, it is particularly suited for use in a metropolitan area network (MAN). In its preferred embodiment, the invention is used in a MAN which operates over a cable television system.

Definition of the Problem

With the growth of the Internet and personal computer communications in general, a technology for high speed delivery of data services to residences and small businesses is emerging. This technology is based on the hybrid fiber-coaxial (HFC) cable infrastructure used to deliver cable television services in metropolitan areas. Such an infrastructure may serve geographic areas ranging from small towns to large metropolitan areas. This size falls between the size of a campus or local area network (LAN) and a public wide area network or (WAN). The term metropolitan area network or MAN has been used to describe networks of this size, regardless of the type of network topology used.

One of the first services offered to subscribers on these MAN's will be IP network access. Subscribers will be able to attach their PC's or other user terminals configured with TCP/IP software to the network via the coaxial cable that feeds their home or business premises. A subscriber can then access any services offered through the system such as on-line services and the Internet. In this environment, the subscriber will need a device such as a cable modem or an adapter which can communicate with the HFC infrastructure. I call this device a "subscriber device." The subscriber's personal computer or terminal will be called the "subscriber terminal." Data will be received and transmitted over the HFC infrastructure to a distribution center, which I call the "head-end." The subscriber device will be connected to the subscriber's personal computer or terminal by a local communication interface.

In an HFC environment, subscribers may be offered different levels of service or levels of access. For example, there may be a basic level that provides access to local content and e-mail, an enhanced level that additionally provides full Internet access and a premium level that provides access to on-line service providers. The network access providers need mechanisms by which they can allow or deny access to these services for individual users as appropriate. It is obviously not possible in this environment to have the level of access depend on geography, since there is no way to predict how many

and what different levels of access will be required in a given neighborhood. Ideally, the level of access should be tied to individual subscribers, with a default level of access for each subscriber device.

The current way to provide differing levels of access to different subscribers is the use of packet filtering on a per IP address basis. Since the subscriber network operating over the HFC infrastructure is an IP network, each subscriber terminal has an IP address. An IP address contains two parts: a network or subnet portion, and a host ID. The network or subnet portion is some number of contiguous high-order bits from the address and the host ID is the remaining low order bits. The network or subnet portion determines how routing will occur through the IP network to reach a particular network segment and the host ID then determines the particular machine on that segment. In a current metropolitan area network, the subnet portion corresponds to the geographical location of the user on the subnet.

With IP packet filtering, all traffic to and from a given address is restricted until a subscriber is identified and associated with that IP address. Then IP packet filters can be added to the HFC infrastructure, usually to a local router, to provide access to certain resources and deny access to other resources. Figure 3 shows a diagram of a packet filter.

The problem with the IP packet filtering solution is the large number of packet filters that would be required in the network. Each user may require several filters to grant and deny access to the appropriate resources. As an example, consider a network that supplies the following six levels of service: basic service; Internet access; and four premium services. The premium services might be such things as commercial on-line services and corporate work-at-home services. In this case, each user could require six filters to control the level of access to the network so that access to each service is either granted or denied. Since one filter for each service is used, the number per user multiplies as the network offers more services. The filters would likely be installed at router ports. Assuming each router port served 500-1000 users, 3000-6000 filters would be required per port. Since each router is likely to have several ports, the number of filters quickly grows so large that it adversely impacts the performance of the router, and becomes an administrative problem. What is needed is a way to provide a default level of access for each subscriber terminal in the network without using so many filters. The access level control method must also be independent of geography, since users in the same area or even on the same street may require different levels of access.

Summary

The present invention solves the above identified problem by making use of a portion of the subscriber address in a new way. Typically, the subnet portion of

the address represents only the geographical location of the subscriber terminal. In my solution, an analogous portion of the address is used to specify a default level of access. I call this portion of the address the access level portion.

In the same way that the subnet portion of an address is some number of contiguous, high-order bits, the access level portion is also some number of contiguous, high-order bits. The number of bits for the access level portion may be less than, equal to, or more than the number of bits used for the subnet, depending on network configuration and the number of access levels required. Since the access level portion of the address determines the level of access for a subscriber, default filters are put in place for the access levels, not for each subscriber.

In a network employing the invention, each subscriber terminal has an address in which the access level portion determines the default level of access for the terminal. The default filters in the network provide a default level of access to each terminal based on the access level portion. Each subscriber terminal is connected to the network by a subscriber device. At least one hybrid communications line is connected to the subscriber devices and a transport network connects the head-end to the hybrid communications lines. In the preferred embodiment, the transport network and the hybrid communications lines form an asynchronous transfer mode (ATM) network. In the preferred embodiment, the network head-end includes a network access manager, a dynamic host configuration protocol (DHCP) server and a service access gateway, which may all reside in the same machine, or may be connected by an IP network.

A subscriber terminal is assigned an address based on the media access control (MAC) address of the subscriber device. A subscriber terminal may have a permanently assigned default address, but preferably the address is dynamically assigned when the subscriber device joins the network. An adapter or blade in the network sends invitation messages out to subscriber devices to allow them to join the network. When a subscriber device is activated, it searches for an invitation and responds. The head-end will then authorize the device and allow it to join if appropriate. At this point the subscriber terminal requests an IP address if dynamic assignment is being used. The head-end assigns an address with an access level portion which will specify the default level of access for the subscriber. In the case where the subscriber terminal has a permanently assigned address, the access level portion of the permanent address specifies the default level of access. In any case, the subscriber identity is then determined based on subscriber-supplied information such as user ID and password, and exception filters are set up if needed. The network can be configured to automatically authorize all subscriber devices, or each subscriber device can be authorized or not based on the media access control

(MAC) information for the subscriber device.

In most cases, the steps outlined above are performed by one or more programmed computers or work stations. Instructions to direct the system to perform these steps are contained in computer readable program code on a computer usable medium. The network access manager function and the DHCP server function are each performed by a workstation which has all the necessary data and programs stored in fixed media. The data includes the subscriber addresses, each with an access level portion.

Brief Description of the Drawings

FIG. 1 shows a metropolitan area network which uses the present invention.

FIG. 2 shows graphical representations of a subscriber terminal address according to the present invention.

FIG. 3 shows a graphical representation of an access control filter used with the present invention.

FIG. 4 shows a workstation in which the invention can be implemented.

FIG. 5 shows the method by which a network head-end allows a subscriber device with a dynamically assigned address to join the network according to the present invention.

FIG. 6 shows a media on which the instructions that cause a computer to perform the methods of the present invention are embodied.

FIG. 7 shows a block diagram of a subscriber device.

FIG. 8 shows the detailed communication flow between a subscriber and the head-end in a network employing the invention. Figure 8 is divided into Figures 8A and 8B for convenience.

Detailed Description of the Preferred Embodiments

Figure 1 shows a metropolitan area network using the present invention. The network head end includes the dynamic host configuration protocol (DHCP) server 105, service access gateway 104 and network access manager 107. Figure 1 shows these three functions interconnected by an internet protocol (IP) network 106. Each of these functions is actually implemented by a computer readable program. These programs can reside in different machines connected by a network as shown in Figure 1, or they can all reside in one machine.

Each subscriber uses a terminal, usually a personal computer, PC in Figure 1, although there are other types of terminals. Each PC is connected to a hybrid communication line 102 via a subscriber device M. The hybrid communication lines are of the hybrid fiber-coax type and are commonly called HFC lines. The subscriber device is commonly called a cable modem. Each subscriber device has a local communication interface which can either be directly connected to a PC or to a hub. Where

the subscriber device is connected to a hub, multiple PC's can also be connected to the hub, so that multiple users can use the same subscriber device for network access. Each subscriber device also has a media access control (MAC) address. The MAC function allows multiple subscriber devices to access the HFC infrastructure in a fair and controlled manner. The MAC function operates like a "traffic cop" and determines which subscriber device can transmit when in an attempt to avoid collisions and loss of data.

A transport network 103 connects the HFC lines 102 to the network head-end. In the preferred embodiment, the transport network and HFC lines form an asynchronous transfer mode (ATM) network and the data is transported between the head-end edge of the transport network and the subscriber devices within ATM cells. In this case, each HFC line is connected to a hybrid fiber-coax (HFC) port on an HFC blade within a switch in the transport network. Any type of transport network structure can be used in a metropolitan area network employing the invention; therefore, the details of the transport network are not shown. In the preferred embodiment however, the data moving between the network head-end and the subscriber terminals is exchanged in TCP/IP format. This data is in ATM cells only between the head-end edge of the transport network and the subscriber devices. Each subscriber terminal has a TCP/IP stack installed, and the address for each subscriber terminal is an IP address. Using TCP/IP allows the subscribers to take advantage of TCP/IP applications which are readily available. The TCP/IP data is transported over ATM virtual circuits which are treated as point-to-point links between IP stations and routers.

In the preferred embodiment, the network head-end components function as follows. The network access manager 107 of Figure 1 contains a database to identify valid subscriber devices based on their MAC addresses. This database can be used to authorize subscriber devices and terminals to join the network, or the network access manager can simply authorize any device to join with some minimum level of access. The network access manager also maintains other addresses that are associated with each subscriber device or its connected subscriber terminal such as an IP address and ATM address. All these parameters can change each time a user accesses the system, so the network access manager keeps track of which IP addresses have been associated with which subscriber device and which device each subscriber terminal has logged in from.

The DHCP server 105 of Figure 1 will receive DHCP messages from the HFC blades acting as relay agents. The DHCP server will access the network access manager database to determine the default level of access that should be given to a device. The DHCP server will then assign an IP address having an access level portion specifying the default level of access for the subscriber terminal when it joins the network, unless an address has been previously, permanently assigned to the

subscriber device.

In any case, the address assigned to a subscriber terminal according to the invention is of the form shown in Figure 2, with an access level portion and a host ID. The IP address will also have a subnet portion. In this case, the access level portion can use the same bits as the subnet portion as in 201, fewer bits than the subnet portion as in 200 or more bits than the subnet portion as in 202. In the simplest case, the access level portion is the same as the subnet portion and that portion of the address no longer determines the geographical location of subscribers, but only their default level of access. In this case, the DHCP server has a configuration file which defines certain subnets to have certain levels of access.

The levels of access are physically controlled in the preferred embodiment by installing access control filters at routers in the transport network. An access control filter is shown in Figure 3. All IP packets that come from the subscriber terminal will flow through the router and as they do, they will be tested against the filter list installed at the router. When the first match of a filter is found for a given IP packet, that filter determines whether the packet is allowed to pass through and be forwarded on through the network or whether the packet is dropped at the router and denied further transport. These filters installed at the routers can use any of the information in the IP packet header to match IP packets, but in the preferred embodiment the source and destination IP addresses are used. If the source address in an IP packet matches the access level portion of the filter address, and the destination also matches that specified in the filter, then the filter action, either permit or deny, is applied. In this way, one filter can be installed to permit or deny traffic to a given range of addresses for the group of subscribers whose access level portion of the source IP address are all the same.

The service access gateway 104 of Figure 1 prompts the user for information so that the specific user or human subscriber can be identified. This normally includes a user ID and password. Once the user is identified the service access gateway sends a message to the network access manager informing it of who the user is and what IP address they are using. If the default level of access is not correct for this user, an exception filter can be set up on the network to handle the level of access for this user in the same way as in the prior art.

The various functional units in the head-end are implemented in software installed in a workstation. Figure 4 shows such a workstation. The workstation includes a display device 401 and a system unit 402. The system unit houses the central processing unit or CPU. The workstation contains a removable media unit 403 and a fixed media unit 404. In one embodiment the removable media unit is a diskette drive or a CD-ROM drive and the fixed media unit is a fixed disk drive. In the case of the network access manager and the DHCP server, the workstation fixed media unit contains the data needed

to perform the various functions required by the invention, including IP addresses, each of which has an access level portion and a host ID according to the invention.

Figure 5 shows how a subscriber device joins the network when the address is dynamically assigned to the subscriber device. This process is managed by the network access manager. An HFC blade sends an invitation for subscriber devices to join the network. At 501 an authorization request is received by the head-end in response to the invitation. The subscriber device is then authorized at 502. Depending on how the network is managed, this may not be a true authorization but simply a transmission of required information if the network is allowing any device to join. If the network is restricted to only certain devices, this authorization will be made based on the MAC information for the subscriber device. An IP address is assigned to the subscriber terminal through the subscriber device at 503. The address includes an access level portion which determines the default level of access to the network. Subscriber identity is determined at 504 based on subscriber-supplied information. A determination is made at 505 as to whether the default level of access is appropriate. If it is not, an exception filter is set up at 506. Otherwise the process is complete.

In the case where the an address is permanently assigned, the subscriber device joins the network in response to an invitation, but no address is assigned by the network head-end. Instead, the access level portion of the already assigned address simply sets the default level of access for the user. Exception filters are put in place if necessary, once the specific user identity is determined.

The steps of the invention are performed under the direction of a computer program product consisting of a computer usable medium with a computer program product embodied on the medium. The computer program can be installed on a workstation by inserting the medium in the removable media device of Figure 4. An example of such a medium is shown in FIG. 6. The medium of FIG. 6 consists of a protective jacket 601 which holds a magnetic disk 602. The computer program instructions are recorded on the magnetic disk. This type of medium is commonly called a diskette. The computer program product can be on other types of media, such as tape, CD-ROM, or computer memory. The diskette is shown as an example.

A network with a head-end operating as described above using the present invention greatly reduces the need for filters even though the head-end does not initially know which human subscriber is accessing the network. The level of access should ultimately be tied to individual subscribers, not to subscriber devices. Thus exception filters are sometimes needed, but the need for filters is greatly reduced. For example, if two members of a household have accounts and one has an "A" level of access and the other has a "B" level of

access, the default can be set to one or the other, and exception filters would only be needed fifty percent of the time. The number of exception filters can be reduced even further by making the initial guess of which access level to assign more intelligent than just assuming a default level of access. Subscriber usage characteristics can be used to control the assignment of access levels. For example, a history of user log-ins for each device can be maintained. Therefore, the network access manager would know what level of access is used most often. The usage could also be correlated to the time of day. For example, the network access manager may "know" that during the day a child account in a household is most often used and during the evening a parental account is most often used. Overall, the total number of filters required in the network will always be significantly less than if they were installed on an address by address basis at all times. Additionally, the invention is transparent to subscriber devices and subscriber terminals, allowing the same user-end hardware to be used with the invention as was used in a prior-art network.

Having described a network head-end and infrastructure which uses subnets for access level control, I now describe the subscriber device which is used with such a network. The subscriber device is usually a modem. If the network is operating over the cable TV system the device is called a cable modem. In the preferred embodiment, the modem is controlled by a microprocessor under the control of a computer program. While the program can be embodied on any media, it is normally embodied in a computer memory inside the modem.

FIG. 7 is a functional block diagram of the subscriber device. An internal bus 706 communicates messages and data between the various components of the subscriber device. Modules 703 are computer memory modules which contain, among other data, the computer readable program code to implement the operation of the modem. Modules 704 are specialized communication protocol circuits that provide functions such as media access control (MAC) and ATM functions, if the network formed by the HFC lines and the transport network is an ATM network. A hybrid interface 705 contains a modulator and demodulator and directly interfaces with the network to exchange data over the network. A local communication interface 702 sends and receives information to the subscriber terminal or a hub if there are multiple user terminals. The information flow is controlled by a microprocessor or microcontroller 701.

The subscriber device can be a stand-alone unit, with its own cabinet and power supply. In this case the local communication interface 702 is preferably an Ethernet interface. The Ethernet interface can be simply connected to a subscriber terminal such as a personal computer, or if desired, can be connected to an Ethernet hub so that multiple terminals can be served by one subscriber device. Other types of serial or parallel interfaces can be used. It is also possible to build the subscriber

device on an adapter card in which case the local communication interface is a bus connector for a personal computer. In this case the modem would receive power through the bus connector and would not require power supply.

Turning to FIG. 1 and FIG. 8, the network infrastructure and the subscriber devices work together as follows. Figure 1 has labels to show the status of the various subscriber devices at a given point in time. A device marked NJ is not joined to the network. A device marked S1 is on subnet 1, S2 is on subnet 2 and S3 is on subnet. The PC's are the subscriber terminals. Each PC has an Ethernet card installed through which the connection is made either to a hub or to the local communication interface of a modem. PC's connected to a hub represent subscriber locations with multiple PC's. For purposes of this embodiment, the access level portion of an address is the subnet portion. In this environment, these PC's may be on a separate logical subnet of their own represented by SS1 (subscriber subnet 1), and SS2 (subscriber subnet 2). These separate subscriber subnets are then connected to the larger general subnets through the subscriber device, which acts as a simplified router, existing on both subnets.

The subnet portion of the IP address determines routing through the network. When IP packets reach routers at the edge of the transport network, the routers make a decision on how to handle the packets based on the subnet portion of the destination address. If the router can communicate directly with the specified subnet, it will send the packet directly to the subscriber terminal. This would be the case for any of the subnets S1, S2 or S3. If however, the router is not directly on the specified subnet, as would be the case for the subscriber subnets SS1 and SS2, the router will have routing tables set up to tell it to forward the packet to the particular subscriber device/modem that is attached or is at least closer to the intended subnet. In our environment, this will be a modem that is attached to both an Sn subnet and the desired SSm subnet.

FIG. 8 shows the detailed flow of messages between the subscriber terminal and the other components of the network during a network session. The HFC blades send out invitations to the subscriber devices on a regular basis and any subscriber device wishing to join the network will respond with an invitation response. The invitation response causes an authorization request to be sent to the network access manager (NAM). The NAM will respond with either permission granted or denied, and all startup parameters required if access is granted. If access is granted, the HFC blade then sends these startup parameters to the subscriber device in "assign params" and "assign IP params" messages and the device is then joined to the network.

If the subscriber terminal is configured to receive IP address dynamically, it will then generate DHCP messages which will flow through the HFC blade to the DHCP server in the head-end. Note that the MAC address

in the DHCP messages may be replaced by the subscriber device so that the IP address will be assigned based on the MAC address of the subscriber device, not the MAC address of the Ethernet card in the subscriber terminal. The responses will pass back in the opposite direction and the subscriber terminal will thus be configured with an IP address. Also note that if the MAC address was replaced by the subscriber device, the original address will be restored before the response is returned to the subscriber terminal. The DHCP messages shown are defined by the DHCP protocol.

After the subscriber device has been joined to the network and the IP address has been assigned, statically or dynamically, the subscriber's IP traffic will be restricted to the service access gateway (SAG). Users can then send a user name and password to the SAG to identify themselves. The SAG will validate a user and exception filters will be added to the routers if necessary. The SAG then sends a message down to the subscriber device, via the NAM, to lift the restriction of IP traffic to the SAG. At this point, the user traffic will only be restricted by the filters in the routers. When a user logs out, the SAG again sends a message down to the subscriber device, via the NAM, telling it to again restrict traffic to the SAG until the next user logs in, causing the process to be repeated.

Claims

1. A metropolitan area network comprising:
 - a plurality of subscriber terminals, each subscriber terminal having an address including an access level portion, where the access level portion determines a default level of access for the subscriber terminal;
 - a plurality of subscriber devices connected to the subscriber terminals;
 - at least one hybrid communications line connected to the plurality of subscriber devices;
 - a head-end for communicating with the subscriber terminals and for providing a default level of access to each subscriber terminal in accordance with the access level portion contained in the address for the subscriber terminal; and
 - a transport network disposed between the hybrid communications line and the head-end.
2. The metropolitan area network of claim 1 wherein the head-end further comprises:
 - a network access manager for identifying sub-

scriber devices and granting network access to subscriber terminals based on media access control information for the subscriber devices;

a dynamic host configuration protocol (DHCP) server for assigning addresses to subscriber terminals; and

a service access gateway for identifying subscribers using subscriber input.

3. The metropolitan area network of claim 2 wherein the network access manager, the DHCP server, and the service access gateway are connected by an internet protocol network.

4. The metropolitan area network according to any of claims 1 through 3 wherein the transport network and hybrid communications lines form an asynchronous transfer mode (ATM) network.

5. The metropolitan area network according to any of claims 1 to 4 wherein the head-end is a network head-end comprising:

a network access manager for identifying subscriber devices and granting subscriber terminals network access;

a dynamic host configuration protocol (DHCP) server for assigning addresses to subscriber terminals, an address containing an access level portion wherein the access level portion determines a default level of access for a subscriber, the DHCP server connected to the network access manager; and

a service access gateway for identifying subscribers using subscriber input, the service access gateway connected to the DHCP server and the network access manager.

6. The network head-end of claim 5 wherein the network access manager, the DHCP server, and the service access gateway are all interconnected by an internet protocol network.

7. The network head-end according to claim 5 or claim 6 wherein access to the subscriber is granted or denied based on the media access control (MAC) information for the subscriber device.

8. The metropolitan area network according to any of claims 2 to 7 wherein the network access manager comprises:

a display device;

a computer system unit connected to the display device wherein the computer system unit includes a CPU, a removable media unit; and a fixed media unit, the fixed media unit having addresses embodied thereon wherein each address comprises:

an access level portion, the access level portion for determining a default level of access for the subscriber terminal to which the address is assigned; and

a host identifier (host ID) for further specifying the subscriber terminal.

9. The metropolitan area network according to any of claims 2 to 8 wherein the dynamic host configuration protocol (DHCP) server comprises:

a display device;

a computer system unit connected to the display device wherein the computer system unit includes a CPU, a removable media unit; and a fixed media unit, the fixed media unit having addresses embodied thereon wherein each address comprises:

an access level portion, the access level portion for determining a default level of access for the subscriber terminal to which the address is assigned; and

a host identifier (host ID) for further specifying the subscriber terminal.

10. A method of joining a subscriber terminal to a network, the method comprising the steps of:

receiving an authorization request in response to an invitation;

authorizing a subscriber terminal;

assigning an address to a subscriber, the address including an access level portion, the access level portion determining a default level of access for subscribers using the subscriber device;

determining a subscriber identity based on subscriber-supplied information;

determining, based on the subscriber identity, if the default level of access is correct; and

setting up an exception filter for the subscriber if the default level of access is not correct.

11. The method of claim 10 wherein the address is assigned to the subscriber based on subscriber usage characteristics.
12. The method according to claim 10 or claim 11 wherein the subscriber terminal is authorized based on media access control (MAC) information for the subscriber device. 5
13. Apparatus for joining a subscriber terminal to a network, the apparatus comprising means for performing the steps according to any of claims 10 to 12. 10
14. A computer program product comprising a computer usable medium having a computer readable program embodied therein for causing the joining of a subscriber terminal to a network, the computer readable program further comprising: 15
- computer readable program code for causing a computer to effect the receiving of an authorization request; 20
- computer readable program code for causing a computer to effect the authorizing of a subscriber terminal connected to the subscriber device; 25
- computer readable program code for causing a computer to effect the assigning of an address to a subscriber, the address including an access level portion, the access level portion determining a default level of access for subscribers using the subscriber device; 30
- computer readable program code for causing a computer to effect the determining of a subscriber identity based on subscriber-supplied information; 35
- computer readable program code for causing a computer to effect the determining, based on the subscriber identity, if the default level of access is correct; and 40
- computer readable program code for causing a computer to effect the setting up of an exception filter for the subscriber if the default level of access is not correct. 45
15. The computer program product of claim 14 wherein the address is assigned to the subscriber based on subscriber usage characteristics. 50
16. The computer program product according to claim 14 or claim 15 wherein the subscriber terminal is authorized based on media access control (MAC) information for the subscriber device. 55

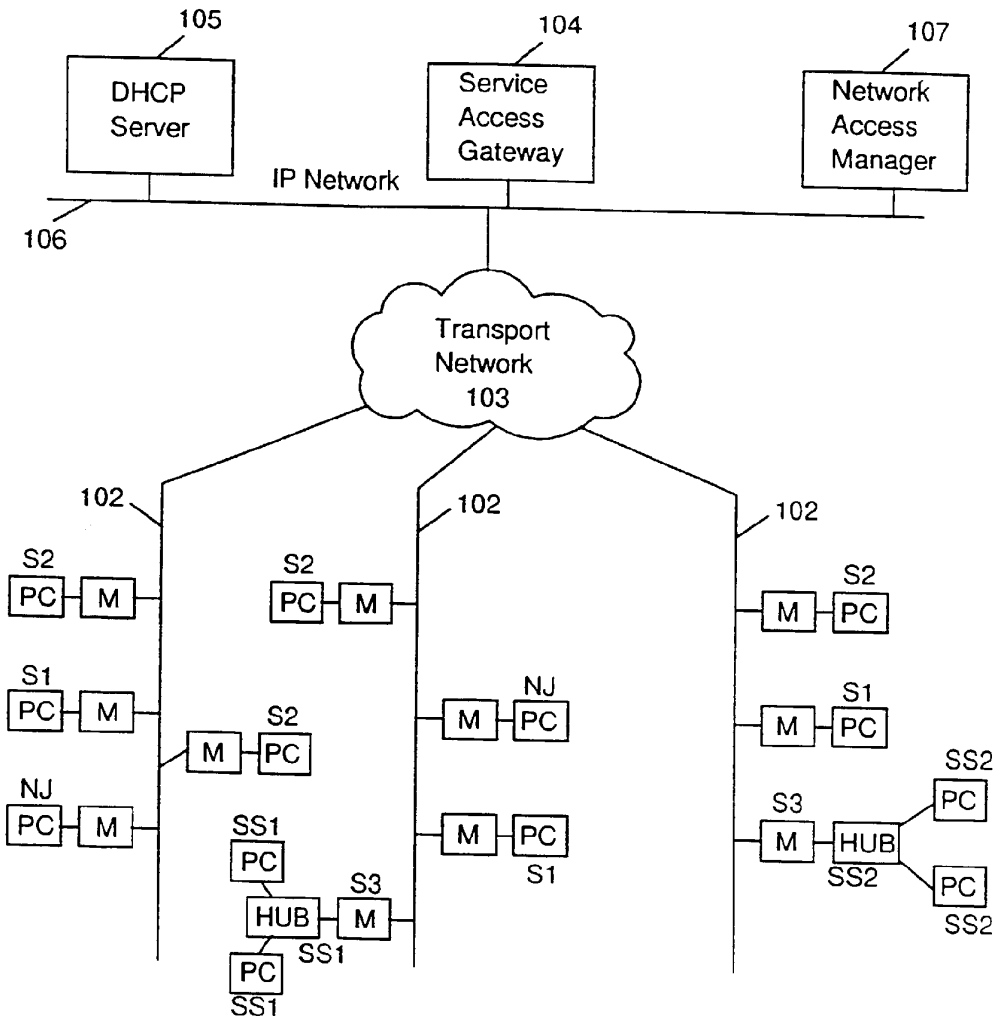


FIG. 1

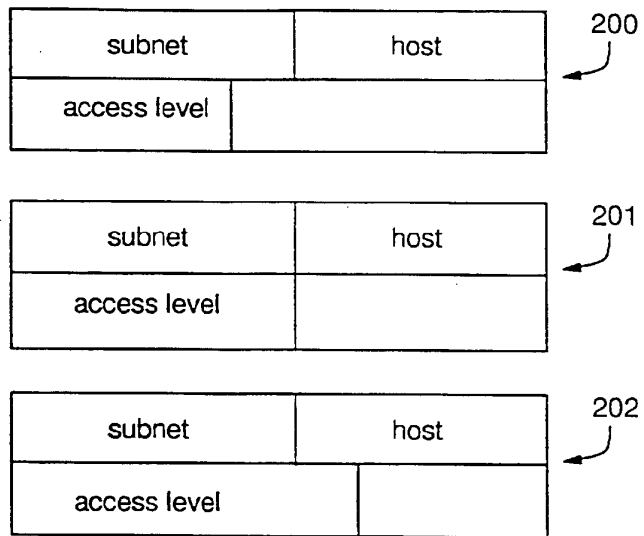


FIG. 2

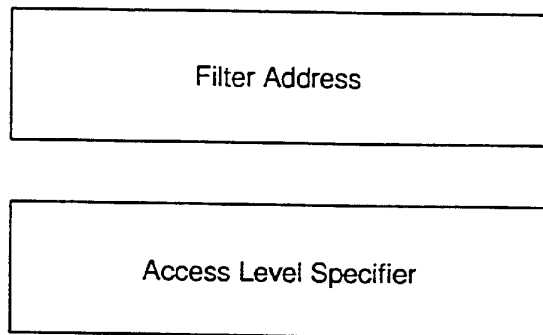


FIG. 3

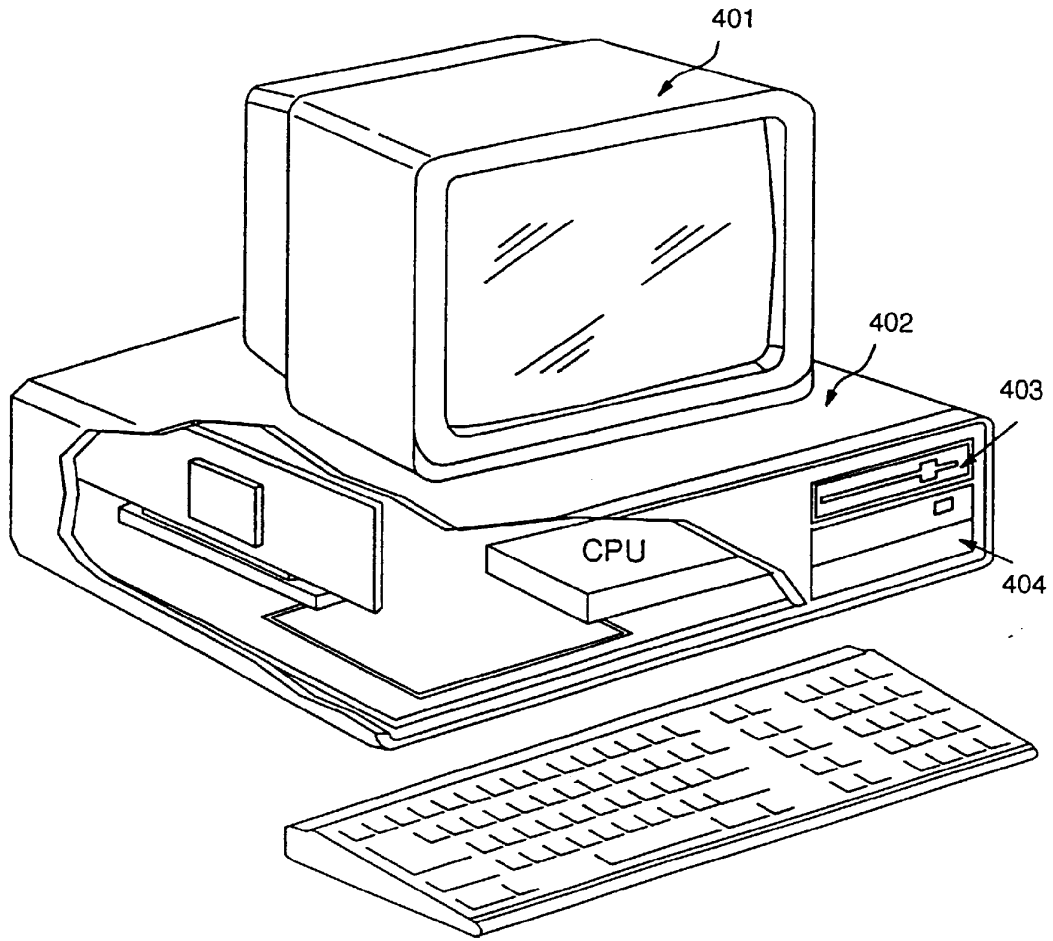


FIG. 4

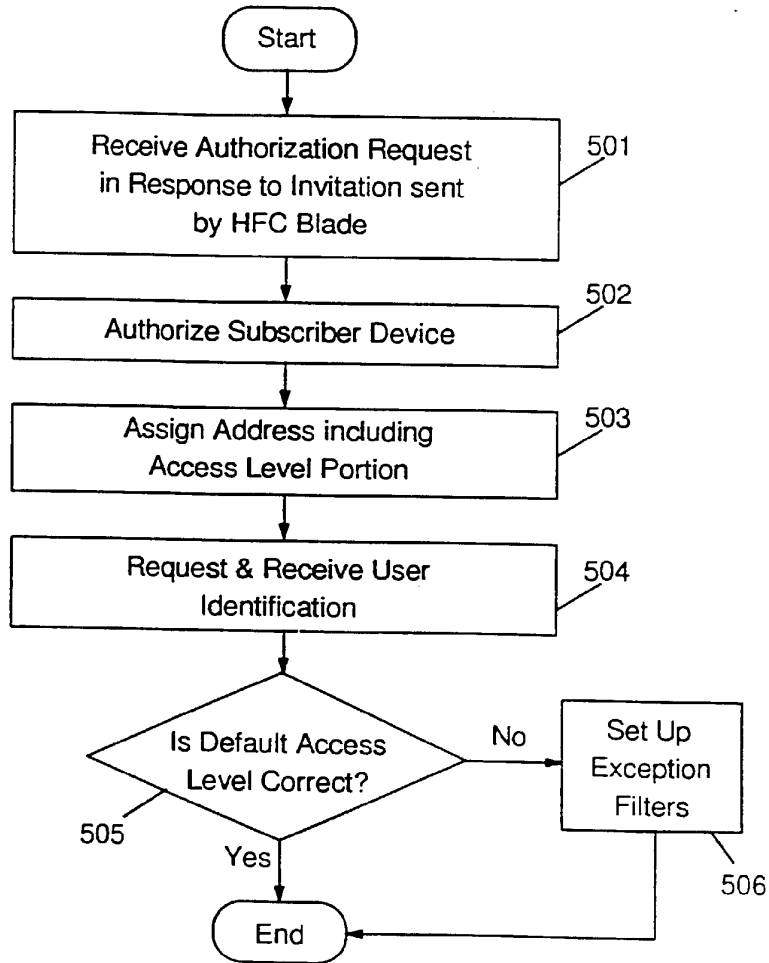


FIG. 5

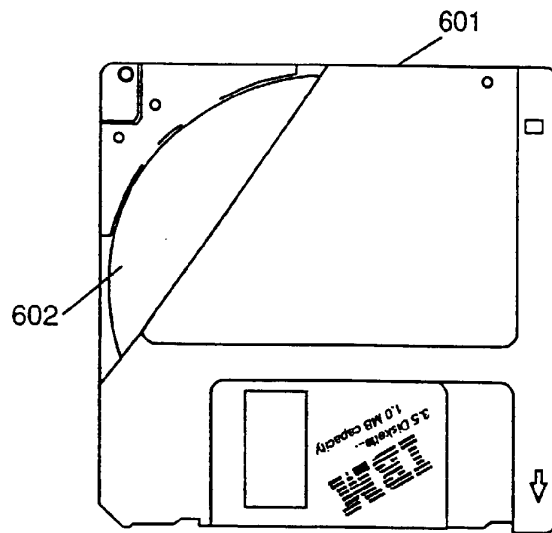


FIG. 6

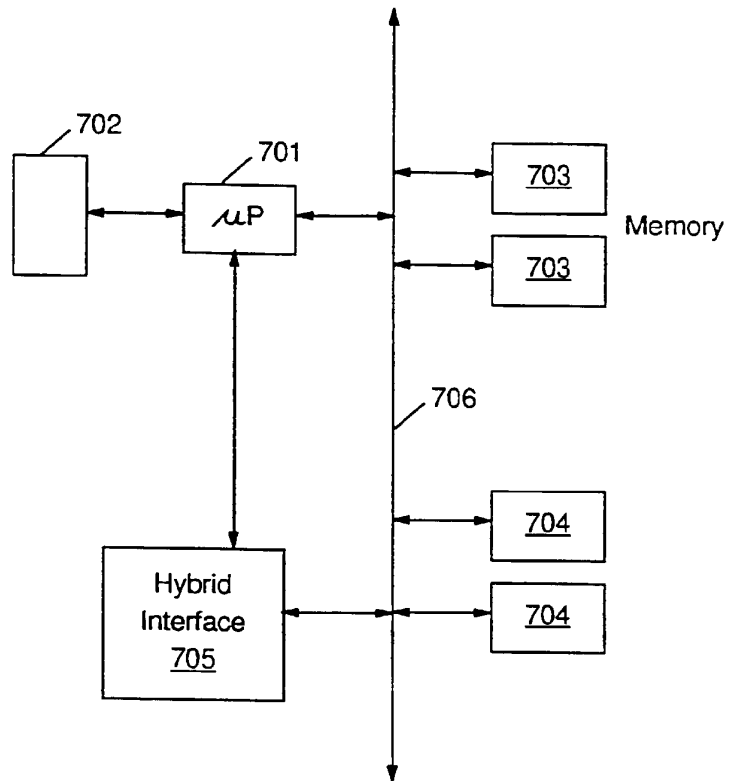


FIG. 7

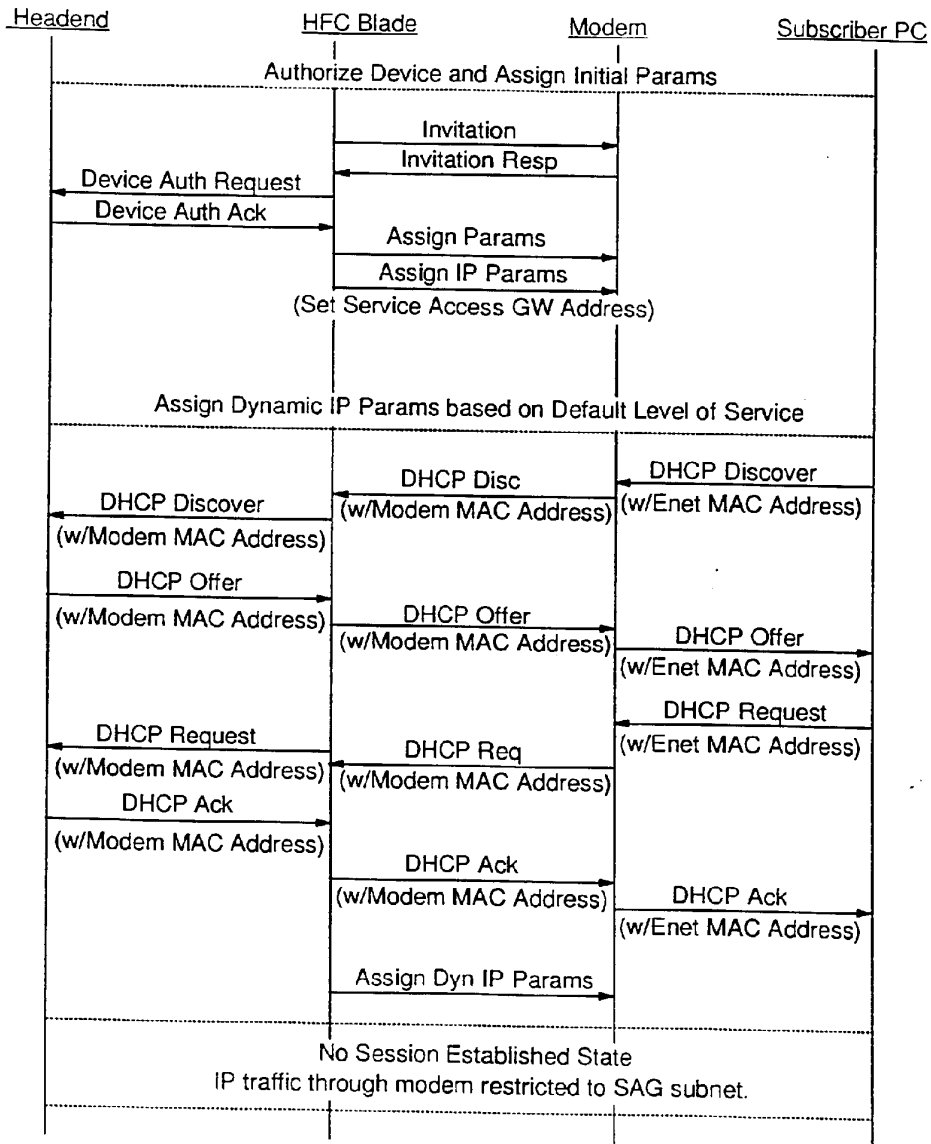


FIG. 8A

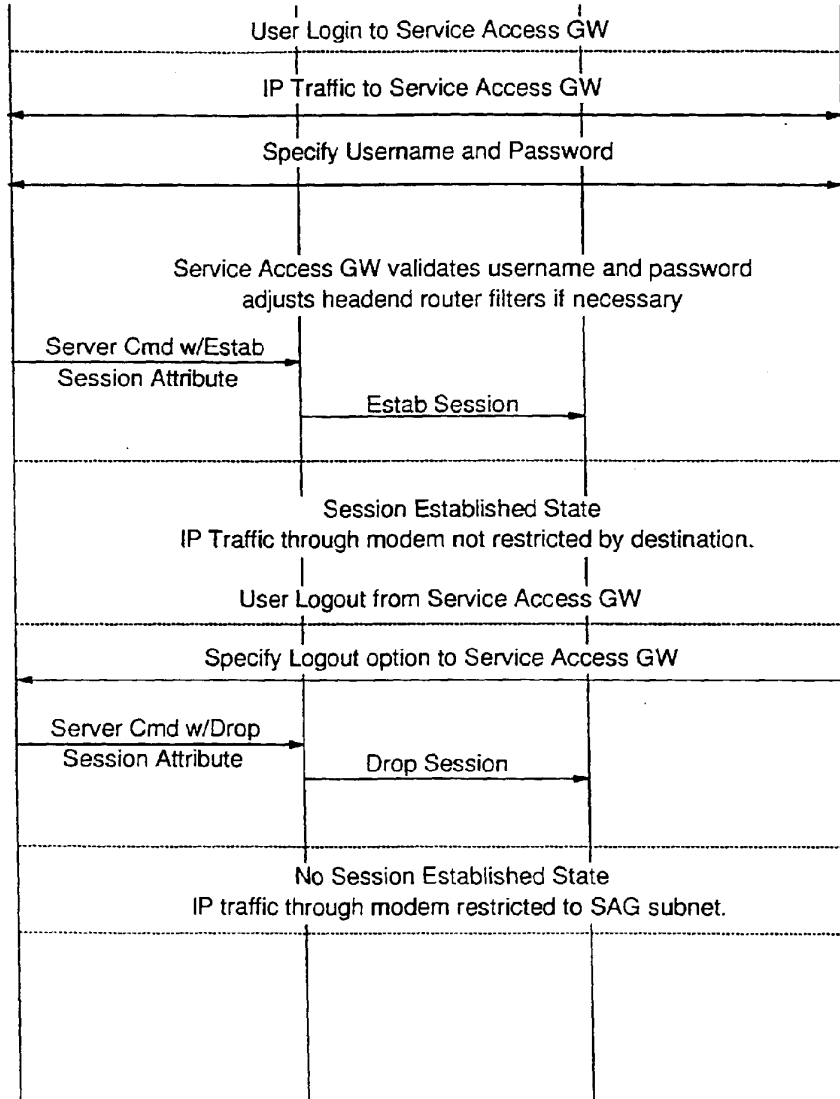


FIG. 8B

FIG. 8A
FIG. 8B

FIG. 8



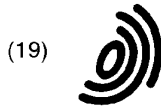
European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 48 0072

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Y	BEDNER I ET AL: "HP BIDS - BROADBAND INTERACTIVE DATA SOLUTION" DIGEST OF PAPERS OF COMPCON (COMPUTER SOCIETY CONFERENCE) 1996, TECHNOLOGIES FOR THE INFORMATION SUPERHIGHWAY SANTA CLARA, FEB. 25 - 28, 1996, no. CONF. 41, 25 February 1996, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, pages 39-44. XP000628463	1	H04L29/06
A	* page 39, right-hand column, line 5 - line 9 * * page 40, left-hand column, line 19 - right-hand column, line 19 * * page 41, left-hand column, line 50 - right-hand column, line 2 * * page 41, right-hand column, line 10 - line 18 * * page 41, right-hand column, line 52 - page 42, left-hand column, line 2 *	2-16	
Y	WO 89 08887 A (QPSX COMMUNICATIONS LTD) * abstract * * page 3, line 26 - line 30 * * page 4, line 6 - line 34 * * page 5, line 12 - page 6, line 14 * * page 9, line 14 - line 33 *	1	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L
A	US 5 513 263 A (WHITE ET AL.) * abstract * * column 1, line 64 - column 2, line 2 * * column 5, line 61 - line 67 *	1-16	
A	US 5 113 499 A (ANKNEY ET AL.) * abstract * * column 3, line 40 - line 56 * * column 5, line 33 - line 67 *	1-16	
The present search report has been drawn up for all claims			
Place of search		Date of completion of the search	Examiner
THE HAGUE		20 January 1998	Larcinese, C
CATEGORY OF CITED DOCUMENTS		1 : theory or principle underlying the invention E : earlier patent document, but published on or after the filing date D : document cited in the application I : document cited for other reasons 6 : member of the same patent family, corresponding document	
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document			

EPO FORM 1400 (01/97)



Europäisches Patentamt
 European Patent Office
 Office européen des brevets



(11) EP 0 915 590 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
 12.05.1999 Bulletin 1999/19

(51) Int Cl.6: H04L 9/32

(21) Application number: 98309195.0

(22) Date of filing: 10.11.1998

(84) Designated Contracting States:
 AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
 MC NL PT SE
 Designated Extension States:
 AL LT LV MK RO SI

- Boyle, Stephen S.
 Fremont, CA 94539 (US)
- King, Peter F.
 Half Moon Bay, CA 94019 (US)
- Schwarz, Bruce V.
 San Mateo, CA 94402 (US)

(30) Priority: 10.11.1997 US 966988

(71) Applicant: Unwired Planet, Inc.
 Redwood City, California 94063 (US)

(74) Representative: Suèr, Steven Johannes et al
 Ablett & Stebbing,
 Caparo House,
 101-103 Baker Street
 London W1M 1FD (GB)

(72) Inventors:
 • Liao, Hanging
 San Ramo, CA 94583 (US)

(54) Method and system for secure lightweight transactions in wireless data networks

(57) The present invention is a method and system for establishing an authenticated and secure communication session for transactions between a server and a client in a wireless data network that generally comprises an airmet, a landline network and a link server therebetween. The client having limited computing resources is remotely located with respect to the server and communicates to the server through the wireless data network. To authenticate each other, the client and the server conduct two rounds of authentication, the client authentication and the server authentication, independent-

ly and respectively, each of the authentication processes is based on a shared secret encrypt key and challenge/response mechanism. To reach for a mutually accepted cipher in the subsequent transactions, the server looks up for a commonly used cipher and forwards the cipher along with a session key to the client. The subsequent transactions between the client and the server are then proceeded in the authenticated and secure communication session and further each transaction secured by the session key is labeled by a transaction ID that is examined before a transaction thereof takes place.

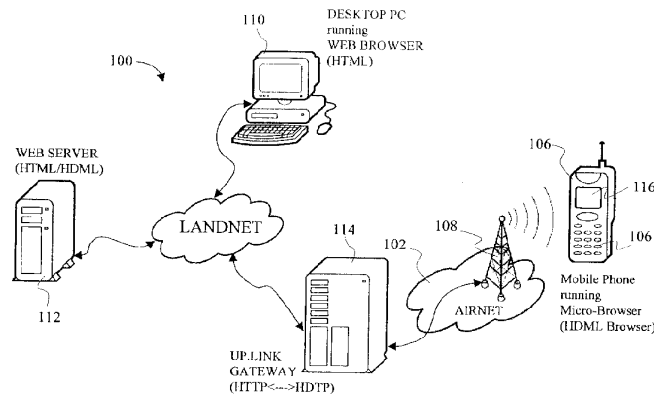


Fig. 1

EP 0 915 590 A2

Description

[0001] A portion of the disclosure of this patent document contains material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyrights whatsoever.

[0002] The invention relates to wireless data communications, and more particularly relates to secure lightweight transactions between mobile devices and landline servers over wireless data networks; wherein the mobile devices have very limited computing power, memory and graphical display capability.

[0003] A fast-growing trend on the Internet is electronic commerce. The electronic commerce is an integrative concept designed to draw together a wide range of business support services, trading support systems for commodities, products, customized products and custom-built goods and services; ordering and logistic support systems; settlement support systems; and management information and statistical reporting systems, all via the Internet. It is well known, however, that the Internet is a wide open, public and international network of interconnected computers and electronic devices around the world. Anyone who has access to a computer in the network can intercept signals carrying proprietary information traveling along the network. To transact business over the open network, companies or individuals must have an efficient, reliable and secured manner to conduct private communications therebetween. Security thus becomes a primary concern over the open Internet and there have been many efforts in progress aimed at protecting the proprietary information travelling in the Internet. One of the efforts is to use cryptographic techniques to secure a private communication between two parties. The cryptographic techniques provide a way to transmit information across untrusted communication channel without disclosing the contents of the information to anyone accessing the communication channel.

[0004] US Patent No. 5,671,279 to Taher Elgarnal discloses a courier electronic payment system for conducting the electronic commerce using a secure courier system. The system governs the relationship between a customer, merchant, and acquirer gateway to perform credit card purchases over the open network by using a secure connection to simplify the problem of Internet-based financial transactions. Visa International Service Association, in collaboration with Microsoft Corporation, provides a secured transaction technology using digital signature to authenticate a credit card and merchant decal, referring to <http://www.visa.com> for detail. The technologies developed by RSA Data Security, Inc. are the global de facto standard for public key encryption and digital signature and may be part of existing and proposed standards for the Internet as well as business and financial networks around the world. More information about the Internet security can be found at <http://www.rsa.com>.

[0005] The above and other ongoing efforts are all primarily targeted at the Internet that is a plurality of landline or wired networks. To use the Internet, one has to have a physical access to a computer wired into the network. To provide the mobility of the network, wireless data networks were introduced, as such the landline networks become an integral part of the wireless data networks. With the wireless data networks, people, as they travel or move about, are able to perform, through wireless computing devices or handheld communication devices, exactly the same tasks as they could do with computers in the landline networks. Similar to the Internet, however, the nature of the wireless communications provides an opportunity for intrusion since the mobile data is sent through the air. Anyone who has an appropriate receiver with a designed antenna can intercept signals being communicated between a wireless computing device and a landline base-station or network. Privacy, authentication, authorization, and integrity are thus deemed the important elements in wireless data network. Therefore additional efforts have been started to ensure that the proprietary information is sent via wireless networks that must be restricted only to those with a need to know.

[0006] Many networks employ encryption and other security measures to protect mobile data from access by unauthorized third party. Certain technologies and access methods contribute to network security. Spread spectrum technology, for example, is inherently secure, but it only provides a link level security. There is no guarantee that a mobile device has a secure communication to a landline device through a complete wireless network that generally comprises an airmet, the Internet and a gateway therebetween. US Patent No. 5,604,806 to Hassan, et al, discloses an apparatus and method for secure radio communication by using key sequences derived from the short-term reciprocity and radio spatial decorrelation of phase of the radio channel. US Patent 5,371,794 to Whitfield, et al, shows another method and apparatus for providing a secure communication between a mobile wireless data processing device and a base data processing device. The mobile device sends the base device a digitally signed mutually trusted certificate according to a public encryption key and the base device sends a modified version to the mobile device upon successfully recovering the certificate. If the mobile device recovers the modified version, both devices enter a secure data communication. The disclosed system by Whitfield may work well with mobile devices that have competitive computing resources to satisfy the public-key-based encryption speed. Nevertheless the connection time in an airmet is expensively measured and many mobile devices such as mobile phones have a small fraction of the computing resources provided in a typical desktop or portable computer. The computing power in a typical cellular phone is less than one percent of what is in a regular desktop computer, the memory capacity thereof is generally less than 250 kilobytes and the LCD

display is perhaps four lines high by twelve or twenty characters, the graphics capabilities thereof are very limited or nearly nonexistent. There has been thus a great need for a generic solution that provides a secure communication with competitive performance between mobile devices of limited computing resources and landline devices through an open network.

5 [0007] Further many current networks operate based on Hypertext Transfer Protocol (HTTP) that is built on the Transmission Control Protocol/Internet Protocol (TCP/IP). But the TCP protocol requires considerable computing power and network bandwidth resources. A single connection, for example, may require an exchange of more than ten packets between a sender and a receiver in the Internet. Therefore there has been further a need for a generic method and system that provide a secure communication between mobile devices and landline devices using fewer number of
10 packets so as to increase transmission efficiency in mobile devices of limited computing resources.

[0008] The present invention has been made in consideration of the above described problems. According to a preferred embodiment, the present invention is a method and system for establishing an authenticated and secure communication session for transactions between a server and a client in a wireless data network that generally comprises an airnet, a landline network and a link server therebetween. The client is remotely located with respect to the
15 server and communicates to the server through the wireless data network. The method comprises the steps of:

- (a) the client sending a session-request signal to the server for creating the session therebetween, the session-request signal comprising at least one client message encrypted according to a shared secret encrypt key;
- (b) the server conducting a first client authentication by decrypting the encrypted client message according to the
20 shared secret encrypt key upon receiving the session-request signal;
- (c) the server generating a session key for the session in creation, a first derivative from the decrypted client message and generating a server message;
- (d) the server sending a session-reply signal comprising the session key, the first derivative and the server message; the session key, the first derivative and the server message being encrypted according to the shared secret
25 encrypt key;
- (e) the client conducting a first server authentication by decrypting the first derivative and the server message being encrypted according to the shared secret encrypt key;
- (f) the client conducting a second server authentication by validating the first derivative with the client message;
- (g) the client generating a second derivative from the server message if the step (f) of the second server authentication
30 succeeds;
- (h) the server conducting a second client authentication by decrypting the second derivative and verifying the second derivative with the server message upon receiving ; thereby the authenticated and secure communication session is established between the client and the server after the first and the second client authentication as well as the first and the second server authentication are all successful.

35 [0009] Upon the establishment of the secure communication between the client and the server, either the client or the server may initiate a transaction therebetween. To ensure the transaction between a valid session, the transaction is encrypted by a mutually accepted cipher according to the session key and identified by a session ID embedded therein. The mutually accepted cipher is obtained by the server through a cipher negotiation with the client and the
40 transaction ID in the transaction is always examined in the server before the server responds to the client with a service reply. Upon receiving the service reply from the server, the client can proceed the transaction with the server.

[0010] The system for establishing an authenticated and secure communication: the system comprises:
45 a landline network running on a first communication protocol that is usually HTTP;
at least one server coupled into the landline network and communicating with the landline network;
an airnet running on a second communication protocol that is usually HDTP;
a client remotely located with respect to the server and communicating with the airnet by radio transmission means;
a link server, coupling the airnet to the landline network, for linking the first communication protocol to the second
50 communication protocol, whereby the client can communicate with the server;
means for generating a session-request signal comprising at least one first message encrypted according to a shared secret encrypt key; the first message usually being a first nonce represented by a first 2-byte numeral, the session-request signal being transmitted to the airnet;
means for sending a session-reply signal comprising at least one second message encrypted according to the
55 shared secret encrypt key; the second message usually being a second nonce represented by a second 2-byte numeral, the session-reply signal sending means comprising:

means for conducting a first client authentication when the session-request signal is received, the first client authentication comprising means for recovering the encrypted first message from the received session-request

signal; and
means for generating a first derivative from the recovered first message;

5 means for conducting server authentication upon receiving the session-reply signal, the conducting server authentication means comprising:

means for recovering the encrypted second message when the session-reply signal is received; and
means for verifying the received first derivative with the first message; and

10 means for generating a second derivative from the second message;
means for generating a session-authentication-complete signal comprising the second derivative;
means for conducting a second client authentication, the second client authentication means comprising means for verifying the received second derivative with the second message when the session-authentication-complete signal is received; and
15 whereby the authenticated and secure communication between the client and the server is established when the first and second client authentication and the server authentication are complete.

[0011] In a further aspect of the present invention there is provided a method for establishing an authenticated and secure communication session for transactions between a client and a server in a wireless data network, the client remotely located with respect to the server, the method comprising the steps of: (a) the client sending a session-request signal to the server for creating the session therebetween, the session-request signal comprising at least one client message encrypted according to a shared secret encrypt key; (b) the server conducting a first client authentication by decrypting the encrypted client message according to the shared secret encrypt key upon receiving the session-request signal; (c) the server generating a session key for the session in creation, a first derivative from the decrypted client message and generating a server message; (d) the server sending a session-reply signal comprising the session key, the first derivative and the server message; the session key, the first derivative and the server message being encrypted according to the shared secret encrypt key; (e) the client conducting a first server authentication by decrypting the first derivative and the server message being encrypted according to the shared secret encrypt key; (f) the client conducting a second server authentication by validating the first derivative with the client message; and (g) the client generating a second derivative from the server message if the step (f) of the second server authentication succeeds.

[0012] Preferably, the session-request signal further comprises a client cipher indicating what encryption the client currently uses.

[0013] In preferred embodiments, the session-request signal further comprises a modified version of the client message, the modified version having an operational relationship with the client message and being encrypted according to the shared secret encrypt key.

[0014] Conveniently, the method further comprises the step of the server negotiating a mutually accepted cipher with the client for the session in creation.

[0015] Preferably, the step of the server negotiating the mutually accepted cipher with the client comprises the steps of examining the client cipher; looking up a server cipher and determining the mutually accepted cipher.

40 [0016] In preferred embodiments, the method further comprises the steps of: the client sending a session-complete signal comprising the second derivative; and the server conducting a second client authentication by validating the second derivative with the server message; and thereby the authenticated and secure communication session is established between the client and the server after the first and the second client authentication as well as the first and the second server authentication are all successful.

45 [0017] Conveniently, the method further comprises the steps of: the client initiating a client transaction request and generating a transaction ID thereof, the client transaction request being encrypted according to the session key; the server examining the transaction ID to see if the transaction ID is in a trans-sequence upon receiving the client transaction request after decrypting the client transaction request according to the session key; the server replying to the client with a reply signal if the step of the server examining the transaction ID is true; and the client sending an acknowledge signal to commit a transaction specified in the client transaction signal.

50 [0018] Preferably, the method further comprises the steps of the server initiating a server transaction signal comprising at least one notification therein; the client replying to the server with a get-notify signal comprising a transaction ID to fetch the notification; the server examining the transaction ID to see if the transaction ID is in a trans-sequence; the server replying to the client with a reply signal if the step of the server examining the second transaction ID is successful; and the client sending an acknowledge signal to commit an transaction specified in the transaction signal initiated by the server.

55 [0019] In preferred embodiments, the method further comprises the steps of: the client initiating a transaction signal comprising a transaction ID to interact with the server; the client coupling the second derivative from the server message

with the transaction signal, thereby a combined signal is formed; the client sending the combined signal to the server; the server conducting a second client authentication by validating the second derivative with the server message upon receiving and decoupling the combined signal; and thereby the authenticated and secure communication session is established between the client and the server after the first and second client authentication as well as the first and the second server authentication are all successful; the server examining the transaction ID to see if the transaction ID is in a trans-sequence; the server replying to the client with a reply signal; and the client sending an acknowledge signal to commit an transaction specified in the transaction signal initiated by the client.

[0020] Conveniently, the transaction request is a service-request signal comprising a URL.

[0021] Preferably, the step of the server replying to the client with a reply signal comprises the steps of contacting a service identified by the URL and sending a result in form of digest from the step of contacting the service identified by the URL.

[0022] In preferred embodiments, the step of the server replying to the client with a reply signal comprises the steps of contacting a service identified by the URL and sending a result in form of digest from the step of contacting the service identified by the URL.

[0023] Conveniently, the transaction request is a post signal comprising a URL and editorial information.

[0024] Preferably, the client message is a client nonce represented by a sequence of digits.

[0025] In preferred embodiments, the client nonce is a non-repeatable two-byte numeral.

[0026] Conveniently, the first derivative has a first relationship with the client nonce.

[0027] Preferably, the session-reply signal further comprises a session ID of the session, the session key and the server cipher, all being encrypted according to the shared secret encrypt key.

[0028] In preferred embodiments, the server message is a server nonce.

[0029] Conveniently, the second nonce is a non-repeatable two-byte numeral.

[0030] Preferably, the second derivative has a second relationship with the server nonce.

[0031] According to a further aspect of the present invention, there is provided a system for establishing an authenticated and secure communication session, the system comprising: a landline network running on a first communication protocol; at least one server coupled into the landline network and communicating with the landline network; an airnet running on a second communication protocol; a client remotely located with respect to the server and communicating with the airnet by radio transmission means; a link server, coupling the airnet to the landline network, for linking the first communication protocol to the second communication protocol, whereby the client can communicate with the server; means, in the client, for generating a session-request signal comprising at least one client message encrypted according to a shared secret encrypt key; the session-request signal being transmitted to the airnet; means, in the server, for sending a session-reply signal comprising at least one server message encrypted according to the shared secret encrypt key; the session-reply signal sending means comprising: means for conducting a first client authentication when the session-request signal is received, the first client authentication comprising means for decrypting the encrypted client message from the received session-request signal; and means for generating a first derivative from the client message; means for conducting server authentication upon receiving the session-reply signal, the conducting server authentication means comprising: means for recovering the encrypted server message when the session-reply signal is received; and means for verifying the received first derivative with the client message; and means for generating a second derivative from the server message.

[0032] Preferably, the system further comprises: means, in the client, for generating a session-complete signal comprising the second derivative; means, in the server, for conducting a second client authentication, the second client authentication means comprising means for verifying the received second derivative with the server message when the session-complete signal is received; and whereby the authenticated and secure communication session between the client and the server is established when the first and second client authentication and the server authentication are complete.

[0033] In preferred embodiments the system further comprises: means, in the client, for initiating a transaction request signal comprising a transaction ID; and means, in the server, for verifying the transaction ID after the transaction request signal is received.

[0034] Conveniently, the system further comprises means, in the server, for sending a reply signal to the client and means, in the client, for acknowledging the reply signal to commit a transaction requested in the transaction request signal.

[0035] According to a further aspect of the present invention there is provided, a method for establishing an authenticated and secure communication session for transactions between a client and a server in a wireless data network, the client remotely located with respect to the server, the method comprising the steps of: (a) the client sending a session-request signal to the server for creating the session therebetween, the session-request signal comprising a client session ID, a client cipher, a C-nonce and a C-nonceModified, at least the C-nonce and the C-nonceModified being encrypted by the client cipher according to a shared secret encrypt key with the server; (b) the server conducting a first client authentication by decrypting the encrypted C-nonce and C-nonceModified according to the shared secret

encrypt key upon receiving the session-request signal; (c) the server generating a server session ID and a session key for the session in creation, deriving a first derivative from the decrypted C-nonce and generating a S-nonce upon examining the client session ID; (d) the server negotiating a mutually accepted cipher with the client for the session in creation, the negotiating step comprising the steps of examining the client cipher, looking up a server cipher and determining the mutually accepted cipher therefor; (e) the server sending a session-reply signal comprising the session key, the first derivative and the S-nonce; the session key, the first derivative and the S-nonce being encrypted therein according to the shared secret encrypt key; (f) the client conducting a first server authentication by decrypting the session key, the first derivative and the S-nonce according to the shared secret encrypt key; (g) the client conducting a second server authentication by validating the first derivative with the C-nonce generated originally in the client; (h) the client generating a second derivative from the S-nonce if the step (g) of the step two server authentication succeeds; (i) the server decrypting the second derivative upon receiving the second derivative that is encrypted at the client according to the shared secret encrypt key; and (j) the server conducting a second client authentication by decrypting the second derivative and verifying the decrypted second derivative with the S-nonce upon receiving the second derivative from the client; thereby the authenticated and secure communication session for transactions between the client and the server is established.

[0036] Preferably, the method further comprises the steps of: the client initiating a transaction request comprising a transaction identified by a transaction ID and encrypted by the mutually accepted cipher according to the session key; the transaction request comprising a URL identifying a service server in the wireless data network; the server verifying the transaction ID, performing a MAC verification and replying to the client with a service reply comprising a result of contacting the service server if the transaction ID is in trans-sequence; and the client committing to the transaction request by sending an acknowledge signal to the server, thereby the transaction is complete in the authenticated and secure communication session.

[0037] In preferred embodiments, the method further comprises the steps of: the server initiating a notification request comprising at least one message notification; the notification request being encrypted by the mutually accepted cipher according to the session key; the client replying to the server with a get-notify signal comprising a transaction ID to fetch the notification; the server examining the transaction ID to see if the transaction ID is in a trans-sequence; the server replying to the client with a reply signal if the step of the server examining the transaction ID is successful; and the client sending an acknowledge signal to commit an transaction specified in the transaction signal initiated by the server.

[0038] According to a further aspect of the present invention there is provided a system for establishing an authenticated and secure communication session, the system comprising: a landline network running on a first communication protocol; at least one server coupled into the landline network and communicating with the landline network; an airnet running on a second communication protocol; a client remotely located with respect to the server and communicating with the airnet by radio transmission means; a link server, coupling the airnet to the landline network, for linking the first communication protocol to the second communication protocol, whereby the client can communicate with the server; means, in the client, for generating a session-request signal comprising a client session ID, a client cipher, a C-nonce and a C-nonceModified, at least the C-nonce and the C-nonceModified being encrypted by the client cipher according to a shared secret encrypt key with the server; the session-request signal being transmitted to the airnet; means, in the server, for sending a session-reply signal to the landline network, the session-reply signal comprising a server session ID, a server cipher, a S-nonce and a first derivative; at least the server cipher, the S-nonce and the first derivative being encrypted by the server cipher according to the shared secret encrypt key; the session-reply signal sending means comprising: means for conducting a step one client authentication when the session-request signal is received, the first client authentication comprising means for decrypting the encrypted the C-nonce and the C-nonce-Modified from the received session-request signal; and means for generating the first derivative from the C-nonce; means, in the client, for conducting server authentication upon receiving the session-reply signal, the conducting server authentication means comprising: means for decrypting the encrypted server session ID, server cipher, S-nonce and first derivative when the session-reply signal is received; means for verifying the decrypted first derivative with the C-nonce therein; and means for generating a second derivative from the S-nonce; means, in the client, for generating a session-complete signal comprising the second derivative; means, in the server, for conducting a second client authentication, the second client authentication means comprising means for verifying the received second derivative with the S-nonce when the session-complete signal is received; and whereby the authenticated and secure communication session between the client and the server is established when the first and second client authentication and the server authentication are complete.

[0039] Preferably, the system further comprises: means, in the client, for initiating a transaction signal comprising a transaction identified by a transaction ID; and means, in the server, for verifying the transaction ID after the transaction signal is received.

[0040] In preferred embodiments, the system as recited in claim 29, further comprises: means, in the server, for replying to the client with a reply signal if the step of the server examining the transaction ID is successful; and means,

in the client, for sending an acknowledge signal to commit the transaction specified in the transaction signal initiated by the server.

[0041] Accordingly, an important object of the present invention is to provide a generic solution for secure lightweight transaction in wireless data networks. Other objects, together with the forgoing are attained in the exercise of the invention in the following description and resulting in the embodiment illustrated in the accompanying drawings.

[0042] These and other features, aspects, and advantages of the present invention will become better understood with regard to the following description, appended claims, and accompanying drawings where:

Figure 1 shows a schematic representation of a mobile data network in which the present invention may be practiced;

Figure 2 depicts a block diagram of a typical GSM digital cellular phone used in the embodiment of the disclosed invention;

Figure 3 illustrates the process of mutual authentication between a client and a sever;

Figure 4.a and Figure 4.b depict a data flowchart representing the session creation process in the client and the server, respectively, of Figure 3 in one embodiment of the present invention;

Figure 5 shows a schematic diagram of a service transaction;

Figure 6 shows a schematic diagram of a notification transaction; and

Figure 7 shows a schematic diagram of a post transaction.

[0043] The detailed description of the present invention in the following are presented largely in data flowing representation that resemble the operations of data processing devices coupled to networks. These process descriptions and representations are the means used by those experienced or skilled in the art to most effectively convey the substance of their work to others skilled in the art. The present invention is a method and system for secure data communications. The method along with the system or architecture to be described in detail below is a self-consistent sequence of steps leading to a desired result. These steps or processes are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities may take the form of electrical signals capable of being stored, transferred, combined, compared, displayed and otherwise manipulated. It proves convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, operations, messages, terms, numbers, or the like. It should be borne in mind that all of these similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities.

[0044] Referring now to the drawings, in which like numerals refer to like parts throughout the several views. Figure 1 shows a schematic representation of a wireless data network 100 in which the present invention may be practiced. The data network 100 comprises an airmet 102 and the landline network 104, each acting as a communication medium for data transmission therethrough. The landline network 104 may be the Internet, the Intranet or other private networks. For simplicity, the landline network 104 will be herein simply referred to as the Internet, literally meaning either the Internet or the Intranet or other private network. Further the airmet 102, meaning unwired network in which data transmission is via the air, is sometimes referred to as a carrier network because each airmet is controlled and operated by a carrier, for example AT&T and GTE, each having its own communication scheme, such as CDPD, CDMA, GSM and TDMA. Referenced by 106 is a mobile data device, but resembling a mobile phone, in communication with the airmet 102 via an antenna 108. It is generally understood that the airmet 102 communicates simultaneously with a plurality of mobile computing devices of which a mobile phone 106 is shown in the figure. Similarly connected to the Internet 104 are a plurality of desktop PCs 110 and a plurality of web servers 112, though only one representative respectively shown in the figure. The PC 110, as shown in the figure, may be a personal computer SPL 300 from NEC Technologies Inc. and runs a web browser via the Internet 104 to access information stored in the web server 112 that may be a workstation from SUN Microsystems Inc. It is understood to those skilled in the art that the PC 110 can store accessible information so as to become a web server as well. Between the Internet 104 and the airmet 102 there is a link server 114 performing data communication between the Internet 104 and the airmet 102. The link server 114, also referred to as link proxy or gateway, may be a workstation or a personal computer and performs a protocol mapping from one communication protocol to another, thereby a mobile device 106 can be in communication with any one of the web servers 112 or the PCs 110, respectively.

[0045] The communication protocol in the Internet 104 is HTTP that runs on TCP and controls the connection of an HTML Web browser to a Web server and the exchange of information therebetween. An extended version thereof, called HTTPS, provides encrypted authentication and session transmission between a client and a server. The communication protocol between the mobile device 106 and the link server 114 via the airmet 102 is Handheld Device Transport Protocol (HDTP), or Secure Uplink Gateway Protocol (SUGP), which preferably runs on User Datagram Protocol (UDP) and controls the connection of a HDML Web browser to a link server, where HDML stands for HandHeld Markup Language. The specification thereof and the HDTP specification are provided at <http://www.w3.org> or <http://www.uplanet.com> that are incorporated herein by reference. Further a reference specification entitled "Magellan SUGP

Protocol" is incorporated herein by reference. The HDTP is a session-level protocol that resembles the HTTP but without incurring the overhead thereof and is highly optimized for use in mobile devices that have significantly less computing power and memory. Further it is understood to those skilled in the art that the UDP does not require a connection to be established between a client and a server before information can be exchanged, which eliminates the need of exchanging a large number of packets during a session creation. Exchanging a very small number of packets during a transaction is one of the desirous features for a mobile device with very limited computing power and memory to effectively interact with a landline device.

[0046] According to one preferred embodiment, the present invention may be practiced with a cellular phone, a typical example of the mobile device 106, that has very limited computing power and memory. The cellular phone 106 is used as a client in communication to a landline device that is often referred to as a server providing accessible information therein to other devices. Figure 2 shows a block diagram of a typical GSM digital cellular phone 120. Each of the hardware components in the cellular phone 120 is known to those skilled in the art and so the hardware components are not to be described in detail herein. Although the user interface of the phone 120 is not shown in the figure, the mobile device 118, resembling a cellular phone, in Figure 1 may be referenced thereto, in which referenced by 116 is a LCD screen and 118 is a key button pad, respectively. Through the screen 116 and the keypad 118 controlled by a user of the phone, the phone can be interactively communicated with a server through the ainet, link server and the Internet. According to one embodiment of the present invention, compiled and linked processes of the present invention are stored in ROM 122 as a client module 124 and support module 126. Upon activation of a predetermined key sequence utilizing the keypad 118, a physical layer processor or microcontroller 118, initiates a session communication to the server using the module 124 in the ROM 122.

[0047] To establish a secured communication between a client and a server, an authentication process must be conducted first to ensure that only interested parties are actually in the communication therebetween. The process is complete through two rounds of independent authentication, one being the client authenticated by the server, referred to as client authentication, and the other being the server authenticated by the client, referred to as server authentication. Further each authentication is completed in two separate steps for high grade of security, which will be described in detail below. The success of the mutual authentication processes provision an evidence that the two communicating parties possesses a valid shared secret encrypt key through a mutual decryption and a challenge/response mechanism. The mutual decryption mechanism comprises the steps of mutually recovering encrypted messages from two involved communicating parties. The challenge/response mechanism, referred to as nonce verification, verifies a predetermined relationship between a sent nonce and a received derivative thereof.

[0048] In one preferred embodiment of the present invention, the authentication process is conducted with three message exchanges; a Session Request (SR), a Session rePly (SP), and a Session Completion (SC). Figure 3 illustrates a schematic representation of the authentication process. The client 140, representing a mobile device, to conduct a transaction with the server 142, representing a landline server or PC, initiates a SR 144 to be sent to the server 142 by first creating a client proto-session. A client proto-session is a session data structure that gets initialized when a session creation starts. The initialized SR 144 comprises the following information:

sessionID - an identifier identifying all requests from the client to the server; In the case of requesting a session creation, sessionID is always assigned to 0;

cipher - a two-byte number representing the choice of the encryption the client is currently using as there are a number of encryption schemes available in a communication protocol;

version - a one byte number representing the HDTP protocol version in use, used to determine the underlying format of the communication protocol such as PDU;

type - either a fixed five-byte number representing what device the client is. e.g. 2PCSI means the client is a PCSI phone version 2.

deviceID - a variable up to 255-byte, representing the device identifier or the client identifier comprising, a phone number of the devcie or an IP address and a port number, e.g. 204,163,165,132,01905 ;

header — up to 32767 bytes, comprising token/value pairs that apply to an entire session and may be automatically applied to subsequent service requests or session specific parameters, therefor the header is generally cached in the server till the current session completes; and

C-nonce — a client nonce represented with a non-repeatable number, usually 2 bytes, used for the client to conduct a following server authentication.

EP 0 915 590 A2

C-nonceModified — a modified version of the client nonce, used for the server to conduct a nonce verification in the following client authentication.

5 [0049] Further the cipher in the SR 144 includes an identifier to an encryption algorithm and associated parameters thereof. To be more specific, the first byte in the cipher represents an identifier to a combination of the encryption algorithm, the key size (e.g. 128-bit for US or 40-bit for foreign countries) and content of a security attachment thereto and the second byte in the cipher indicates the additional parameters related to the first byte. For example, value 1 in the first byte indicates that the encryption algorithm is block cipher RC5, the key size thereof is 128 bit, a two byte check-sum therein is used as the MAC (Message Authentication Code), no IV (Initialization Vector for block ciphers) therefor is transmitted over the network, and padding bytes are added if necessary. The block cipher algorithm RC5 is part of the RSA's BSAFE product. It can be further appreciated that the identifier in the cipher may be assigned to a unique value to identify a non-secure session if so desired. The C-nonce is a non-repeatable number initially and randomly generated in the client and the modified version thereof, C-nonceModified, is generated from the C-nonce through a operational relationship; for example the Exclusive-OR relationship or expressed as follows:

15

$$\text{C-nonceModified} = \text{2-byte-number} \oplus \text{C-nonce.}$$

20 It can be appreciated by those who are skilled in the art that there are many ways to get the C-nonceModified from a C-nonce, the Exclusive-OR is one of the operational relationships used in one embodiment of the present invention. Both C-nonce and C-nonceModified are encrypted using the shared secret encrypt key between the client 140 and the server 142. The purpose of the C-nonceModified is to provide the server that receives the SR with means for ensuring that C-nonce is correctly decrypted and validated by examining the C-nonce and its relationship with the C-nonceModified. Both should not be altered after a successful decryption of the C-nonce and the C-nonceModified. In other words, a SR message or signal may be expressed as follows:

25

$$\text{SR} = \{\text{session ID, cipher, version, type, device ID, header, Encry}[\text{nonce, nonceModified}]\};$$

30 where Encry[] means that the parameters or contents in the bracket are encrypted accordingly. When the SR is sent by the client to the server to request a session creation, both C-nonce, C-nonceModified are encrypted according to the cipher the client is using at the time the SR is sent out.

[0050] Upon receiving the SR from the client 140, the server 142 creates a server proto session for the client 140 with a session identifier, referred to as session ID, to identify the session context for the session just created in the server 142. A server proto-session is a session entry marked as a proto status in a session table, which indicates that the session is not authenticated and is not able to conduct any transactions with the client. It is understood to those skilled in the art that the proto-session can be kept in the RAM of the server. If a proto-session already exists for that client, it is re-used. The information in the received SR is saved in the server proto-session. If the server 142 is satisfied with the fact that the client is known, namely Encry[C-nonce, C-nonceModified] in the received SR are successfully decrypted with the shared secret encrypt key, the step one in the client authentication is successful and a corresponding session key is generated and stored with the server proto session entry. It may be noted herein that many encryption schemes used in this invention, such as RC5, have a procedure that adds and validates the Message Authentication Code such as the check-sum, to assure that the encrypted message is correctly decrypted, the procedure, every time the decryption takes place, is used herein to examine the transaction integrity, namely to assure the received messages or signals are unaltered in the cause of data transmission. If the step one client authentication is not successful, namely Encry[C-nonce, C-nonceModified] in the received SR are not fully decrypted or supported, the proto session is aborted and removed from the proto session table, resulting in a failed session creation. What the support means herein is the cipher proposed or used by the client is also used by the server, for example the client uses the RC5 encryption to encrypt Encry[C-nonce, C-nonceModified], to decrypt Encry[C-nonce, C-nonceModified], the server must be equipped with the same RC5 encryption capability therein. If Encry[C-nonce, C-nonceModified] can not be successfully decrypted due to other reasons such as transmission errors, the client must reinitiate a new session request to the server in order to establish a secure communication with the server. To challenge a step two server authentication subsequently at the client side, a derivative of the client nonce or C-nonce, is generated therefor. In one embodiment of the present invention, the derivative is created by adding a constant to the client nonce, for example derivative = C-nonce + 1. The purpose of the derivative is to provide the client with means for reassuring that the C-nonce is correctly decrypted by the server and the server is the authenticated one in communication with.

55

[0051] Right after the successful step one client authentication, the server 142 responds to the client with a Session rePly (SP) 146 to begin a second round authentication; server authentication. The SP 146 comprises the following

EP 0 915 590 A2

information: C-SID - a one byte number indicates the sessionID originally assigned in the client, to be more specific C-SID = 0 indicates a clear text client session, C-SID = 1 indicates a shared secret key encrypted session, and C-SID = 2 indicates a session key encrypted session. In the context of the current description, C-SID = 1.

5 sessionID - a four-byte number representing an identification and parameters, such as a session encrypt key, of the session created by the server for the client;

key — a session key to be used with a mutually acceptable encryption, and to be used for encryption and decryption in all transactions in the session;

10 derivative - a number derived from the C-nonce for the client to perform the subsequent server authentication;

S-nonce - a non-repeatable number, used for the server to conduct a following step-two client authentication; it should be noted that S-nonce is generated by the server and generally different from the C-nonce by the client; and

15 cipher - a two-byte number representing the choice of the encryption the server proposes after the client proposed cipher is received, it may or may not be the same as the one used in the client, to be more specific, the cipher is the same as the one proposed by the client when the server supports the client proposed cipher, otherwise the cipher is the one currently used in the server.

20 [0052] In other words, the SP can be expressed as follows:

$$SP = \{C-SID, Encry[sessionID, key, S-nonce, derivative, cipher]\};$$

25 When the client 140 receives the SP 146 from the server 142, it performs the step one server authentication, which is considered successful if Encry[sessionID, key, S-nonce, derivative, cipher] in the received SP 146 is decrypted successfully with the shared encrypt key. If the step one server authentication fails, the client 140 discards the SP 146 and a new session creation may be started over again. Upon the success of the step one server authentication, the client 140 proceeds with the step two server authentication; namely the predetermined relationship between the C-nonce and the derivative thereof should hold for a successful step-two server authentication:

$$C-nonce = derivative - 1$$

35 [0053] If the C-nonce derived from the SP 146 is the same as the C-nonce originally generated by the client, the step two server authentication is successful, hence the server 142 is considered authenticated, trusted from the viewpoint of the client, and the SP 146 is accepted as a valid message, which means that the client 140 then uses the session key and other information in the SP 146 for the session being created. Only with both successful steps of the server authentication, the client 140 marks the session as committed, which means that transactions can be conducted subsequently in the session, again only from the viewpoint of the client 140. If the predetermined relationship between the client nonce and the derivative thereof does not hold, the step two server authentication fails and the received SP 146 is discarded. The client 140 may abort the session creation process if no further SP's are received and pass both steps of the server authentication during the time period allowed for a session creation. To provide the server with means for reassuring the client authentication by itself through the client, a derivative of the S-nonce, similar to the derivative of the C-nonce, is generated.

40 [0054] The client 140 then sends the server 142 a SC 148 to complete the session creation process. The SC 148 comprises the following information:

50 $SC = \{Encry[derivative]\};$

where the derivative is the client's response to the server nonce challenge, namely the result of the verification, the derivative is used by the server 142 for step two client authentication. Further it is noted that the SC 148 is an encrypted message, meaning that the client encrypts the information in the SC 148 according to either its own cipher or the server proposed cipher. Generally the client 140 encrypts the information in the SC 148 according to the server proposed cipher if it accepts the server proposed cipher, otherwise, it encrypts the SC according to its own cipher.

55 [0055] It must be noted in one embodiment of the present invention that the SC unlike the SR 144 and SP 146, is

piggybacked by a following transaction request to increase data transmission efficient. The data piggybacking means that independent data units may be logically grouped together in one physical data unit to be transmitted to a receiver that recovers all the independent data units upon the receipt of the physical data unit as if all the independent data units were sent, independently and respectively, in separate physical data units.

5 [0056] Upon receiving of Session Complete or SC 148, the server 142 tests if the client 140 uses its own proposed cipher or the server proposed cipher by decrypting the SC twice using the two ciphers if necessary. If the server 142 decrypts the encrypted message in the SC 148 and verifies the relationship thereof with the S-nonce, the step two client authentication is succeeded. Subsequently the server 142 promotes the server proto session to the active session and the session creation process is completed; otherwise, the proto session is removed and the session creation is aborted.

10 [0057] Referring now to Figure 4.a and Figure 4.b, there are shown two data flowcharts 180 and 181 representing a session creation process in the client and the server, respectively, in one embodiment of the present invention. There are generally three types of transactions that are conducted between a mobile device and a landline server; service transaction, notification transaction, and post transaction. Both service and post transactions are initiated by the mobile device that is considered as a client herein and the notification transaction is initiated by the landline server that is considered a server herein. All transactions must be conducted in the context of a valid and established session. If there is no session or valid session, a session must be created before any transaction can start. For the sake of simplicity, it is assumed that the transaction is initiated at the client side at 182. As described above, for a transaction to take place in a secure communication, a session between a client and a server must be established first. Therefore

15 at 184, the existence of a valid session is examined. If a valid session is in place, the transaction can proceed at 186. If there is no established session, for example, a mobile device is just powered on for the first time or a previous session is beyond a time limit, for example 8 hours, a session request must be initiated and sent to the server at 188. The client is then in a mode of waiting for a reply from the server, constantly looking up for the reply at 190 and 192. If there is no reply from the server, the client may initiate another session request if a fixed time period lapses at 194 or errors occur to have to abort the initiated session request at 196 and 198. The errors occur when the client is out of a service area covered by an airnet that communicates with the server or simply either the client or the server malfunctions at 199.

20 [0058] Meanwhile the session request is received by the server at 216. A proto session is created at 222 per the session request from the client if the session request is not a duplicated one. It is very common that a session request may be retransmitted or re-requested by the client due to some unexpected error conditions in the wireless data network so that duplicated requests may be received. The server, however, uses a tag, which is generated from the encrypted message in the session request first received and is unique for each session request from a particular client, to prevent creating multiple proto sessions from the duplicated session requests. Some of the information in the session request, such as protocol version and device ID are verified at 224. If the verified information is not supported, there might be device error at 226, which results in the removal of the proto session just created. If the verifying process at 224 succeeds, the server proceeds a decryption process, according to a shared secret encrypt key as described above, to decrypt the C-nonce and C-nonceModified at 230. If the operational relationship between the C-nonce and C-nonceModified holds at the server side, the step one client authentication completes. CIP at 203 in Figure 4.a and 234 and 236 of figure 4.b stands for crypto ignition process which is a process to equip a client with a updated encrypt information, for example, to update the share secret key. As the CIP is an added process and not a key element in the present invention, and no detail description thereof is provided therefore. With the successful step one client authentication, the server at 238 sends a session reply to the client.

25 [0059] When a server is reached and successfully processes the session request from the client, namely the step one client authentication as described above, a session reply is sent by the server to the client to start server authentication at the client side. Upon receiving the session reply from the server being connected, the client examines the reply signal at 200 and 201 and the session reply should be in a recognized format, such as uncorrupted essential information therein. If the received session reply is not recognized or supported, the client discards the received session reply at 202 and continues to wait for a valid session reply, otherwise problems with devices may be claimed in step 199. Upon receiving the session reply from the server, the client proceeds two steps of the server authentication at 204, which has been described above in detail. Logically the session is discarded at 202 if the server authentication fails, namely the client fails to decrypt and verify the encrypted S-nonce and to validate the derivative of the C-nonce generated by the server. When the server authentication passes, the client chooses either its own cipher or the server proposed cipher obtained from the session reply from the server at 208 and 210 and further the client retrieves the session key therefrom and sends a session complete signal to the server to complete the session creation at 212 and 214.

30 [0060] Meanwhile the server expects a session complete signal from the client it just sends the session reply to at 238. For security purpose, the server drops the proto session at 242 if the time waiting for the session complete signal goes beyond a threshold 240. Upon receiving the session complete signal at 244, the server proceeds the step two client authentication at 246 and 248 by decrypting the encrypted derivative of the S-nonce and verifying the relationship

thereof with the original S-nonce. If the decryption of the derivation or the verification with the S-nonce fails, the session creation fails, hence the removal of the proto session. If the step two client authentication succeeds, that means the step one client authentication and the step one and two server authentication have all completed. the session is successfully created by promoting the proto session to the regular session at 250, thereby the transaction originally initiated by the client at 182 of Figure 4.a can proceed therefrom.

[0061] To perform transactions in an authentic and secure session, each transaction must be assigned to a transaction ID. In one embodiment of the invention, a new transaction must have a new transaction ID and has to be in a trans-sequence, namely the transaction ID must be greater than any other completed and pending transaction IDs and less than 255 at the time the new transaction is started in the session, for example, transaction ID = 12 for a current transaction, the next transaction ID from the client must be 13 or greater in order for the transaction to be accepted by the server. The constant 255 is the maximum number of transactions that can be performed in a valid session. If a transaction ID is smaller than what the session expects, the transaction is discarded without notice. If the transaction ID is greater than 255, a new session is automatically created to accommodate the corresponding transaction. All the data units related to transactions are encrypted with the session key created in the session creation process and the cipher used therein is either the client proposed cipher or the server proposed cipher.

[0062] Referring to Figure 5, there is shown a schematic diagram of a service transaction. The mobile client 140 initiates a Service Request (tSR) 152 to the server 142. A service transaction is typically involved in interaction with a service provider identified by a universal Resource Locator URL in a landline server, therefore the information in a tSR comprising URL and optional header that provides additional session information. Upon receiving the tSR 152, the server 142 processes the received tSR 152 to examine the sessionID and transaction ID therein. If the transaction ID is less than what it expects, the tSR 152 is discarded. In addition, the tSR 152 is discarded if the transaction ID in the received tSR 152 is greater than 255. As described above, for security reason, a maximum of 256 transactions is allowed in a session. If more than the allowed number of transaction occurs in one established session, a new session will be automatically initiated with the transaction ID being started from 0. Upon the successful examination of the service request tSR 152, the server 142 responds with a Service Reply (tSP) 154 that comprises a result in the form of digest of the URL service request and an optional header. Upon receiving the tSP 154 from the server 142, the client 140 sends the server 142 an acknowledge (ACK) 156 to commit the transaction if the result in the received tSP 154 is positive. Alternatively, the hand-held client can send the server a Cancel to abort the transaction. A typical example is that the client 140 requests to access information stored and identified by the URL as www.abc.com supported at the server 142, however, the URL in the tSR 152 is entered as www.abcd.com, the result in the tSP 154 returns a error message indicating the desired URL could not be found, otherwise the result in the tSP 154 shows the desired URL has been found, now it is up to the user of the client to determine if the client shall proceed with the tSP 156 or cancel to abort the current transaction to try a new or different URL.

[0063] Referring now to Figure 6, there is shown a schematic diagram of a notification transaction. A notification transaction can be initiated by either the client 140 or the server 142. In the case of server initiation, the server 142 initiates the notification transaction by sending to the client 140 a signal data unit, or notification request (NR) 162, to inform the client 140 that there is a notification in pending in the server 142, such as an electronic mail, waiting for immediate attentions from the identified client. Upon receiving of the NS 162, the client 140 sends a Get-Notify (GN) 164 to the server 142 and retrieves its notification contents such as alerts and emails. The server 142, as in the service transaction, replies with a tSR 146. The transaction is committed after an acknowledge signal (AS) 156 is sent to the server 142 and the server 142 receives it. In the case of the client notification, the client 140 initiates the notification transaction when it powers on or switches back to the data mode from voice mode by asking the server 142 if there is any notification in pending. If there is notification in pending, the client 140 handles the notification transaction as if a signal is received. The AS 156 may be piggybacked with a GN when multiple notification transactions are conducted sequentially. If there are multiple notifications are pending at the server 142, the optional header in the tSR 146 indicates that so that the client will automatically start another notification transaction.

[0064] Referring now to Figure 7, there is shown the post transaction. Post transaction is initiated by the mobile client 140. The post transaction is used for a mobile device to update information stored in a WWW service as specified in the URL. The client 140 sends a Post Request (PR) 172, which contains a URL, data for updating, and an optional header. The server 142 processes the PR 172 and responds to the client with a tSR 146. The result in the tSR 146 comes from the WWW service and normally indicates if information update is done. Upon receiving of the tSR 146, the client 140 sends the server 142 an AS 156 to commit the transaction. Alternatively, the mobile client 140 can send the server 142 a Cancel to abort the transaction.

[0065] The present invention has been described in sufficient detail with one exemplary embodiment. Alternative embodiments will become apparent to those skilled in the art to which the present invention pertains without departing from its spirit and scope. For example, wireless communications between a server and a personal digital assistant such as Palm Pilot from 3 Corn Corporation and also a portable computer that runs under a operating system, for example, Window CE from Microsoft Corporation. Accordingly, the scope of the present invention is defined by the

appended claims rather than the forgoing description of one embodiment.

Claims

5

1. A method for establishing an authenticated and secure communication session for transactions between a client and a server in a wireless data network, said client remotely located with respect to said server, said method comprising:

10

sending a session-request signal from said client over said wireless data network to said server, said session-request signal comprising one client message encrypted according to a shared secret encrypt key; conducting a first server authentication by decrypting a server message sent from said server in response to said session-request signal; wherein said server message is generated by said server after said one client message is decrypted in said server according to said shared secret encrypt key and further said server message comprises a session key for said session and a first derivative from said decrypted client message; conducting a second server authentication by validating said first derivative with said client message; and generating a second derivative from said server message if said second server authentication succeeds; and sending to said server a session-complete signal comprising said second derivative, wherein said authenticated and secure communication session is established between said client and said server after a second client authentication in said server succeeds by validating said second derivative with said server message.

15

20

2. A method as recited in claim 1, wherein said session-request signal further comprises a client cipher indicating what encryption said client currently uses and a modified version of said client message, said modified version having an operational relationship with said client message and being encrypted according to said shared secret encrypt key.

25

3. A method as recited in claim 1 or 2, wherein said client message comprises a client nonce and a modified version thereof and wherein said first derivative has a first mathematical relationship with said client nonce.

30

4. A method as recited in any one of claims 1 to 3, wherein said server message comprises said session key, a server nonce, and said first derivative and wherein said second derivative has a second mathematical relationship with said server nonce.

35

5. A method as recited in any preceding claim, wherein said session-complete signal is piggybacked by a transaction request from said client, said transaction request comprising a URL identifying a service server coupled to said server.

40

6. A method as recited in claim 5, wherein said transaction request is encrypted according to said session key.

7. An apparatus for establishing an authenticated and secure communication with a server over a wireless data network, said server remotely located with respect to said apparatus, said apparatus comprising:

45

a display screen;
a memory for storing code for a client module;
a processor coupled to said memory, said processor executing said code in said memory to cause said client module to:
send a session-request signal over said wireless data network to said server, said session-request signal comprising one client message encrypted according to a shared secret encrypt key;
conduct a first server authentication by decrypting a server message sent from said server in response to said session-request signal; wherein said server message is generated by said server after said one client message is decrypted in said server according to said shared secret encrypt key and further said server message comprises a session key for said session and a first derivative from said decrypted client message;
conduct a second server authentication by validating said first derivative with said client message; and generating a second derivative from said server message if said second server authentication succeeds; and send to said server a session-complete signal comprising said second derivative, wherein said authenticated and secure communication session is established between said client and said server after a second client authentication in said server succeeds by validating said second derivative with said server message.

50

55

EP 0 915 590 A2

8. Apparatus as recited in claim 7, wherein said session-request signal further comprises a client cipher indicating what encryption said client currently uses and a modified version of said client message, said modified version having an operational relationship with said client message and being encrypted according to said shared secret encrypt key.

5

9. Apparatus as recited in claim 7 or 8, wherein said client message comprises a client nonce and a modified version thereof and wherein said first derivative has a first mathematical relationship with said client nonce.

10

10. Apparatus as recited in any one of claims 7, 8 or 9, wherein said server message comprises said session key, a server nonce, and said first derivative and wherein said second derivative has a second mathematical relationship with said server nonce.

15

11. Apparatus as recited in any one of claims 7 to 10, wherein said session-complete signal is piggybacked by a transaction request from said client, said transaction request comprising a URL identifying a service server coupled to said server.

20

25

30

35

40

45

50

55

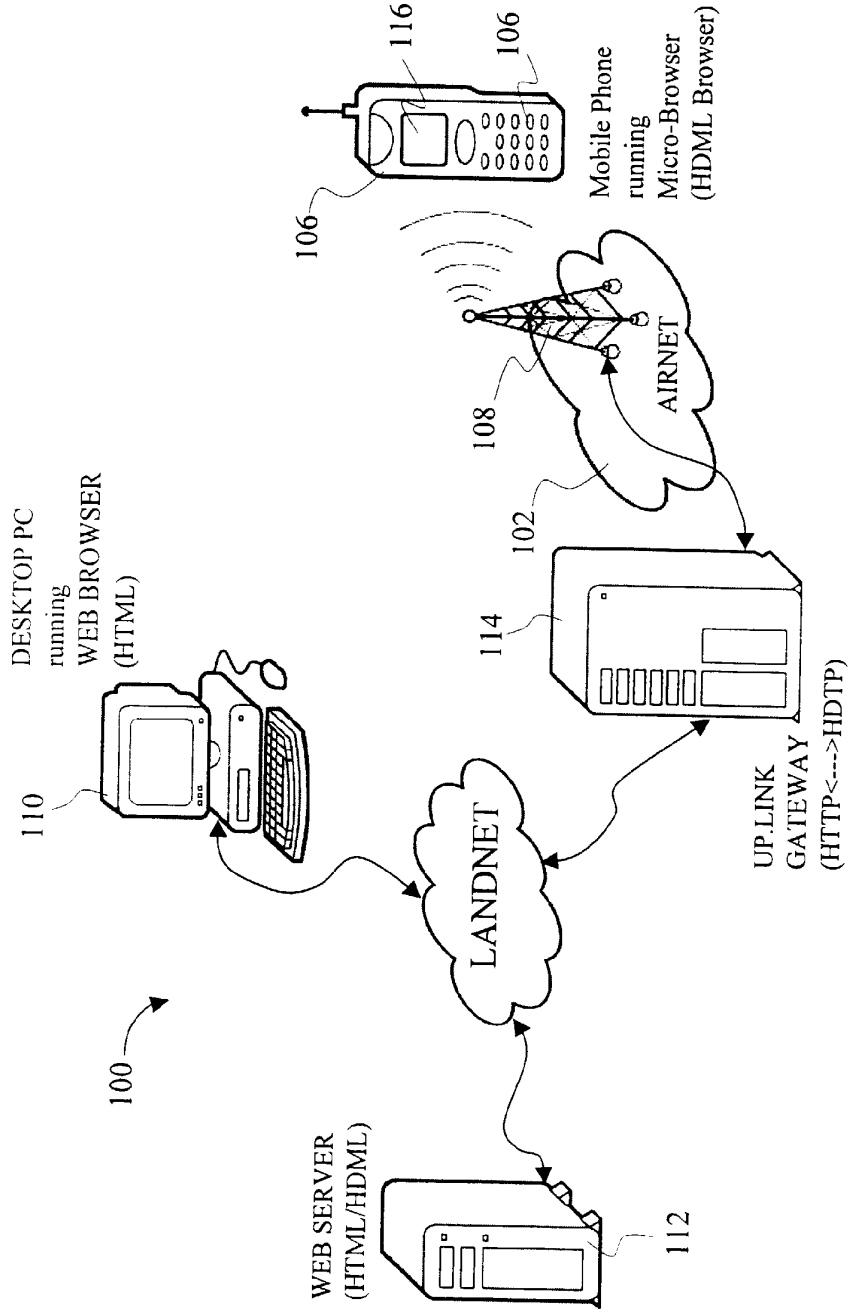


Fig. 1

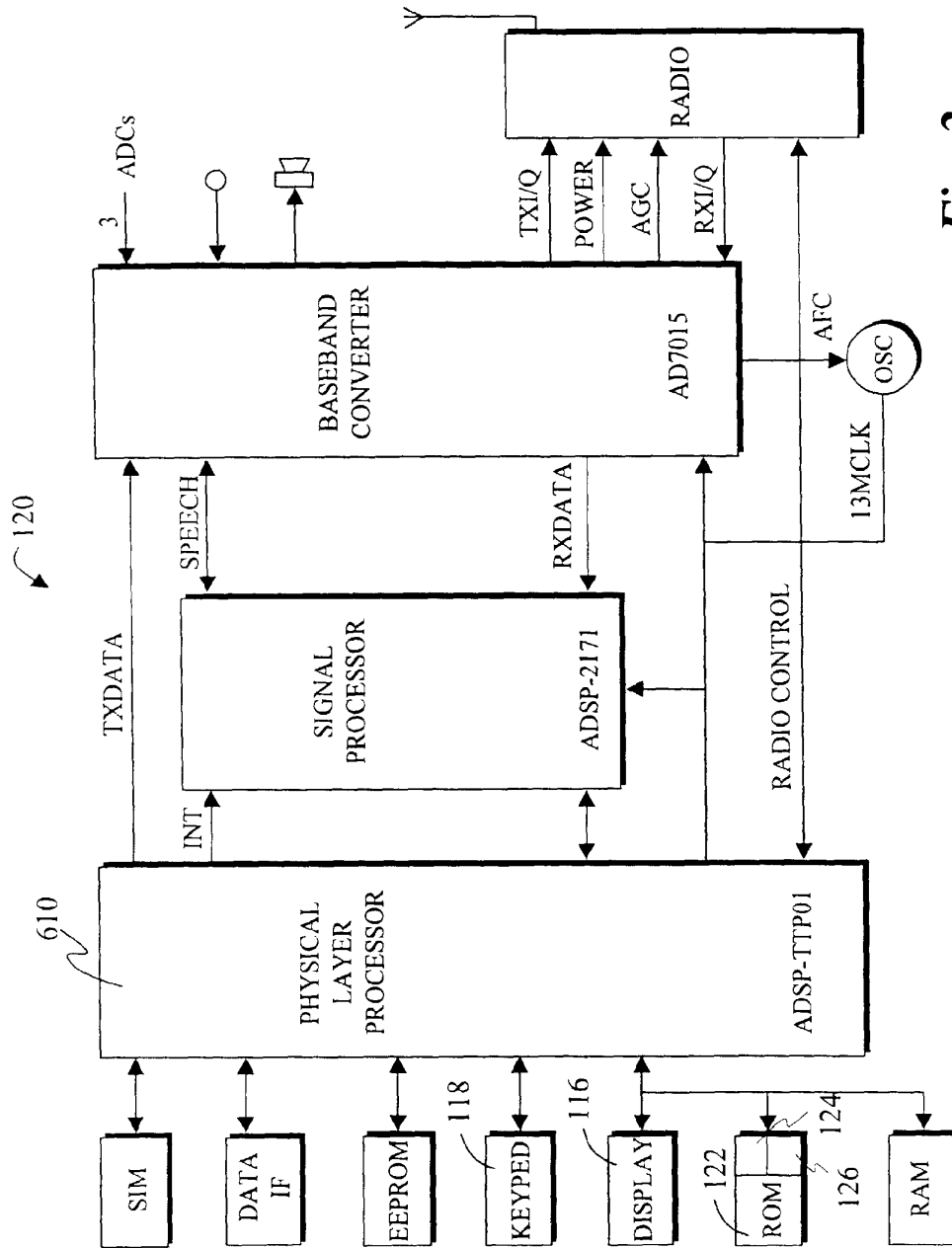


Fig. 2

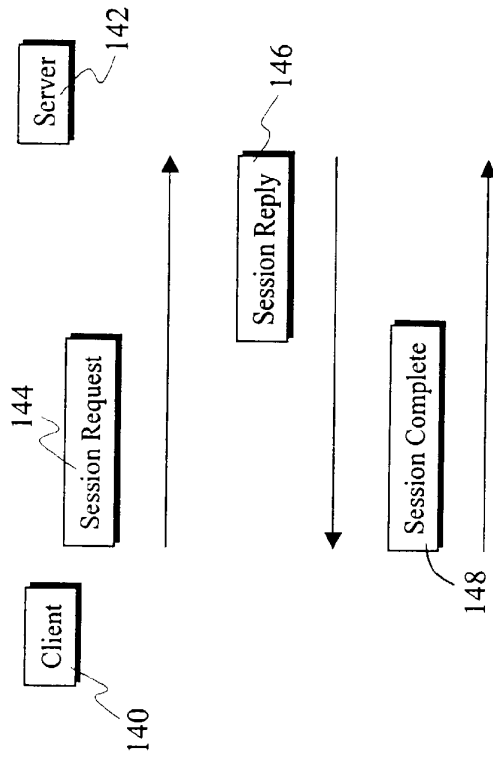
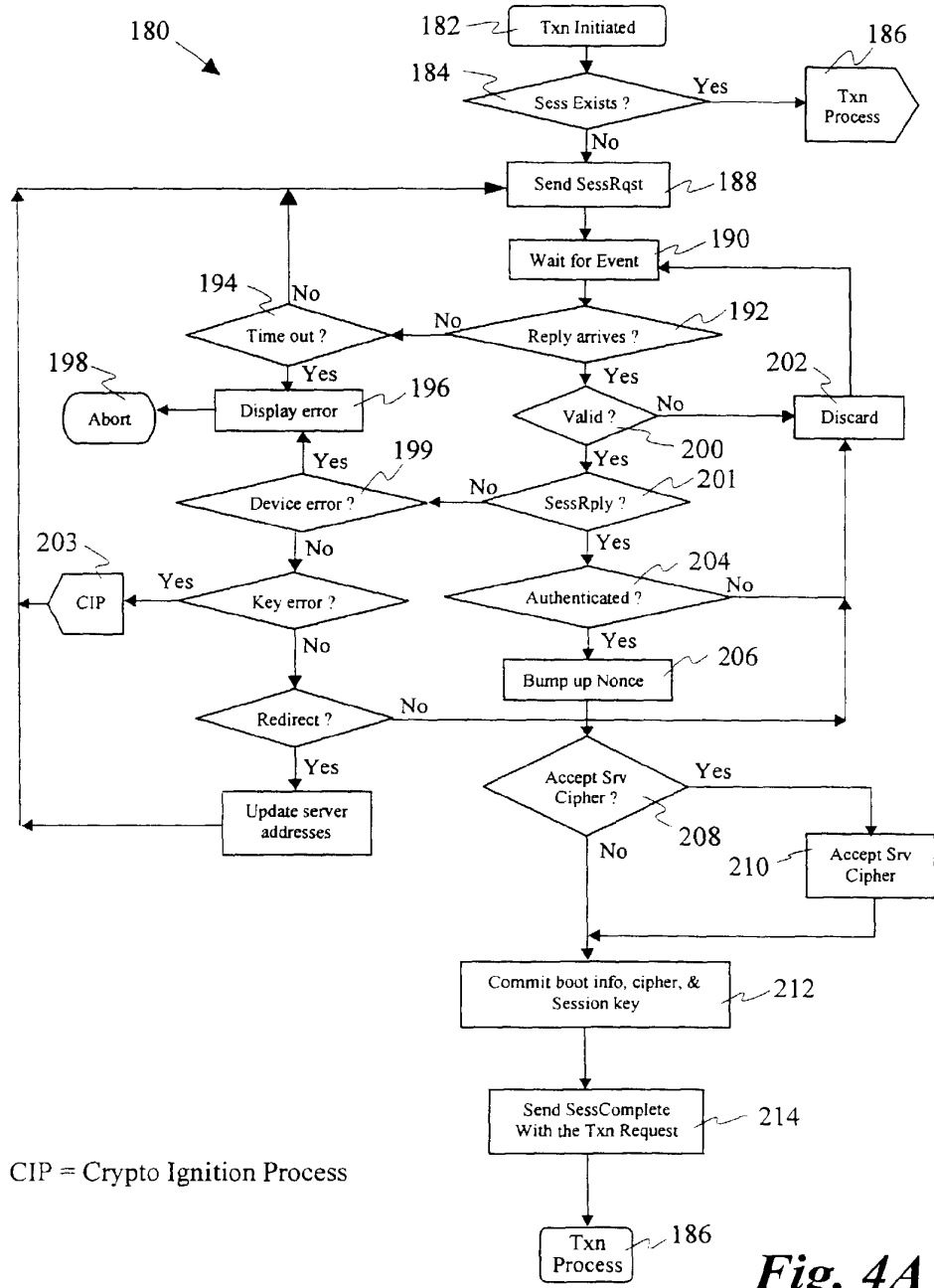
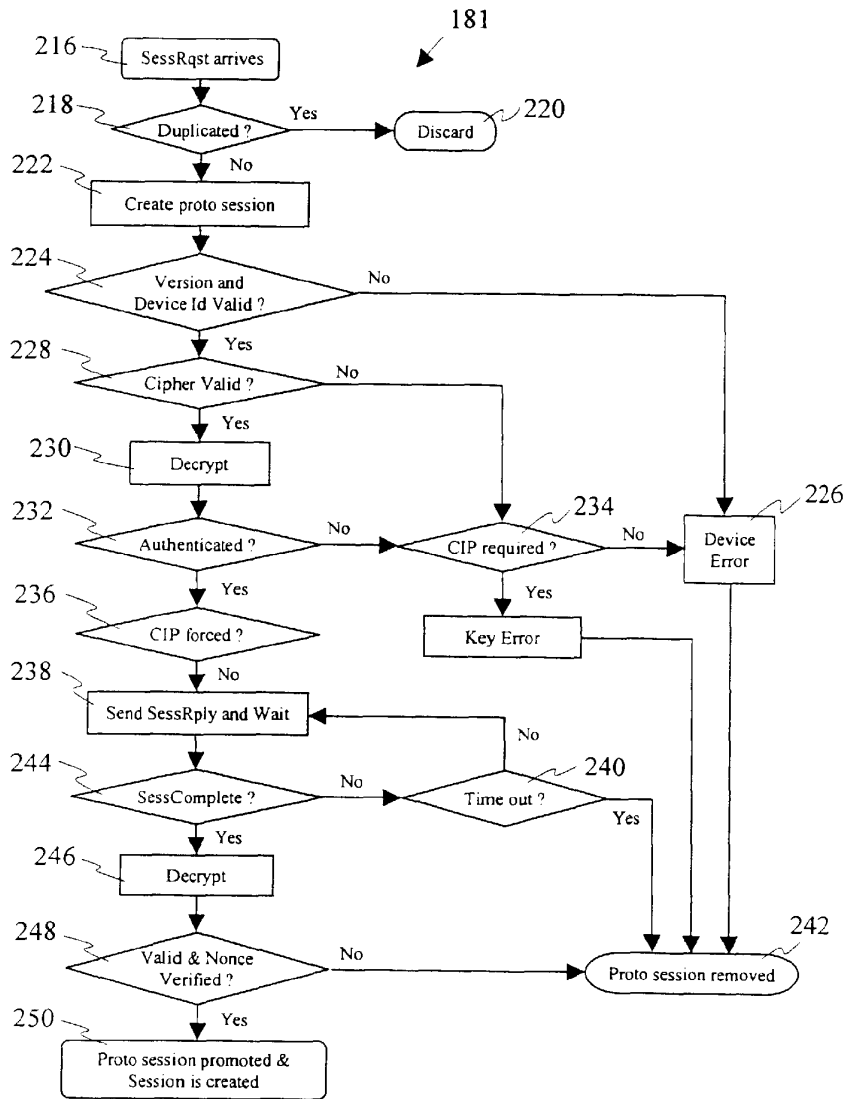


Fig. 3





CIP = Crypto Ignition Process

Fig. 4B

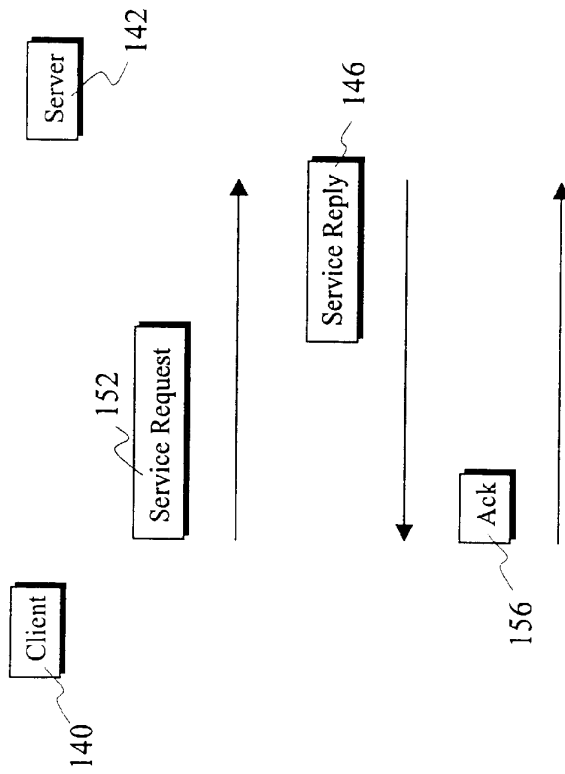


Fig. 5

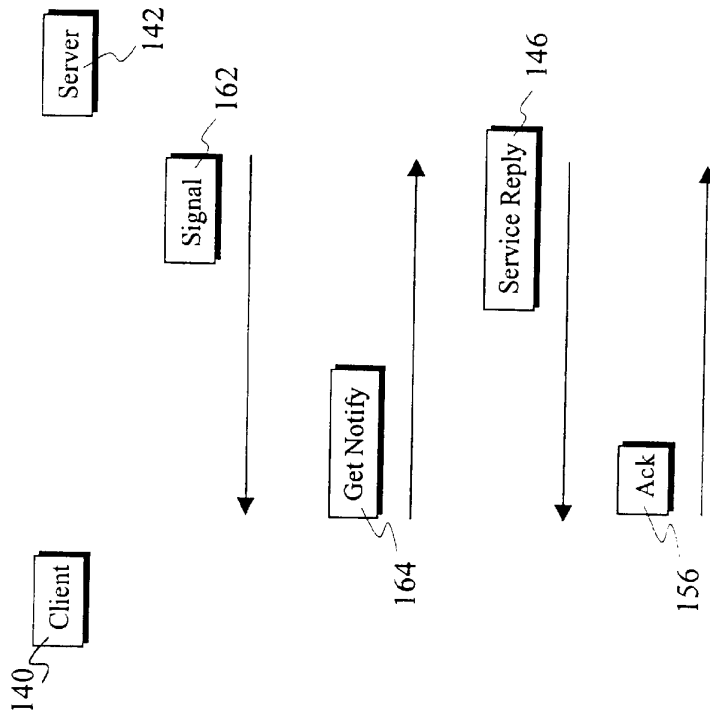


Fig. 6

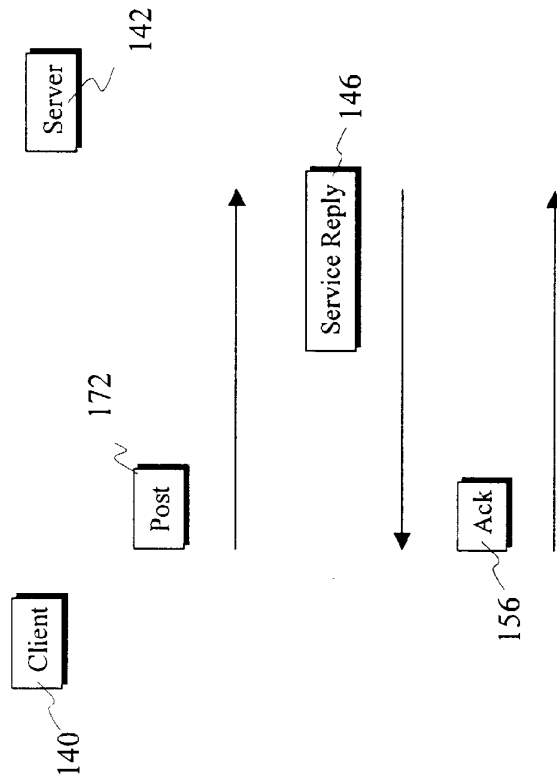
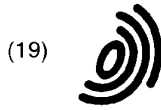


Fig. 7



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) EP 0 917 320 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
19.05.1999 Bulletin 1999/20

(51) Int Cl.®: H04L 12/56, H04Q 7/22,
H04L 12/46

(21) Application number: 98308329.6

(22) Date of filing: 13.10.1998

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(72) Inventors:
• Chuah, Mooi Choo
Eaton Town, Monmouth, New Jersey 07724 (US)
• Rai, Girish
Bartlett, Du Page, Illinois 60103 (US)

(30) Priority: 14.10.1997 US 61915 P
24.08.1998 US 138683

(74) Representative:
Watts, Christopher Malcolm Kelway, Dr. et al
Lucent Technologies (UK) Ltd,
5 Mornington Road
Woodford Green Essex, IG8 0TU (GB)

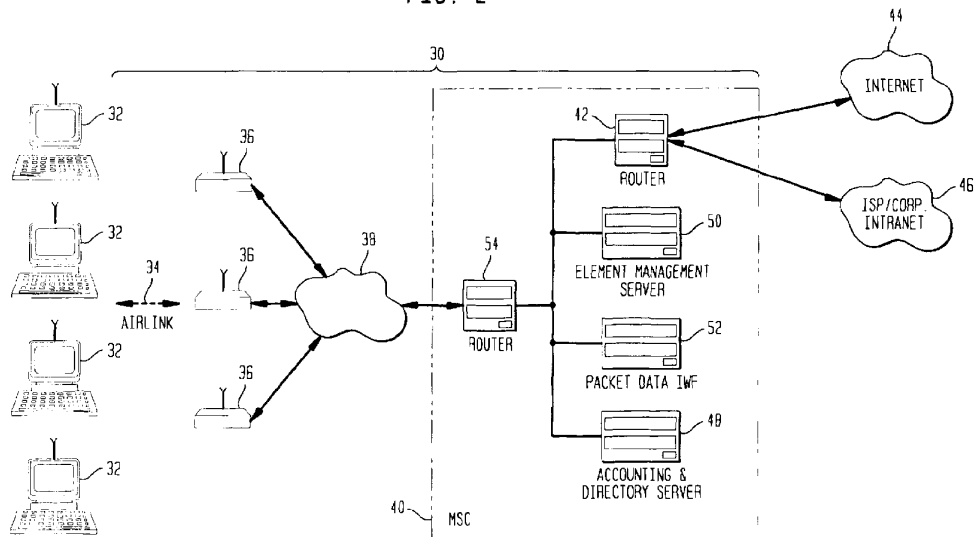
(71) Applicant: LUCENT TECHNOLOGIES INC.
Murray Hill, New Jersey 07974-0636 (US)

(54) Optimum routing system

(57) A wireless data network includes a wireless packet switched data network for end users that divides mobility management into local, micro, macro and global connection handover categories and minimizes handoff updates according to the handover category. The network integrates MAC handoff messages with network handoff messages. The network separately directs registration functions to a registration server and direct routing functions to inter-working function units.

The network provides an intermediate XTunnel channel between a wireless hub (also called access hub AH) and an inter-working function unit (IWF unit) in a foreign network, and it provides an IXTunnel channel between an inter-working function unit in a foreign network and an inter-working function unit in a home network. The network enhances the layer two tunneling protocol (L2TP) to support a mobile end system, and it performs network layer registration before the start of a PPP communication session.

FIG. 2



EP 0 917 320 A2

DescriptionBackground of the InventionField of the Invention

[0001] The present invention relates to the management of mobile end systems in a packet switched data network that provides computer users with remote access to the internet and to private intranets using virtual private network services over a high speed, packet switched, wireless data link. In particular, the invention relates to the optimization of routing mobile end systems to desired communications servers.

Description Of Related Art

[0002] FIG. 1 depicts three business entities, whose equipment, working together typically provide remote internet access to user computers 2 through user modems 4. User computers 2 and modems 4 constitute end systems.

[0003] The first business entity is the telephone company (telco) that owns and operates the dial-up plain old telephone system (POTS) or integrated services data network (ISDN) network. The telco provides the media in the form of public switched telephone network (PSTN) 6 over which bits (or packets) can flow between users and the other two business entities.

[0004] The second business entity is the internet service provider (ISP). The ISP deploys and manages one or more points of presence (POPs) 8 in its service area to which end users connect for network service. An ISP typically establishes a POP in each major local calling area in which the ISP expects to subscribe customers. The POP converts message traffic from the PSTN run by the telco into a digital form to be carried over intranet backbone 10 owned by the ISP or leased from an intranet backbone provider like MCI, Inc. An ISP typically leases fractional or full T1 lines or fractional or full T3 lines from the telco for connectivity to the PSTN. The POPs and the ISP's medium data center 14 are connected together over the intranet backbone through router 12A. The data center houses the ISP's web servers, mail servers, accounting and registration servers, enabling the ISP to provide web content, e-mail and web hosting services to end users. Future value added services may be added by deploying additional types of servers in the data center. The ISP also maintains router 12A to connect to public internet backbone 20. In the current model for remote access, end users have service relationships with their telco and their ISP and usually get separate bills from both. End users access the ISP, and through the ISP, public internet 20, by dialing the nearest POP and running a communication protocol known as the Internet Engineering Task Force (IETF) point-to-point protocol (PPP).

[0005] The third business entity is the private corpo-

ration which owns and operates its own private intranet 18 through router 12B for business reasons. Corporate employees may access corporate network 18 (e.g., from home or while on the road) by making POTS/ISDN calls to corporate remote access server 16 and running the IETF PPP protocol. For corporate access, end users only pay for the cost of connecting to corporate remote access server 16. The ISP is not involved. The private corporation maintains router 12B to connect an end user to either corporate intranet 18 or public internet 20 or both.

[0006] End users pay the telco for the cost of making phone calls and for the cost of a phone line into their home. End users also pay the ISP for accessing the ISP's network and services. The present invention will benefit wireless service providers like Sprint PCS, PrimeCo, etc. and benefit internet service providers like AOL, AT&T Worldnet, etc.

[0007] Today, internet service providers offer internet access services, web content services, e-mail services, content hosting services and roaming to end users. Because of low margins and no scope of doing market segmentation based on features and price, ISPs are looking for value added services to improve margins. In the short term, equipment vendors will be able to offer solutions to ISPs to enable them to offer faster access, virtual private networking (which is the ability to use public network securely as private networks and to connect to intranets), roaming consortiums, push technologies and quality of service. In the longer term, voice over internet and mobility will also be offered. ISPs will use these value added services to escape from the low margin strait-jacket. Many of these value added services fall in the category of network services and can be offered only through the network infrastructure equipment. Others fall in the category of application services which require support from the network infrastructure, while others do not require any support from the network infrastructure. Services like faster access, virtual private networking, roaming, mobility, voice, quality of service, quality of service based accounting all need enhanced network infrastructure. The invention described here will be either directly provide these enhanced services or provide hooks so that these services can be added later as future enhancements. Wireless service providers will be able to capture a larger share of the revenue stream. The ISP will be able to offer more services and with better market segmentation.

SUMMARY OF THE INVENTION

[0008] The present invention provide end users with remote wireless access to the public internet, private intranets and internet service providers. Wireless access is provided through base stations in a home network and base stations in foreign networks with interchange agreements. The optimum route between the serving inter-working function and the desired communication server is determined.

[0009] It is an object of the present invention to provide a wireless packet switched data network for end users that divides mobility management into local, micro, macro and global connection handover categories and minimizes handoff updates according to the handover category. It is another object to integrate MAC handoff messages with network handoff messages. It is a further object of the present invention to separately direct registration functions to a registration server and direct routing functions to inter-working function units. It is yet another object to provide an intermediate XTunnel channel between a wireless hub (also called access hub AH) and an inter-working function unit (IWF unit) in a foreign network. It is yet another object to provide an IXTunnel channel between an inter-working function unit in a foreign network and an inter-working function unit in a home network. It is yet another object to enhance the layer two tunneling protocol (L2TP) to support a mobile end system. It is yet another object to perform network layer registration before the start of a PPP communication session.

[0010] These and other objects are achieved in a network that includes a home network, a foreign network and an end station. The foreign network includes a base station and a foreign mobile switching center with a serving registration server. The base station including an access hub with serving inter-working function. The home network includes a home mobile switching center with a home registration server and a home inter-working function. The end system subscribes to the home network and operates within the foreign network. The end system includes an end registration agent to form a registration request. The registration request includes an indication of a desired communications network having a desired communications server. The end system sends the registration request to the serving registration server. The serving registration server includes a first module to process the registration request and to determine an optimum route between the desired communications server and one of the home inter-working function and the serving inter-working function. The serving registration server further includes a second module to link the serving inter-working function to the desired communications server when the first module determines that the optimum route is between the serving inter-working function and the desired communications server.

BRIEF DESCRIPTION OF DRAWINGS

[0011] The invention will be described in detail in the following description of preferred embodiments with reference to the following figures wherein:

FIG. 1 is a configuration diagram of a known remote access architecture through a public switched telephone network;

FIG. 2 is a configuration diagram of a remote access

architecture through a wireless packet switched data network according to the present invention;

FIG. 3 illustrates an end system configuration according to one embodiment of the present invention;

FIG. 4 illustrates another end system configuration according to one embodiment of the present invention;

FIG. 5 illustrates another end system configuration according to one embodiment of the present invention;

FIG. 6 is a configuration diagram of selected parts of the architecture of the network of FIG. 2 showing a roaming scenario;

FIG. 7 is a configuration diagram of a base station with local access points;

FIG. 8 is a configuration diagram of a base station with remote access points;

FIG. 9 is a configuration diagram of a base station with remote access points, some of which are connected using a wireless trunk connection;

FIG. 10 is a diagram of a protocol stack for a local access point;

FIG. 11 is a diagram of a protocol stack for a remote access point with a wireless trunk;

FIG. 12 is a diagram of a protocol stack for a relay function in the base station for supporting remote access points with wireless trunks;

FIG. 13 is a diagram of protocol stacks for implementing the relay function depicted in FIG. 12;

FIG. 14 is a diagram of protocol stacks for a relay function in the base station for supporting local access points;

FIG. 15 is a configuration diagram of selected parts of the architecture of the network of FIG. 2 showing a first end system registering in the home network from the home network and a second system registering in the home network from a foreign network using a home inter-working function for an anchor;

FIG. 16 is a configuration diagram of selected parts of the architecture of the network of FIG. 2 showing a first end system registering in the home network from the home network and a second system registering in the home network from a foreign network using a serving inter-working function for an anchor;

FIG. 17 is a ladder diagram of the request and response messages to register in a home network from a foreign network and to establish, authenticate and configure a data link;

FIG. 18 is a configuration diagram of selected parts of the architecture of the network of FIG. 2 showing registration requests and responses for registering a mobile in a home network from the home network;

FIG. 19 is a configuration diagram of selected parts of the architecture of the network of FIG. 2 showing registration requests and responses for registering a mobile in a home network from a foreign network;

FIG. 20 is a configuration diagram of protocol stacks

showing communications between an end system in a home network and an inter-working function in the home network where the cell site has local access points;

FIG. 21 is a configuration diagram of protocol stacks showing communications between an end system in a home network and an inter-working function in the home network where the cell site has remote access points coupled to a wireless hub through a wireless trunk;

FIG. 22 is a configuration diagram of protocol stacks showing communications between a base station coupled to a roaming end system and a home inter-working function;

FIG. 23 is a configuration diagram of protocol stacks showing communications between an end system in a home network through an inter-working function in the home network to an internet service provider;

FIG. 24 is a configuration diagram of protocol stacks showing communications between an end system in a foreign network and a home registration server in a home network during the registration phase;

FIG. 25 is a processing flow diagram showing the processing of accounting data through to the customer billing system;

FIGS. 26 and 27 are ladder diagrams depicting the registration process for an end system in a home network and in a foreign network, respectively;

FIGS. 28 and 29 are protocol stack diagrams depicting an end system connection in a home network where a PPP protocol terminates in an inter-working function of the home network and where the PPP protocol terminates in an ISP or intranet, respectively;

FIGS. 30 and 31 are protocol stack diagrams depicting an end system connection in a foreign network where a PPP protocol terminates in an inter-working function of the foreign network and where the PPP protocol terminates in an ISP or intranet, respectively;

FIGS. 32, 33 and 34 are ladder diagrams depicting a local handoff scenario, a micro handoff scenario and a macro handoff scenario, respectively;

FIG. 35 is a ladder diagram depicting a global handoff scenario where the foreign registration server changes and where home inter-working function does not change;

FIG. 36 is a ladder diagram depicting a global handoff scenario where both the foreign registration server and the home inter-working function change;

FIGS. 37 and 38 are system configuration diagrams which illustrate possible connections; and

FIGS. 39-42 illustrates various handoff scenarios.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0012] The present invention provides computer us-

ers with remote access to the internet and to private intranets using virtual private network services over a high speed, packet switched, wireless data link. These users are able to access the public internet, private intranets and their internet service providers over a wireless link. The network supports roaming, that is, the ability to access the internet and private intranets using virtual private network services from anywhere that the services offered by the present invention are available. The network also supports handoffs, that is, the ability to change the point of attachment of the user to the network without disturbing the PPP link between the PPP client and the PPP server. The network targets users running horizontal internet and intranet applications. These applications include electronic mail, file transfer, browser based WWW access and other business applications built around the internet. Because the network will be based on the IETF standards, it is possible to run streaming media protocols like RTP and conferencing protocols like H.323 over it.

[0013] Other internet remote access technologies that are already deployed or are in various stages of deployment include: wire line dial-up access based on POTS and ISDN, XDSL access, wireless circuit switched access based on GSM/CDMA/TDMA, wireless packet switched access based on GSM/CDMA/TDMA, cable modems; and satellite based systems. However, the present invention offers a low cost of deployment, ease of maintenance, a broad feature set, scalability, an ability to degrade gracefully under heavy load conditions and support for enhanced network services like virtual private networking, roaming, mobility and quality of service to the relative benefit of users and service providers.

[0014] For wireless service providers who own personal communications system (PCS) spectrum, the present invention will enable them to offer wireless packet switched data access services that can compete with services provided by the traditional wire line telcos who own and operate the PSTN. Wireless service providers may also decide to become internet service providers themselves, in which case, they will own and operate the whole network and provide end to end services to users.

[0015] For internet service providers the present invention will allow them to by-pass the telcos (provided they purchase or lease the spectrum) and offer direct end to end services to users, perhaps saving access charges to the telcos, which may increase in the future as the internet grows to become even bigger than it is now.

[0016] The present invention is flexible so that it can benefit wireless service providers who are not internet service providers and who just provide ISP, internet or private intranet access to end users. The invention can also benefit service providers who provide wireless access and internet services to end users. The invention can also benefit service providers who provide wireless

access and internet services but also allow the wireless portion of the network to be used for access to other ISPs or to private intranets.

[0017] In FIG. 2, end systems 32 (e.g., based on, for example, Win 95 personal computer) connect to wireless network 30 using external or internal modems. These modems allow end systems to send and receive medium access control (MAC) frames over air link 34. External modems attach to the PC via a wired or wireless link. External modems are fixed, and, for example, co-located with roof top mounted directional antennae. External modems may be connected to the user's PC using any one of following means: 802.3, universal serial bus, parallel port, infra-red, or even an ISM radio link. Internal modems are preferably PCMCIA cards for laptops and are plugged into the laptop's backplane. Using a small omni-directional antenna, they send and receive MAC frames over the air link.

[0018] The end system consists of the equipment that is located at the subscribers location. In the case of a fixed installation, the end system consists of a rooftop mounted antenna, radio components, digital components, and finally a desktop computer. It is presumed that a subscriber will already own the desktop computer, thus the wireless system must connect to the PC through standard interfaces. Figures 3-5 illustrate the different options for typical fixed installations of the wireless system. Each of the choices outlined in these figures have consequences associated with them, ranging from installation costs, equipment costs, practical installation to environmental with the installation, which will be discussed below.

[0019] The installation show in Figure 3 is presently the least expensive. In this configuration, only an antenna 21 is located outdoors and an RF cable 22 is connected to the radio 23. The installer, either the paid professional or the subscriber, will only have to install the antenna 21 at the roof or on the side of the building, and drop an inexpensive external cable 22 alongside the building to an entry point, typically through a hole in the corner of a window frame or through a hole in the wall near an internal floor. The radio 23 is external to the desktop computer 24 with a PCMCIA interface to the PC 24. Losses in long RF cable runs for users located at distant points from the access point can be compensated for with in-line bi-directional RF amplifiers. Users close to an access point can tolerate the additional losses of long cable runs since their propagation losses will not be as large as users at the periphery of the cell.

[0020] Another design illustrated in Figure 4 involves integrating the radio electronics and the antenna into a common device 25. The connection to the PC 24 would be through a proprietary interface and PCMCIA. Power would be supplied to the device from a wall transformer 27 via a multi twisted-paired cable 26 carrying both power and digital data. The challenge of designing an integrated device includes weatherproofing, heating and cooling, and server temperature extremes.

[0021] Another design which consists of an outdoor antenna and an attic mounted subscriber unit. This alleviated some of the low temperature and weatherproofing requirements, however, cooling will need to be provided. The subscriber unit is then connected to the PC via a cable.

[0022] The last and most expensive means by which to move the digital data from the radio to a computer, or multiple computers, is to use an ISM band LAN, such as WaveLAN as illustrated in Figure 5. The antenna 21 will be located on the rooftop, as in the previous installation, and the radio can be located at the antenna or elsewhere. An 802.3 connection will connect the radio to a wireless LAN access point. Each of the remote computer devices within the house will now have access to the wireless LAN 28. Ideally, the wireless LAN access point antenna 29 should be a directional antenna located high in the building pointing downward to provide coverage in the house while minimizing RF leakage outside the house. Locating the antenna in the attic presents various problems from powering the device in the attic to cooling the LAN radios. Practically, it seems that a LAN antenna located anywhere in the house will be acceptable, as long as LAN access point antenna cable lengths are short.

[0023] There may be a need to provide service to the roaming subscribers who choose to take their laptop computer away from their home service area to another service area. The laptop user will need to use a flat panel directional antenna which will be pointed toward the access points. The alignment of the access point will be critical to ensure service quality. As part of the laptop software, an alignment indicator will provide guidance in aligning the antenna.

[0024] It is envisioned that the antenna will approximately $\frac{1}{2}$ to $\frac{3}{4}$ of an inch thick, with an aperture approximately the same size as the laptop ($8\frac{1}{2}$ " x 11"). Some means of temporarily attaching the antenna panel to the back of the laptop, such as hook and loop fasteners, is convenient for transporting the antenna. Once the laptop user arrives at the location where access is desired, the antenna can either be removed from the back of the laptop and oriented for best performance, or left attached to the laptop in very strong signal areas. The laptop antenna may even be hinged to the laptop with a bi-axis alignment mechanism which changes the azimuth and elevation of the antenna. The antenna panels will support 45° dual slant polarization with conical beam shapes to eliminate any propagation effects which can affect signal quality. Furthermore, since the beam shapes are conical with dual polarization, standing the antenna on either side should not change signal quality.

[0025] Wide-area wireless coverage is provided by base stations 36. The range of coverage provided by base stations 36 depends on factors like link budget, capacity and coverage. Base stations are typically installed in cell sites by PCS (personal communication services) wireless service providers. Base stations mul-

tiplex end system traffic from their coverage area to the system's mobile switching center (MSC) 40 over wire line or microwave backhaul network 38.

[0026] A wireless communication system with multi-sector directional antenna arrangements entitled "Multi-Sector Cell Pattern For A Wireless Communication System", filed on December 26, 1997, by Walter Honcharenko, can be used to provide the wireless coverage and is incorporated herein by reference.

[0027] The invention is independent of the MAC and PHY (physical) layer of the air link and the type of modem. The architecture is also independent of the physical layer and topology of backhaul network 38. The only requirements for the backhaul network are that it must be capable of routing internet protocol (IP) packets between base stations and the MSC with adequate performance. At Mobile Switching Center 40 (MSC 40), packet data inter-working function (IWF) 52 terminates the wireless protocols for this network. IP router 42 connects MSC 40 to public internet 44, private intranets 46 or to internet service providers 46. Accounting and directory servers 48 in MSC 40 store accounting data and directory information. Element management server 50 manages the equipment which includes the base stations, the IWFs and accounting/directory servers.

[0028] The accounting server will collect accounting data on behalf of users and send the data to the service provider's billing system. The interface supported by the accounting server will send accounting information in American Management Association (AMA) billing record format or any other suitable billing format over a TCP/IP (transport control protocol/internet protocol) transport to the billing system (which is not shown in the figure).

[0029] The network infrastructure provides PPP (point-to-point protocol) service to end systems. The network provides (1) fixed wireless access with roaming (log-in anywhere that the wireless coverage is available) to end systems and (2) low speed mobility and hand-offs. When an end system logs on to a network, it may request either fixed service (i.e., stationary and not requiring handoff services) or mobile service (i.e., needing handoff services). An end system that does not specify fixed or mobile is regarded as specifying mobile service. The actual registration of the end system is the result of a negotiation with a home registration server based on requested level of service, the level of services subscribed to by the user of the end system and the facilities available in the network.

[0030] If the end system negotiates a fixed service registration (i.e., not requiring handoff services) and the end system is located in the home network, an IWF (inter-working function) is implemented in the base station to relay traffic between the end user and a communications server such as a PPP server (i.e., the point with which to be connected, for example, an ISP PPP server or a corporate intranet PPP server or a PPP server operated by the wireless service provider to provide cus-

tomers with direct access to the public internet). It is anticipated that perhaps 80% of the message traffic will be of this category, and thus, this architecture distributes IWF processing into the base stations and avoids message traffic congestion in a central mobile switching center.

[0031] If the end system requests mobile service (from a home network or a foreign network) or if the end system request roaming service (i.e., service from the home network through a foreign network), two IWFs are established: a sorting IWF typically established in the base station of the network to which the end system is attached (be it the home network or a foreign network) and a home IWF typically established in mobile switching center MSC of the home network. Since this situation is anticipated to involve only about 20% of the message traffic, the message traffic congestion around the mobile switching center is minimized. The serving IWF and the wireless hub may be co-located in the same nest of computers or may even be programmed in the same computer so that a tunnel using an XTunnel protocol need not be established between the wireless hub and the serving IWF.

[0032] However, based on available facilities and the type and quality of service requested, a serving IWF in a foreign network may alternatively be chosen from facilities in the foreign MSC. Generally, the home IWF becomes an anchor point that is not changed during the communications session, while the serving IWF may change if the end system moves sufficiently.

[0033] The base station includes an access hub and at least one access point (be it remote or collocated with the access hub). Typically, the access hub serves multiple access points. While the end system may be attached to an access point by a wire or cable according to the teachings of this invention, in a preferred embodiment the end system is attached to the access point by a wireless "air link", in which case the access hub is conveniently referred to as a wireless hub. While the access hub is referred to as a "wireless hub" throughout the description herein, it will be appreciated that an end system coupled through an access point to an access hub by wire or cable is an equivalent implementation and is contemplated by the term "access hub".

[0034] In the invention, an end system includes an end user registration agent (e.g., software running on a computer of the end system, its modem or both) that communicates with an access point, and through the access point to a wireless hub. The wireless hub includes a proxy registration agent (e.g., software running on a processor in the wireless hub) acting as a proxy for the end user registration agent. Similar concepts used in, for example, the IETF proposed Mobile IP standard are commonly referred to as a foreign agent (FA). For this reason, the proxy registration agent of the present invention will be referred to as a foreign agent, and aspects of the foreign agent of the present invention that differ from the foreign agent of Mobile IP are as de-

scribed throughout this description.

[0035] Using the proxy registration agent (i.e., foreign agent FA) in a base station, the user registration agent of an end system is able to discover a point of attachment to the network and register with a registration server in the MSC (mobile switching center) of the home network. The home registration server determines the availability of each of the plural inter-working function modules (IWFs) in the network (actually software modules that run on processors in both the MSC and the wireless hubs) and assigns IWF(s) to the registered end system. For each registered end system, a tunnel (using the *XTunnel* protocol) is created between the wireless hub in the base station and an inter-working friction (IWF) in the mobile switching center (MSC), this tunnel transporting PPP frames between the end system and the IWF.

[0036] As used herein, the *XTunnel* protocol is a protocol that provides in-sequence transport of PPP data frames with flow control. This protocol may run over standard IP networks or over point-to-point networks or over switched network like ATM data networks or frame relay data networks. Such networks may be based on T1 or T3 links or based on radio links, whether land based or space based. The *XTunnel* protocol may be built by adapting algorithms from L2TP (layer 2 tunneling protocol). In networks based on links where lost data packets may be encountered, a re-transmission feature may be a desirable option.

[0037] The end system's PPP peer (i.e., a communications server) may reside in the IWF or in a corporate intranet or ISP's network. When the PPP peer resides in the IWF, an end system is provided with direct internet access. When the PPP peer resides in an intranet or ISP, an end system is provided with intranet access or access to an ISP. In order to support intranet or ISP access, the IWF uses the layer two tunneling protocol (L2TP) to connect to the intranet or ISP's PPP server. From the point of view of the intranet or ISP's PPP server, the IWF looks like a network access server (NAS). PPP traffic between the end system and the IWF is relayed by the foreign agent in the base station.

[0038] In the reverse (up link) direction, PPP frames traveling from the end system to the IWF are sent over the MAC and air link to the base station. The base station relays these frames to the IWF in the MSC using the *XTunnel* protocol. The IWF delivers them to a PPP server for processing. For internet access, the PPP server may be in the same machine as the IWF. For ISP or intranet access, the PPP server is in a private network and the IWF uses the layer two tunneling protocol (L2TP) to correct to it.

[0039] In the forward (down link) direction, PPP frames from the PPP server are relayed by the IWF to the base station using the *XTunnel* protocol. The base station de-tunnels down link frames and relays them over the air link to the end system, where they are processed by the end system's PPP layer.

[0040] To support mobility, support for hand-offs are included. The MAC layer assists the mobility management software in the base station and the end system to perform hand-offs efficiently. Hand-offs are handled transparently from the peer PPP entities and the L2TP tunnel. If an end system moves from one base station to another, a new *XTunnel* is created between the new base station and the original IWF. The old *XTunnel* from the old base station will be deleted. PPP frames will transparently traverse the new path.

[0041] The network supports roaming (i.e., when the end user connects to its home wireless service provider through a foreign wireless service provider). Using this feature, end systems are able to roam away from the home network to a foreign network and still get service, provided of course that the foreign wireless service provider and the end system's home wireless service provider have a service agreement.

[0042] In FIG. 6, roaming end system 60 has traveled to a location at which foreign wireless service provider 62 provides coverage. However, roaming end system 60 has a subscriber relationship with home wireless service provider 70. In the present invention, home wireless service provider 70 has a contractual relationship with foreign wireless service provider 62 to provide access services. Therefore, roaming end system 60 connects to base station 64 of foreign wireless service provider 62 over the air link. Then, data is relayed from roaming end system 60 through base station 64, through serving IWF 66 of foreign wireless service provider 62, to home IWF 72 of home wireless service provider 70, or possibly through home IWF 72 of home wireless service provider 70 to internet service provider 74.

[0043] An inter-service provider interface, called the I-interface, is used for communications across wireless service provider (WSP) boundaries to support roaming. This interface is used for authenticating, registering and for transporting the end system's PPP frames between the foreign WSP and the home WSP.

[0044] PPP frames in the up link and the down link directions travel through the end system's home wireless service provider (WSP). Alternatively, PPP frames directly transit from the foreign WSP to the destination network. The base station in the foreign WSP is the end system's point of attachment in the foreign network. This base station sends (and receives) PPP frames to (and from) a serving in the foreign WSP's mobile switching center. The serving IWF connects over the I-interface to the home IWF using a layer two tunnel to transport the end system's PPP frames in both directions. The serving IWF in the foreign WSP collects accounting data for auditing. The home IWF in the home WSP collects accounting data for billing.

[0045] The serving IWF in the foreign WSP may be combined with the base station in the same system, thus eliminating the need for the X-Tunnel.

[0046] During the registration phase, a registration server in the foreign WSP determines the identity of the

roaming end system's home network. Using this information, the foreign registration server communicates with the home registration server to authenticate and register the end system. These registration messages flow over the I-interface. Once the end system has been authenticated and registered, a layer two tunnel is created between the base station and the serving IWF using the *XTUNNEL* protocol and another layer two tunnel is created between the serving IWF and the home IWF over the I-X Tunnel. The home IWF connects to the end system's PPP peer as before, using L2TP (layer 2 tunneling protocol). During hand-offs, the location of the home IWF and the L2TP tunnel remains fixed. As the end system moves from one base station to another base station, a new tunnel is created between the new base station and the serving IWF and the old tunnel between the old base station and the serving IWF is deleted. If the end system moves far enough, so that a new serving IWF is needed, a new I-X tunnel will be created between the new serving IWF and the home IWF. The old tunnel between the old serving and the home will be deleted.

[0047] To support foaming, the I-interface supports authentication, registration and data transport services across wireless service provider boundaries. Authentication and registration services are supported using the IETF Radius protocol. Data transport services to transfer PPP frames over a layer two tunnel are supported using the *I-XTunnel* protocol. This protocol is based on the IETF L2TP protocol.

[0048] As used in this description, the term home IWF refers to the IWF in the end system's home network. The term serving IWF refers to the IWF in the foreign network which is temporarily providing service to the end system. Similarly, the term home registration server refers to the registration server in the end system's home network and the term foreign registration server refers to the registration server in the foreign network through which the end system registers while it is roaming.

[0049] The network supports both fixed and dynamic IP address assignment for end systems. There are two types of IP addresses that need to be considered. The first is the identity of the end system in its home network. This may be a structured user name in the format *user@domain*. This is different from the home IP address used in mobile IP. The second address is the IP address assigned to the end system via the PPP IPCP address protocol. The domain sub-field of the home address is used to identify the user's home domain and is a fully qualified domain name. The user sub-field of the home address is used to identify the user in the home domain. The User-Name is stored on the end system and in the subscriber data-base at the MSC and is assigned to the user when he or she subscribes to the service. The domain sub-field of the User-Name is used during roaming to identify roaming relationships and the home registration server for purposes of registration and authentication. Instead of the structured user name, another

unique identifier may be used to identify the user's home network and the user's identity in the home network. This identifier is sent in the registration request by the end system.

[0050] The PPP IPCP is used to negotiate the IP address for the end system. Using IP configuration protocol IPCP, the end system is able to negotiate a fixed or dynamic IP address.

[0051] Although the use of the structured user-name field and the non-use of an IP home address is a feature that characterizes the present invention over a known mobile IP, the network may be enhanced to also support end systems that have no user-name and only a non-null home IP address, if mobile IP and its use in conjunction with PPP end systems becomes popular. The PPP server may be configured by the service provider to assign IP addresses during the IPCP address assignment phase that are the same as the end system's home IP address. In this case, the home address and the IPCP assigned IP address will be identical.

[0052] In FIG. 7, base station 64 and air links from end systems form wireless sub-network 80 that includes the air links for end user access, at least one base station (e.g., station 64) and at least one backhaul network (e.g., 38 of FIG. 2) from the base station to MSC 40 (FIG. 2). The wireless sub-network architecture of, for example, a 3-sectored base station includes the following logical functions.

1. *Access point function.* Access points 82 perform MAC layer bridging and MAC layer association and dissociation procedures. An access point includes a processor (preferably in the form of custom application specific integrated circuit ASIC), a link to a wireless hub (preferably in the form of an Ethernet link on a card or built into the ASIC), a link to an antenna (preferably in the form of a card with a data modulator/demodulator and a transmitter/receiver), and the antenna to which the end system is coupled. The processor runs software to perform a data bridging function and various other functions in support of registration and mobility handovers as further described herein. See discussion with respect to FIGS. 10, 11 and 14.

Access points (APs) take MAC layer frames from the air link and relay them to a wireless hub and vice versa. The MAC layer association and dissociation procedures are used by APs to maintain a list of end system MAC addresses in their MAC address filter table. An AP will only perform MAC layer bridging on behalf of end systems whose MAC addresses are present in the table. An access point and its associated wireless hub are typically co-located. In its simplest form, an access point is just a port into a wireless hub. When the APs and the wireless hub are co-located in the same cell site, they may be connected together via a IEEE 802.3 link. Sometimes, access points are located remote-

ly from the wireless hub and connected via a long distance link like a wired T1 trunk or even a wireless trunk. For multi-sector cells, multiple access points (i.e., one per sector) are used.

2. *Wireless hub function.* Wireless hub 84 performs the foreign agent (FA) procedures, backhaul load balancing (e.g., over multiple T1's), backhaul network interfacing, and the *xtunnel* procedures. When support for quality of service (QOS) is present, the wireless hub implements the support for QOS by running the *xtunnel* protocol over backhauls with different QOS attributes. In a multi-sector cell site, a single wireless hub function is typically shared by multiple access points.

A wireless hub includes a processor, a link to one or more access points preferably in the form of an Ethernet link on a card or built into an ASIC), and a link to a backhaul line. The backhaul line is typically a T1 or T3 communications line that terminates in the mobile switching center of the wireless service provider. The link to the backhaul line formats data into a preferred format, for example, an Ethernet format, a frame relay format or an ATM format. The wireless hub processor runs software to support data bridging and various other functions as described herein. See discussion with respect to FIGS. 12, 13 and 14.

[0053] The base station design supports the following types of cell architectures.

1. *Local AP architecture.* In a local AP architecture, access points have a large (> = 2km, typically) range. They are co-located in the cell site with the wireless hub (FIG. 4). Access points may be connected to the wireless hub using an IEEE 802.3 network or may be directly plugged into the wireless hub's backplane or connected to the wireless hub using some other mechanism (e.g. universal serial bus, printer port, infra-red, etc.). It will be assumed that the first alternative is used for the rest of this discussion. The cell site may be omni or sectored by adding multiple access points and sectored antennas to a wireless hub.

2. *Remote AP architecture.* In a remote AP architecture, access points usually have a very small range, typically around 1 km radius. They are located remotely (either indoors or outdoors) from the wireless hub. A T1 or a wireless trunk preferably links remote access points to the cell site where the wireless hub is located. From the cell site, a wire line backhaul or a microwave link is typically used to connect to the IWF in the MSC. If wireless trunking between the remote AP and the wireless hub is used, omni or sectored wireless radios for trunking are utilized. The devices for trunking to remote ac-

cess points are preferably co-located with the wireless hub and may be connected to it using an IEEE 802.3 network or may be directly plugged into the wireless hub's backplane. These devices will be referred to by the term *trunk AP*.

3. *Mixed AP architecture.* In a mixed architecture, the wireless sub-network will have to support remote and local access points. Remote access points may be added for hole filling and other capacity reasons. As described earlier, T1 or wireless trunks may be used to connect the remote AP to the wireless hub.

15 **[0054]** FIGS. 37 and 38 are system configuration diagrams which illustrate possible connections. For case (i), the IWF1 is the anchor IWF and acts as the home agent, while the WH1 acts as the foreign agent. An Xtunnel is used between the WH1 and IWF1 and a layer 2
20 Tunneling protocol (L2TP) tunnel is used between the IWF1 and the PPP server. For case (ii), the WH and the serving IWF are collocated. The IWF1 is the anchor IWF and the serving IWF. IWF2 acts as the Foreign agent. An I-X tunnel is used between IWF and IWF2 and a
25 L2TP tunnel is used between IWF1 and the PPP server. For case (iii), the serving IWF is IWF3 and the anchor IWF is IWF1. An Xtunnel is used between WH3 and IWF3, an I-Xtunnel is used between IWF3 and IWF1, and a L2TP tunnel is used between IWF1 and the PPP
30 server.

[0055] FIG. 38 illustrates the addition of a wireless hop (trunk AP) wherein the trunk AP may be collocated with WH. For this case, apart from all three possibilities described above, the following possibilities may also occur. For case (i), the Trunk AP1 is the foreign agent and IWF1 is the anchor IWF. An Xtunnel is used between the Trunk AP1 and the anchor IWF, and a L2TP tunnel is used between the anchor IWF and the PPP server. For case (ii), the serving IWF2 is the foreign agent. An Xtunnel is used between the trunk AP2 and the IWF2, an I-Xtunnel is used between the IWF2 and the anchor IWF1 and a L2TP tunnel is used between the anchor IWF and the PPP server. For case (iii), the serving IWF is the foreign agent. An Xtunnel is used between the trunk AP3 and the IWF3, an I-Xtunnel is used between IWF3 and anchor IWF1 and a L2TP tunnel is used between the anchor IWF1 and the PPP server.

[0056] FIGS. 39-42 illustrate several handoff scenarios as well as various connections between the elements of the systems.

[0057] FIG. 8 shows a cell with three sectors using local APs only. The access points and the wireless hub are co-located in the base station and are connected to each other with 802.3 links.

55 **[0058]** FIG. 9 shows an architecture with remote access points 82 connected to wireless hub 84 using wireless trunks 86. Each trunk access point in the base station provides a point to multi-point wireless radio link to

the remote micro access points (R-AP in figure). The remote access points provide air link service to end systems. The wireless hub and the trunk access points are co-located in the base station and connected together via 802.3 links. This figure also shows remote access points 82R connected to the wireless hub via point to point T1 links. In this scenario, no trunk APs are required.

[0059] To support all of the above cell architectures and the different types of access points that each cell might use, the network architecture follows the following rules:

1. Access points function as MAC layer bridges. Remote access points perform MAC bridging between the air link to the end systems and the wireless or T1 trunk to the cell site. Local access points perform MAC bridging between the air link to the end systems and the wireless hub.
2. Trunk access points also function as MAC layer bridges. They perform MAC bridging between the trunk (which goes to the access points) and the wireless hub.
3. The wireless flub is connected to all co-located MAC bridges (i.e. local access points or trunk access points) using a 802.3 link initially.

[0060] Additionally, where local access points or remote access points with T1 trunks are used, the following rules are followed.

1. Local access points are co-located with the wireless hub and connected to it using point to point 802.3 links or a shared 802.3 network. Remote access points are connected to the wireless hub using point to point T1 trunks.
2. Sectorization is supported by adding access points with sectorized antennas to the cell site.
3. For each access point connected to the wireless hub, there is a foreign agent executing in the wireless hub which participates in end system registration. MAC layer association procedures are used to keep the MAC address filter tables of the access points up to date and to perform MAC layer bridging efficiently. The wireless hub participates in MAC association functions so that only valid MAC addresses are added to the MAC address filter tables of the access points.
4. The wireless hub relays frames from the access points to the MSC IWF and vice versa using the *xtunnel* protocol unless the IWF is co-located with the wireless hub. The MAC address filter table is used to filter out those unicast MAC data frames

whose MAC addresses are not present in the table. The APs always forward MAC broadcast frames and MAC frames associated with end system registration functions regardless of the contents of the MAC address filter table.

5. Local access points use ARP to resolve MAC addresses for routing IP traffic to the wireless hub. Conversely, the wireless hub also uses ARP to route IP packets to access points. UDP/IP is used for network management of access points.

6. Remote access points connected via T1 do not use ARP since the link will be a point to point link.

7. Support for hand-offs is done with assistance from the MAC layer.

[0061] In a cell architecture using wireless trunks and trunk APs, the following rules are followed.

1. Trunk access points are co-located with the wireless hub and connected to it using point to point 802.3 links or other suitable means.
2. Wireless trunk sectorization is supported by adding trunk access points with sectorized antennas to the cell site.
3. Hand-offs across backhaul sectors are done using the foreign agent in the wireless hub. For each backhaul sector, there is a foreign agent executing in the wireless hub.
4. The trunk APs do not need to participate in MAC layer end system association and hand off procedures. Their MAC address filter tables will be dynamically programmed by the wireless hub as end systems register with the network. The MAC address filter table is used to filter out unicast MAC frames. Broadcast MAC frames or MAC frames containing registration packets are allowed to always pass through.
5. Trunk APs use ARP to resolve MAC addresses for routing IP traffic to the wireless hub. Conversely, the wireless hub use ARP to route IP packets to trunk APs. UDP/IP is used for network management of trunk APs.
6. In a single wireless trunk sector, MAC association and hand-offs from one access point to another is done using the MAC layer with the assistance of the foreign agent in the wireless hub. Using these MAC layer procedures, end systems associate with access points. As end systems move from one access point to another access point, the access points will use a MAC hand off protocol to update their MAC

address filter tables. The wireless hub at the cell site provides assistance to access points to perform this function. This assistance includes relaying MAC layer hand off messages (since access points will not be able to communicate directly over the MAC layer with each other) and authenticating the end system for MAC layer registration and hand off and for updating the MAC address filter tables of the access points.

7. The foreign agent for a wireless trunk sector is responsible for relaying frames from its trunk AP to the MSC and vice versa using the *xtunnel* protocol. Thus, the foreign agent for a trunk AP does not care about the location of the end system with respect to access points within that wireless trunk sector. In the down link direction, it just forwards frames from the mobile IP tunnel to the appropriate trunk AP which uses MAC layer bridging to send the frames to all the remote access points attached in that backhaul sector. The access points consult their MAC address filter tables and either forward the MAC frames over the access network or drop the MAC frames. As described above, the MAC address filter tables are kept up to date using MAC layer association and hand off procedures. In the up link direction, MAC frames are forwarded by the access points to the backhaul bridge which forwards them to the foreign agent in the wireless hub using the 802.3 link.

8. ARP is not used for sending or receiving IP packets to the remote access points. The trunk access points determine the MAC address of the wireless hub using BOOTP procedures. Conversely, the wireless hub is configured with the MAC address of remote access points. UDP/IP is used for network management of access points and for end system association and hand off messages.

[0062] IEEE 802.3 links in the cell site may be replaced by higher speed links.

[0063] FIG. 10 shows the protocol stack for a local access point. At the base of the stack is physical layer PHY. Physical layer PHY carries data to and from an end system over the air using radio waves as an example. When received from an end system, the AP receives data from the physical layer and unpacks it from the MAC frames (the MAC layer). The end system data frames are then repacked into an Ethernet physical layer format (IEEE 802.3 format) where it is sent via the Ethernet link to the wireless hub. When the AP's processor receives data from the wireless hub via its Ethernet link (i.e., the physical layer), the data to be transmitted to an end system, the AP packs the data in a medium access control (MAC) format, and sends the MAC layer data to its modulator to be transmitted to the end system using the PHY layer.

[0064] In FIG. 11, the MAC and PHY layers to/from the end system of FIG. 10 are replaced by a MAC and PHY for the trunk to the cell site for a remote access point. Specifically, for a T1 trunk, the high level data link control protocol (HDLC protocol) is preferably used over the T1.

[0065] FIG. 12 depicts the protocol stack for the wireless hub that bridges the backhaul line and the trunk to the remote access point. The trunk to the remote APs are only required to support remote access points (as distinct from Ethernet coupled access points). The MAC and PHY layers for the wireless trunk to the remote APs provide a point to multipoint link so that one trunk may be used to communicate with many remote APs in the same sector.

[0066] The wireless hub bridges the trunk to the remote APs and the backhaul line (e.g., T1 or T3) to the network's mobile switching center (MSC). The protocol stack in the wireless hub implements MAC and PHY layers to the MSC on top of which is implemented an IP layer (Internet Protocol) on top of which is implemented a UDP layer (Universal Datagram Protocol, in combination referred to as UDP/IP) for network management on top of which is implemented an XTunnel protocol. The XTunnel protocol is a new format that includes aspects of mobility (e.g. as in mobile IP) and aspects of the Layer 2 Tunnel Protocol (L2TP). The XTunnel protocol is used to communicate from the wireless hub to the MSC and between inter-working functions (IWFs) in different networks or the same network.

[0067] In FIG. 13, the protocol stack for the relay function in the base station for supporting remote access points is shown. The relay function includes an interface to the backhaul line (depicted as the wireless hub) and an interface to the remote AP (depicted as a trunk AP). From the point of view of the wireless hub, the trunk AP (depicted in FIG. 13) actually behaves like the AP depicted in FIG. 10. Preferably, the base station protocol stacks are split up into a wireless hub and a trunk AP with an Ethernet in between. In an N-sector wireless trunk, there are N wireless trunk APs in the cell site and one wireless hub.

[0068] In FIG. 14, the base station protocol stack for a cell architecture using a local AP is shown. The relay function includes an interface to the backhaul line (depicted as the wireless hub) and an air link interface to the end system (depicted as an AP). From the point of view of the wireless hub, the AP (depicted in FIGS. 11 and 14) actually behaves like the trunk AP depicted in FIG. 11. Preferably, the base station protocol stacks are split up into a wireless hub and a trunk AP with an Ethernet in between. In a N-sector cell, there are N access points and a single wireless hub.

[0069] The backhaul network from the base station to the MSC has the following attributes.

1. The network is capable of routing IP datagrams between the base station and the MSC.

2. The network is secure. It is not a public internet. Traffic from trusted nodes only are allowed onto the network since the network will be used for not only transporting end system traffic, but also for transporting authentication, accounting, registration and management traffic.
3. The network has the necessary performance characteristics.
4. Base stations support IP over Ethernet links.

In typical application, the service provider is responsible for installing and maintaining the backhaul network on which the equipment is installed.

[0070] The base stations supports the following backhaul interfaces for communicating with the MSC.

1. Base stations support IP over PPP with HDLC links using point to point T1 or fractional T3 links.
2. Base stations support IP over frame relay using T1 or fractional T3 links.
3. Base stations support IP over AAL5/ATM using T1 or fractional T3 links.

[0071] Since all of the above interfaces are based on IETF standard encapsulations, commercial routers may be used in the MSC to terminate the physical links of the backhaul network. Higher layers are passed on and processed by the various servers and other processors.

[0072] End system registration procedures above the MAC layer are supported. In the following, end system registration procedures at the MAC layer are ignored except where they impact the layers above.

[0073] End systems may register for service on their home network or from a foreign network. In both scenarios, the end system uses a foreign agent (FA) in the base station to discover a point of attachment to the network and to register. In the former case, the FA is in the end system's home network. In the latter case, the FA is in a foreign network. In either case, the network uses an IWF in the end system's home network as an anchor point (i.e., unchanging throughout the session in spite of mobility). PPP frames to and from the end system travel via the FA in the base station to the IWF in the home network. If the end system is at home, the home IWF is directly connected by means of the *xtunnel* protocol to the base station. Note that the home IWF may be combined with the base station in the same mode. If the end system is roaming, a serving IWF in the foreign network is connected to the home IWF over an I-interface. The serving IWF relays frames between the base station and the home IWF. Note that the serving IWF may also be combined with the base station in the same mode. From the home IWF, data is sent to a PPP server which may reside in the same IWF or to a separate serv-

er using the L2TP protocol. The separate server may be owned and operated by a private network operator (e.g. ISP or corporate intranet) who is different from the wireless service provider. For the duration of the session, the location of the home IWF and the PPP server remains fixed. If the end system moves while connected, it will have to re-register with a new foreign agent. However, the same home IWF and PPP server continues to be used. A new *xtunnel* is created between the new FA and the IWF and the old *xtunnel* between the old foreign agent and the IWF is destroyed.

[0074] FIG. 15 shows this network configuration for two end systems A and B, both of whose home wireless network is wireless service provider A (WSP-A). One end system is registered from the home wireless network and the other from a foreign wireless network. The home IWF in WSP-A serves as the anchor point for both end systems. For both end systems, data is relayed to the home IWF. The home IWF connects to an internet service provider's PPP server owned by ISP-A. Here it is assumed that both end systems have subscribed to the same ISP. If that were not the case, then the home IWF would be shown also connected to another ISP.

[0075] Within a wireless service providers network, data between base stations and the IWF is carried using the *xtunnel* protocol. Data between the IWF and the PPP server is carried using Layer 2 Tunneling Protocol (L2TP). Data between the serving IWF and the home IWF is carried using the *I-xtunnel* protocol.

[0076] In a simple scenario, for a user in their home network requiring fixed service, the home IWF function may be dynamically actuated in the base station. Also, the serving IWF function may be activated for a roaming user in the base station.

[0077] Always using an IWF in the home network has its advantages and disadvantages. An obvious advantage is simplicity. A disadvantage is that of always having to relay data to and from a possibly remote home IWF. The alternative is to send all the necessary information to the serving IWF so that it may connect to the end system's ISP/intranet and for the serving IWF to send accounting information in near real time back to the accounting server in the home network. This functionality is more complex to implement, but more efficient because it reduces the need to relay data over potentially long distances from the foreign network to the home network.

[0078] For example, consider a case of a user who roams from Chicago to Hong Kong. If the user's home network is in Chicago and the user registers using a wireless service provider in Hong Kong, then in the first configuration, the anchor point will be the home IWF in Chicago and all data will have to be relayed from Hong Kong to Chicago and vice versa. The home IWF in Chicago will connect to the user's ISP in Chicago. With the second configuration, the end system user will be assigned an ISP in Hong Kong. Thus, data will not always have to be relayed back and forth between Chicago and

Hong Kong. In the second configuration, the serving IWF will serve as the anchor and never change for the duration of the session even if the end system moves. However, the location of the FA may change as a result of end system movement in Hong Kong.

[0079] FIG. 16 shows the second network configuration. In this figure, the home network for end system A and B is WSP-A. End system A registers from its home network, using its home IWF as an anchor point, and also connects to its ISP-A using the ISP's PPP server. End system B registers from the foreign network of WSP-B and uses a serving IWF which serves as the anchor point and connects the end system to an ISP using the ISP's PPP server. In this configuration, data for end system B does not have to be relayed from the foreign network to the home network and vice versa.

[0080] In order for this configuration to work, not only must there be roaming agreements between the home and the foreign wireless service providers, but there also must be agreements between the foreign wireless service provider and the end system's internet service provider directly or through an intermediary. In the example above, not only must the wireless service provider in Hong Kong have a business agreement with the wireless service provider in Chicago, but the WSP in Hong Kong must have a business agreement with the user's Chicago ISP and access to the Chicago ISP's PPP server in Hong Kong or a business agreement with another ISP locally in Hong Kong who has a business agreement for roaming with the user's Chicago ISP. Additionally, the WSP in Hong Kong must be able to discover these roaming relationships dynamically in order to do user authentication and accounting and to set up the appropriate tunnels.

[0081] It is difficult for those companies who are in the Internet infrastructure business to work out suitable standards in the IETF for all of these scenarios. Thus, a preferable embodiment for the present invention is to implement the simpler, potentially less efficient configuration, where the IWF in the home network is always used as the anchor point. However, in the presence of suitable industry standardization of protocols for Internet roaming, the second configuration should be regarded as equivalent or alternative embodiment.

[0082] An end system will have to register with the wireless network before it can start PPP and send and receive data. The end system first goes through the FA discovery and registration phases. These phases authenticate and register the end system to the wireless service provider. Once these phases are over, the end system starts PPP. This includes the PPP link establishment phase, the PPP authentication phase and the PPP network control protocol phase. Once these phases are over, the end system is able to send and receive IP packets using PPP.

[0083] The following discussion assumes that the end system is roaming and registering from a foreign network. During the FA discovery phase, the end system

(through its user registration agent) waits for or solicits an advertisement from the foreign agent. The user registration agent uses advertisement messages sent by a near by foreign agent to discover the identity of the FA and to register. During this phase, the user registration agent of the end system selects a FA and issues a registration request to it. The FA acting as a proxy registration agent forwards the registration request to its registration server (the registration server in the foreign WSP). The registration server uses User-Name from the user registration agent's request to determine the end system's home network, and forwards the registration request for authentication to a registration server in the home network. Upon receiving the registration request relayed by the foreign registration server, the home registration server authenticates the identity of the foreign registration server and also authenticates the identity of the end system. If authentication and registration succeeds, the home registration server selects an IWF in the home network to create an *I-tunnel* link between the home IWF and the serving IWF (in the foreign WSP). The IWF in the home network serves as the anchor point for the duration of the PPP session.

[0084] Once the authentication and registration phases are over, the various PPP phases will be started. At the start of PPP, an L2TP connection is created between the home IWF and requested ISP/intranet PPP server. In the PPP authentication phase, PPP passwords using PAP or CHAP are exchanged and the ISP or intranet PPP server independently authenticates the identity of the end system.

[0085] Once this succeeds, the PPP network control phase is started. In this phase, an IP address is negotiated and assigned to the end system by the PPP server and the use of TCP/IP header compression is also negotiated. When this is complete, the end system is able to send and receive IP packets using PPP to its ISP or a corporate intranet.

[0086] Note that two levels of authentication are performed. The authentication authenticates the identity of the end system to the registration server in the home network and the identities of the foreign network and the home network to each other. To perform this function, the foreign agent forwards the end system's registration request using, for example, an IETF Radius protocol to a registration server in its local MSC in a Radius Access-Request packet. Using the end system's domain name, the foreign registration server determines the identity of the end system's home network and home registration server, and acting as a Radius proxy, encapsulates and forwards the request to the end system's home registration server. If the foreign registration server cannot determine the identity of the end system's home, it may optionally forward the Radius request to a registration server that acts like a broker (e.g. one that is owned by a consortium of wireless service providers), which can in turn proxy the Radius Access-Request to the final home registration server. If the local registration server

is unable to service the registration request locally or by proxying, then it rejects the foreign agent's registration request and the foreign agent rejects the end system's registration request. Upon receiving the Radius Access-Request, the home registration server performs the necessary authentication of the identifies of the foreign network and the end system. If authentication and registration succeeds, the home registration server responds with a Radius Access-Response packet to the foreign registration server which sends a response to the foreign agent so that a round trip can be completed. The registration request is rejected if the home registration server is unable to comply for any reason.

[0087] The second level of authentication verifies the identity of the end system to the intranet or ISP PPP server. PPP authentication, separate from mobility authentication allows the infrastructure equipment to be deployed and owned separately from the ISP.

[0088] FIG. 17 is a ladder diagram showing the registration sequence for a roaming end system. It is assumed that the PPP server and the home IWF are in the same server and L2TP is not required. Note the interactions with accounting servers to start accounting on behalf of the registering end system and also directory servers to determine the identity of the home registration server and to authenticate the end system's identity. More information on accounting, billing, roaming (between service providers) and settlement will be provided below.

[0089] MAC layer messages from the user registration agent of the end system may be used to initiate Agent Solicitation. The MAC layer messages are not shown for clarity.

[0090] In FIG. 17, the end system (mobile) initially solicits an advertisement and the foreign agent replies with an advertisement that provides the end system with information about the network to which the foreign agent belongs including a care of address of the foreign agent. Alternatively, this phase may be removed and all network advertisements may be done by a continuously emitted MAC layer beacon message. In this case, the network is assumed to be a foreign wireless service provider. Then, a user registration agent (in the end system) incorporates the information about the foreign agent (including the user name and other security credentials) and its network into a request and sends the request to the foreign agent. The foreign agent, as a proxy registration agent, relays the request to the foreign registration server (i.e., the registration server for the foreign wireless service provider. Then, the foreign registration server, recognizing that it is not the home directory, accesses the foreign directory server with the FDD in the foreign wireless service provider to learn how to direct the registration request to the home registration server of the wireless service provider to which the end system belongs. The foreign registration server responds with the necessary forwarding information. Then, the foreign registration server encapsulates the end system's reg-

istration request in a Radius access request and relays the encapsulated request to the home registration server of the wireless service provider to which the end system belongs. The home registration server accesses the home directory server with the HDD of the home registration server to learn at least authentication information about the foreign service provider. Optionally, the home registration server accesses the subscriber's directory to learn detail subscriber service profile information (e.g., quality of service options subscribed to, etc.). When all parties are authenticated, the home registration server sends a start IWF request to the home IWF and PPP server. The home IWF and PPP server starts the home accounting server and then sends a start IWF response to the home registration server. The home registration server then sends a Radius access response to the foreign registration server. The foreign registration server then sends a start IWF request to the serving IWF server. The serving IWF server starts the serving accounting server and then sends a start IWF response to the foreign registration server. The foreign registration server sends a registration reply to the foreign agent, and the foreign agent relays the registration reply to the end system.

[0091] A link control protocol (LCP) configuration request is send by the end system through the foreign registration server to the home IWF and PPP server. The home IWF and PPP server sends an LCP configuration acknowledgment through the foreign registration server to the end system.

[0092] Similarly, a password authentication protocol (PAP) authentication request is sent to and acknowledged by the home IWF and PPP server. Alternatively, a challenge authentication protocol (CHAP) may be used to authenticate. Both protocols may be used to authenticate or this phase may be skipped.

[0093] Similarly, an IP configuration protocol (IPCP) configure request is sent to and acknowledged by the home IWF and PPP server.

[0094] The connection to the end system may be terminated because of any one of the following reasons.

1. *User initiated termination.* Under this scenario, the end system first terminates the PPP gracefully. This includes terminating the PPP network control protocol (NCP) followed by terminating the PPP link protocol. Once this is done, the end system de-registers from the network followed by termination of the radio link to the access point.

2. *Loss of wireless link.* This scenario is detected by the modem and reported to the modem driver in the end system. The upper layers of the software are notified to terminate the stacks and notify the user.

3. *Loss of connection to the foreign agent.* This scenario is detected by the mobility driver in the end

system. After trying to re-establish contact with a (potentially new) foreign agent and failing, the driver sends an appropriate notification up the protocol stack and also signals the modem hardware below to terminate the wireless link.

4. *Loss of connection to the IWF.* This is substantially the same as for loss of connection to the foreign agent.

5. *Termination of PPP by IWF or PPP server.* This scenario is detected by the PPP software in the end system. The end system's PPP driver is notified of this event. It initiates de-registration from the network followed by termination of the wireless link to the access point.

[0095] End system service configuration refers to the concept of configuring the network service for an end system based on the subscriber's service profile. The subscriber's service profile is stored in a subscriber directory. The service profile contains information to enable the software to customize wireless data service on behalf of the subscriber. This includes information to authenticate the end system, allow the end system to roam and set up connections to the end system's internet service provider. Preferably, this information also includes other parameters, like, quality of service. In addition to the subscriber directory, a home domain directory (HDD) and a foreign domain directory (FDD) are used for roaming and for authenticating the foreign and home registration servers to each other. The HDD stores information about the end system's home network and the FDD stores information about foreign networks that a subscriber may visit.

[0096] FIG. 18 shows how these directories map into the network architecture and are used during registration for an end system that is registering at home. In step 0 the end system (mobile) solicits and receives an advertisement from the foreign agent to provides the end system with information about the network to which the foreign agent belongs. In this case, the network is the home wireless service provider. In step 1, user registration agent (in the end system) incorporates the information about the foreign agent and its network and its security credentials into a request and sends the request to the foreign agent. In step 2, the foreign agent, as a proxy registration agent, relays the request to the home registration server. In step 3, the home registration server accesses the HDD of the home wireless service provider to learn at least authentication information. In step 4, the home registration server accesses the subscriber directory to learn detail subscriber service profile information (e.g., quality of service options subscribed to, etc.). In step 5, the home registration server notifies the foreign agent of the access response. In steps 6 and 7, the foreign agent notifies the end system (i.e., mobile) of the registration reply.

[0097] FIG. 19 shows directory usage for an end system that is registering from a foreign network. In step 0 the end system (mobile) solicits an advertisement and the foreign agent advertises which provides the end system with information about the network to which the foreign agent belongs. In this case, the network is a foreign wireless service provider. In step 1, user registration agent (in the end system) incorporates the information about the foreign agent and its network and its security credentials into a request and sends the request to the foreign agent. In step 2, the foreign agent, as a proxy registration agent, relays the request to the foreign registration server (i.e., the registration server for the foreign wireless service provider. In step 3, the foreign registration server accesses the HDD of foreign wireless service provider to learn the network to which the end system belongs. In step 4, the foreign registration server forwards the end system's request to the home registration server of the end system's home wireless service provider. In step 5, the home registration server accesses the FDD of the home registration server to learn at least authentication information about the foreign service provider. In step 6, the home registration server accesses the subscriber's directory to learn detail subscriber service profile information (e.g., quality of service options subscribed to, etc.). In step 7, the home registration server notifies the foreign registration server of the access response. In step 8, the foreign registration server forwards to the foreign agent the access response. In step 9, the foreign agent notifies the end system (i.e., mobile) of the registration reply.

[0098] Protocol handling scenarios for handling bearer data and the associated stacks for transporting bearer data to and from an end system, the protocol stacks for the cell architectures using local APs (FIG. 20) and remote APs (FIG. 21).

[0099] FIG. 20 shows the protocol stacks for handling communications between an end system (in its home network) and a home IWF for End System @ Home. FIG. 20 shows the protocol handling for a cell architecture where the access point and the wireless hub are co-located.

[0100] FIG. 21 shows the protocol handling for a cell architecture where the access point is located remotely from the wireless hub. As shown, PPP terminates in the IWF and the configuration provides direct internet access. The configuration for the case where the PPP server is separate from the IWF is described later.

[0101] In FIG. 21, PPP frames from the end system are encapsulated in RLP (radio link protocol) frames which are encapsulated at the remote access point in MAC frames for communicating with the trunk access point (i.e., an access point physically located near the wireless hub), the remote access point being coupled to the access point by, for example, a wireless truck). The access point functions as a MAC layer bridge and relays frames from the air link to the foreign agent in the wireless hub. The foreign agent de-encapsulates the RLP

frames out of the MAC frames, and using the *xtunnel* protocol, relays the RLP frames to the IWF. A similar, albeit reverse, process occurs for transmitting frames from the IWF to the end system.

[0102] If the end system moves to another foreign agent, then a new *xtunnel* will be automatically created between the new foreign agent and the IWF, so that PPP traffic continues to flow between them, without interruption.

[0103] In the remote AP cell architecture (FIG. 21) using wireless trunks between the remote AP and the trunk AP, the air link between the end system and the access point may operate at a different frequency (f1) and use a different radio technology as compared to the frequency (f2) and radio technology of the trunk.

[0104] FIG. 22 shows the protocol stacks for a roaming end system. The serving IWF uses the *l-xtunnel* protocol between the serving IWF and home IWF. The rest of the protocol stacks remain unchanged and are not shown. This architecture may be simplified by merging the serving IWF into the base station, thus eliminating the XWD protocol.

[0105] The RLP layer uses sequence numbers to drop duplicate PPP datagrams and provide in-sequence delivery of PPP datagrams between the end system and the IWF. It also provides a configurable keep-alive mechanism to monitor link connectivity between the end system and the IWF. Additionally, in an alternative embodiment, the RLP layer also provides re-transmission and flow control services in order to reduce the overall bit error rate of the link between the end system and the IWF. The RLP between the end system and the IWF is started at the beginning of the session and remains active throughout the session and even across hand-offs.

[0106] In contrast to the specification in the mobile IP RFC (RFC 2003), IP in IP encapsulation is not used for tunneling between the foreign agent and the home IWF. Instead a new tunneling protocol, implemented on top of UDP is used. This tunneling protocol is a simplified version of the L2TP protocol. The reasons for this choice are as follows.

1. The encapsulation protocol specified in RFC 2003 does not provide flow control or in-sequence delivery of packets. The presently described network may need these services in the tunnel over the backhaul. Flow control may be needed to reduce the amount of retransmissions over the air link because of packet loss due to flow control problems over the network between the base station and the MSC or because of flow control problems in the base station or the IWF.

2. By using a UDP based tunneling protocol, the implementation can be done at the user level and then put into the kernel for performance reasons, after it has been debugged.

3. Using RFC 2003, there is no easy way of creating tunnels taking into account quality of service and load balancing. In order to take QOS into account, it should be possible to set up tunnels over links that already provide the required QOS. Secondly, using RFC 2003, there is no easy way to provide load balancing to distribute bearer traffic load over multiple links between the base station and the MSC.

4. In order to implement IP in IP encapsulation as specified in RFC 2003, developers require access to IP source code. In commercial operating systems, source code for the TCP/IP stack is generally proprietary to other equipment manufacturers. Purchasing the TCP/IP stack from a vendor and making changes to the IP layer to support mobile IP tunneling would require a developer to continue supporting a variant version of the TCP/IP stack. This adds cost and risk.

[0107] While it is noted that the tunneling protocol between the base station and the IWF is non-standard and that the wireless service provider will not be able to mix and match equipment from different vendors, the use of a non-standard tunneling protocol within a single wireless service provider network is transparent to end systems and equipment from other vendors.

[0108] The new tunneling protocol is based on L2TP. By itself, L2TP is a heavyweight tunneling protocol so that L2TP has a lot of overhead associated with tunnel creation and authentication. The new tunneling protocol of the present invention has less overhead. The new *xtunnel* and *l-x* tunnel protocol may have the following features.

1. The *xtunnel* and *l-x* tunnel creation adds vendor specific extensions to Radius Access Request and Radius Access Response messages between the base station and the registration server. These extensions negotiate tunnel parameters and to create the tunnel.

2. The registration server is able to delegate the actual work of tunneling and relaying packets to a different IP address, and therefore, to a different server in the MSC. This permits the registration server to do load balancing across multiple IWF servers and to provide different QOS to various users.

3. The *xtunnel* and *l-x* tunnel protocol supports in-band control messages for tunnel management. These messages include echo request/response to test tunnel connectivity, disconnect request/response/notify to disconnect the tunnel and error notify for error notifications. These messages are sent over the tunneling media, for example, UDP/IP.

4. The *xtunnel* and *l-x* tunnel protocol sends pay-

load data over the tunneling media, for example, UDP/IP. The *xtunnel* I-X tunnel protocol supports flow control and in-sequence packet delivery.

5. The *xtunnel* and I-X tunnel protocol may be implemented over media other than UDP/IP for quality of service.

[0109] The network supports direct internet connectivity by terminating the PPP in the home IWF and routing IP packets from the IWF to the internet via a router using standard IP routing techniques. Preferably, the IWF runs RIP, and the router also runs RIP and possibly other routing protocols like OSPF.

[0110] The network supports a first configuration for a wireless service provider who is also an internet service provider. In this configuration, the home IWF in the MSC also functions as a PPP server. This IWF also runs internet routing protocols like RIP and uses a router to connect to the internet service provider's backbone network.

[0111] The network supports a second configuration for a wireless service provider who wishes to allow end systems to connect to one or more internet service providers, either because the WSP itself is not ISPs, or because the WSP has agreements with other ISPs to provide access to end users. For example, a wireless service provider may elect to offer network access to an end user and may have an agreement with a 3rd party ISP to allow the user who also has an account with the 3rd party ISP to access the ISP from the WSP network. In this configuration, the PPP server does not run in the home IWF installed at the MSC. Instead, a tunneling protocol like L2TP (Layer Two Tunneling Protocol) is used to tunnel back to the ISP's PPP server. FIG. 10 shows the protocol stacks for this configuration for an end system that is at home.

[0112] The location of the home IWF and the ISP PPP server remains fixed throughout the PPP session. Also, the L2TP tunnel between the IWF and the ISP's PPP server remains up throughout the PPP session. The physical link between the IWF and the PPP server is via a router using a dedicated T1 or T3 or frame relay or ATM network. The actual nature of the physical link is not important from the point of view of the architecture.

[0113] This configuration also supports intranet access. For intranet access, the PPP server resides in the corporate intranet and the home IWF uses L2TP to tunnel to it.

[0114] For a fixed end system, the protocol handling for intranet or ISP access is as shown in FIG. 23 with the difference that the roaming end system uses a serving IWF to connect to its home IWF. The protocol handling between a serving IWF and a home IWF has been described earlier. In Figure 23, the home IWF may be merged into the wireless hub eliminating the X-tunnel protocol. Also, the serving IWF may be merged into the wireless hub, thus eliminating the X-tunnel protocol.

[0115] FIG. 24 shows the protocol stacks used during the registration phase (end system registration) for a local AP cell architecture. The stack for a remote AP cell architecture is very similar.

[0116] The scenario shown above is for a roaming end system. For an end system at home, there is no foreign registration server in the registration path.

[0117] Note the mobility agent in the end system. The mobility agent in the end system and foreign agent in the wireless hub are conceptually similar to the mobile IP RFC 2002. The mobility agent handles network errors using time-outs and re-tries. Unlike the known protocol stacks for bearer data, RLP is not used. The foreign agent and the registration servers use Radius over UDP/IP to communicate with each other for registering the end system.

[0118] Several aspects of security must be considered. The first, authenticating the identities of the end system and the foreign/home networks during the wireless registration phase. Second, authenticating the identity of the end system with its PPP server during the PPP authentication phase. Third, authentication for storing accounting data, for billing and for updating home domain information. Fourth, encryption of bearer traffic transmitted to and from the end system. Fifth, encryption for exchanging billing information across service provider boundaries.

[0119] Shared secrets are used to authenticate the identity of end systems with their home networks and the identity of the home and foreign networks with each other during wireless registration.

[0120] End system authentication uses a 128-bit shared secret to create an authenticator for its registration request. The authenticator is created using the known MD5 message digest algorithm as described in the mobile IP RFC 2002. Alternatively, a different algorithm may be used. The shared secret is not sent in the registration request by the end system. Only the authenticator is sent. On receiving the registration request from the end system, the home registration server re-computes the authenticator over the registration request data using the shared secret. If the computed authenticator value matches the authenticator value sent by the end system, the home registration server allows the registration process to proceed. If the values do not match, the home registration server logs the event, generates a security violation alarm and a nak (i.e., a negative acknowledgment) to the request.

[0121] In the registration reply, the home registration server does the same - that is to say, uses the shared secret to create an authenticator for the registration reply that it sends to the end system. Upon receiving the reply, the end system re-computes the authenticator using the shared secret. If the computed value does not match the authenticator value sent by the home registration server in the reply, the end system discards the reply and tries again.

[0122] These network security concepts are similar to

the concepts defined in mobile IP RFC 2002. According to the RFC, a mobility security association exist between each end system and its home network. Each mobility security association defines a collection of security contexts. Each security context defines an authentication algorithm, a mode, a secret (shared or public-private), style of replay protection and the type of encryption to use. In the context of the present network, the end system's User-Name (in lieu of the mobile IP home address) is used to identify the mobility security association between the end system and its home network. Another parameter, called the security parameter index (SPI), is used to select a security context within the mobility security association. In a basic embodiment of the invention, only the default mobile IP authentication algorithm (keyed-MD5) and the default mode ("prefix+suffix") are supported with 128-bit shared secrets. Network users are allowed to define multiple shared secrets with their home networks. The mechanism for creating security contexts for end users, assigning an SPI to each security context and for setting the contents of the security context (which includes the shared secret) and for modifying then contents are described below. During registration, a 128-bit message digest is computed by the end system in prefix+suffix mode using the MD5 algorithm. The shared secret is used as the prefix and the suffix for the data to be protected in the registration request. The authenticator thus computed, along with the SPI and the User-Name are transmitted in the registration request by the end system. Upon receiving the end system's registration request, the foreign registration server relays the request along with the authenticator and the SPI, unchanged to the home registration server. Upon receiving the registration request directly from the end system or indirectly via a foreign registration server, the home registration server uses the SPI and the User-Name to select the security context. The home server re-computes the authenticator using the shared secret. If the computed authenticator value matches the value of the authenticator sent in the request by the end system, the user's identity will have been successfully authenticated. Otherwise, the home registration server naks (negatively acknowledges) the registration request sent by the end system.

[0123] The registration reply sent by the home registration server to the end system is also authenticated using the algorithm described above. The SPI and the computed authenticator value is transmitted in the registration reply message by the home server to the end system. Upon receiving the reply, the end system re-computes the authenticator, and if the computed value does not match the transmitted value, it will discard the reply and retry.

[0124] The user's end system has to be configured with the shared secret and SPIs for all security contexts that the user shares with its registration server(s). This configuration information is preferably stored in a Win 95 registry for Windows 95 based end systems. During

registration, this information is accessed and used for authentication purposes.

[0125] In the network, Radius protocols are used by foreign agent FA to register the end system and to configure the *xtunnel* between the wireless hub and the home and serving IWFs on behalf of the end system. On receiving a registration request from the end system, the FA creates a Radius Access-Request packet, stores its own attributes into the packet, copies the end system's registration request attributes unchanged into this packet and sends the combined request to the registration server in the MSC.

[0126] Radius authentication requires that the Radius client (in this case, the FA in the base station) and the Radius server (in this case, the registration server in the MSC) share a secret for authentication purposes. This shared secret is also used to encrypt any private information communicated between the Radius client and the Radius server. The shared secret is a configurable parameter. The network follows the recommendations in the Radius RFC and uses the shared secret and the MD5 algorithm for authentication and for encryption, where encryption is needed. The Radius-Access-Request packet sent by the FA contains a Radius User-Name attribute (which is provided by the end system) and a Radius User-Password attribute. The value of the User-Password attribute is also a configurable value and encrypted in the way recommended by the Radius protocol. Other network specific attributes, which are non-standard attributes from the point of view of the Radius RFC standards, are encoded as vendor specific Radius attributes and sent in the Access-Request packet.

[0127] The following attributes are sent by the FA to its registration server in the Radius Access-Request packet.

1. *User-Name Attribute*. This is the end system's user-name as supplied by the end system in its registration request.
2. *User-Password Attribute*. This user password is supplied by the base station/wireless hub on behalf of the user. It is encoded as described in the Radius RFC using the secret shared between the base station and its registration server.
3. *NAS-Port*. This is the port on the base station.
4. *NAS-IP-Address*. This is the IP address of the base station.
5. *Service-Type*. This is framed service.
6. *Framed Protocol*. This is a PPP protocol.
7. *Xtunnel Protocol Parameters*. These parameters are sent by the base station to specify the param-

ters necessary to setup the *xtunnel* protocol on behalf of the end system. This is a vendor-specific attribute.

8. *AP-IP-Address*. This is the IP address of the AP through which the user is registering. This is a vendor-specific attribute.

9. *AP-MAC-Address*. This is the MAC address of the AP through which the user is registering. This is a vendor-specific attribute.

10. *End system's Registration Request*. The registration request from the end system is copied unchanged into this vendor specific attribute.

[0128] The following attributes are sent to the FA from the registration server in the Radius Access-Response packet.

1. *Service Type*. This is a framed service.

2. *Framed-Protocol*. This is a PPP.

3. *Xtunnel Protocol Parameters*. These parameters are sent by the registration server to specify the parameters necessary to setup the *xtunnel* protocol on behalf of the end system. This is a vendor-specific attribute.

4. *Home Registration Server's Registration Reply*. This attribute is sent to the FA from the home registration server. The FA relays this attribute unchanged to the end system in a registration reply packet. If there is a foreign registration server in the path, this attribute is relayed by it to the FA unchanged. It is coded as a vendor-specific attribute.

[0129] To provide service to roaming end systems, the foreign network and the home network are authenticated to each other for accounting and billing purposes using the Radius protocol for authentication and configuration. This authentication is performed at the time of end system registration. As described earlier, when the registration server in the foreign network receives a registration request from an end system (encapsulated as a vendor specific attribute in a Radius-Access Request packet by the FA), it uses the end system's User-Name to determine the identity of the end system's home registration server by consulting its home domain directory HDD. The following information is stored in home domain directory HDD and accessed by the foreign registration server in order to forward the end system's registration request.

1. *Home Registration Server IP Address*. This is the IP address of the home registration server to forward the registration request.

2. *Foreign Registration Server Machine Id*. This is the machine ID of the foreign registration server in SMTP (simplified mail transfer protocol) format (e.g., machine@fqdn where machine is the name of the foreign registration server machine and fqdn is the fully qualified domain name of the foreign registration server's domain).

3. *Tunneling Protocol Parameters*. These are parameters for configuring the tunnel between the serving IWF and the home IWF on behalf of the end system. These include the tunneling protocol to be used between them and the parameters for configuring the tunnel.

4. *Shared Secret*. This is the shared secret to be used for authentication between the foreign registration server and the home registration server. This secret is used for computing the Radius User-Password attribute in the Radius packet sent by the foreign registration server to the home registration server. It is defined between the two wireless service providers.

5. *User-Password*. This is the user password to be used on behalf of the roaming end system. This user password is defined between the two wireless service providers. This password is encrypted using the shared secret as described in the Radius RFC.

6. *Accounting Parameters*. These are parameters for configuring accounting on behalf of the end system that is registering. These parameters are sent by the registration server to its IWF for configuring accounting on behalf of the end system.

[0130] Using this information, the foreign registration server creates a Radius Access-Request, adds its own registration and authentication information into the Radius Access-Request, copies the registration information sent by the end system unchanged into the Radius Access-Request and sends the combined request to the home registration server.

[0131] Upon receiving the Radius-Access Request from the foreign registration server (for a roaming end system) or directly from the FA (for an end system at home), the home registration server consults its own directory server for the shared secrets to verify the identity of the end system and the identity of the foreign registration server in a roaming scenario by re-computing authenticators.

[0132] After processing the request successfully, the home registration server creates a Radius Access-Accept response packet and sends it to the foreign registration server if the end system is roaming, or directly to the FA from which it received the Radius Access-Request. The response contains the registration reply attribute that the FA relays to the end system.

[0133] If the request can not be processed successfully, the home registration server creates a Radius Access-Reject response packet and sends it to the foreign registration server if the end system is roaming, or directly to the FA from which it received the Radius Access-Request. The response contains the registration reply attribute that the FA will relay to the end system.

[0134] In a roaming scenario, the response from the home registration server is received by the foreign registration server. It is authenticated by the foreign registration server using the shared secret. After authenticating, the foreign registration server processes the response, and in turn it generates a Radius response packet (Accept or Reject) to send to the FA. The foreign registration server copies the registration reply attribute from the home registration server's Radius response packet, unchanged, into its Radius response packet.

[0135] When the FA receives the Radius Access-Response or Radius Access-Reject response packet, it creates a registration reply packet using the registration reply attributes from the Radius response, and sends the reply to the end system, thus completing the round trip registration sequence.

[0136] Mobile IP standards specifies that replay protection for registrations are implemented using time stamps, or optionally, using nonces. However, since replay protection using time stamps requires adequately synchronized time-of-day clocks between the corresponding nodes, the present invention implements replay protection during registration, using nonces even though replay protection using time stamps is mandatory in the Mobile IP standards and the use nonces is optional. However, replay protection using time stamps as an alternative embodiment is envisioned.

[0137] The style of replay protection used between nodes is stored in the security context in addition to the authentication context, mode, secret and type of encryption.

[0138] The network supports the use of PPP PAP (password authentication) and CHAP (challenge authenticated password) between the end system and its PPP server. This is done independently of the registration and authentication mechanisms described earlier. This allows a private intranet or an ISP to independently verify the identity of the user.

[0139] Authentication for accounting and directory services is described below with respect to accounting security. Access to directory servers from network equipment in the same MSC need not be authenticated.

[0140] The network supports encryption of bearer data sent between the end system and the home IWF. End systems negotiate encryption to be on or off by selecting the appropriate security context. Upon receiving the registration request, the home registration server grants the end system's request for encryption based upon the security context. In addition to storing the authentication algorithm, mode, shared secret and style of replay protection, the security context is also used to specify the

style of encryption algorithm to use. If encryption is negotiated between the end system and the home agent, then the complete PPP frame is so encrypted before encapsulation in RLP.

[0141] The IWF, the accounting server and the billing system are part of the same trusted domain in the MSC. These entities are either connected on the same LAN or part of a trusted intranet owned and operated by the wireless service provider. Transfer of accounting statistics between the IWF and the accounting server and between the accounting server and the customer's billing system need not be encrypted using Internet IP security protocols like IP-Sec.

[0142] The network makes it more difficult to monitor the location of the end system because it appears that all PPP frames going to and from the end system go through the home IWF regardless of the actual location of the end system device.

[0143] Accounting data is collected by the serving IWF and the home IWF in the network. Accounting data collected by the serving IWF is sent to an accounting server in the serving IWF's MSC. Accounting data collected by the home IWF is sent to an accounting server in the home IWF's MSC. The accounting data collected by the serving IWF is used by the foreign wireless service provider for auditing and for settlement of bills across wireless service provider boundaries (to support roaming and mobility). The accounting data collected by the home IWF is used for billing the end user and also for settlement across wireless service provider boundaries to handle roaming and mobility.

[0144] Since all data traffic flows through the home IWF, regardless of the end system's location and the foreign agent's location, the home IWF has all the information to generate bills for the customer and also settlement information for the use of foreign networks.

[0145] The serving IWF and the home IWF preferably use the Radius accounting protocol for sending accounting records for registered end systems. The Radius accounting protocol is as documented in a draft IETF RFC. For the present invention, the protocol has to be extended by adding vendor specific attributes for the network and by adding check-pointing to the Radius Accounting protocol. Check-pointing in this context refers to the periodic updating of accounting data to minimize risk of loss of accounting records.

[0146] The Radius accounting protocol runs over UDP/IP and uses re-trys based on acknowledgment and time outs. The Radius accounting client (serving IWFs or home IWFs) send UDP accounting request packets to their accounting servers which send acknowledgments back to the accounting clients.

[0147] In the network, the accounting clients (serving IWF and the home IWF) emit an accounting start indication at the start of the user's session and an accounting stop indication at the end of the user's session. In the middle of the session, the accounting clients emit accounting checkpoint indications. In contrast, the Ra-

dius accounting RFC does not specify an accounting checkpoint indication. The software of the present invention creates a vendor specific accounting attribute for this purpose. This accounting attribute is present in all Radius Accounting-Request packets which have Acct-Status-Type of Start (accounting start indications). The value of this attribute is used to convey to the accounting server whether the accounting record is a check-pointing record or not. Check-pointing accounting reports have a time attribute and contain cumulative accounting data from the start of the session. The frequency of transmitting check-point packets is configurable in the present invention.

[0148] The serving IWF and the home IWF are configured by their respective registration servers for connecting to their accounting servers during the registration phase. The configurable accounting parameters include the IP address and UDP port of the accounting server, the frequency of check-pointing, the session/multi-session id and the shared secret to be used between the accounting client and the accounting server.

[0149] The network records the following accounting attributes for each registered end system. These accounting attributes are reported in Radius accounting packets at the start of the session, at the end of the session and in the middle (check-point) by accounting clients to their accounting servers.

1. *User Name*. This is like the Radius User-Name attribute discussed above. This attribute is used to identify the user and is present in all accounting reports. The format is "user@domain" where domain is the fully qualified domain name of the user's home.

2. *NAS IP Address*. This is like the Radius NAS-IP-Address attribute discussed above. This attribute is used to identify the IP address of the machine running the home IWF or the serving IWF.

3. *Radio Port*. This attribute identifies the radio port on the access point providing service to the user. This attribute is encoded as a vendor specific attribute.

4. *Access Point IP Address*. This attribute identifies the IP address of the access point providing service to the user. This attribute is encoded as a vendor specific attribute.

5. *Service Type*. This is like the Radius Service-Type attribute described above. The value of this attribute is Framed.

6. *Framed Protocol*. This is like the Radius Framed-Protocol attribute described above. The value of this attribute is set to indicate PPP.

7. *Accounting Status Type*. This is like the Radius Acct-Status-Type attribute described above. The value of this attribute may be Start to mark the start of a user's session with the Radius client and Stop to mark the end of the user's session with the Radius client. For accounting clients, the Acct-Status-Type/Start attribute is generated when the end system registers. The Acct-Status-type/Stop attribute is generated when the end system de-registers for any reason. For checkpoints, the value of this attribute is also Start and the *Accounting Checkpoint* attribute is also present.

8. *Accounting Session Id*. This is like the Radius Acct-Session-Id described above. In a roaming scenario, this session id is assigned by the foreign registration server when the end system issues a registration request. It is communicated to the home registration server by the foreign registration server during the registration sequence. The home network and the foreign network both know the Acct-Session-Id attribute and are able to emit this attribute while sending accounting records to their respective accounting servers. In a "end system-at-home" scenario, this attribute is generated by the home registration server. The registration server communicates the value of this attribute to the IWF which emits it in all accounting records.

9. *Accounting Multi-Session Id*. This is like the Radius Acct-Multi-Session-Id discussed above. This id is assigned by the home registration server when a registration request is received from a FA directly or via a foreign registration server on behalf of an end system. It is communicated to the foreign registration server by the home registration server in the registration reply message. The registration server(s) communicates the value of this attribute to the IWF(s) which emit it in all accounting records.

[0150] With true mobility added to the architecture, the id is used to relate together the accounting records from different IWFs for the same end system if the end system moves from one IWF to another. For hand-offs across IWF boundaries, the Acct-Session-Id is different for accounting records emanating from different IWFs. However, the Acct-Multi-Session-Id attribute is the same for accounting records emitted by all IWFs that have provided service to the user. Since the session id and the multi-session id are known to both the foreign network and the home network, they are able to emit these attributes in accounting reports to their respective accounting servers. With the session id and the multi-session id, billing systems are able to correlate accounting records across IWF boundaries in the same wireless service provider and even across wireless service provider boundaries.

1. *Accounting Delay Time*. See Radius Acct-Delay-Time attribute.

2. *Accounting Input Octets*. See Radius Acct-Input-Octets. This attribute is used to keep track of the number of octets sent by the end system (input to the network from the end system). This count is used to track the PPP frames only. The air link overhead, or any overhead imposed by RLP, etc. and is not counted.

3. *Accounting Output Octets*. See Radius Acct-Output-Octets. This attribute is used to keep track of the number of octets sent to the end system (output from the network to the end system). This count is used to track the PPP frames only. The air link overhead, or any overhead imposed by RLP, etc. and is not counted.

4. *Accounting Authentic*. See Radius Acct-Authentic attribute. The value of this attribute is Local or Remote depending on whether the serving IWF or the home IWF generates the accounting record.

5. *Accounting Session Time*. See Radius Acct-Session-Time attribute. This attribute indicates the amount of time that the user has been receiving service. If sent by the serving IWF, this attribute tracks the amount of time that the user has been receiving service from that serving IWF. If sent by the home IWF, this attribute tracks the amount of time that the user has been receiving service from the home IWF.

6. *Accounting Input Packets*. See Radius Acct-Input-Packets attribute. 3. This attribute indicates the number of packets received from the end system. For a serving IWF, this attribute tracks the number of PPP frames input into the serving IWF from an end system. For a home IWF, this attribute tracks the number of PPP frames input into the home IWF from an end system.

7. *Accounting Output Packets*. See Radius Acct-Output-Packets attribute. This attribute indicates the number of packets sent to the end system. For a serving IWF, this attribute tracks the number of PPP frames output by the serving IWF to the end system. For a home IWF, this attribute tracks the number of PPP frames sent to the end system from the home IWF.

8. *Accounting Terminate Cause*. See Radius Acct-Terminate-Cause attribute. This attribute indicates the reason why a user session was terminated. In addition, a specific cause code is also present to provide additional details. This attribute is only present in accounting reports at the end of the ses-

sion.

9. *Network Accounting Terminate Cause*. This attribute indicates a detailed reason for terminating a session. This specific attribute is encoded as a vendor specific attribute and is only reported in a Radius Accounting attribute at the end of session The standard Radius attribute Acct-Terminate-Cause is also present. This attribute provides specific cause codes, not covered by the Acct-Terminate-Cause attribute.

10. *Network Air link Access Protocol*. This attribute indicates the air link access protocol used by the end system. This attribute is encoded as a vendor specific attribute.

11. *Network Backhaul Access Protocol*. This attribute indicates the backhaul access protocol used by the access point to ferry data to and from the end system. This attribute is encoded as a vendor specific attribute.

12. *Network Agent Machine Name*. This attribute is the fully qualified domain name of the machine running the home IWF or the serving IWF. This specific attribute is encoded in vendor specific format.

13. *Network Accounting Check-point*. Since the Radius accounting RFC does not define a check-point packet, the present network embodiment uses a Radius accounting start packet with this attribute to mark a check-point. The absence of a check-point attribute means a conventional accounting start packet. The presence of this attribute in an accounting start packet means a accounting check-point packet. Accounting stop packets do not have this attribute.

[0151] In the preferred embodiment, every accounting packet and the corresponding reply must be authenticated using MD5 and a shared secret. The IWFs are configured with a shared secret that are used by them for authentication during communication with their Radius accounting server. The shared secrets used by the IWFs for communicating with accounting servers are stored in the home/foreign domain directory located in the MSC. The shared secrets for accounting security are communicated to the IWFs by their registration servers during the end system registration sequence.

[0152] The accounting server software runs in a computer located in the MSC. The role of the accounting server in the system is to collect raw accounting data from the network elements (the home and the serving IWFs), process the data and store it for transfer to the wireless service provider's billing system. The accounting server does not include a billing system. Instead, it includes support for an automatic or manual accounting

data transfer mechanism. Using the automatic accounting data transfer mechanism, the accounting server transfers accounting records in AMA billing format to the customer's billing System over a TCP/IP transport. For this purpose, the system defines AMA billing record formats for packer data. Using the manual transfer mechanism, customers are able to build a tape to transfer accounting records to their billing system. In order to build the tape to their specifications, customers are provided with information to access accounting records so that they may process them before writing them to tape.

[0153] In FIG. 25, the raw accounting data received by the accounting server from the home or serving IWFs are processed and stored by the accounting server. The processing done by the accounting server includes filtering, compression and correlation of the raw accounting data received from the IWF. A high availability file server using dual active/standby processors and hot swappable RAID disks is used for buffering the accounting data while it is transiting through the accounting server.

[0154] The accounting server delays processing of the raw accounting data until an end system has terminated its session. When an end system terminates its session, the accounting server processes the raw accounting data that it has collected for the session and stores an accounting summary record in a SQL database. The accounting summary record stored in the SQL data base points to an ASN.1 encoded file. This file contains detailed accounting information about the end system's session. The data stored in the accounting server is then transferred by the billing data transfer agent to the customer's billing system. Alternatively, the wireless service provider may transfer the accounting data from the SQL database and/or the ASN.1 encoded file to the billing system via a tape. The data base scheme and the format of the ASN.1 encoded file are documented and made available to customers for this purpose. If the volume of processed accounting data stored in the accounting system exceeds a high water mark, the accounting server generates an NMS alarm. This alarm is cleared when the volume of data stored in the accounting server falls below a low water mark. The high and low water marks for generating and clearing the alarm are configurable. The accounting server also generates an NMS alarm if the age of the stored accounting data exceeds a configurable threshold. Conversely, the alarm is cleared, when the age of the accounting data falls below the threshold.

[0155] The subscriber directory is used to store information about subscribers and is located in the home network. The home registration server consults this directory during the registration phase to authenticate and register an end system. For each subscriber, the subscriber directory stores the following information.

1. *User-Name*. This field in the subscriber record will be in SMTP format (e.g., *user@fqdn*) where the

user sub-field will identify the subscriber in his or her wireless home domain and the *fqdn* sub-field will identify the wireless home domain of the subscriber. This field is sent by the end system in its registration request during the registration phase. This field is assigned by the wireless service provider to the subscriber at the time of subscription to the network service. This field is different than the user name field used in PPP.

2. *Mobility Security Association*. This field in the subscriber record contains the mobility security association between the subscriber and his or her home network. As described above, a mobility security association exists between each subscriber and its home registration server. The mobility security association defines a collection of security contexts. Each security context defines an authentication algorithm, an authentication mode, a shared secret, style of replay protection and the type of encryption (including no encryption) to use between the end system and its home server. During registration, the home registration server retrieves information about the subscriber's security context from the subscriber directory using the *User-Name* and the *security parameter index (SPI)* supplied by the end system in its registration request. The information in the security context is used for enforcing authentication, encryption and replay protection during the session. The mobility security association is created by the wireless service provider at the time of subscription. It is up to the wireless service provider to permit the subscriber to modify this association either by calling up a customer service representative or by letting subscribers access to a secure Web site. The Web site software will export web pages which the wireless service provider may make accessible to subscribers from a secure web server. In this way, subscribers are able to view/modify the contents of the mobility security association in addition to other subscriber information that the service provider may make accessible.

3. *Modem MAC Address*. This field contains the MAC address of the modem owned by the subscriber. In addition to the shared secret, this field is used during registration to authenticate the user. It is possible to turn off MAC address based authentication on a per user basis. The MAC address is communicated to the home registration server during registration.

4. *Enable MAC Address Authentication*. This field is used to determine if MAC address based authentication is *enabled* or *disabled*. If *enabled*, the home registration server checks the MAC address of the registering end system against this field to validate the end system's identity. If *disabled*, then no check-

ing is done.

5. *Roaming Enabled Flag*. If this field is set to *enabled*, then the end system is allowed to roam to foreign networks. If this field is *disabled*, then the end system is not permitted to roam to foreign networks.

6. *Roaming Domain List*. This field is meaningful only if the *Roaming Enabled Flag* is set to *enabled*. This field contains a list of foreign domains that the end system is allowed to roam to. When the contents of this list is null and the *Roaming Enabled Flag* is set to *enabled*, the end system is allowed to roam freely.

7. *Service Enable/Disable Flag*. This field may be set to *disabled* by the system administrator to disable service to a subscriber. If this field is disabled, then the subscriber is not permitted to register for service. If the subscriber is registered and the value of this field is set to disabled, then the subscriber's end system is immediately disconnected by the network.

8. *Internet Service Provider Association*. This field contains information about the subscriber's internet service provider. This information is used by the IWF during the PPP registration phase to perform authentication with the internet service provider on behalf of the end system and also to create a L2TP tunnel between the IWF and the internet service provider's PPP server. This field contains the identity of the subscriber's ISP. The IWF uses this information to access the ISP directory for performing authentication and setting up the L2TP tunnel on behalf of the end system.

9. *Subscriber's Name & Address Information*. This field contains the subscriber's name, address, phone, fax, e-mail address, etc.

[0156] The home domain directory (HDD) is used by the registration server to retrieve parameters about the end system to complete registration on behalf of the end system. Using this information, the registration server determines if the end system is registering at home or if the end system is a roaming end system. In the former case, the registration server assumes the role of a home registration server and proceed with end system registration. In the latter case, the registration server assumes the role of a foreign registration server and, acting as a Radius proxy, it forwards the request to the real home registration server whose identity it gets from this directory. For roaming end system, the parameters stored in the HDD include the IP address of the home registration server, the home-foreign shared secret, the home-serving IWF tunnel configuration etc. The HDD is located in the MSC.

[0157] The following information is stored in the HDD.

1. *Home Domain Name*. This field is used as the key to search the HDD for an entry that matches the fully qualified home domain name provided by the end system in its registration request.

2. *Proxy Registration Request*. This field is used by the registration server to determine if it should act as a foreign registration server and proxy the end system's registration request to the real home registration server.

3. *Home Registration Server DNS Name*. If the *proxy registration request* flag is TRUE, this field is used to access the DNS name of the real home registration server. Otherwise, this field is ignored. The DNS name is translated to an IP address by the foreign registration server. The foreign registration server uses the IP address to relay the end system's registration request.

4. *Foreign Domain Name*. If the *proxy registration request* flag is TRUE, this field is used to identify the foreign domain name to the end system's home registration server. Otherwise, this field is ignored. The foreign registration server uses this information to create the foreign server machine id in SMTP format, for example, *machine@fqdn*. This machine id is sent to the home registration server by the foreign registration server in the Radius-Access Request.

5. *Shared Secret*. If the *proxy registration request* flag is TRUE, the shared secret is used between the foreign and home registration servers to authenticate their identity with each other. Otherwise this field is ignored.

6. *Tunneling Protocol Parameters*. This field is used to store parameters to configure the tunnels to provide service to the end system. For an end system at home, this includes information on tunnel parameters between the base station and the home IWF and from the home IWF to the PPP server. For a roaming end system, this includes tunneling parameters from the base station to the serving IWF and from the serving IWF to the home IWF. At a minimum, for each tunnel, this field contains the type of tunneling protocol to use and any tunneling protocol specific parameters. For example, this field may contain the identifier for the tunneling protocol L2TP and any additional parameters required to configure the L2TP tunnel between the IWF and its peer.

7. *Accounting Server Association*. This field is used to store information needed by the IWF to generate accounting data on behalf of the end system. It contains the name of the accounting protocol (e.g. RA-

DIUS), the DNS name of the accounting server and additional parameters specific to the accounting protocol like the UDP port number, the shared secret that the IWF must use in the Radius Accounting protocol, the frequency of check-pointing, the seed for creating the session/multi-session id, etc. The accounting server's DNS name is translated to the accounting server's IP address, which is sent to the IWF.

[0158] For wireless service providers that have roaming agreements with each other, the HDD is used for authentication and to complete the registration process. If an end system roams from its home network to a foreign network, the foreign registration server in that network consults the HDD in its MSC to get information about the visiting end system's home registration and to authenticate the home network before it provides service to the visiting end system.

[0159] The software for home domain directory management preferably provides a graphical user interface (GUI) based HDD management interface for system administrators. Using this GUI, system administrators are able to view and update entries in the HDD. This GUI is not intended for use by foreign wireless network service providers to perform remote updates based on roaming agreements. It is only intended for use by trusted personnel of the home wireless service provider operating behind fire walls.

[0160] The foreign domain directory (FDD) provides functionality that is the reverse of the home domain directory. The FDD is used by the home registration server to retrieve parameters about The foreign registration server and the foreign network in order to authenticate the foreign network and create a tunnel between a serving IWF and a home IWF. These parameters include the home-foreign shared secret, the home IWF-serving IWF tunnel configuration, etc. The FDD is preferably located in the home registration server's MSC. The FDD is used by home registration servers for registering roaming end systems.

[0161] The following information will be stored in the FDD.

1. *Foreign Domain Name.* This field is used as the key to search the FDD for an entry that matches the fully qualified domain name of the foreign registration server relaying the registration request.

2. *Shared Secret.* This is the shared secret used between the foreign and home registration servers to authenticate their identity mutually with each other.

3. *Home IWF-Serving IWF Tunneling Protocol Parameters.* This field is used to store parameters to configure the tunnel between the home IWF and the serving IWF. At a minimum, this field contains the

type of tunneling protocol to use and any tunneling protocol specific parameters. For example, this field may contain the identifier for the tunneling protocol L2TP and any additional parameters required to configure the L2TP tunnel between the serving IWF and the home IWF.

4. *Accounting Server Association.* This field is used to store information needed by the home IWF to generate accounting data on behalf of the end system. It contains the name of the accounting protocol (e.g. RADIUS), the DNS name of the accounting server and additional parameters specific to the accounting protocol like the UDP port number, the shared secret that the IWF must use in the Radius Accounting protocol, the frequency of check-pointing, the seed for creating the session/multi-session id, etc. The accounting server's DNS name is translated to the accounting server's IP address, which is sent to the foreign agent.

[0162] For wireless service providers that have roaming agreements with each other, the FDD is used to do authentication and complete the registration process. If an end system roams from its home network to a foreign network, the registration server in the home network consults the FDD in its MSC to get information and authenticate the foreign network providing service to the end system.

[0163] The foreign domain directory management software provides a graphical user interface (GUI) based FDD management interface for system administrators. Using this GUI, system administrators are able to view and update entries in the FDD. This GUI is not intended for use by foreign wireless network service providers to perform remote updates based on roaming agreements. It is only intended for use by trusted personnel of the home wireless service provider operating behind firewalls.

[0164] The internet service provider directory (ISPD) is used by the home IWF to manage connectivity with ISPs that have service agreements with the wireless service provider so that subscribers may access their ISPs using the network. For each subscriber, the subscriber directory has an entry for the subscriber's ISP. This field points to an entry in the ISPD. The home IWF uses this information to set up the connection to the ISP on behalf of the subscriber.

[0165] The network architecture supports roaming. In order for roaming to work between wireless service providers, the architecture must support the setting up of roaming agreements between wireless service providers. This implies two things: (1) updating system directories across wireless service providers and (2) settlement of bills between service providers.

[0166] In order to allow subscribers access to internet service providers, the architecture supports roaming agreements with internet service providers. This implies

that the architecture must be able to send data to and receive data from ISP PPP servers (i.e., that support industry standard protocols like PPP, L2TP and Radius). It also implies that the architecture handles directory updates for ISP access and settlement of bills with ISPs.

[0167] When roaming agreements are established between two wireless service providers, both providers have to update their home and foreign domain directories in order to support authentication and registration functions for end systems visiting their networks from the other network. At a minimum, the architecture of the present embodiment supports manual directory updates. When a roaming agreement is established between two wireless service providers, then the two parties to the agreement exchange information for populating their home and foreign domain directories. The actual updates of the directories is done manually by the personnel of the respective service providers. If later, the information in the home and foreign domain directories needs to be updated, the two parties to the agreement exchange the updated information and then manually apply their updates to the directories.

[0168] In an alternative embodiment, the directory management software incorporates developing standards in the IETF to enable roaming between internet service providers and to enable ISPs to automatically manage and discover roaming relationships. This makes annual directory management no longer necessary. The network system automatically propagates roaming relationships, and discovers them, to authenticate and register visiting end systems.

[0169] At a minimum, the network architecture just processes and stores the accounting data and makes the data available to the wireless service provider's billing system. It is up to the billing system to handle settlement of bills for roaming.

[0170] In an alternative embodiment, developing standards in the IETF to handle distribution of accounting records between internet service providers are incorporated into the network architecture to enable ISPs to do billing settlement for roaming end systems.

[0171] The system software supports access to ISPs and private intranets by supporting L2TP between the home IWF and the ISPs or intranet PPP server. The internet service provider directory contains information useful to the IWF for creating these tunnels. As access agreements between the wireless service provider and internet service providers are put in place, this directory is updated manually by the wireless service provider's personnel. Automatic updates and discovery of access relationships between the wireless service provider and internet service providers are presently contemplated and implemented as the internet standards evolve. While accessing an internet service provider, the subscriber receives two bills - one from the wireless service provider for the use of the wireless network and the second from the internet service provider. Although common billing that combines both types of charges is not

handled by the minimum embodiment software, it is contemplated that the software will take advantage of internet standards for billing settlement as they evolve so that subscribers may receive a common bill based on roaming agreements between the ISP and wireless service providers.

[0172] The system includes a element management system for managing the network elements. From the element manager, system administrators perform configuration, performance and fault/alarm management functions. The element management applications run on top of a web browser. Using a web browser, system administrators manage the network from anywhere that they have TCP/IP access. The element manager also performs an agent role for a higher level manager. In this role it exports an SNMP MIB for alarm and fault monitoring.

[0173] A higher level SNMP manager is notified of alarm conditions via SNMP traps. The higher level SNMP manager periodically polls the element manager's MIB for the health and status of the network. System management personnel at the higher level manager are able to view an icon representation of the network and its current alarm state. By pointing and clicking on the network element icon, systems management personnel execute element management applications using a web browser and perform more detailed management functions.

[0174] Inside the network management of the physical and logical network elements is performed using a combination of the SNMP protocol and internal management application programming interfaces. Applications in the element manager use SNMP or other management APIs to perform network management functions.

[0175] Architecturally, the element management system includes of two distinct sets of functional elements. The first set of functional elements, including the configuration data server, performance data monitor and health/status monitor and network element recovery software, executes on an HA server equipped with RAID disks. The second set of functional elements, including the management applications, executes on a dedicated, non-HA management system. Even if the element manager System becomes non-operational, the network elements continue to be able to run and report alarms and even be able to recover from fault conditions. However, since all the management applications execute in the non-HA element manager, if the element manager goes down, then recovery actions requiring human intervention are not possible until the element manager becomes operational.

[0176] The wireless hubs (WHs) in the base stations are typically owned by a wireless service provider (WSP), and they are connected to the WSP's registration server (RS) either via point-to-point links, intranets or the internet. The WSP's registration server is typically a software module executing on a processor to perform certain registration functions. Inter-working function

units (IWF units) are typically software modules executing on a processor to perform certain interfacing functions. IWF units are typically connected to the registration servers via intranets/WAN, and the IWF units are typically owned by the WSP. However, the IWF units need not be located within the same LAN as the registration servers. Typically, accounting and directory servers (also software modules executing on a processor) are connected to the registration servers via a LAN in the service provider's Data Center (e.g., a center including one or more processors that hosts various servers and other software modules). Traffic from the end system is then routed via a router (connected to the LAN) to the public Internet or to an ISP's intranet. The registration server located in a foreign WSP's network is referred to as the foreign registration server (FRS), and the registration server located in the end system's home network (where the mobile purchases its service) is referred to as the home registration server (HRS). The inter-working function unit in the home network is referred to as the home IWF while the inter-working function unit in the foreign network (i.e., the network the end system is visiting) is referred to as the serving IWF.

[0177] For fixed wireless service (i.e., a non-moving end system), an end system may register for service on the home network from the home network (e.g. at home service) or from a foreign network (e.g., roaming service). The end system receives an advertisement sent by an agent (e.g., an agent function implemented in software) in the wireless hub via the access point. There are both MAC-layer registration as well as network-layer registration to be accomplished. These may be combined together for efficiency.

[0178] For end systems at home (FIG. 26), the network layer registration is sent (like a local registration) to the home registration server via the wireless hub to which the end system is currently attached. An IWF in the end system's home network will become the anchor or home IWF. Thus, PPP frames to and from the end system travel via the wireless hub to the home IWF in the home network. If the end system is at home, the home IWF is connected to the wireless hub via an XTunnel protocol.

[0179] For roaming wireless service (FIG. 27), the foreign registration server determines the identity of the home network of the roaming end system during the registration phase. Using this information, the foreign registration server communicates with the home registration server to authenticate and register the end system. The foreign registration server then assigns a serving IWF, and an I-XTunnel protocol connection is established between the home IWF and the serving IWF for the roaming end system. The serving IWF relays frames between the wireless hub and the home IWF. From the home IWF, data is sent to a PPP server (i.e., point-to-point protocol server) which may reside in the same IWF. However, if the data is to go to a corporate intranet or an ISP's intranet that has its own PPP server, the data

is sent to the separate PPP server via the L2TP protocol. The separate server is typically owned and operated by an Internet service provider who is different from the wireless service provider. For the duration of the session, the locations of the home IWF and PPP server remain fixed. The MAC layer registration can be combined with the network registration to economize on the overhead of separate communications for MAC layer and network layer registration; however, it may be advantageous to not combine these registration processes so that the WSP's equipment will be interoperable with other wireless networks that supports pure IETF Mobile-IP.

[0180] Registration sets up three tables. Table 1 is associated with each access point, and Table 1 identifies each connection (e.g., each end system) by a connection id (CID) and associates the connection id with a particular wireless (WM) modem address (i.e., the address of the end system or end system). Table 2 is associated with each wireless hub (WH), and Table 2 associates each connection id with a corresponding wireless modem address, access point and XTunnel id (XID). Table 3 is associated with each inter-working function (IWF), and Table 3 associates each connection id with a corresponding wireless modem address, wireless hub address, XTunnel id and IP port (IP/port). The entries described for these tables are described to include only relevant entries that support the discussion of mobility management. In reality, there are other important fields that need to be included as well.

Table 1:

Connection Table at AP	
CID	WM
C1	WM1
C2	WM1
C1	WM2

Table 2:

Connection Table at WH			
CID	WM	AP	XID
C1	WM1	AP1	5
C2	WM1	AP1	5
C1	WM2	AP1	6
C1	WM3	AP2	7

Table 3:

Connection Table at IWF				
CID	WM	WH	XID	IP/Port
C1	WM1	WH1	5	IP1/P1
C2	WM1	WH1	5	IP1/P2
C1	WM2	WH1	6	IP2/P3

Table 3: (continued)

Connection Table at IWF				
CID	WM	WH	XID	IP/Port
C1	WM3	WH1	7	IP3/P1
C5	WM5	WH2	8	IP4/P1

[0181] The protocol stacks for dial-up users at home in a network as well as roaming users are illustrated in FIGS. 28-31. FIG. 28 depicts protocol stacks used for direct internet access by a fixed (i.e., non-moving) end system at home where a PPP protocol message terminates in the home IWF (typically collocated with the wireless hub) which relays message to and from an IP router and from there to the public internet. FIG. 29 depicts protocol stacks used for remote intranet access (i.e., either private corporate nets or an ISP) by a fixed (i.e., non-moving) end system at home where a PPP protocol message is relayed through the home IWF (typically collocated with the wireless hub) to a PPP server of the private corporate intranet or ISP. FIG. 30 depicts protocol stacks used for direct internet access by a roaming but fixed (i.e., non-moving) or a moving end system where the PPP protocol terminates in the home IWF (typically located in a mobile switching center of the home network) which relays message to and from an IP router. In FIG. 30, note how message traffic passes through a serving IWF (typically collocated with the wireless hub) in addition to the home IMF. FIG. 31 depicts protocol stacks used for remote intranet access (i.e., either private corporate nets or an ISP) by a roaming but fixed (i.e., non-moving) or a moving end system where a PPP protocol message is relayed through the home IWF (typically located in a mobile switching center of the home network) to a PPP server of the private corporate intranet or ISP. In FIG. 31, note how message traffic passes through a serving IWF (typically collocated with the wireless hub) in addition to the home IWF. When the serving IWF and the wireless hub are co-located in the same nest of computers or are even programmed into the same computer, it is not necessary to establish a tunnel using the XTunnel protocol between the serving IWF and the wireless hub.

[0182] Equivalent variations to these protocol stacks (e.g. the RLP can be terminated at the wireless hub rather than at the serving IWF or home IWF for mobiles at home) are also envisioned. If the IWF is located far from the wireless hub, and the packets can potentially be carried over a lossy IP network between the IWF and wireless hub, then it would be preferred to terminate the RLP protocol at the wireless hub. Another variation is the Xtunnel between wireless hub and IWF need not be built on top of the UDP/IP. Xtunnels can be built using the Frame Relay/ATM link layer. However, the use of UDP/IP makes it easier to move the wireless hub and IWF software from one network to another.

[0183] Four types of handoff scenarios may occur,

and they are labeled: (i) local mobility, (ii) micro mobility, (iii) macro mobility, and (iv) global mobility. In all four scenarios (in one embodiment of the invention), a route optimization option is not considered so that the locations of the home registration server and the ISP's PPP server do not change. In another embodiment of the invention with route optimization, the ISP's PPP server may change. However, this aspect is discussed below. In addition, the locations of the foreign registration server and IWF do not change in the first three scenarios.

[0184] The proposed IETF Mobile IP standard requires that whenever an end system changes the IP subnet to which it is attached, it sends a registration request message to a home agent in its home subnet. This message carries a care-of address where the end system can be reached in the new subnet. When traffic is sent, for example, from an ISP to an end system, the home agent intercepts the traffic that is bound for the end system as it arrives in the home subnet, and then forwards the traffic to the care-of address. The care-of address identifies a particular foreign agent in the foreign subnet. An end system's foreign agent can reside in the end system itself, or in a separate node that in turn forwards traffic to the end system (i.e., proxy registration agent). Mobile IP handoffs involve exchange of control messages between an end system's agent, the end system's home agent and potentially its corresponding hosts (CHs) (with route optimization option).

[0185] The proposed IETF Mobile IP standard would find it difficult to meet the latency and scalability goals for all movements in a large internetwork. However, the present hierarchical mobility management meets such goals. For small movements (e.g. a change of Access Points), only MAC-layer re-registrations are needed. For larger movements, network-layer re-registrations are performed. The present hierarchical mobility management is different from the flat-structure used in the IETF proposed Mobile-IP standard as well as the serving/anchor inter-working function model used in cellular systems like CDPD (based on a standard sponsored by the Cellular Digital Packet Data forum).

[0186] As depicted in FIG. 32, the local mobility handoff handles end system (designated MN for mobile node) movement between APs that belong to the same wireless hub. Thus, only MAC layer re-registration is required. The end system receives a wireless hub advertisement from a new AP and responds with a registration request addressed to the new AP.

[0187] The new AP (i.e., the one that receives the registration request from the end system) creates new entries in its connection table and relays the registration message to its wireless hub. In local mobility handoffs, the wireless hub does not change. The wireless hub recognizes the end system's registration request as a MAC level registration request, and it updates its connection table to reflect the connection to the new AP. Then, the old AP deletes the connection entry from its connection table. There are at least three ways whereby the old AP

can delete the old entries, namely (i) upon time out, (ii) upon receiving a copy of the relayed MAC layer association message from the new AP to the wireless hub (if this relay message is a broadcast message), and (iii) upon being informed by the wireless hub of the need to delete the entry,

[0188] As depicted in FIG. 33, the micro mobility handoff handles end system (designated MN for mobile node) movement between wireless hubs that belong to the same registration server and where the end system can still be served by the existing serving IWF. When an advertisement is received from a new wireless hub (through a new AP), the end system sends a message to request registration to the registration server. The registration request is relayed from the new AP to the new wireless hub to the registration server.

[0189] When the registration server determines that the existing IWF can still be used, the registration server sends a build XTunnel Request message to request the existing IWF to build an XTunnel to the new wireless hub. Later, the registration server sends a tear down XTunnel request message to request the existing IWF to tear down the existing XTunnel with the old wireless hub. The build and tear XTunnel Request messages can be combined into one message. A foreign registration server does not forward the registration message to the home registration server since there is no change of IWF, either the serving IWF or home IWF.

[0190] Upon receiving a positive build XTunnel reply and a positive tear XTunnel reply from IWF, the registration server sends a registration reply to end system. As the registration reply reaches the new wireless hub, the connection table at the new wireless hub is updated to reflect the connection to the new AP. The new AP updates its MAC filter address table and connection table after receiving a message from the new wireless hub, and the registration reply is forwarded to the end system.

[0191] The registration server sends a release message to the old wireless hub. When the old wireless hub receives the release message, it updates its connection table and the MAC filter address table and connection table of the old AP.

[0192] As depicted in FIG. 34, the macro mobility handoff case handles movement between wireless hubs that involves a change of the serving IWF in the foreign network, but it does not involve a change in the registration server. When an advertisement is received from a new wireless hub (through a new AP), the end system sends a message to request a network layer registration to the registration server. The registration request is relayed from the new AP to the new wireless hub to the registration server.

[0193] The registration server recognizes that it is a foreign registration server when the end system does not belong to the present registration server's network. This foreign registration server determines the identity of the home registration server by using a request, preferably a Radius Access request (RA request), to the foreign directory server (like a big yellow pages) and then assigns an appropriate IWF to be the serving IWF, and it forwards a registration request to the home registration server, preferably through a Radius Access request (RA request), informing the home registration server of the newly selected IWF.

[0194] The home registration server authenticates the registration request by using a request, preferably a Radius Access request (RA request), to the home directory server. Upon authenticating the request and determining that the existing home IWF can still be used, the home registration server instructs the home IWF to build a new I-XTunnel to the newly assigned serving IWF and to tear down the existing I-XTunnel to the old serving IWF. Upon receiving a positive build I-XTunnel reply and a positive tear I-XTunnel reply from the home IWF, the home registration server sends a registration reply to the foreign registration server.

[0195] The foreign registration server then instructs the newly assigned IWF to build an XTunnel to the new wireless hub. Upon receiving a positive build XTunnel reply, the foreign registration server instructs the old IWF to tear down the XTunnel to the old wireless hub. Upon receiving a positive build XTunnel reply and a positive tear XTunnel reply, the foreign registration server sends a registration reply to end system.

[0196] As the registration reply reaches the new wireless hub, the connection table at the new wireless hub is updated to reflect the connection to the new AP. The new AP updates its MAC filter address table and connection table after receiving a message from the new wireless hub, and the registration reply is forwarded to the end system.

[0197] The registration server sends a release message to the old wireless hub. When the old wireless hub receives the release message, it updates its connection table and the MAC filter address table, and the old AP updates its MAC filter address table and connection table after receiving a message from the old wireless hub.

[0198] The global mobility handoff case handles movement between wireless hubs that involves a change of registration servers. FIG. 35 depicts a global mobility handoff where the home IWF does not change, and FIG. 36 depicts a global mobility handoff where the home IWF changes. When an advertisement is received from a new wireless hub (through a new AP) in a new foreign network, the end system sends a message to request a network layer registration to the new foreign registration server. The registration request is relayed from the new AP to the new wireless hub to the new foreign registration server.

[0199] The registration server recognizes that it is a new foreign registration server when the end system does not belong to the present registration server's network. This foreign registration server determines the identity of the home registration server by using a request, preferably a Radius Access request (RA request), to the foreign directory server (like a big yellow pages) and then assigns an appropriate IWF to be the serving IWF, and it forwards a registration request to the home registration server, preferably through a Radius Access request (RA request), informing the home registration server of the newly selected IWF.

quest), to the foreign directory server (like a big yellow pages) and then assigns an appropriate IWF to be the serving IWF, and it forwards the registration request to the home registration server, preferably through a Radius Access request (RA request), informing the home registration server of the newly selected IWF.

[0200] The home registration server authenticates the registration request by using a request, preferably a Radius Access request (RA request), to the home directory server. Upon authenticating the request and determining that the existing home IWF can still be used (FIG. 35), the home registration server instructs the home IWF to build a new I-XTunnel to the serving IWF newly assigned by the new foreign registration server. The home registration server also sends a de-registration message to the old foreign registration server and instructs the home IWF to tear down the existing I-XTunnel to the existing serving IWF of the old foreign network. Upon receiving a positive build I-XTunnel reply and a positive tear I-XTunnel reply from the home IWF, the home registration server sends a registration reply to the new foreign registration server.

[0201] The new foreign registration server then instructs the newly assigned IWF to build an XTunnel to the new wireless hub. Upon receiving a positive build XTunnel reply, the foreign registration server sends a registration reply to end System. As the registration reply reaches the new wireless hub, the connection table at the new wireless hub is updated to reflect the connection to the new AP. The new AP updates its MAC filter address table and connection table after receiving a message from the new wireless hub, and the registration reply is forwarded to the end system.

[0202] The old foreign registration server instructs the old IWF to tear down the XTunnel to the old wireless hub. Upon receiving a positive tear XTunnel reply or contemporaneously with the tear down XTunnel request, the old foreign registration server sends a release message to the old wireless hub. When the old wireless hub receives the release message, it updates its connection table and the MAC filter address table, and the old AP updates its MAC filter address table and connection table after receiving a message from the old wireless hub.

[0203] Alternatively, after the home registration server authenticates the registration request from the new foreign registration server and determines that the existing home IWF cannot be used (FIG. 36), the home registration server chooses a new home IWF and instructs the new home IWF to build a new level 2 tunnel protocol tunnel (L2TP tunnel) to the present PPP server (e.g., the PPP server in a connected ISP intranet). Then, the home registration server instructs the old home IWF to transfer its L2TP tunnel traffic to the new home IWF.

[0204] Then the home registration server instructs the new home IWF to build a new I-XTunnel to the serving IWF newly assigned by the new foreign registration server. The home registration server also sends a de-

registration message to the old foreign' registration server and instructs the home IWF to tear down the existing I-XTunnel to the existing serving IWF of the old foreign network. Upon receiving a positive build I-XTunnel reply and a positive tear I-XTunnel reply from the home IWF, the home registration server sends a registration reply to the new foreign registration server.

[0205] The new foreign registration server then instructs the newly assigned IWF to build an XTunnel to the new wireless hub. Upon receiving a positive build XTunnel reply, the foreign registration server sends a registration reply to end system. As the registration reply reaches the new wireless hub, the connection table at the new wireless hub is updated to reflect the connection to the new AP. The new AP updates its MAC filter address table and connection table after receiving a message from the new wireless hub, and the registration reply is forwarded to the end system.

[0206] The old foreign registration server instructs the old IWF to tear down the XTunnel to the old wireless hub. Upon receiving a positive tear XTunnel reply or contemporaneously with the tear down XTunnel request, the old foreign registration server sends a release message to the old wireless hub. When the old wireless hub receives the release message, it updates its connection table and the MAC filter address table, and the old AP updates its MAC filter address table and connection table after receiving a message from the old wireless hub.

[0207] End systems constructed according to the present invention interoperate with networks constructed according to the proposed. IETF Mobile-IP standards, and end systems constructed according to the proposed IETF Mobile-IP standards interoperate with networks constructed according to the present invention.

[0208] The main differences between the present invention and the IETF Mobile-IP (RFC2002, a standards document) are:

(i) The present invention uses a hierarchical concept for mobility management rather than a flat structure as in the proposed IETF Mobile-IP standard. Small mobility within a small area does not result in a network level registration. Micro mobility involves setting up of a new Xtunnel and tearing down of an existing Xtunnel. Global mobility, at the minimum, involves setting up of new I-XTunnel and tearing down of an existing I-XTunnel apart from the setting up/tearing down of XTunnel. Global mobility sometimes also involves setting up a new L2TP Tunnel and transferring of L2TP state from the existing L2TP Tunnel to the new L2TP Tunnel.

(ii) In the present invention, a user name plus a realm is used to identify a remote dial-up user rather than a fixed home address as in the case of the proposed IETF Mobile-IP standard.

(iii) In the present invention, registration and routing functions are carried out by separate entities. The two functions are carried out by the home agent in the proposed IETF Mobile IP standard, and both functions are carried out by the foreign agent in the proposed IETF Mobile IP standard. In contrast, in an embodiment of the present invention, registration is carried out in the registration server and routing functions are carried out by both the home and foreign IWF and the wireless hub (also referred to as the access hub).

(iv) The present invention utilizes three tunnels per PPP session. The XTunnel is more of a link-layer tunnel between the wireless hub and the serving IWF. The I-XTunnel between the serving IWF and the home IWF is more like the tunnel between home and foreign agents in the proposed IETF Mobile-IP standard. But it also has additional capabilities beyond the tunnels proposed by the Mobile-IP standard. The L2TP tunnel is used only when home IWF is not a PPP server. The number of these tunnels may be reduced by combining some functions in the same node as described above.

(v) In the present invention, wireless registration occurs before PPP session starts while in the proposed IETF Mobile-IP standard, Mobile-IP registration occurs after PPP session enters into the open state.

(vi) In the present invention, the network entity that advertises the agent advertisement (i.e., the wireless hub) is not on a direct link to the end systems whereas for the proposed IETF Mobile-IP standard, the agent advertisement must have a TTL of 1 which means that the end systems have a direct link with the foreign agent. In addition, the agent advertisement in the present invention is not an extension to the ICMP router advertisements as in the proposed IETF Mobile-IP standard.

[0209] End systems in the present invention, should support agent solicitation. When an end system in the present invention visits a network which is supporting the proposed IETF Mobile-IP standard, it waits until it hears an agent advertisement. If it does not receive an agent advertisement within a reasonable time frame, it broadcasts an agent solicitation.

[0210] In the present invention, network operators may negotiate with other networks that support the proposed IETF Mobile-IP standard such that home addresses can be assigned to the end systems of the present invention that wish to use other networks. When the end system of the present invention receives the agent advertisement, it can determine that the network it is visiting is not a network according to the present invention and hence uses the assigned home address

to register.

[0211] For networks supporting the proposed IETF Mobile-IP standard, the PPP session starts before Mobile-IP registration, and the PPP server is assumed to be collocated with the foreign agent in such networks. In one embodiment an SNAP header is used to encapsulate PPP frames in the MAC frames of the present invention (in a manner similar to Ethernet format), and the foreign agent interprets this format as a proprietary PPP format over Ethernet encapsulation. Thus, the end system of the present invention and its PPP peer can enter into an open state before the foreign agent . starts transmitting an agent advertisement, and the end system of the present invention can register.

[0212] To allow end systems supporting the proposed IETF Mobile-IP standard to work in networks of the type of the present invention, such mobiles are at least capable of performing similar MAC layer registrations. By making the agent advertisement message format similar to the proposed Mobile-IP standard agent advertisement message format, a visiting end system can interpret the agent advertisement and register with a wireless hub. In the present invention, registration request and reply messages are similar to the proposed IETF Mobile-IP standard registration request and reply, messages (without any unnecessary extensions) so that the rest of the mobility management features of the present invention are transparent to the visiting end systems.

[0213] Since end systems supporting the proposed IETF Mobile-IP standard expect a PPP session to start before Mobile-IP registration, an optional feature in wireless hubs of the present invention starts to interpret PPP LCP, NCP packets after MAC-layer registrations.

[0214] To avoid losing traffic during handoffs, the mobility management of the present invention uses the make before break concept. For local mobility, a make before break connection is achieved by turning the MAC-layer registration message relayed by the new AP to the wireless hub into a broadcast message. That way, the old AP can hear about the new registration and forward packets destined for the end system that have not been transmitted to the new AP.

[0215] For micro mobility, information about the new wireless hub is included in the Tear XTunnel message exchanged between the serving IWF and the old WH. That way, the old wireless hub can forward buffered packets to the new wireless hub upon hearing a TearX-Tunnel message from the serving IWF. Alternatively, the RLP layer at the IWF knows the sequence number that has been acknowledged by the old wireless hub so far.

[0216] At the same time, the IWF knows the current send sequence number of the latest packet sent to the old wireless hub. Therefore, the IWF can forward those packets that are ordered in between these two numbers to the new wireless hub before sending newer packets to the new wireless hub. The RLP layer is assumed to be able to filter duplicate packet. The second approach is probably preferable to the first approach for the old

wireless hub may not be able to communicate with one another directly.

[0217] For macro mobility, the old serving IWF can forward packets to the new serving IWF, in addition to the packet forwarding done from the old wireless hub to the new wireless. All we need to do is to forward the new serving IWF identity to the new serving IWF in the tear down I-XTunnel message. Another way to achieve the same result is to let the home IWF forward the missing packets to the new serving IWF rather than asking the old serving IWF to do the job since the home IWF knows the I-XTunnel sequence number last acknowledged by the old serving IWF and the current I-XTunnel sequence number sent by the home IWF.

[0218] The method of estimating how much buffer should be allocated per mobile per AP per wireless hub per IWF such that the traffic loss between handoffs can be minimized is to let the end system for the AP for the wireless hub for the IWF estimate the packet arrival rate and the handoff time. This information is passed to the old AP of the wireless hub of the IWF to determine how much traffic should be transferred to the new AP of the wireless hub of the IWF, respectively, upon handoffs.

[0219] To achieve route optimization in the present invention, the end system chooses the PPP server closest to the serving IWF. Without route optimization, excessive transport delays and physical line usage may be experienced.

[0220] For example, an end system subscribed to a home network in New York City may roam to Hong Kong. To establish a link to a Hong Kong ISP, the end system would have a serving IWF established in a wireless hub in Hong Kong and a home IWF established in the home network in New York City. A message would then be routed from the end system (roamed to Hong Kong) through the serving IWF (in Hong Kong) and through the home IWF (in New York City) and back to the Hong Kong ISP.

[0221] A preferred approach is to connect from the serving IWF (in Hong Kong) directly to the Hong Kong ISP. The serving IWF acts like the home IWF. In this embodiment, roaming agreements exist between the home and foreign wireless providers. In addition, the various accounting/billing systems communicate with one another automatically such that billing information is shared. Accounting and billing information exchange may be implemented using standards such as the standard proposed by the ROAMOPS working group of the IETF.

[0222] However, the serving IWF must still discover the closest PPP server (e.g. the Hong Kong ISP). In the present embodiment, the foreign registration server learns of the end system's desire to connect to a PPP server (e.g., a Hong Kong ISP) when it receives a registration request from the end system. When the foreign registration server determines that the serving IWF is closer to the desired PPP server (e.g., the Hong Kong ISP) than the home IWF is, the foreign registration serv-

er instructs the serving IWF to establish an L2TP tunnel to its nearest PPP server (in contrast to the PPP server closest to the home registration server and home IWF). Then, the foreign registration server informs the home registration server that the end system is being served by the serving IWF and the foreign PPP.

[0223] In an alternative embodiment, the foreign registration server determines that the serving IWF is closer to the desired PPP server (e.g., the Hong Kong ISP) than the home IWF is, when it receives a registration request from the end system. The foreign registration server relays the registration request message to the home registration server with an attached message indicating the serving IWF information and a notification that route optimization is preferred. At the same time, the foreign registration server instructs the serving IWF to establish an L2TP tunnel to the PPP server. Upon approving the registration request, the home registration server instructs the home IWF to transfer the L2TP state to the foreign IWF.

[0224] Having described preferred embodiments of a novel network architecture with wireless end users able to roam (which are intended to be illustrative and not limiting), it is noted that modifications and variations can be made by persons skilled in the art in light of the above teachings. For example, connection links described herein may make reference to known connection protocols (e.g., IP, TCP/IP, L2TP, IEEE 802.3, etc.); however, the invention contemplates other connection protocols in the connections links that provide the same or similar data delivery capabilities. Acting agents in the above described embodiments may be in the form of software controlled processors or may be other form of controls (e.g., programmable logic arrays, etc.). Acting agents may be grouped as described above or grouped otherwise in keeping with the connection teachings described herein and subject to security and authentication teachings as described herein. Furthermore, a single access point, access hub (i.e., wireless hub) or into-working function unit (IWF unit) may provide multi-channel capability. Thus, a single access point or access hub or IWF unit may act on traffic from multiple end systems, and what is described herein as separate access points, access hubs or IWF units contemplates equivalence with a single multichannel access point, access hub or IWF unit. It is therefore to be understood that changes may be made in the particular embodiments of the invention disclosed which are within the scope and spirit of the invention as defined by the appended claims.

Claims

1. A coupled data network comprising:
 - a foreign network that includes a base station and a foreign mobile switching center with a serving registration server, the base station in-

cluding an access hub with a serving inter-working function;
 a home network that includes a home mobile switching center with a home registration server and a home inter-working function; and
 an end system subscribed to the home network and operating within the foreign network, the end system including an end registration agent to form a registration request, the registration request including an indication of a desired communications network having a desired communications server, the end system sending the registration request to the serving registration server, the serving registration server including a first module to process the registration request and to determine an optimum route between the desired communications server and one of the home inter-working function and the serving inter-working function, the serving registration server further including a second module to link the serving inter-working function to the desired communications server when the first module determines that the optimum route is between the serving inter-working function and the desired communications server.

2. The data network of claim 1, wherein the serving registration server further includes a third module to send to the home registration server the registration request with an appended indication that the service registration server has linked the serving inter-working function and the desired communications server.

3. A coupled data network comprising:

a foreign network that includes a base station and a foreign mobile switching center with a serving registration server, the base station including an access hub with a serving inter-working function;
 a home network that includes a home mobile switching center with a home registration server and a home inter-working function; and
 an end system subscribed to the home network and operating within the foreign network, the end system including an end registration agent to form a registration request, the registration request including and indication of a desired communications network having a desired communications server, the end system sending the registration request to the serving registration server, the serving registration server including a first module to process the registration request and to determine an optimum route between the desired communications server and one of the home inter-working function and

the serving inter-working function, the serving registration server further including a second module to send to the home registration server the registration request with a first appended indication that the serving registration server has determined that the optimum route is between the serving inter-working function and the desired communications server and a second appended indication that route optimization is preferred.

4. The data network of claim 3, wherein the serving registration server includes a third module to establish a link between the serving inter-working function and the desired communications processor after sending the registration request and the first and second appended indications to the home registration server.

5. The data network of claim 4, wherein:

the home registration server includes a fourth module to send a registration reply to the serving registration server, the registration reply including an indication of that the link between the serving inter-working function and the desired communications server is approved; and the home registration server further includes a fifth module to instruct the home inter-working function to transfer a link state to the serving inter-working function.

6. A method for optimizing routing in a coupled data network wherein the coupled data network comprises a foreign network that includes a base station and a foreign mobile switching center with a serving registration server, the base station including an access hub with a serving inter-working function, a home network that includes a home mobile switching center with a home registration server and a home inter-working function, and an end system subscribed to the home network and operating within the foreign network, the end system including an end registration agent to form a registration request, comprising the steps of:

generating a registration request at the end system, said registration request including an indication of a desired communications network having a desired communications server; sending the registration request from the end system to the serving registration server; processing the registration request in a first module in the serving registration server to determine an optimum route between the desired communications server and one of the home inter-working function and the serving inter-working function;

linking the serving inter-working function to the desired communications server when the first module determines that the optimum route is between the serving inter-working function and the desired communications server.

5

- 7. The method of claim 6, further comprising the step of:

 sending to the home registration server the registration request with an appended indication that the service registration server has linked the serving inter-working function and the desired communications server.

10

- 8. The method of claim 6 or the network of claim 1 or claim 3 wherein:

 the desired communications server is one communication server of a plurality of communications servers in the desired communications network; and
 the first module includes a sub-module to determine the select the desired communications server from among the plurality of communications servers.

20

25

- 9. The method of claim 6 or the network of claim 1 or claim 3, wherein said home network and said foreign network share billing information for the end system when the end system is operating in the foreign network.

30

- 10. A method for optimizing routing in a coupled data network wherein the coupled data network comprises a foreign network that includes a base station and a foreign mobile switching center with a serving registration server, the base station including an access hub with a serving inter-working function, a home network that includes a home mobile switching center with a home registration server and a home inter-working function, and an end system subscribed to the home network and operating within the foreign network, the end system including an end registration agent to form a registration request, comprising the steps of:

35

40

45

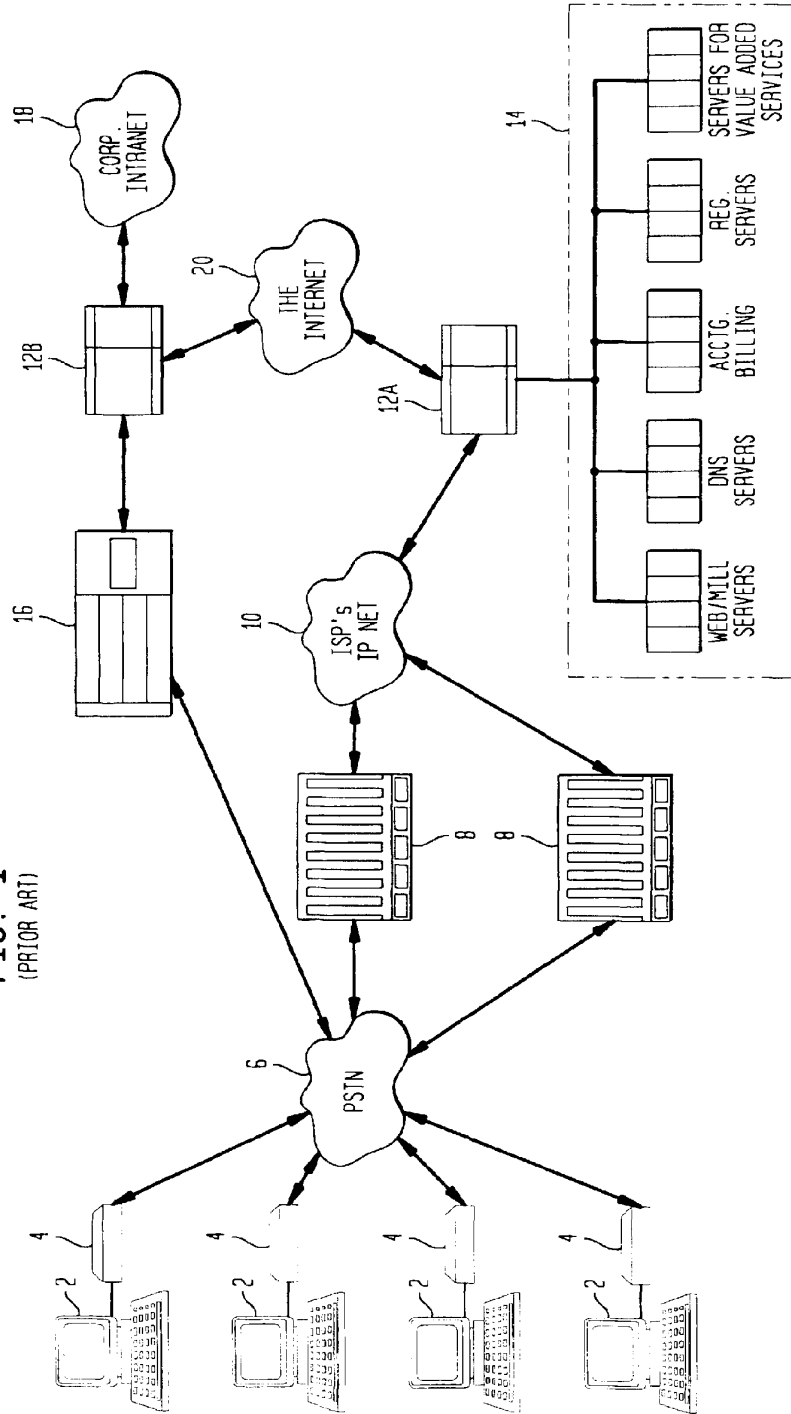
 generating a registration request at the end system, said registration request including an indication of a desired communications network having a desired communications server;
 sending the registration request from the end system to the serving registration server;
 determining whether the server inter-working function or the home inter-working function is closer to the desired communications server;
 instructing the serving inter-working function to establish a connection to the desired communications server when the serving inter-working

50

55

function is closer to the desired communications server than the home inter-working function;
informing the home registration server that the end system is being served by the serving inter-working function and the desired communications server.

FIG. 1
(PRIOR ART)



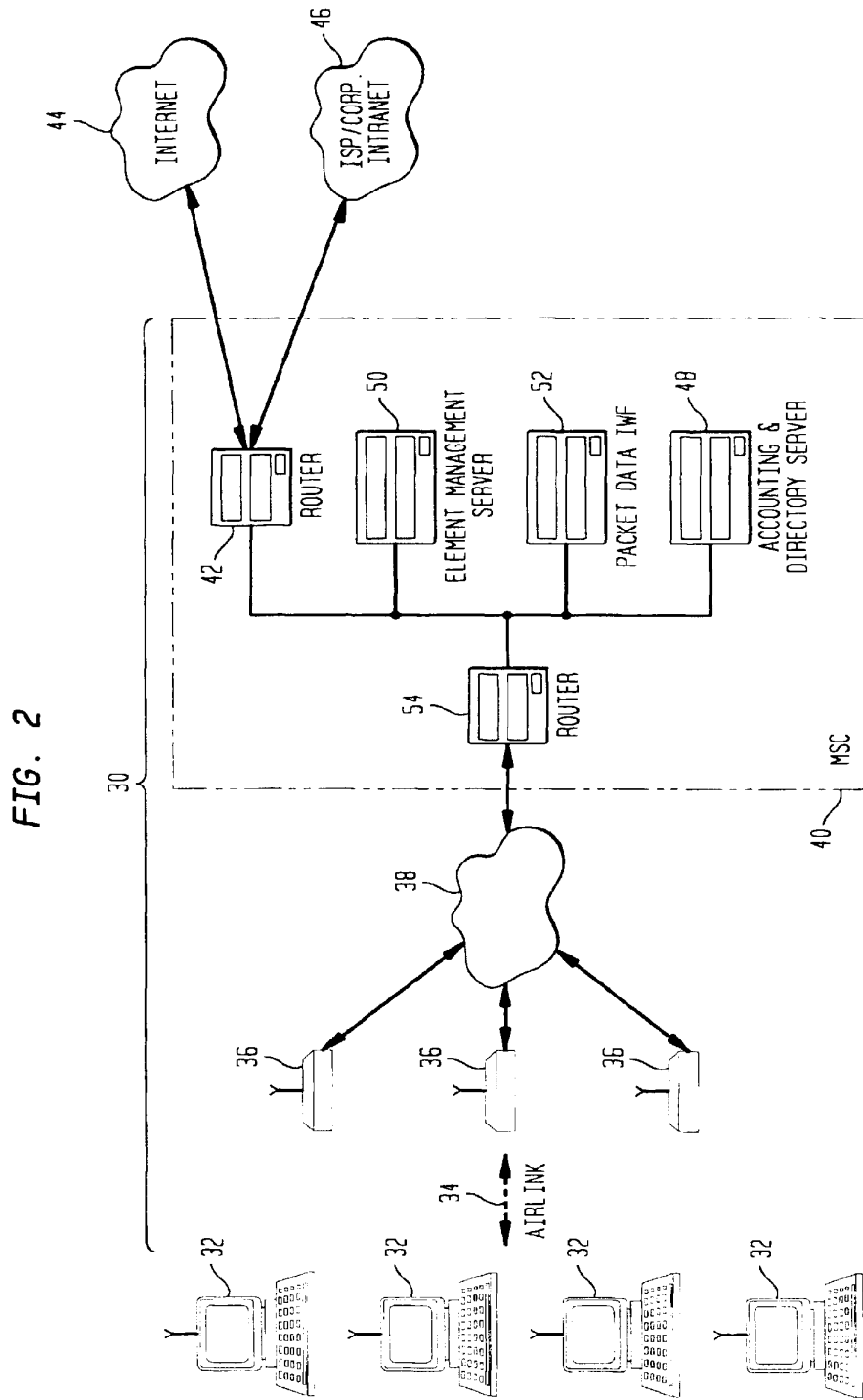


FIG. 3

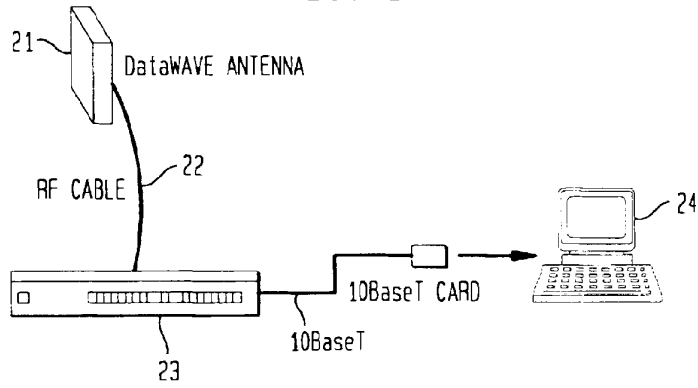


FIG. 4

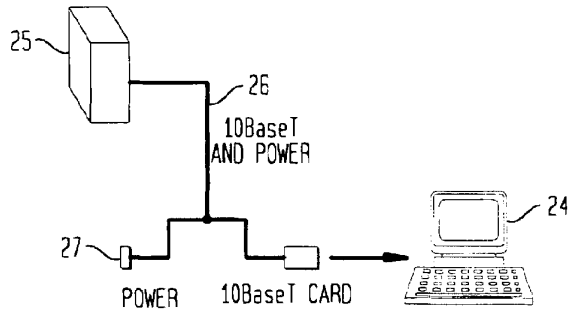


FIG. 5

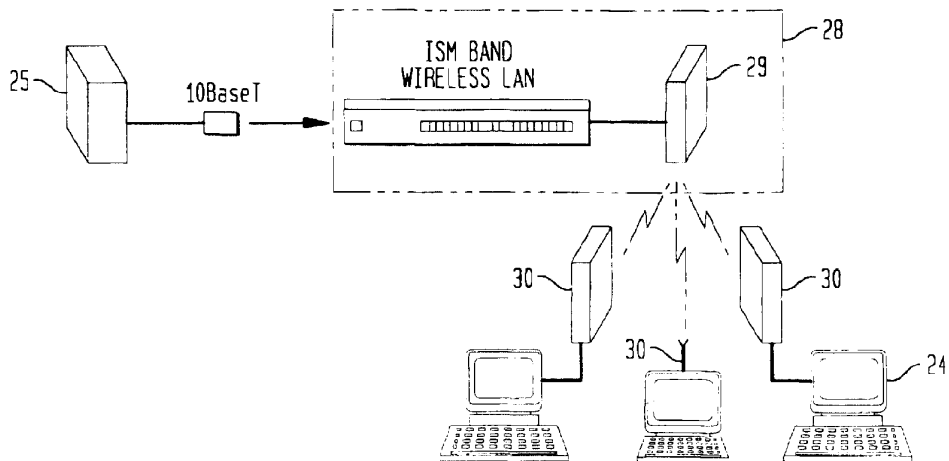


FIG. 6

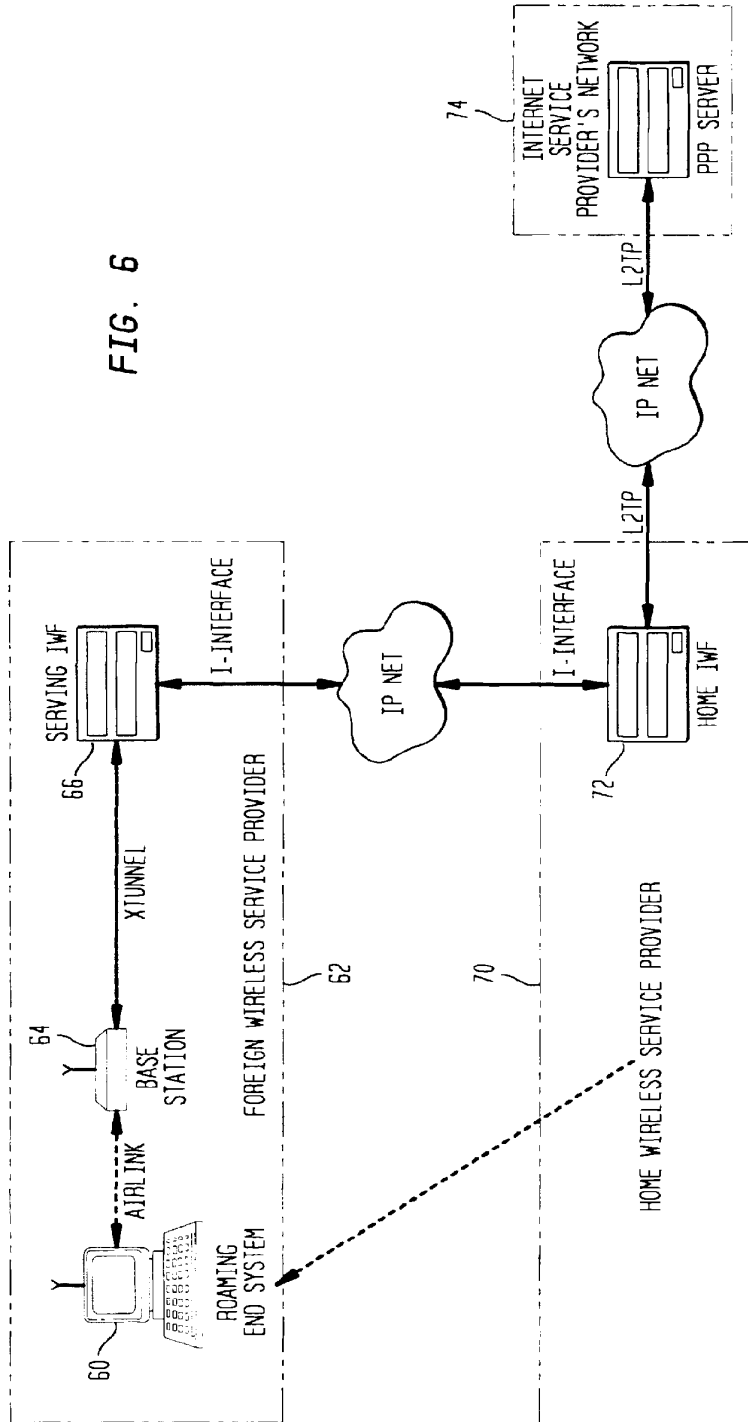


FIG. 7

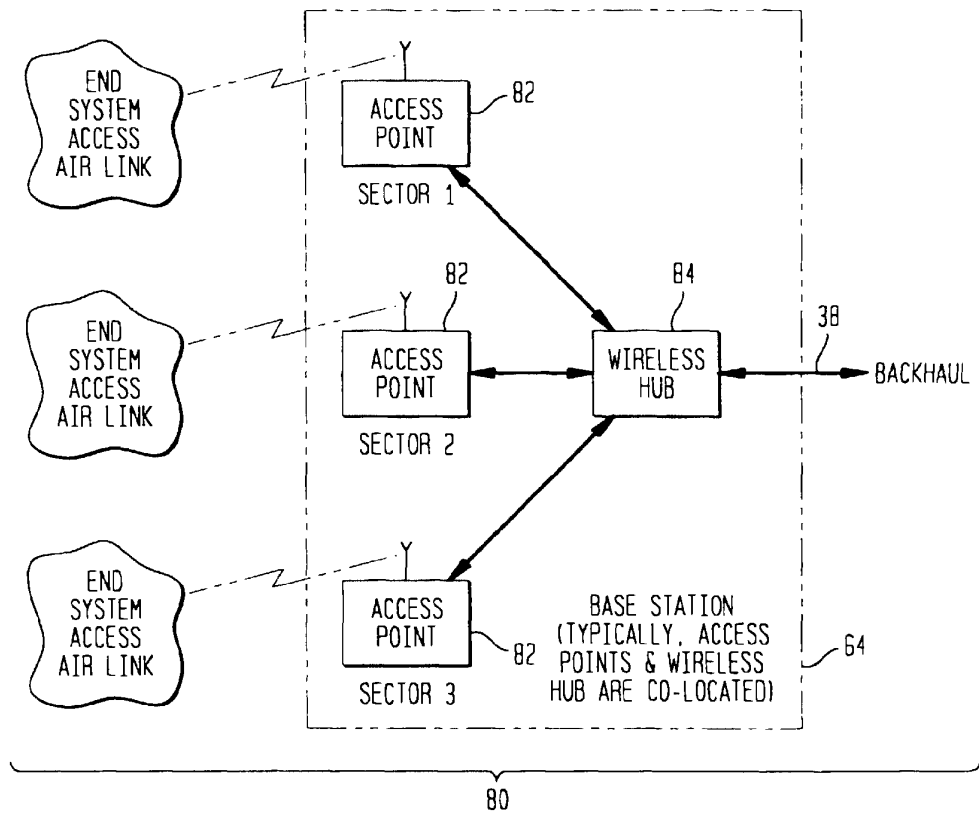


FIG. 8

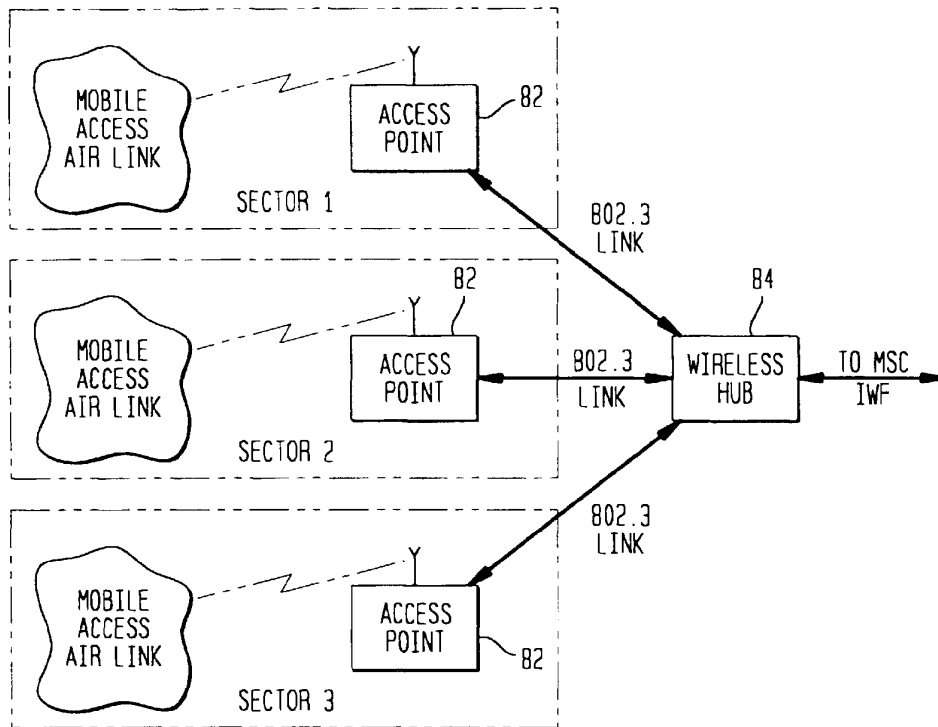


FIG. 9

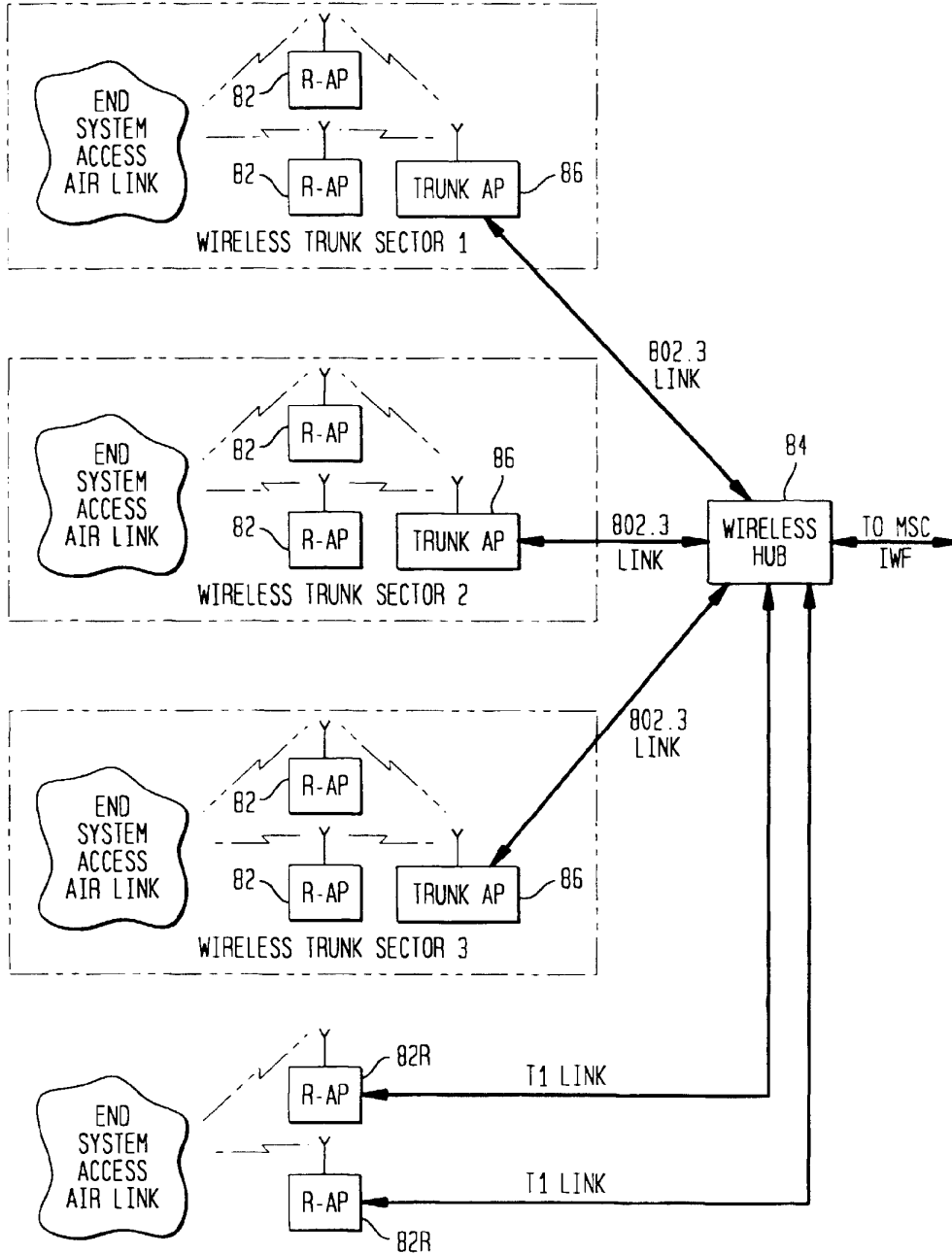


FIG. 10

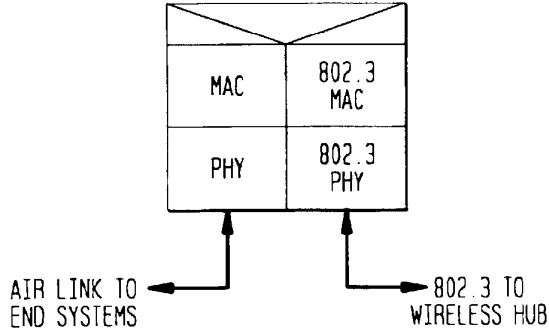


FIG. 11

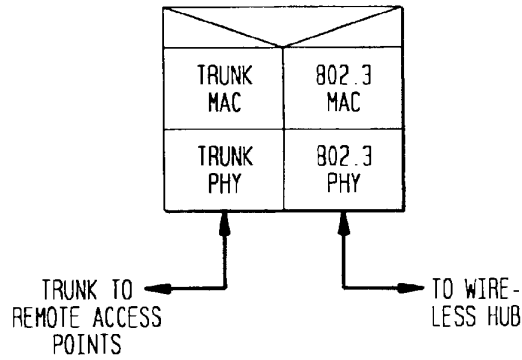


FIG. 12

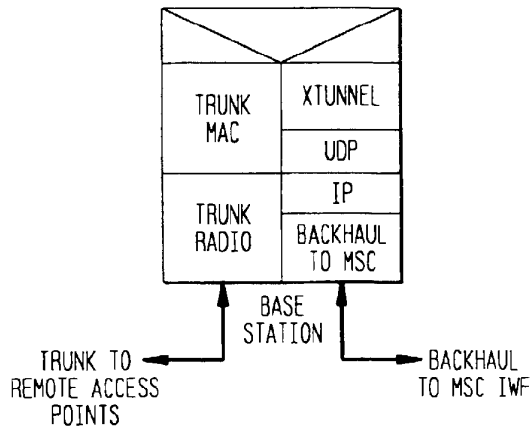


FIG. 13

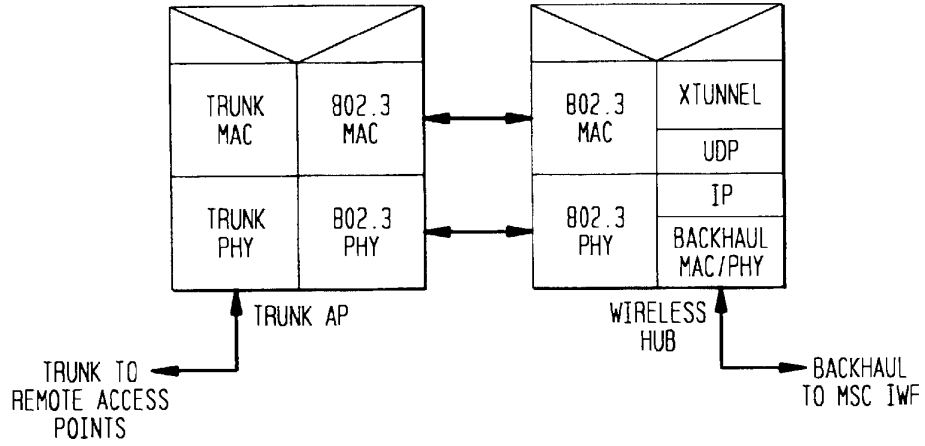


FIG. 14

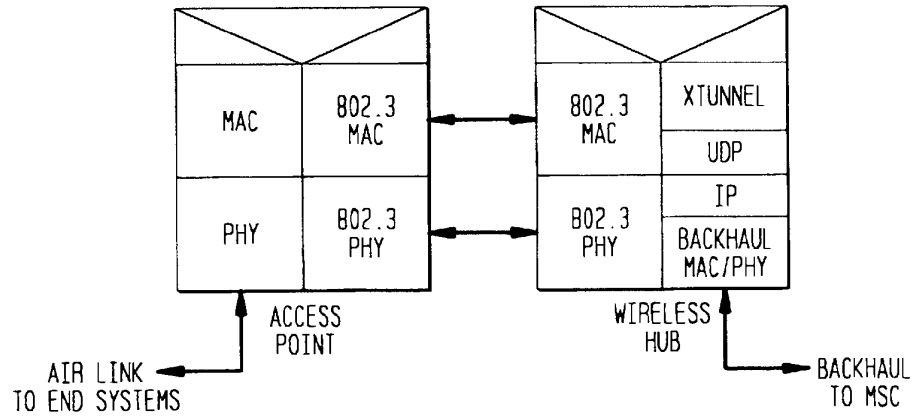


FIG. 15

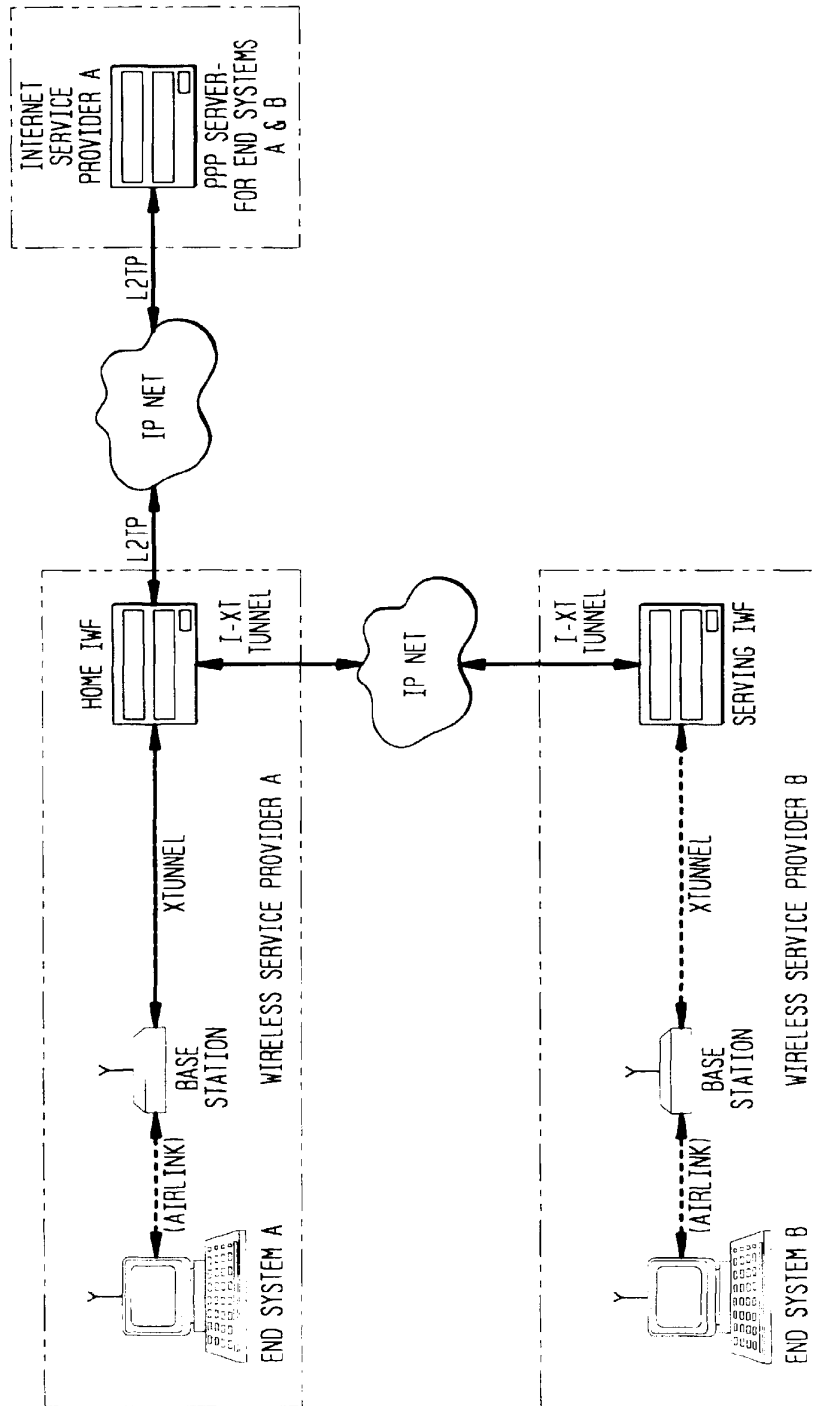


FIG. 16

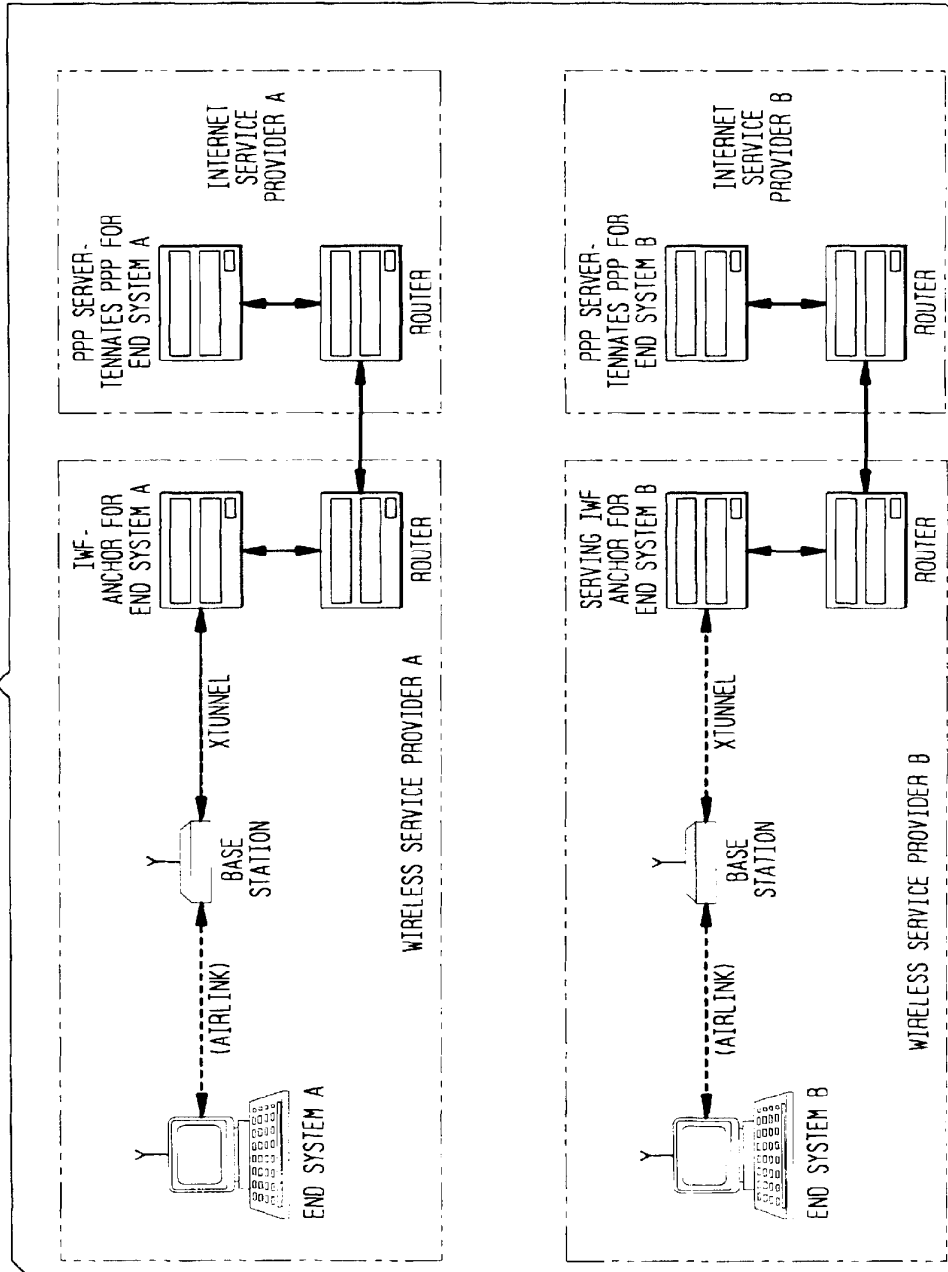


FIG. 17

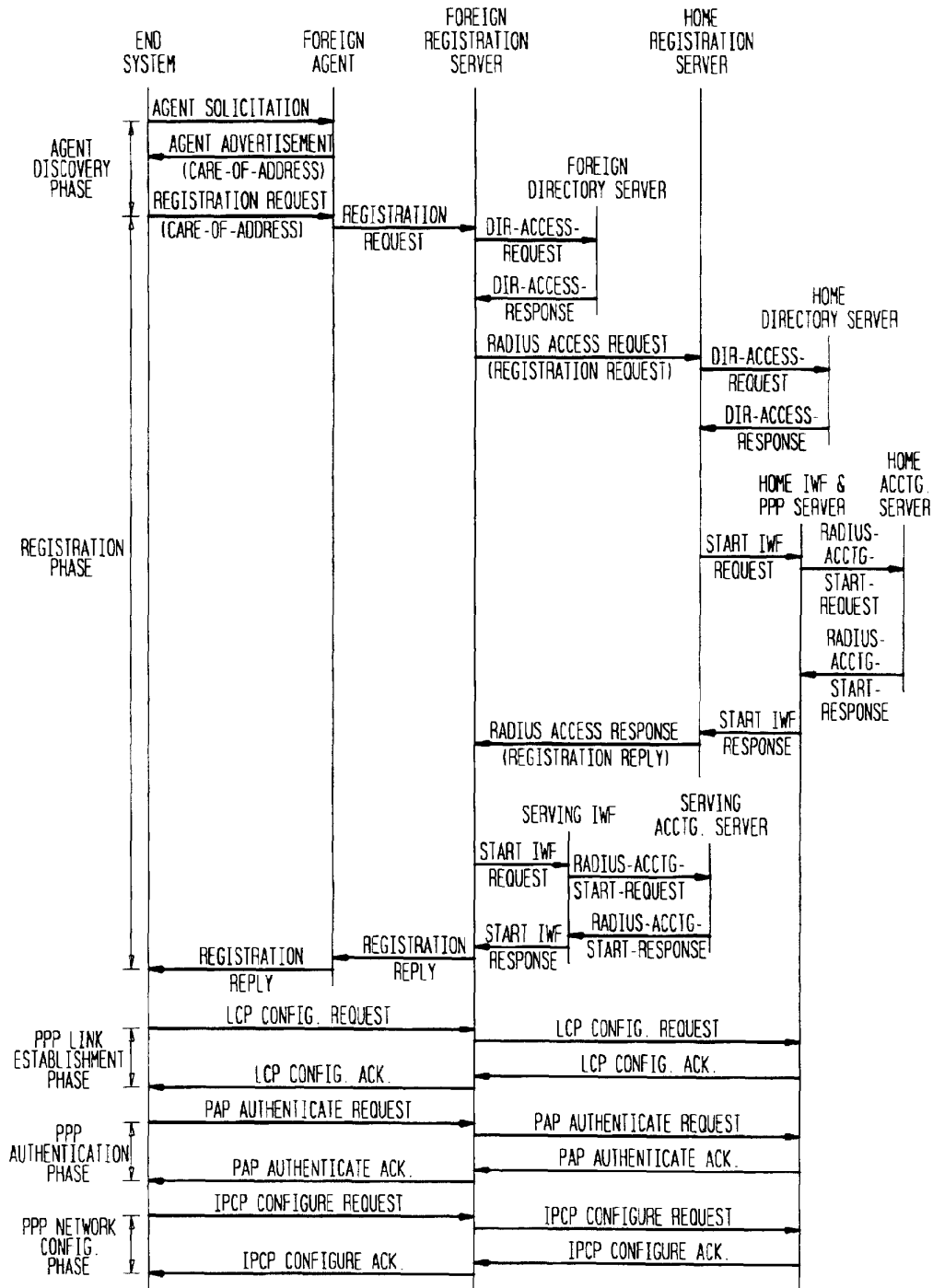


FIG. 18

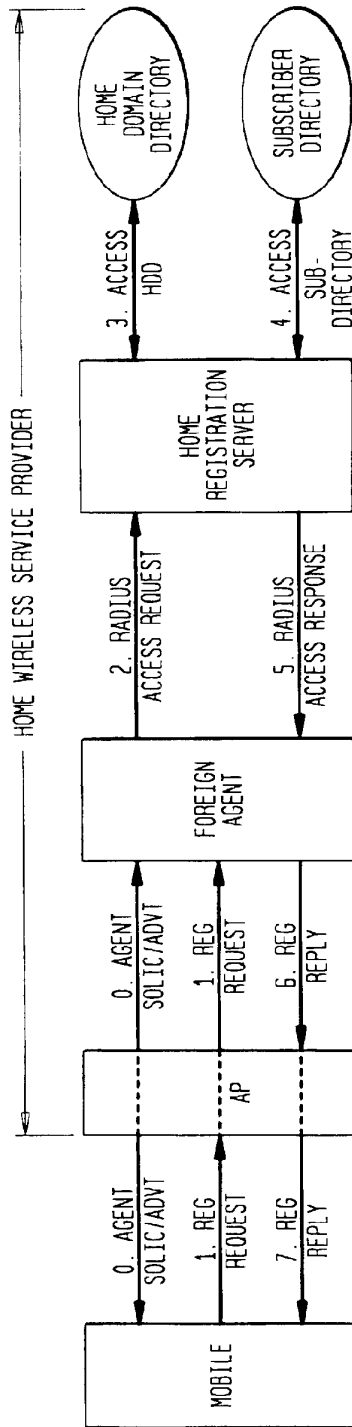


FIG. 19

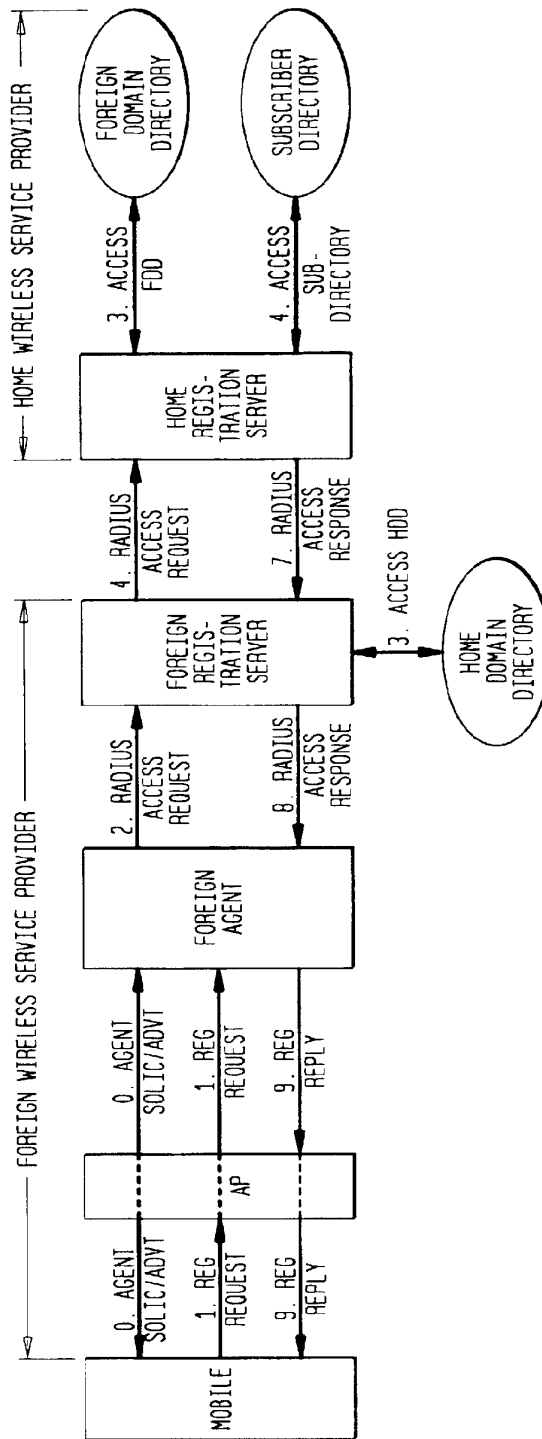


FIG. 20

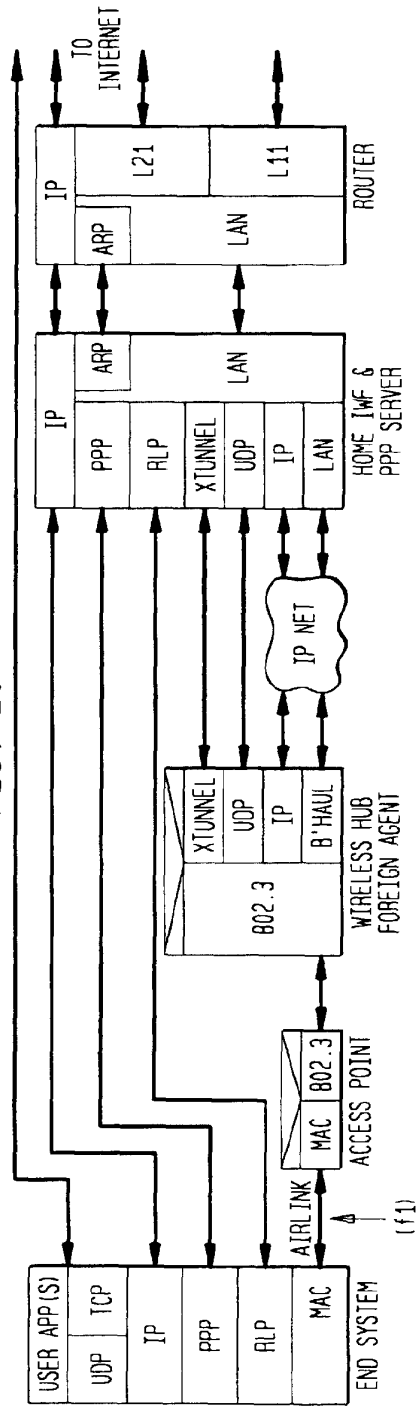


FIG. 21

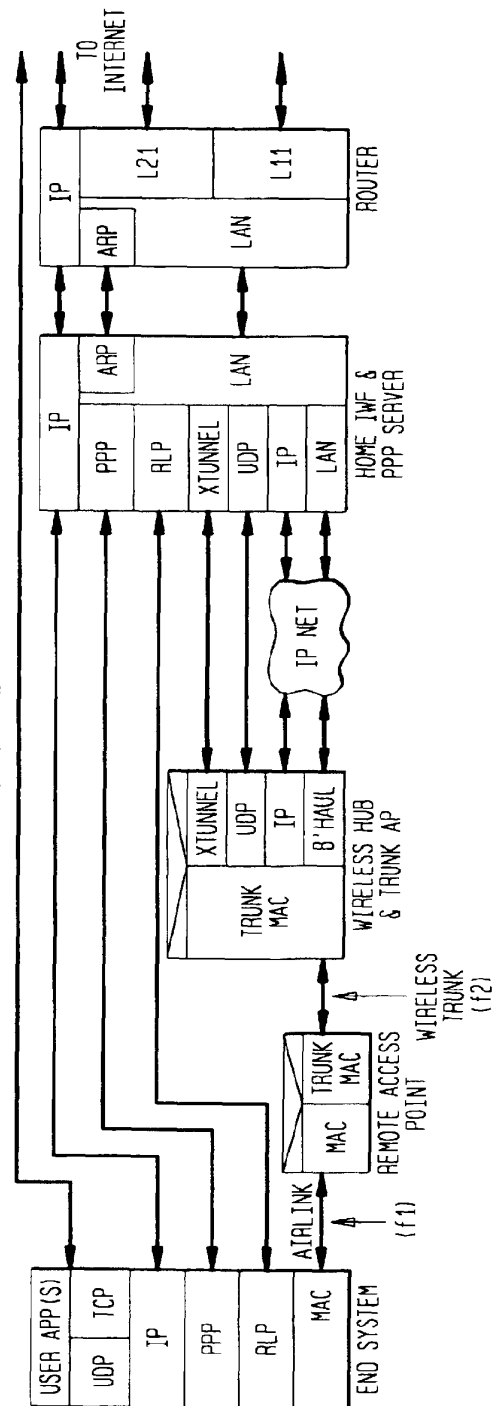


FIG. 22

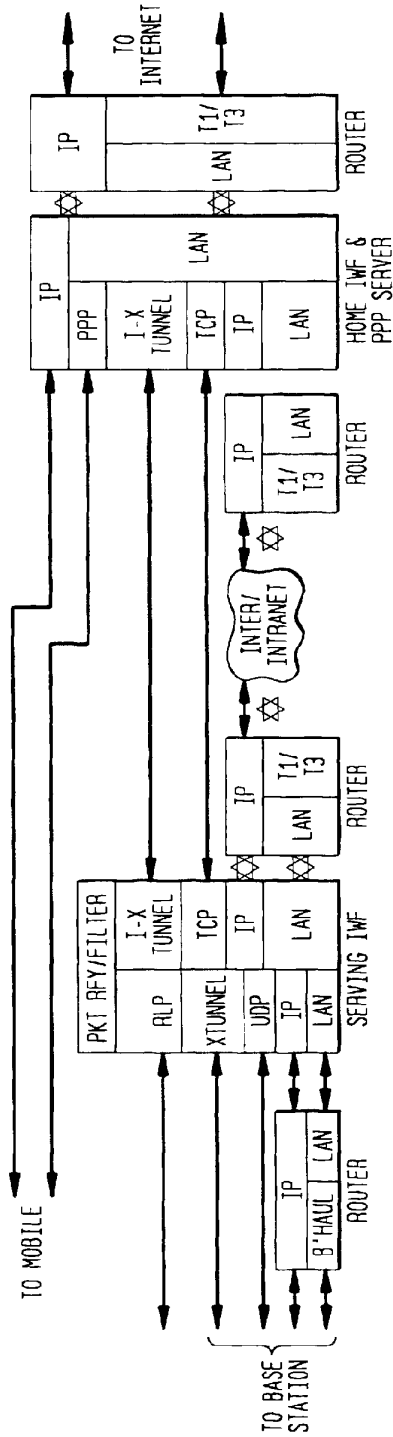


FIG. 23

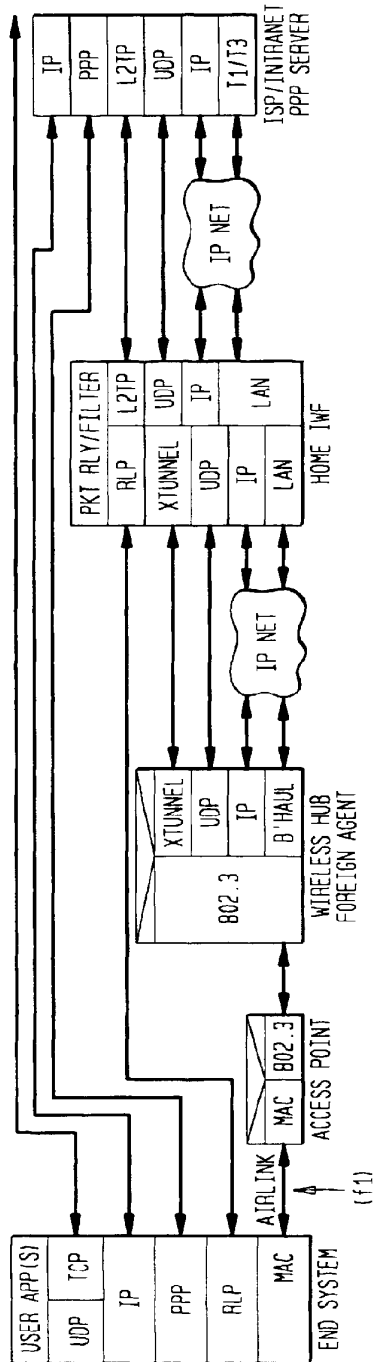


FIG. 24

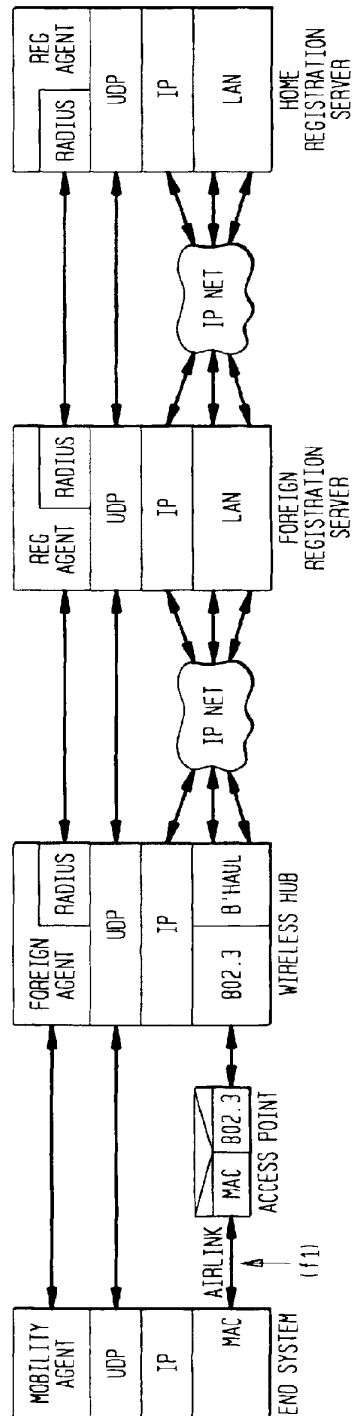


FIG. 25

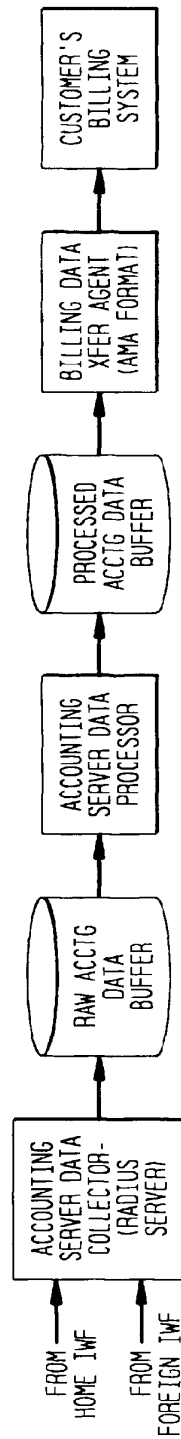
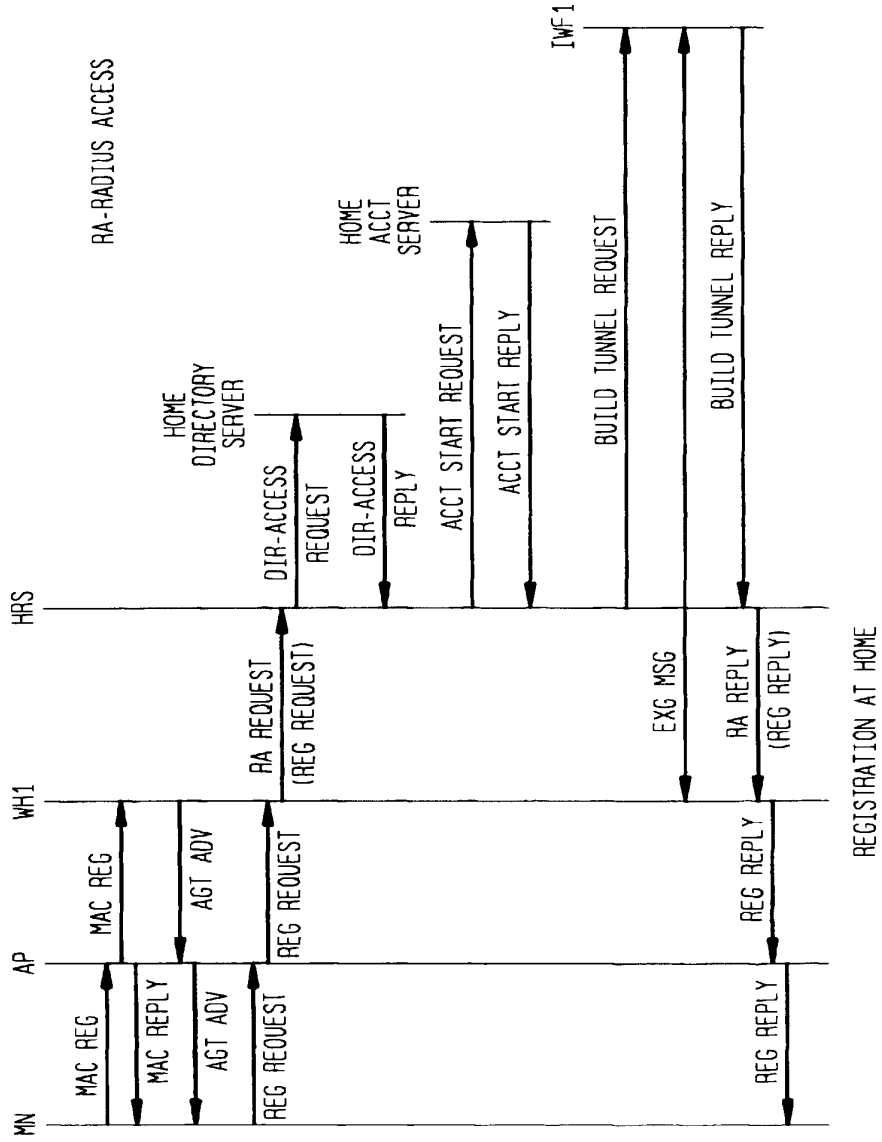


FIG. 26



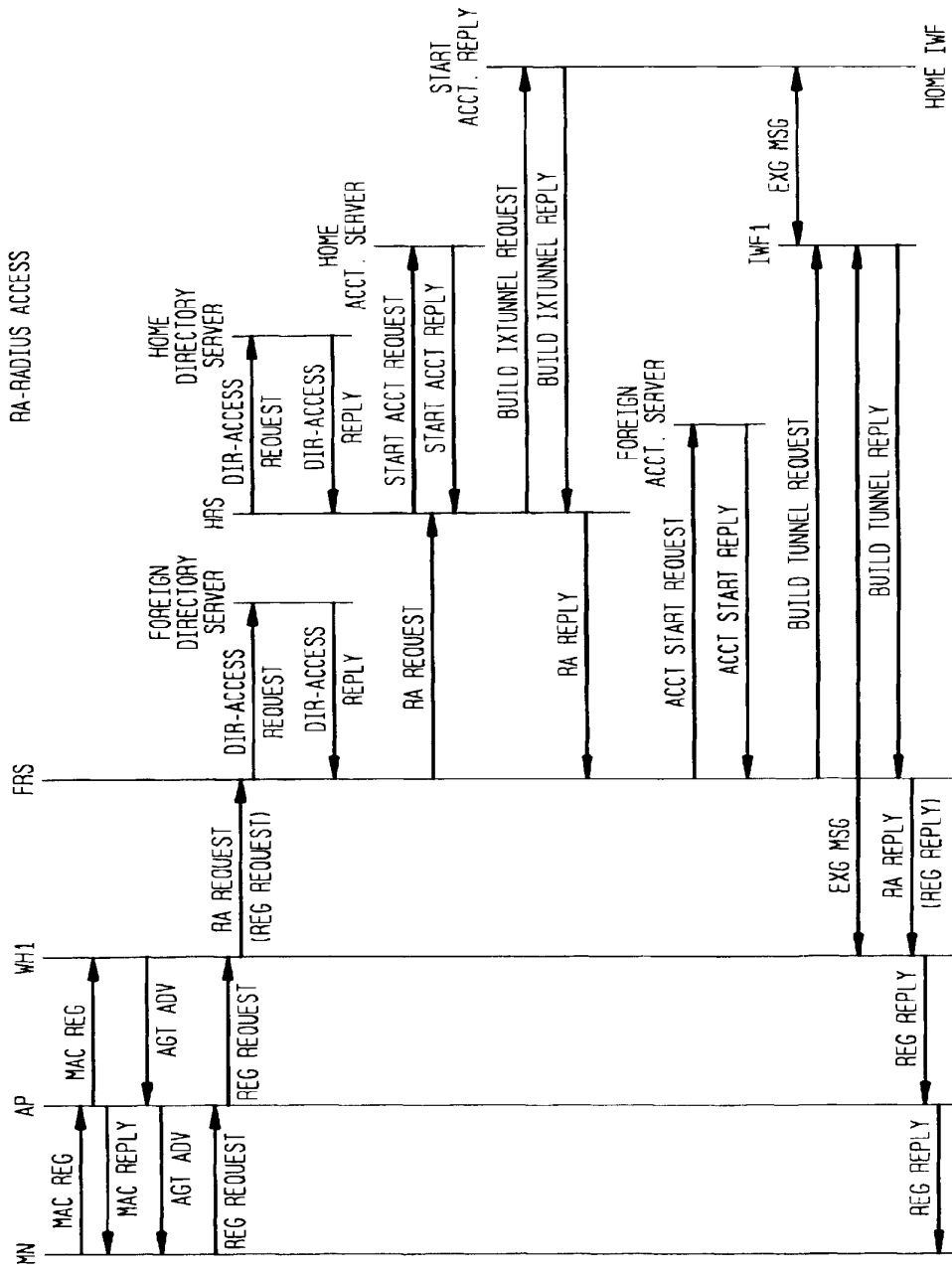


FIG. 27

FIG. 28

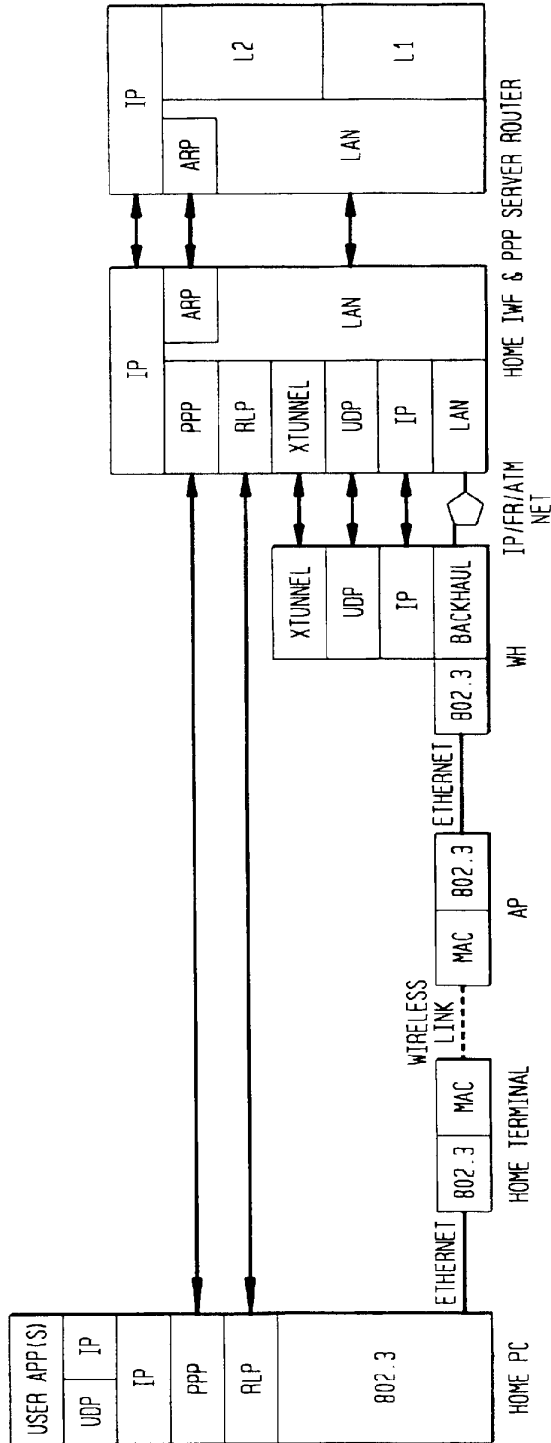


FIG. 29

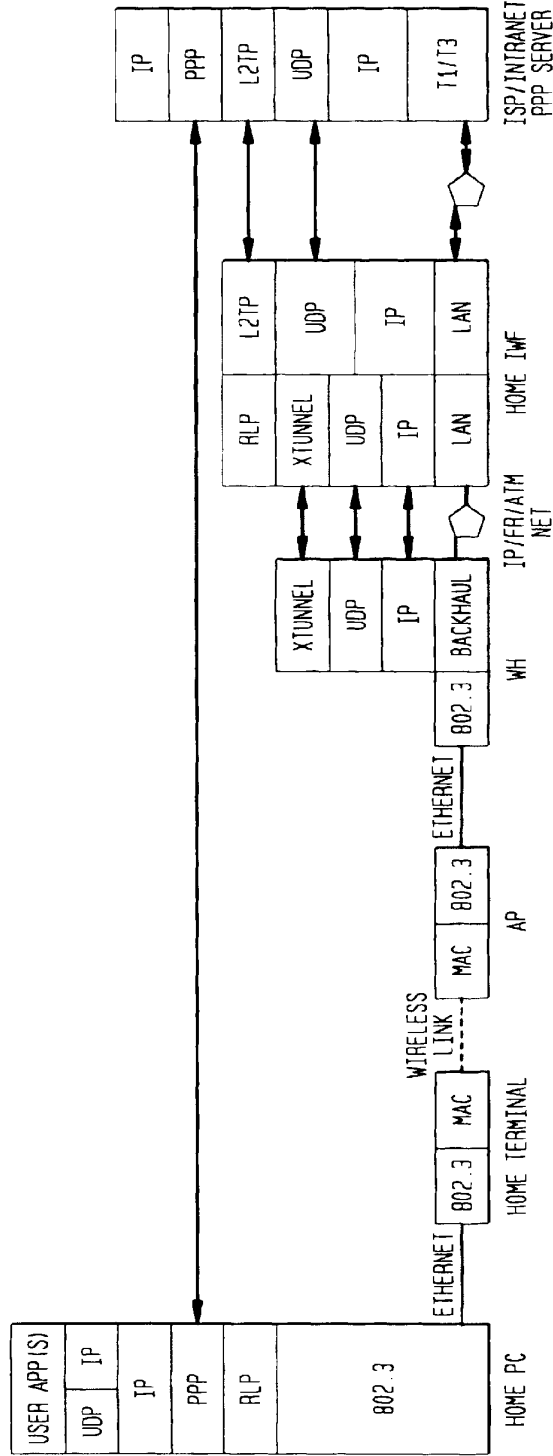
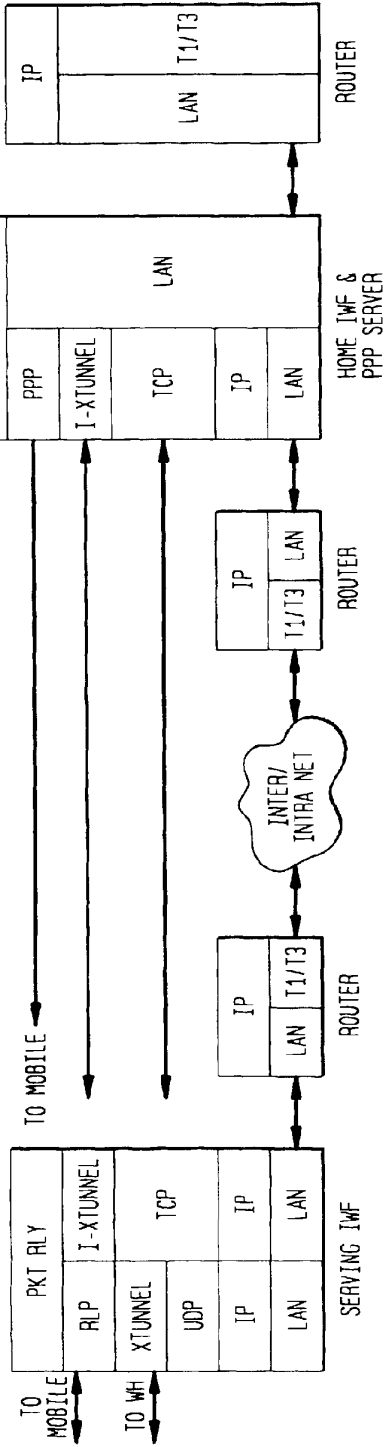
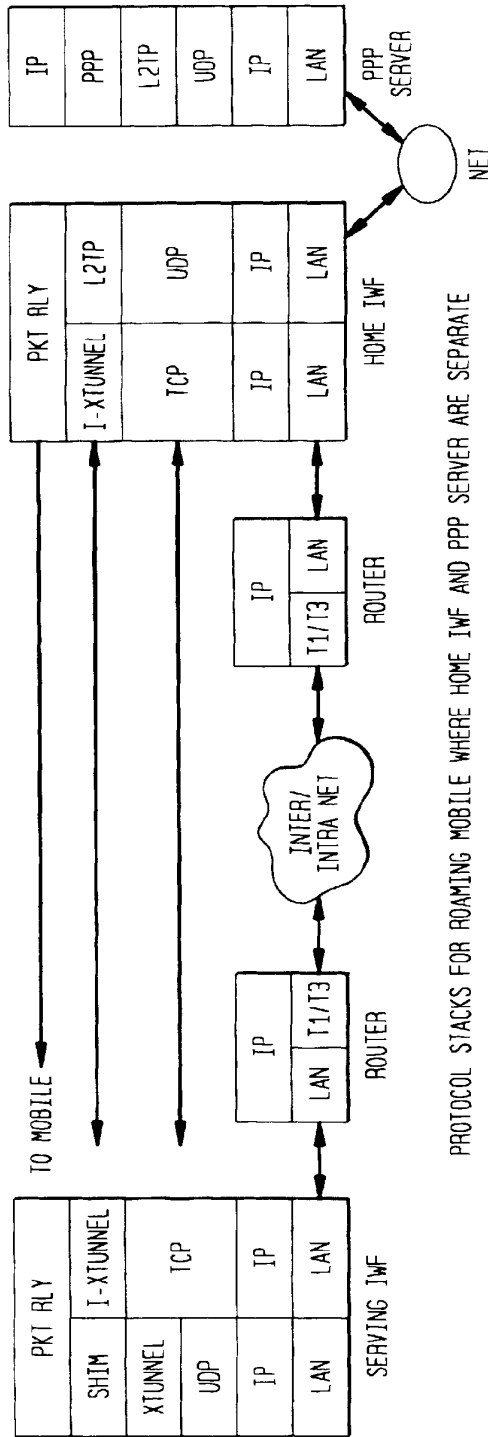


FIG. 30



PROTOCOL STACKS FOR ROAMING MOBILE WHERE HOME IWF IS ALSO A PPP SERVER

FIG. 31



PROTOCOL STACKS FOR ROAMING MOBILE WHERE HOME IWF AND PPP SERVER ARE SEPARATE

FIG. 32

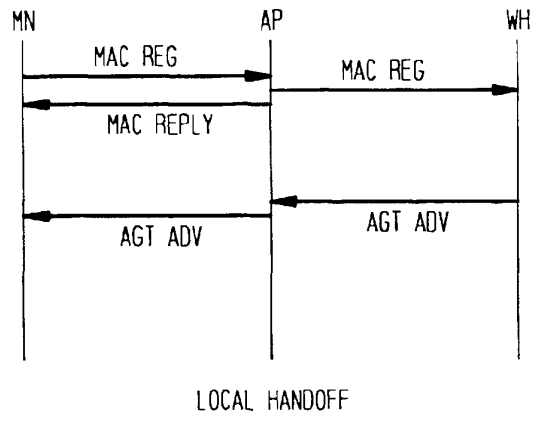


FIG. 33

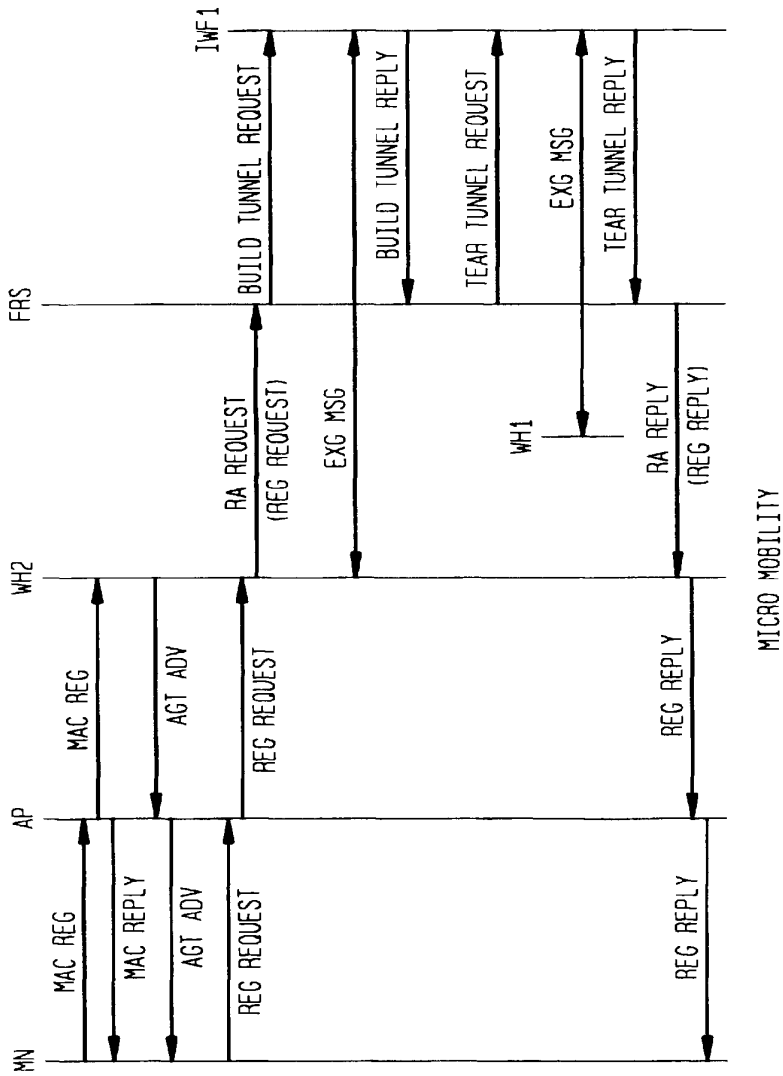


FIG. 34

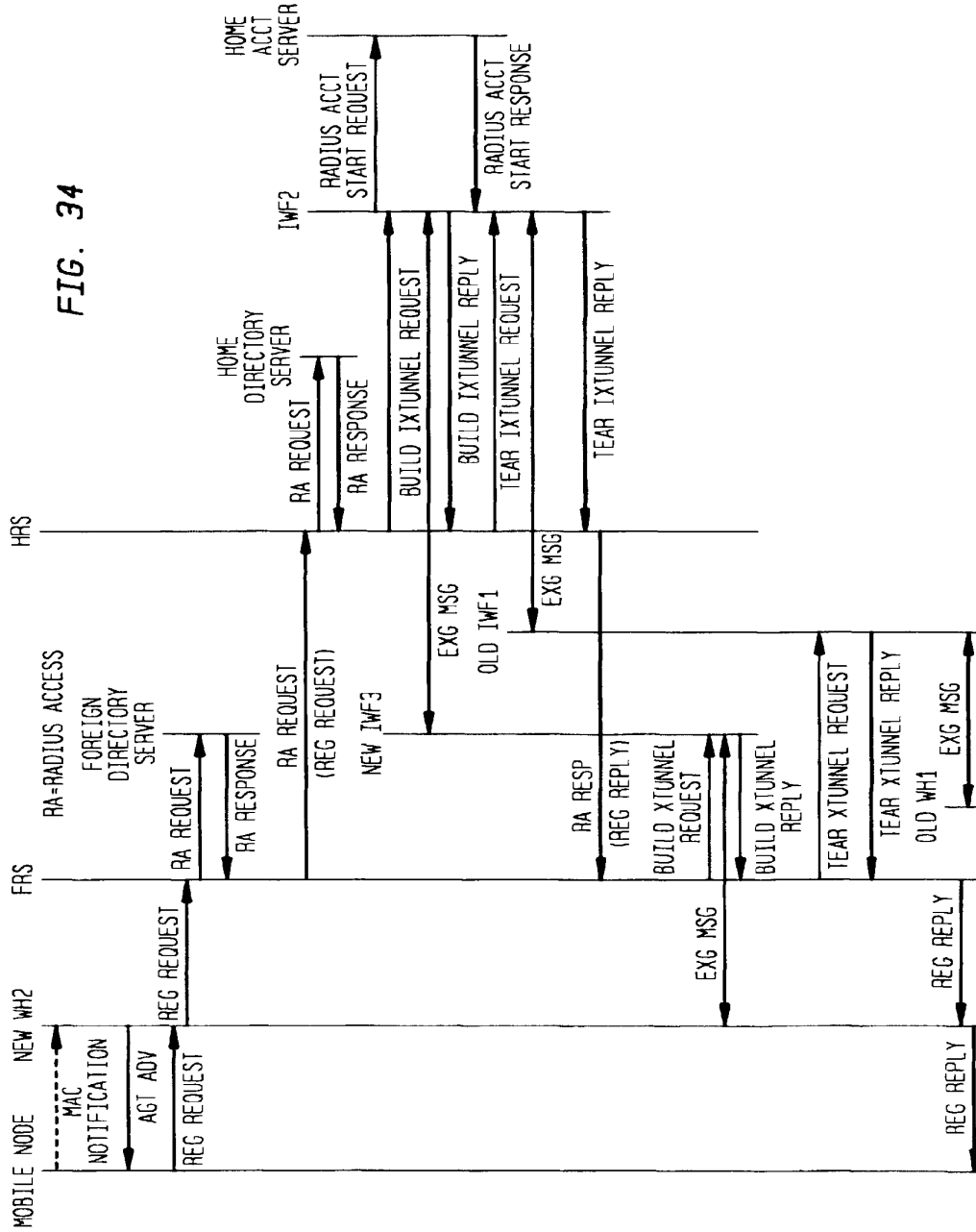


FIG. 35

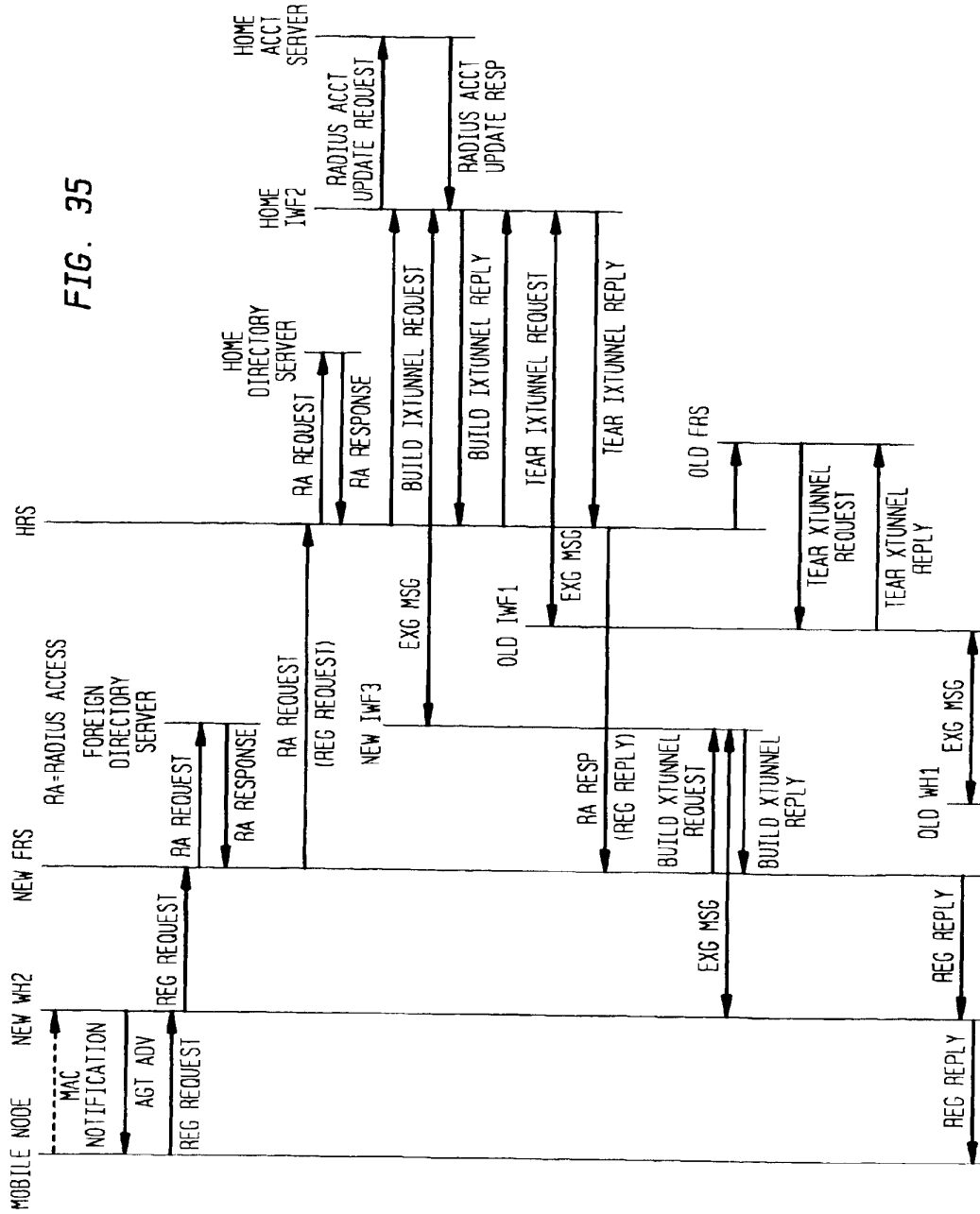


FIG. 36

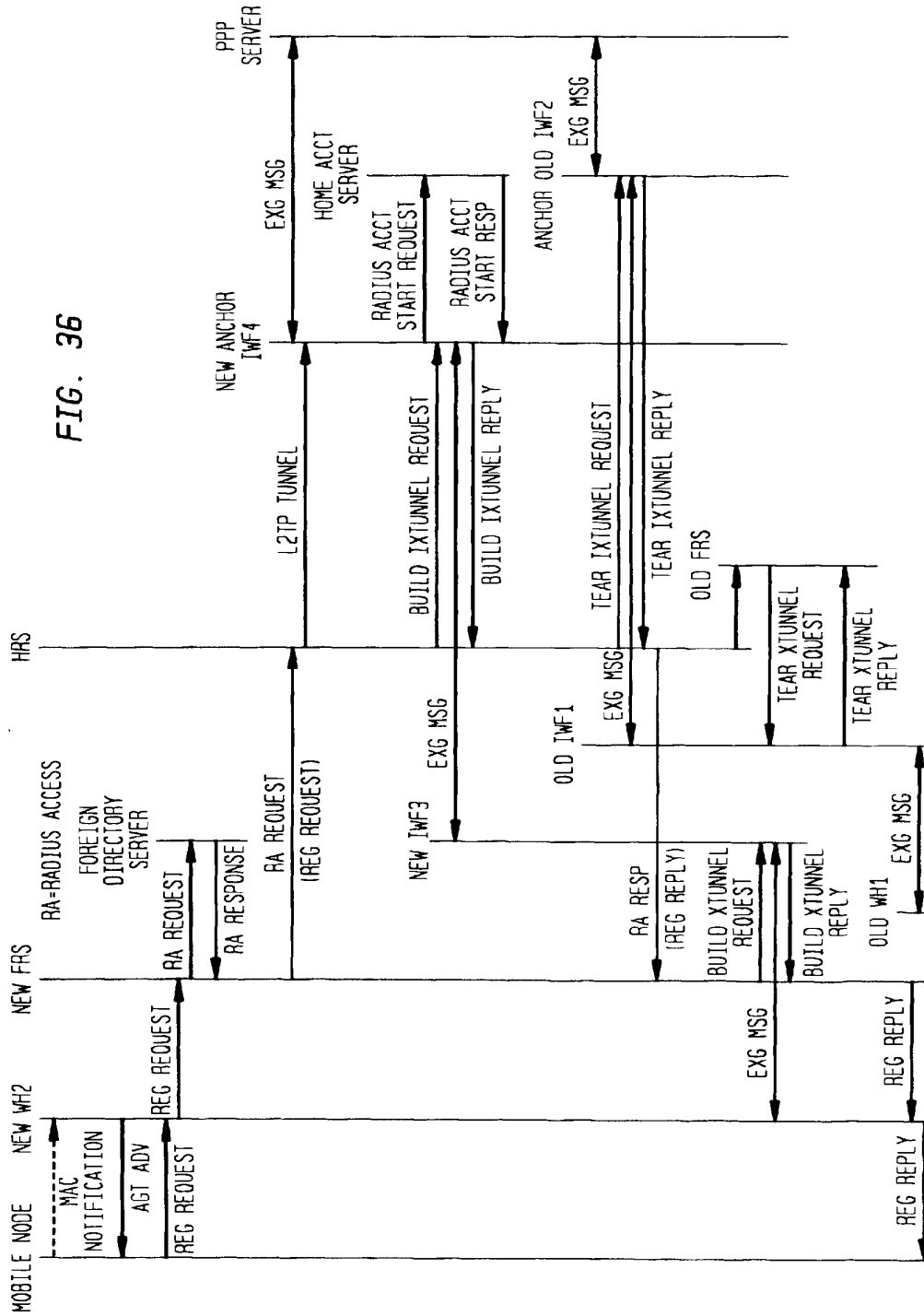


FIG. 37

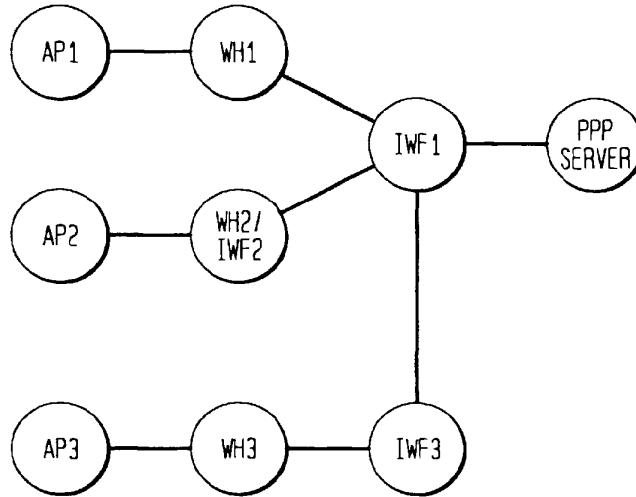
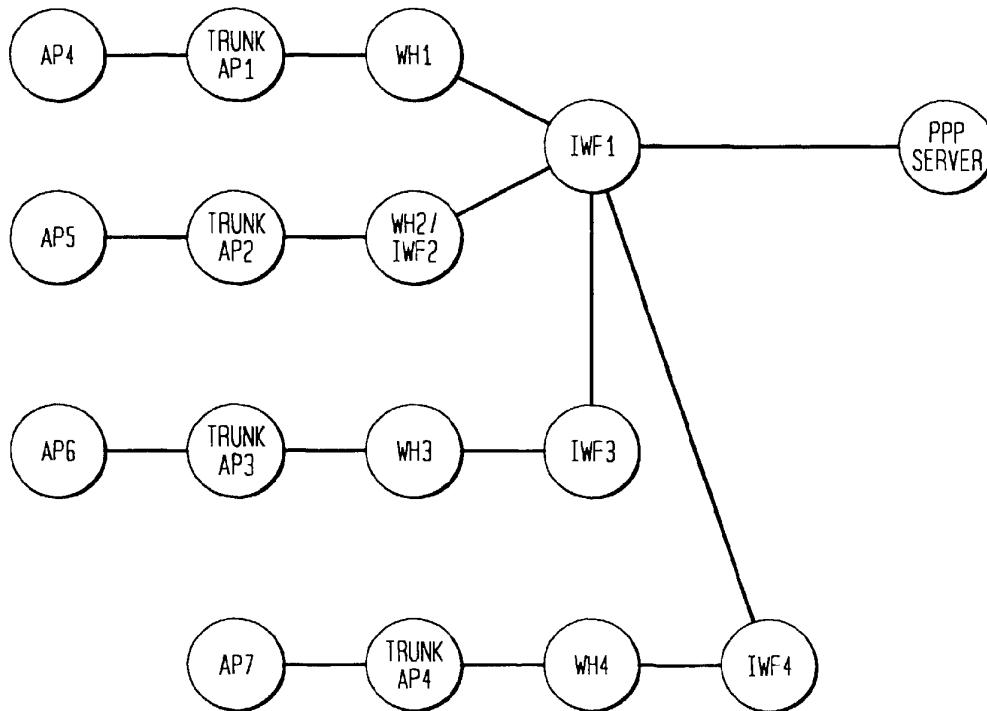


FIG. 38



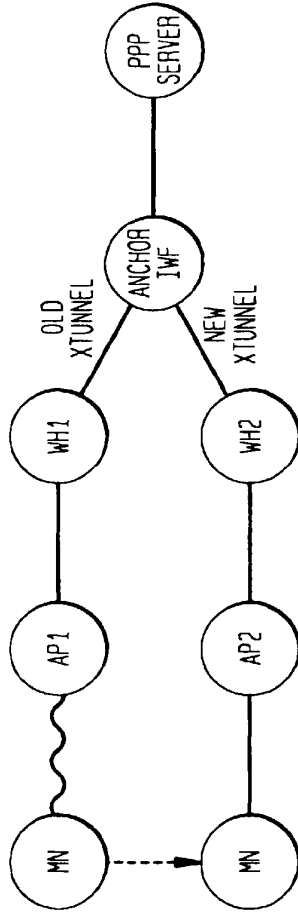


FIG. 39

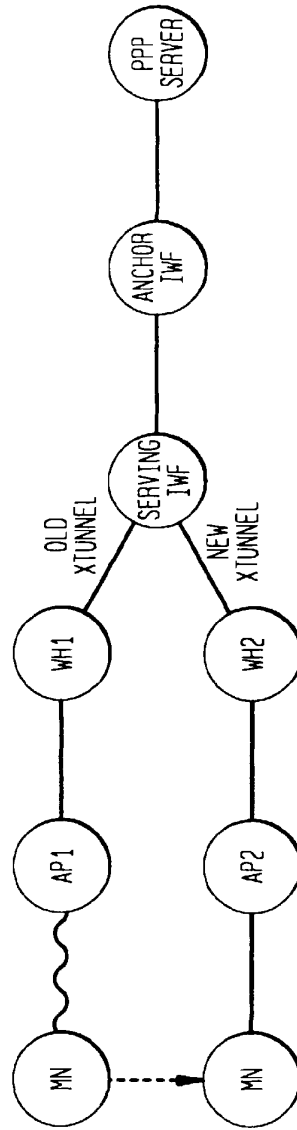


FIG. 40

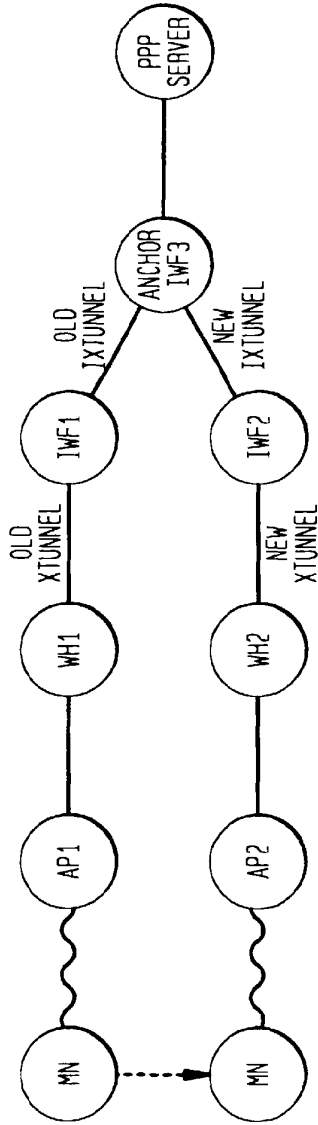


FIG. 41

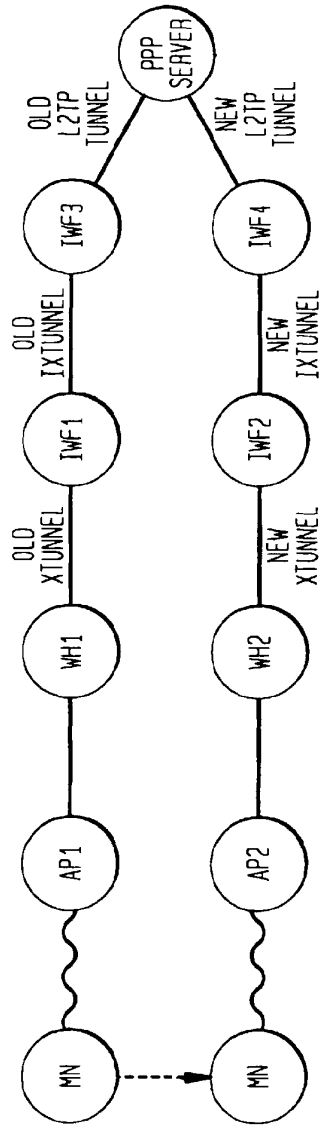
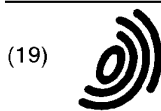


FIG. 42



Europäisches Patentamt
 European Patent Office
 Office européen des brevets



(11) EP 0 924 914 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
 23.06.1999 Bulletin 1999/25

(51) Int Cl. 6: H04L 29/06

(21) Application number: 98660119.3

(22) Date of filing: 10.11.1998

(84) Designated Contracting States:
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
 MC NL PT SE**
 Designated Extension States:
AL LT LV MK RO SI

(72) Inventor: **Turunen, Matti**
 33560 Tampere (FI)

(74) Representative: **Johansson, Folke Anders et al**
Nokia Mobile Phones Ltd.,
Intellectual Property Rights,
Keilalahdentie 4
02150 Espoo (FI)

(30) Priority: 18.12.1997 FI 974557

(71) Applicant: **NOKIA MOBILE PHONES LTD.**
 02150 Espoo (FI)

(54) Mobile internet protocol

(57) A method of enabling roaming of a mobile internet-access terminal from a first to a second internet access network each of which has a home agent for routing internet datagrams between networks. The method comprises de-registering the mobile terminal from said first network and registering it with said second network and allocating to the mobile terminal a new internet address in said second network. This new internet address

is transmitted to the first network's home agent which registers that address as a care-of-address or co-located care-of-address for the mobile host. Datagrams addressed to the new internet address are sent directly to the mobile host via the second network's home agent. Datagrams addressed to a previous internet address of the mobile terminal in said first network are forwarded from that network's home agent to the mobile host, via the second network's home agent.

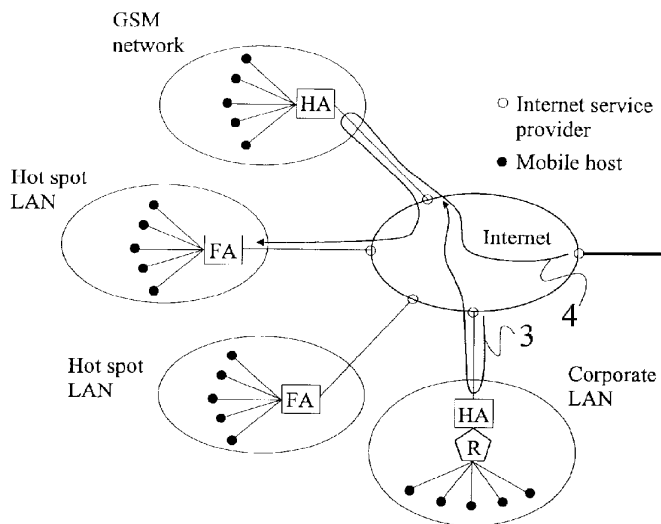


Figure 3

EP 0 924 914 A2

Description

[0001] The present invention relates to mobile internet protocol and in particular to a mobile internet protocol which provides for the mobility of mobile internet access hosts between two or more internet access networks.

[0002] Corporate users have traditionally accessed the internet from a fixed location within a Local Area Network (LAN), a user's LAN often being referred to as his "home" network (HN). The user interface to the internet is typically a personal computer (the "host"). As is illustrated in Figure 1, the home network is connected to an internet service provider which routes internet data, so-called "datagrams", between the home network and the internet, the internet in turn comprising other routers and service providers which route data to and from other "foreign" networks (FN).

[0003] In order to be able to transmit and receive datagrams to and from the internet, a host requires an internet address. A corporate home network is typically allocated a set of internet addresses by a national authority and the home network can assign these either fixedly or dynamically to hosts attached to the home network (using for example the Dynamic Host Configuration Protocol DHCP). The allocated set of internet addresses comprise a common prefix portion which identifies the home network, whilst a suffix portion identifies the destination host. When a datagram is received by a home network, a router (R) of the home network polls the attached hosts to determine which host corresponds to the internet address conveyed with the datagram. The datagram is then forwarded by the router to the identified host.

[0004] With the recent rapid advances in mobile communication technology, and in particular of wireless technologies, there has come a desire to gain internet access from mobile hosts or terminals, for example a laptop computer coupled to a cellular telephone. At present, this is available via certain digital telephone networks (e.g. GSM). As with conventional fixed line internet access, a mobile host may have a fixedly or dynamically assigned internet address, allocated by a service provider who is usually the cellular telephone network operator. In the case of mobile internet access, a communication channel between the mobile host and the network is reserved for the duration of the call. Internet data destined for the mobile host is received by the network and is sent to the host over the reserved channel.

[0005] This system works satisfactorily whilst a mobile host remains within one homogeneous network. However, it does not provide for "roaming" between different types of networks or between networks operated by different operators. When a mobile host "de-registers" with one network and registers with a new network, there is no mechanism for forwarding internet datagrams, addressed to the old network, to the new network

as the communication channel between the mobile host and the old network no longer exists. It is therefore necessary to open a new communication channel between the mobile host and the new network. All datagrams addressed to the old network and not yet received by the mobile host are lost as a result of this channel change.

[0006] The desire for roaming is likely to increase in the near future as the provision of corporate wireless LANs becomes commonplace. A corporate user will have the opportunity to make wireless voice and data calls from a mobile terminal via the corporate LAN whilst he is inside the coverage area of that LAN. When the user leaves that area, he will then be able to connect to a digital cellular telephone network. In addition, so-called "hot-spot" LANs are likely to be provided in areas where high data capacity is required, e.g. airports, shopping centres. In all probability, hot-spot LANs will be operated by the cellular network operators although they may of course be operated by the property owners themselves.

[0007] A mobile internet access protocol which provides for roaming is currently being standardised by the Internet Engineering Task Force (IETF). This protocol is known as RFC2002. A mobile internet protocol is also described in EP556012. These protocols make use of a "home agent", located in a mobile host's home network, to keep track of the host when it leaves the home network. A mobile host is fixedly allocated an internet address corresponding to the home network.

[0008] When a mobile host is registered to its home network, the functionality of the network's home agent is off for that host (i.e. the host is "deregistered" with the home agent) so that the home agent does not alter the flow of datagrams from the internet to the network's router and the mobile host (as indicated by reference numeral 1 in Figure 2). When the mobile host leaves its home network and contacts a foreign network (FN), the host is registered with a foreign agent (FA) of that network. The foreign agent then transmits to the mobile host an internet address of the foreign agent, and the mobile host in turn transmits the received internet address to the home network's home agent, together with a registration instruction. The home agent registers the new status of the mobile host and records the newly allocated internet address as a "care-of-address" for the host. Whenever the mobile host registers with a new foreign network, a new care-of-address is sent to the home network's home agent to replace the previously registered care-of-address.

[0009] It will be appreciated that, as a mobile host has a fixed internet address allocated to it, datagrams destined for the host will always be sent to the home network. If a mobile host has an active internet connection when it passes from its home network to a foreign network, and a datagram destined for the host subsequently arrives at the home network, the home agent determines that the mobile host is registered with a foreign agent and forwards the datagrams to the registered

care-of-address. A communication channel will have been reserved between the mobile host and the foreign agent, and the redirected datagram can be sent to the mobile host over this channel. Similarly, if a mobile host initiates a new internet access when registered with a foreign network, the host continues to use its allocated internet address. The home agent has already received the care-of-address and can again forward datagrams destined for the mobile host to the foreign agent for transfer to the host.

[0010] In some cases, the foreign network may dynamically assign an internet address to a visiting mobile host, e.g. if the foreign network does not have a foreign agent. This address is sent to the mobile host which in turn sends it to the home network's home agent as a care-of-address. Rather than just merely redirecting datagrams to the care-of-address, the home agent actually replaces the old internet address contained in the datagram with the co-located care-of-address before retransmitting the datagram. This particular form of care-of-address which identifies the mobile host as the end point for the redirected datagrams, rather than a foreign agent, is known as a "co-located care-of-address". It is noted however, that when the mobile host is accessing the internet via the foreign network, it still uses its fixedly allocated internet address. It will therefore be appreciated that regardless of whether the home agent receives a care-of-address or a co-located care-of-address all datagrams directed to a mobile host pass through the home network's home agent (as indicated by reference numeral 2 in Figure 2).

[0011] Where a cellular telephone operator operates a number of different networks, e.g. GSM and hot-spot LANs, in order to bill a subscriber using the roaming facility, the operator must collect details, e.g. call duration, location, from the foreign agents of each of the operated networks. This is necessary because internet data is not routed through any central facility of the operator but is rather routed through the home network's home agent to which the operator does not have access. Collecting this information for billing purposes is complex and time consuming.

[0012] It is an object of the present invention to obviate or at least mitigate the above noted problem of the currently proposed mobile internet protocol.

[0013] This and other objects are achieved by providing a home agent in a foreign network, in addition to the home agent in the home network.

[0014] According to a first aspect of the present invention there is provided a method of enabling roaming of a mobile host from a first to a second internet access network each of which has a home agent for routing internet datagrams between networks, the method comprising:

de-registering the mobile host from said first network and registering it with said second network; assigning to the mobile host a new internet address

in said second network;
transmitting said new internet address to the first network's home agent, and registering that transmitted address at the first network's home agent as a care-of-address or co-located care-of-address for the mobile host,
wherein datagrams addressed to said new internet address are sent directly to the mobile host via the second network's home agent, and datagrams addressed to an internet address previously assigned to the mobile host in said first network are forwarded, using said registered care-of-address or co-located care-of-address, from that network's home agent to the mobile host via the second network's home agent.

[0015] Preferably, the method set out above is performed in reverse when the mobile host roams from the second network to the first network, so that datagrams sent to an old address in the second network are forwarded to the mobile host in the first network.

[0016] The present invention may be applied to provide mobility for a mobile host between a corporate local area network (LAN) or wide area network (WAN), and a cellular telephone network. The corporate LAN or WAN may be a fixed line network or a wireless network. The cellular telephone network may comprise, for example, a GSM (Global System for Mobile Communications) network. The cellular telephone network may alternatively, or in addition, comprise one or more subnetworks, i.e. wireless LANs or WANs (known as "hot-spot" LANs or WANs). As the cellular telephone network has a single home agent through which all internet datagrams are routed when the mobile host is registered to the cellular network, the network operator can collect all internet call data for a mobile host from its own home agent. There is thus no need to obtain such information from the home agent of the corporate network or from a number of foreign agents associated with the different GSM and hot-spot LAN/WAN networks. When the mobile host is registered with the corporate network however, all new internet connections are made using the corporate network's home agent as home internet address. This typically presents a more cost effective option for the subscriber.

[0017] An advantage of embodiments of the present invention is that the transmission route from a source host to the destination mobile host may be shortened when the mobile host is visiting a foreign network, as compared to prior proposals. This is because datagrams do not necessarily have to be routed via the mobile host's home network but instead can be sent directly to the foreign network.

[0018] It will be appreciated that the mobile host comprises an access point to the internet. The user interface may be a personal computer, e.g. a laptop computer, coupled to the access point. In order to allow the user interface to connect to the access point, the user inter-

face may be connected to a cellular telephone. Alternatively, the user interface may be a computer or personal digital assistant incorporating a cellular telephone.

[0019] The new internet address in the second network assigned to the mobile host may be an internet address allocated to the second network's home agent. In this case the address is a care-of-address. Alternatively, the internet address may be an address dynamically assigned to the mobile host, in which case the address is a co-located care-of-address.

[0020] According to a second aspect of the present invention there is provided apparatus for enabling roaming of a mobile host from a first to a second internet access network, the apparatus comprising:

second network control means for registering the mobile host to the second network and for transmitting to the mobile host a new internet address in the second network to replace any internet address previously allocated to the host;

transmission means for transmitting said new internet address from the mobile host to the home agent in the first network;

first network control means for registering said transmitted address at the first network's home agent as a care-of-address or co-located care-of-address for the mobile host; and

datagram routing means in said first network for forwarding datagrams received at said first network and destined for the mobile host to the mobile host via the second network's home agent.

[0021] For a better understanding of the present invention and in order to show how the same may be carried into effect reference will now be made, by way of example, to the accompanying drawings, in which:

Figure 1 illustrates schematically a fixed host internet access system according to the prior art;

Figure 2 illustrates schematically a mobile host internet access system according to the prior art; and

Figure 3 illustrates schematically a mobile host internet access system according to an embodiment of the present invention.

[0022] As has already been described, Figures 1 and 2 illustrate respectively, conventional fixed host and mobile host internet access systems.

[0023] With reference to Figure 3, there is illustrated a wireless corporate LAN in which a number of mobile hosts are coupled to a common network home agent (HA) via a router (R). The corporate LAN is connected via one or more fixed land lines to an internet service provider which provides connectivity and routing functions between the corporate LAN and the internet.

[0024] Whilst a mobile host is registered to the corporate LAN, the host either has a fixed internet address or an address dynamically assigned by the router. In either

case, the host's address is one of those assigned to the corporate LAN. The home address is attached to datagrams sent from the mobile host to the internet and enables return datagrams to be correctly delivered back to the home agent at the corporate LAN.

[0025] Figure 3 also illustrates a GSM cellular telephone network together with two so-called hot spot LANs. The GSM network provides cellular telephone services to subscribers over a wide geographical area whilst the hot spot LANs provide relatively high capacity telephone services over a smaller, local area. The geographical coverage of the GSM network may overlap with that of the hot spot LANs. In the present example, the GSM network and the two hot spot LANs are operated by the same operator which bills subscribers using any or all of the operated networks by way of a single bill.

[0026] If a mobile host subscribing to the corporate LAN and to the cellular telephone network leaves the coverage area of the corporate LAN and enters that of the cellular telephone network (either GSM or hot spot LAN), the host will deregister with the former whilst registering with the latter. Upon registration with the telephone network, the network assigns and transmits to the mobile host a new internet address in that network. This new address is either one of a number of addresses allocated to the GSM network and defining the home agent as the end point, or is dynamically assigned to the mobile host (e.g. using DHCP) to define the mobile host as the end point. In either case, the new address replaces the internet address allocated to the host when it was registered to the corporate LAN. Datagrams destined for the mobile host, and initiated via the cellular telephone network, are now sent directly to the cellular telephone network (see reference numeral 4 in Figure 3). This contrasts with previously proposed roaming protocols where the host retained the internet address assigned by the corporate LAN (i.e. the home network) and used an address assigned by the foreign network only as a care-of-address.

[0027] However, whilst new datagrams will be directed to the mobile host at the new internet address, some datagrams initiated using the old address in the corporate LAN may still be in transit. A registration message is therefore transmitted from the mobile host to the corporate LAN's home agent to register the mobile host's new internet address with the home agent (either as a care-of-address or as a co-located care-of-address). If the corporate LAN subsequently receives datagrams destined for the mobile host, the corporate LAN's home agent determines that the mobile host is now registered with a foreign network and it redirects the datagrams to the care-of-address or co-located care-of-address now registered for the mobile host. The GSM network's home agent receives these forwarded datagrams and redirects them to the mobile host, either directly or via a foreign agent in a hot spot LAN. This redirection route is indicated in Figure 3 by reference numeral 3.

[0028] When the mobile host moves between differ-

ent "sub-networks" of the cellular telephone network, e.g. from the GSM network to a hot spot LAN, there is no need to update the care-of-address or co-located care-of-address at the corporate network's home agent. It is only necessary to update the location details of the mobile host at the GSM network's home agent.

[0029] On the mobile host returning from the cellular telephone network to the corporate LAN, the process described above is repeated in reverse. The mobile host deregisters to the cellular telephone network and registers with the corporate LAN. The mobile host sends its new internet address in the corporate LAN to the home agent of the GSM network as a care-of-address (or co-located care-of-address) for the mobile host.

[0030] When the cellular telephone operator wishes to bill a subscriber for using its networks, all the necessary information is held in the GSM network's home agent. However, the subscriber remains able to avoid using the cellular telephone network, and therefore minimise his costs, when he is connected to the corporate LAN (except of course when receiving datagrams directed to an old cellular telephone network home address).

[0031] It will be appreciated that the cellular telephone network described above may comprise more or fewer than three subnetworks. It will also be appreciated that the corporate network may comprise a number of different subnetworks, all sharing a common home agent. The invention may also be applied to more than two networks, e.g. to a corporate network and to two cellular telephone networks operated by different operators.

[0032] It will be appreciated by a person of skill in the art that modifications may be made to the above described embodiment without departing from the scope of the present invention.

Claims

1. A method of enabling roaming of a mobile host from a first to a second internet access network each of which has a home agent for routing internet datagrams between networks, the method comprising:

de-registering the mobile host from said first network and registering it with said second network;
 assigning to the mobile host a new internet address in said second network;
 transmitting said new internet address to the first network's home agent, and registering that transmitted address at the first network's home agent as a care-of-address or co-located care-of-address for the mobile host,
 wherein datagrams addressed to said new internet address are sent directly to the mobile host via the second network's home agent, and datagrams addressed to an internet address previously assigned to the mobile host in said

first network are forwarded, using said registered care-of-address or co-located care-of-address, from that network's home agent to the mobile host via the second network's home agent.

2. A method according to claim 1, wherein said first and second networks are one of a corporate local area network (LAN) or wide area network (WAN), and a cellular telephone network.
3. A method according to claim 2, wherein the corporate LAN or WAN is one of a fixed line network or a wireless network.
4. A method according to claim 2 or 3, wherein the cellular telephone network comprises a GSM (Global System for Mobile Communications) network.
5. A method according to any one of claims 2 to 4, wherein the cellular telephone network comprises a plurality of subnetworks.
6. A method according to claim 5, wherein one or more of said subnetworks is/are wireless LANs or WANs.
7. Apparatus for enabling roaming of a mobile host from a first to a second internet access network, the apparatus comprising:

second network control means for registering the mobile host to the second network and for transmitting to the mobile host a new internet address in the second network to replace any internet address previously allocated to the host;
 transmission means for transmitting said new internet address from the mobile host to the home agent in the first network;
 first network control means for registering said transmitted address at the first network's home agent as a care-of-address or co-located care-of-address for the mobile host; and
 datagram routing means in said first network for forwarding datagrams received at said first network and destined for the mobile host to the mobile host via the second network's home agent.

8. Apparatus according to claim 7, wherein at least one of said first and second networks is a wireless telephone network and said mobile host is a wireless terminal.

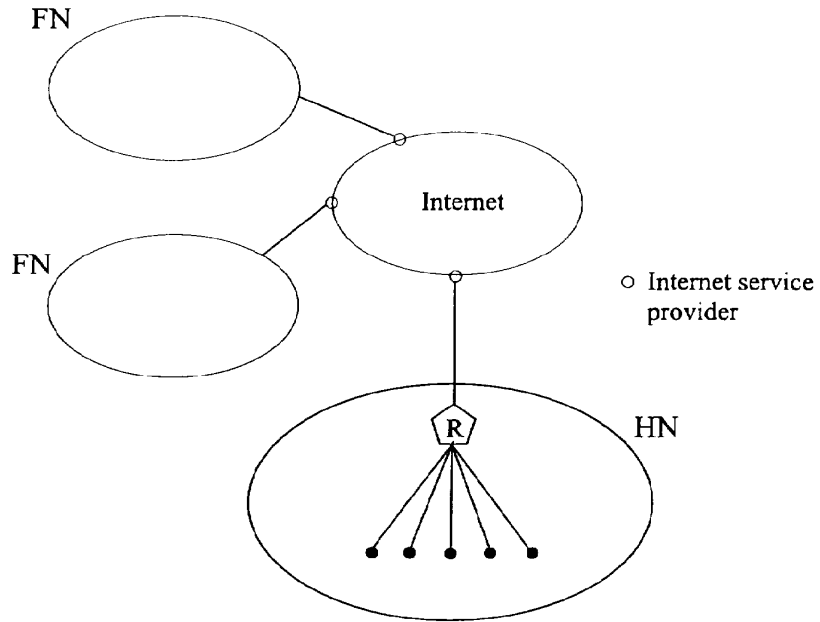


Figure 1

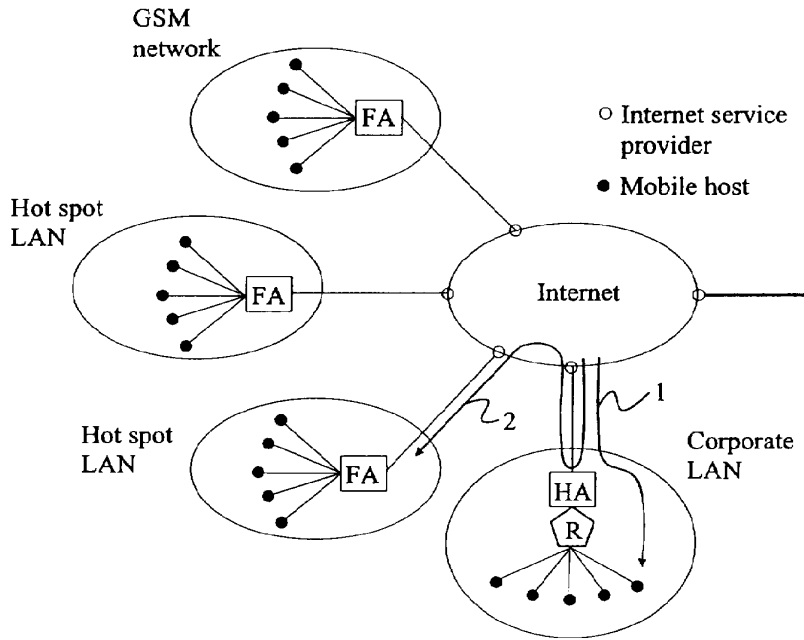


Figure 2

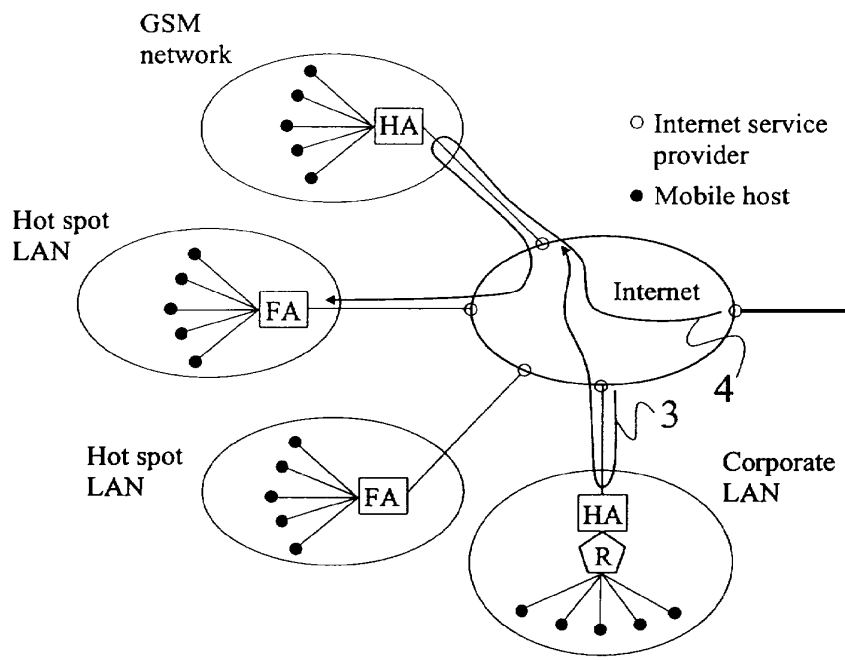


Figure 3



Europäisches Patentamt
 European Patent Office
 Office européen des brevets



(11) EP 0 935 364 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication: 11.08.1999 Bulletin 1999/32
 (51) Int. Cl.⁶: H04L 12/24, H04M 11/06
 (21) Application number: 98124499.9
 (22) Date of filing: 29.12.1998

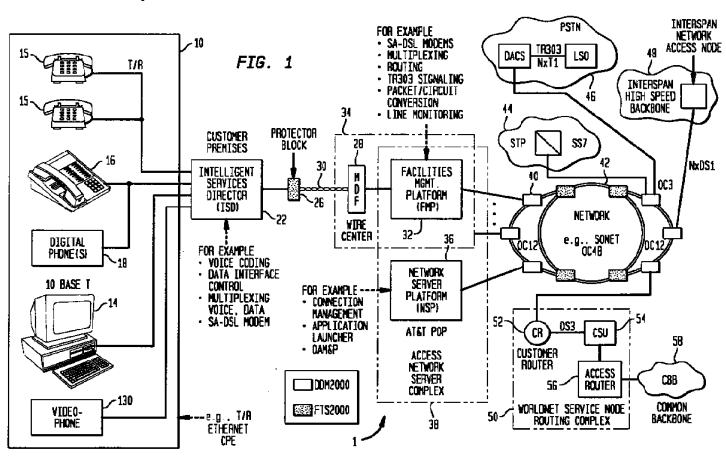
(84) Designated Contracting States:
 AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
 MC NL PT SE
 Designated Extension States:
 AL LT LV MK RO SI
 (30) Priority: 31.12.1997 US 1582
 (71) Applicant: AT&T Corp.
 New York, NY 10013-2412 (US)
 (72) Inventors:
 • Gerszberg, Irwin
 Kendall-Park, New Jersey 08824 (US)

• Huang, Kenny Xiaojian
 Somerset, New Jersey 08873 (US)
 • Kwabi, Christopher K.
 Englewood, New Jersey 07631 (US)
 • Roy, Sumit
 Scotch Plains, 2New Jersey 07076 (US)
 (74) Representative:
 Modiano, Guido, Dr.-Ing. et al
 Modiano, Josif, Pisanty & Staub,
 Baaderstrasse 3
 80469 München (DE)

(54) A network server platform for a hybrid fiber twisted pair local loop network service architecture

(57) This invention provides a network server platform forming part of a new local loop network architecture designed to overcome the limitations of current art local access loop technologies. This invention allows end users to seamlessly connect to the numerous disparate networks in order to access the multiplicity of services that these networks have to offer. The network server platform allows interconnection between networks with varying networking protocols. The network server platform is a key component of the new architecture and interacts to allow for easy and seamless inte-

gration with network components on both the local access level as well as the core network. The network server platform offers external networking capabilities to the local access network. As a result, the local access network terminates on the network server platform. The network server platform provides subscribers or end users the capabilities to access services from a multiplicity of disparate networks offering a variety of services.



EP 0 935 364 A2

Description

Field of the Invention

[0001] This invention discloses a network server platform that terminates the network layer of the local access loop and handles connection management between the local access facilities and the communications network for maintaining services for those facilities.

Background

[0002] As deregulation of the telephone industry continues and as companies prepare to enter the local telephone access market, there is a need to offer new and innovative services that distinguish common carriers from their competitors. This cannot be accomplished without introducing new local access network architectures that will be able to support these new and innovative services.

[0003] Conventionally, customer premises telephone and/or data connections contain splitters for separating analog voice calls from other data services such as Ethernet transported over digital subscriber line (DSL) modems. Voice band data and voice signals are sent through a communications switch in a central or local office to an interexchange carrier or Internet service provider. DSL data is sent through a digital subscriber loop asynchronous mode (DSLAM) switch which may include a router. The DSLAM switch connects many lines and routes the digital data to a telephone company's digital switch.

[0004] A major problem with this configuration is that interexchange carriers attempting to penetrate the local telephone company's territory must lease trunk lines from the local telephone company switch to the interexchange company's network for digital traffic. Furthermore, the Internet service provider must lease a modem from the local phone company in the DSLAM switch and route its data through the local phone company's digital switch. Thus, the local phone company leases and/or provides a significant amount of equipment, driving up the cost of entry for any other company trying to provide local telephone services and making it difficult for the interexchange companies to differentiate their services. Furthermore, since DSL modem technology is not standardized, in order to ensure compatibility, the DSL modem provided by the local telephone company must also be provided to the end user in the customer premises equipment (CPE). Additionally, since the network is not completely controlled by the interexchange companies, it is difficult for the interexchange companies to provide data at committed delivery rates. Any performance improvements implemented by the interexchange companies may not be realized by their customers, because the capabilities of the local telephone company equipment may or may not meet their

performance needs. Thus, it is difficult for the interexchange companies to convince potential customers to switch to their equipment or to use their services. These factors ensure the continued market presence of the local telephone company.

[0005] As part of this system, there is a need for improved architectures, services and equipment utilized to distinguish the interexchange companies' products and services. Current local access network topologies suffer from major drawbacks which limit their applications and their ability to expand with changing technology. Interexchange companies are restricted by the current infrastructure and are limited in the number and variety of new and enhanced services that can be offered to end users. In the expansion of new services, end users desire a seamless connect to the numerous disparate networks in order to access the multiplicity of services that these networks have to offer. The network server platform allows interconnection between networks with varying networking protocols.

Summary of the Invention

[0006] In order to provide an improved network, it is desirable for the interexchange companies to have access to at least one of the twisted-pair lines or alternate wireless facility connecting each of the individual users to the local telephone network before the lines are routed through the conventional local telephone network equipment. It is preferable to have access to these lines prior to the splitter and modem technology offered by the local service providers. By having access to the twisted-pair wires entering the customer's premises, interexchange companies can differentiate their services by providing higher bandwidth, improving the capabilities of the customer premises equipment, and lowering overall system costs to the customer by providing competitive service alternatives.

[0007] The new architecture may utilize a video phone and/or other devices to provide new services to an end user; an intelligent services director (ISD) disposed near the customer's premises for multiplexing and coordinating many digital services onto a single twisted-pair line; a facilities management platform (FMP) disposed in the local telephone network's central office for routing data to an appropriate interexchange company network; and a network server platform (NSP) coupled to the FMP for providing new and innovative services to the customer and for distinguishing services provided by the interexchange companies from those services provided by the local telephone network.

[0008] As part of this system, one aspect of the invention provides a network server platform forming part of a new local loop network architecture designed to overcome the limitations of current art local access loop technologies. This invention allows end users to seamlessly connect to the numerous disparate networks in order to access the multiplicity of services that these

networks have to offer. The network server platform allows interconnection between networks with varying networking protocols.

[0009] The network server platform is a key component of the new architecture and interacts to allow for easy and seamless integration with network components on both the local access level as well as the core network. The network server platform offers external networking capabilities to the local access network. As a result, the local access network terminates on the network server platform. The network server platform provides subscribers or end users the capabilities to access services from a multiplicity of disparate networks offering a variety of services. Brief Description of the Drawings

[0010] The foregoing summary of the invention, as well as the following detailed description of preferred embodiments, is better understood when read in conjunction with the accompanying drawings, which are included by way of example, and not by way of limitation with regard to the claimed invention.

Fig. 1 illustrates an embodiment of a hybrid fiber twisted pair local loop architecture.

Fig. 2 is a block diagram of an embodiment of an intelligent services director consistent with the architecture shown in Fig. 1.

Fig. 3A and 3B illustrate an embodiment of a video phone consistent with the architecture shown in Fig. 1.

Fig. 4A is a block diagram of an embodiment of a facilities management platform consistent with the architecture shown in Fig. 1.

Fig. 4B illustrates a block diagram of an embodiment of a network server platform consistent with the architecture shown in Fig. 1.

Figure 5 illustrates a diagram of the network server platform internal architecture;

Figure 6 illustrates a diagram of the network server platform;

Figure 7 illustrates a diagram of the network server platform building blocks;

Figure 8 illustrates a diagram of the network server platform software layer architecture;

Figure 9 illustrates a diagram of the application server platform software architecture;

Figure 10 illustrates a diagram of the operations, administration, maintenance and provision services in the server platform software architecture;

Figure 11 illustrates a diagram of a single network server platform connected to a plurality of facilities management platforms that are in turn connected to a plurality of intelligent services directors.

Figure 12 illustrates a diagram of the systems and services voice protocol stack option from the facilities management platform to the network;

Figure 13 illustrates a diagram of the systems and services data protocol stack from the facilities man-

agement platform to the network;

Figure 14 illustrates a diagram of the systems and services protocol stack for voice services (Option 1) from the intelligent services director to the public switched telephone network using asynchronous transfer mode;

Figure 15 illustrates a diagram of the protocol stack for voice services (Option 2) from the intelligent services director to the public switched telephone network using a TR303 interface;

Figure 16 illustrates a diagram of the systems and services architecture protocol stack for data services using point-to-point protocol in asynchronous transfer mode;

Figure 17 illustrates a diagram of the systems and services protocol stack for data services using asynchronous transfer mode signaling;

Figure 18 illustrates a diagram of the systems and services architecture employing a virtual private data network "ExtraNet";

Figure 19 illustrates a diagram of systems and services architecture of the virtual private data network "ExtraNet" protocol;

Figure 20 illustrates a diagram of the systems and services architecture user service menu launcher;

Figure 21 illustrates a diagram of the systems and services architecture user service application manager;

Figure 22 illustrates a diagram of the systems and services architecture for basic voice;

Figure 23 illustrates a diagram of the systems and services architecture for Internet connectivity;

Figure 24 illustrates a diagram of the systems and services architecture for AT&T bill viewing services;

Figure 25 illustrates a diagram of the systems and services architecture describing the telecommute over MetroLan using a frame relay backbone;

Figure 26 illustrates a diagram of the systems and services architecture describing the telecommute over MetroLan using the Internet;

Figure 27 illustrates a diagram of the systems and services architecture for directory services employing network server platform hosting; Figure 28 illustrates a diagram of the systems and services architecture for video delivery services employing network server platform hosting; and

Figure 29 illustrates a diagram of the systems and services architecture for information pushing services and information auto-delivery services.

Detailed Description of Preferred Embodiments

[0011] The following applications, filed concurrently herewith, are hereby incorporated by reference:

1. A Hybrid Fiber Twisted-pair Local Loop Network Service Architecture (Gerszberg 41-3-13);
2. Dynamic Bandwidth Allocation for use in the

- Hybrid Fiber Twisted-pair Local Loop Network Service Architecture (Gerszberg 42-4-14);
- 3. The VideoPhone (Gerszberg 43-9-2);
- 4. VideoPhone Privacy Activator (Gerszberg 44-10-3);
- 5. VideoPhone Form Factor (Gerszberg 45-11-4);
- 6. VideoPhone Centrally Controlled User Interface With User Selectable Options (Gerszberg 46-12-5);
- 7. VideoPhone User Interface Having Multiple Menu Hierarchies (Gerszberg 47-13-6);
- 8. VideoPhone Blocker (Gerszberg 79-38-26);
- 9. VideoPhone Inter-com For Extension Phones (Gerszberg 48-14-7);
- 10. Advertising Screen Saver (53-17);
- 11. VideoPhone FlexiView Advertising (Gerszberg 49-15-8);
- 12. VideoPhone Multimedia Announcement Answering Machine (Gerszberg 73-32-20);
- 13. VideoPhone Multimedia Announcement Message Toolkit (Gerszberg 74-33-21);
- 14. VideoPhone Multimedia Video Message Reception (Gerszberg 75-34-22);
- 15. VideoPhone Multimedia Interactive Corporate Menu Answering Machine Announcement (Gerszberg 76-35-23);
- 16. VideoPhone Multimedia Interactive On-Hold Information Menus (Gerszberg 77-36-24);
- 17. VideoPhone Advertisement When Calling Video Non-enabled VideoPhone Users (Gerszberg 78-37-25);
- 18. Motion Detection Advertising (Gerszberg 54-18-10);
- 19. Interactive Commercials (Gerszberg 55-19);
- 20. VideoPhone Electronic Catalogue Service (Gerszberg 50-16-9);
- 21. A Facilities Management Platform For Hybrid Fiber Twisted-pair Local Loop Network, Service Architecture (Barzegar 18-56-17);
- 22. Multiple Service Access on Single Twisted-pair (Barzegar (16-51-15);
- 23. Life Line Support for Multiple Service Access on Single Twisted-pair (Barzegar 17-52-16);
- 24. A Network Server Platform for a Hybrid Fiber Twisted Pair Local Loop Network Service Architecture (Gerszberg 57-4-2-2-4)
- 25. A Communication Server Apparatus For Interactive Commercial Service (Gerszberg 58-20-11);
- 26. NSP Multicast, PPV Server (Gerszberg 59-21-12);
- 27. NSP Internet, JAVA Server and VideoPhone Application Server (Gerszberg 60-5-3-22-18);
- 28. NSP WAN Interconnectivity Services for Corporate Telecommuters (Gerszberg 71-9-7-4-21-6);
- 29. NSP Telephone Directory White-Yellow Page Services (Gerszberg 61-6-4-23-19);
- 30. NSP Integrated Billing System For NSP services and Telephone services (Gerszberg 62-7-5-24-20);

- 31. Network Server Platform / Facility Management Platform Caching Server (Gerszberg 63-8-6-3-5);
- 32. An Integrated Services Director (ISD) For HFTP Local Loop Network Service Architecture (Gerszberg 72-36-22-12);
- 33. ISD and VideoPhone Customer Premise Network (Gerszberg 64-25-34-13-5);
- 34. ISD Wireless Network (Gerszberg 65-26-35-14-6);
- 35. ISD Controlled Set-Top Box (Gerszberg 66-27-15-7);
- 36. Integrated Remote Control and Phone (Gerszberg 67-28-16-8);
- 37. Integrated Remote Control and Phone User Interface (Gerszberg 68-29-17-9);
- 38. Integrated Remote Control and Phone Form Factor (Gerszberg 69-30-18-10);
- 39. VideoPhone Mail Machine (Attorney Docket No. 3493.73170);
- 40. Restaurant Ordering Via VideoPhone (Attorney Docket No. 3493.73171);
- 41. Ticket Ordering Via VideoPhone (Attorney Docket No. 3493.73712);
- 42. Multi-Channel Parallel/Serial Concatenated Convolutional Codes And Trellis Coded Modulation Encode/Decoder (Gelblum 4-3);
- 43. Spread Spectrum Bit Allocation Algorithm (Shively 19-2);
- 44. Digital Channelizer With Arbitrary Output Frequency (Helms 5-3);
- 45. Method And Apparatus For Allocating Data Via Discrete Multiple Tones (filed 12/22/97, Attorney Docket No. 3493.20096--Sankaranarayanan 1 - 1);
- 46. Method And Apparatus For Reducing Near-End Cross Talk In Discrete Multi-Tone Modulators/Demodulators (filed 12/22/97, Attorney Docket No. 3493.37219--Helms 4-32-18).

[0012] The present application is number 24 on this list.

[0013] In addition, the following two patent applications are incorporated by reference:

- 1. U.S. Patent Application 08/943,312 filed October 14, 1997 entitled Wideband Communication System for the Home, to Robert R. Miller, II and Jesse E. Russell, and
- 2. U.S. Patent Application No. 08/858,170, filed May 14, 1997, entitled Wide Band Transmission Through Wire, to Robert R. Miller, II, Jesse E. Russell and Richard R. Shively.

[0014] Referring to Fig. 1, a first exemplary communication network architecture employing a hybrid fiber, twisted-pair (HFTP) local loop 1 architecture is shown. An intelligent services director (ISD) 22 may be coupled to a central office 34 via a twisted-pair wire, hybrid fiber interconnection, wireless and/or other customer con-

nection 30, a connector block 26, and/or a main distribution frame (MDF) 28. The ISD 22 and the central or local office 34 may communicate with each other using, for example, framed, time division, frequency-division, synchronous, asynchronous and/or spread spectrum formats, but in exemplary embodiments uses DSL modem technology. The central office 34 preferably includes a facilities management platform (FMP) 32 for processing data exchanged across the customer connection 30. The FMP 32 may be configured to separate the plain old telephone service (POTS) from the remainder of the data on the customer connection 30 using, for example, a tethered virtual radio channel (TVRC) modem (shown in Fig. 4A). The remaining data may be output to a high speed backbone network (e.g., a fiber-optic network) such as an asynchronous transfer mode (ATM) switching network. The analog POTS data may be output directly to a public switch telephone network (PSTN) 46, and/or it may be digitized, routed through the high speed backbone network, and then output to the PSTN 46.

[0015] The FMP 32 may process data and/or analog/digitized voice between customer premise equipment (CPE) 10 and any number of networks. For example, the FMP 32 may be interconnected with a synchronous optical network (SONET) 42 for interconnection to any number of additional networks such as an InterSpan backbone 48, the PSTN 46, a public switch switching network (e.g. call setup SS7-type network 44), and/or a network server platform (NSP) 36. Alternatively, the FMP 32 may be directly connected to any of these networks. One or more FMPs 32 may be connected directly to the high speed backbone network (e.g., direct fiber connection with the SONET network 42) or they may be linked via a trunk line (e.g., trunks 40 or 42) to one or more additional networks.

[0016] The NSP 36 may provide a massive cache storage for various information that may be provided across the SONET net 42 to the FMP 32 and out to the ISD 22. The NSP 36 and the FMP 32 may collectively define an access network server complex 38. The NSP 36 may be interconnected with multiple FMPs 32. Furthermore, each FMP 32 may interconnect with one or more ISDs 22. The NSP 36 may be located anywhere but is preferably located in a point-of-presence (POP) facility. The NSP 36 may further act as a gateway to, for example, any number of additional services.

[0017] The ISD 22 may be interconnected to various devices such as a videophone 130, other digital phones 18, set-top devices, computers, and/or other devices comprising the customer premise equipment 10. The customer premise equipment may individually or collectively serve as a local network computer at the customer site. Application applets may be downloaded from the NSP 36 into some or all of the individual devices within the customer premise equipment 10. Where applets are provided by the NSP 36, the programming of the applets may be updated such that the applets are continually

configured to the latest software version by the interexchange carrier. In this way, the CPE 10 may be kept up to date by simply re-loading updated applets. In addition, certain applets may be resident on any of the CPE 10. These resident applets may be periodically reinitialized by simply sending a request from, for example, a digital phone 18 and/or a videophone 130 to the FMP 32 and thereafter to the NSP 36 for reinitialization and downloading of new applets. To ensure widespread availability of the new features made possible by the present architecture, the customer premise equipment may be provided to end users either at a subsidized cost or given away for free, with the cost of the equipment being amortized over the services sold to the user through the equipment.

[0018] Referring to Fig. 2, the ISD 22 may connect with a variety of devices including analog and digital voice telephones 15, 18; digital videophones 130, devices for monitoring home security, meter reading devices (not shown), utilities devices/energy management facilities (not shown), facsimile devices 16, personal computers 14, and/or other digital or analog devices. Some or all of these devices may be connected with the ISD 22 via any suitable mechanism such as a single and/or multiple twisted-pair wires and/or a wireless connection. For example, a number of digital devices may be multi-dropped on a single twisted-pair connection. Similarly, analog phones and other analog devices may be multi-dropped using conventional techniques.

[0019] The ISD 22 may be located within the home/business or mounted exterior to the home/business. The ISD 22 may operate from electrical power supplied by the local or central office 34 and/or from the customer's power supplied by the customer's power company. Where the ISD 22 includes a modem, it may be desirable to power the ISD 22 with supplemental power from the home in order to provide sufficient power to enable the optimal operation of the modem.

[0020] As shown in Fig. 2, in some embodiments the ISD 22 may include a controller 100 which may have any of a variety of elements such as a central processing unit 102, a DRAM 103, an SRAM 104, a ROM 105 and/or an Internet protocol (IP) bridge router 106 connecting the controller 100 to a system bus 111. The system bus 111 may be connected with a variety of network interface devices 110. The network interface devices 110 may be variously configured to include an integrated services digital network (ISDN) interface 113, an Ethernet interface 119 (e.g., for 28.8 kbps data, 56 kbps data, or ISDN), an IEEE 1394 "fire wire" interface 112 (e.g., for a digital videodisc device (DVD)), a TVRC modem interface 114 (e.g., for a digital subscriber line (DSL) modem), a residential interface 114, (e.g., standard POTS phone systems such as tip ring), a business interface 116 (e.g., a T1 line and/or PABX interface), a radio frequency (RF) audio/video interface 120 (e.g., a cable television connection), and a cordless phone

interface 123 (e.g., a 900 MHz transceiver). Connected to one of the network interfaces and/or the system bus 111 may be any number of devices such as an audio interface 122 (e.g., for digital audio, digital telephones, digital audio tape (DAT) recorders/players, music for restaurants, MIDI interface, DVD, etc.), a digital phone 121, a videophone / user interface 130, a television set-top device 131 and/or other devices. Where the network interface is utilized, it may be desirable to use, for example, the IEEE 1394 interface 112 and/or the Ethernet interface 119.

[0021] A lifeline 126 may be provided for continuous telephone service in the event of a power failure at the CPE 10. The lifeline 126 may be utilized to connect the ISD 22 to the local telecommunications company's central office 34 and, in particular, to the FMP 32 located in the central office 34.

[0022] The ISD may be variously configured to provide any number of suitable services. For example, the ISD 22 may offer high fidelity radio channels by allowing the user to select a particular channel and obtaining a digitized radio channel from a remote location and outputting the digital audio, for example, on audio interface 122, video phone 130, and/or digital phones 121. A digital telephone may be connected to the audio interface 122 such that a user may select any one of a number of digital audio service channels by simply having the user push a digital audio service channel button on the telephone and have the speaker phone output particular channels. The telephone may be preprogrammed to provide the digital audio channels at a particular time, such as a wake up call for bedroom mounted telephone, or elsewhere in the house. The user may select any number of services on the video phone and/or other user interface such as a cable set-top device. These services may include any number of suitable services such as weather, headlines in the news, stock quotes, neighborhood community services information, ticket information, restaurant information, service directories (e.g., yellow pages), call conferencing, billing systems, mailing systems, coupons, advertisements, maps, classes, Internet, pay-per-view (PPV), and/or other services using any suitable user interface such as the audio interface 122, the video phone / user interface 130, digital phones, 121 and/or another suitable device such as a set top device 131.

[0023] In further embodiments, the ISD 22 may be configured as an IP proxy server such that each of the devices connected to the server utilizes transmission control protocol / Internet protocol (TCP/IP) protocol. This configuration allows any device associated with the ISD to access the Internet via an IP connection through the FMP 32. Where the ISD 22 is configured as an IP proxy server, it may accommodate additional devices that do not support the TCP/IP protocol. In this embodiment, the ISD 22 may have a proprietary or conventional interface connecting the ISD 22 to any associated device such as to the set top box 131, the personal com-

puter 14, the video telephone 130, the digital telephone 18, and/or some other end user device.

[0024] In still further embodiments, the ISD 22 may be compatible with multicast broadcast services where multicast information is broadcast by a central location and/or other server on one of the networks connected to the FMP 32, e.g., an ATM-switched network. The ISD 22 may download the multicast information via the FMP 32 to any of the devices connected to the ISD 22. The ISD 22 and/or CPE 10 devices may selectively filter the information in accordance with a specific customer user's preferences. For example, one user may select all country music broadcasts on a particular day while another user may select financial information. The ISD 22 and/or any of the CPE 10 devices may also be programmed to store information representing users' preferences and/or the received uni-cast or multicast information in memory or other storage media for later replay. Thus, for example, video clips or movies may be multicast to all customers in the community with certain users being preconfigured to select the desired video clip/ movie in real time for immediate viewing and/or into storage for later viewing.

[0025] Referring to Fig. 3A, a videophone 130 may include a touch screen display 141 and soft keys 142 around the perimeter of the display 141. The display may be responsive to touch, pressure, and/or light input. Some or all of the soft keys 142 may be programmable and may vary in function depending upon, for example, the applet being run by the videophone 130. The function of each soft key may be displayed next to the key on the display 141. The functions of the soft keys 142 may also be manually changed by the user by pressing scroll buttons 143. The videophone 140 may also include a handset 144 (which may be connected via a cord or wireless connection to the rest of the videophone and/or directly to the ISD), a keypad 150, a video camera 145, a credit card reader 146, a smart card slot 147, a microphone 149, a motion and/or light detector 148, built-in speaker(s) 155, a printer/scanner/facsimile 152, and/or external speakers 154 (e.g., stereo speakers). A keyboard 153 and/or a postage scale 151 may also be connected to the videophone 130. Any or all of the above-mentioned items may be integrated with the videophone unit itself or may be physically separate from the videophone unit. A block diagram of the video phone unit is shown in Fig. 3B. Referring to Fig. 3B, in addition to the items above, the video phone 130 may also include a signal processor 171, high speed interface circuitry 172, memory 173, power supply 174, all interconnected via a controller 170.

[0026] When the videophone 130 is used as a video telephone, the display 141 may include one or more video window(s) 160 for viewing a person to whom a user is speaking and/or showing the picture seen by the person on the other end of the video phone. The display may also include a dialed-telephone-number window 161 for displaying the phone number dialed, a virtual

keypad 162, virtual buttons 163 for performing various telephone functions, service directory icons 165, a mail icon 164, and/or various other service icons 166 which may be used, for example, for obtaining coupons or connecting with an operator. Any or all of these items may be displayed as virtual buttons and/or graphic icons and may be arranged in any combination. Additionally, any number of other display features may be shown on the video phone in accordance with one or more of the applications incorporated by reference below.

[0027] Referring to Fig. 4A, the FMP 32 may coordinate the flow of data packets, separate voice signals from other signals, perform line monitoring and switching functions, and/or convert between analog and digital signals. The FMP 32 may process data sent from the CPE 10 to the central or local office 34 by separating and reconstructing analog voice signals, data, and control frames. The FMP 32 may process data sent from the central or local office 34 to the CPE 10 by separating control messages from user information, and configure this information into segments that for transport across the digital subscriber loop. The FMP 32 may also terminate the link layer associated with the digital subscriber loop.

[0028] In some embodiments, the FMP 32 may include an access module 70 and a digital loop carrier 87. The access module 70 may include a line protector 71, a cross-connector 73, a plurality of TVRC modems 80, a plurality of digital filters 82, a controller multiplexer 84, and/or a router and facilities interface 86. The digital loop carrier 87 may include a plurality of line cards 96, a time domain multiplexing (TDM) multiplexor (MUX) 88, a TDM bus 90, a controller 92, and/or a facilities interface 94.

[0029] During normal operations, digital signals on the customer connection 30 (e.g., twisted-pair lines) containing both voice and data may be received by the TVRC modems 80 via the line protector 71 and the cross-connector 73. Preferably, the line protector 71 includes lightning blocks for grounding power surges due to lightning or other stray voltage surges. The TVRC modems 80 may send the digital voice and/or data signals to the controller multiplexer 84 and the digital filters 82. The digital filters 82 may separate the voice signals from the digital data signals, and the controller multiplexer 84 may then multiplex the voice signals and/or data signals received from the digital filters 82. The controller multiplexer 84 may then send multiplexed voice signals to the TDM MUX 88 and the data signals to the router and facilities interface 86 for transmission to one or more external networks. The TDM MUX 88 may multiplex the voice signals from the controller multiplexer 84 and/or send the voice signals to the TDM bus 90, which may then send the digital voice signals to the controller 92 and then to the facilities interface 94 for transmission to one or more external networks. Both the router and facilities interface 86 and the facilities interface 94 may convert between electrical

signals and optical signals when a fiber optic link is utilized.

[0030] When there is a failure of the digital data link (e.g., if there is a failure of the TVRC modems 80 at the FMP 32 or the TVRC modem 114 at the ISD 22), only analog voice signals might be sent over the subscriber lines 30. In such a case, the analog voice signals may be directly routed to the line cards 96, bypassing the TVRC modems 80, the digital filters 82, the controller multiplexer 84, and the TDM MUX 88. Thus, voice communication is ensured despite a failure of the digital data link. The line cards 96 may convert the analog voice signals into digital format (e.g., TDM format) and send the digitized voice data onto the TDM bus 90 and eventually through the controller 92 and the facilities interface 94 for transmission to one or more external networks.

[0031] Referring to Fig. 4B, the NSP 36 may be variously configured to provide any number of services provided by a server such as information services, Internet services, pay-per-view movie services, data-base services, commercial services, and/or other suitable services. In the embodiment shown in Fig. 4B, the NSP 36 includes a router 185 having a backbone 180 (e.g., a fiber distributed data interface (FDDI) backbone) that interconnects a management server 182, an information/database server 183, and/or one or more application server clusters 184. The NSP 36 may be connected via the router 185 by a link 181 to one or more external networks, NSPs 36, and/or an FMPs 32. The information/data base server 183 may perform storage and/or database functions. The application server cluster 184 may maintain and control the downloading of applets to the ISD 22. The NSP 36 may also include a voice/call processor 186 configured to handle call and data routing functions, set-up functions, distributed operating system functions, voice recognition functions for spoken commands input from any of the ISD connected devices as well as other functions.

[0032] Implementation of this new architecture allows for differentiation of local service, will provide new revenue streams from value-added services, and have the potential to significantly reduce operational costs. The architecture is constructed such that additional performance benefits from the existing loop plant are extracted and maximizes use of the existing infrastructure and current systems.

[0033] The new architecture implements active services where the user triggers a stimulus by touch, voice or a combination of touch and voice commands to obtain a network based response to expand traditional services as well as provide entirely new services. These responses and the associated services include call connection, information delivery, trigger network response, and performance transactions.

[0034] Call connection services provide for calls to be initiated by touching icons corresponding to the called party. It also enables self scheduling of conference calls

without the need for an operator as well as initiation of interactive calls with white board augmentation. Class services can likewise be invoked via icons and prompts in a natural manner without requiring memorization of numerical codes.

[0035] Information delivery services provide for a simple user interface that enables data base and search engine technology (formerly accessible only to networked computers) to be leveraged for telephony services. For example, access to regional, national or international electronic interaction with yellow and white page directories, navigation and access for voice, e-mail, and fax messages, review of AT&T bill for services, review of AT&T calling plans, review of CLASS and other service offerings. Thus certain marketing, operator services, billing, and customer care functions can be accessed by the customer without the need for an intermediate service representative -- reducing operations cost while increasing customer convenience. The screen phone eliminates the need for an intermediary to call up information on a screen and read it to the customer and streamlines customer access to information.

[0036] The trigger network response provides a screen interface that enables the customer to obtain operator services without accessing a human operator, obtain credit for wrong numbers automatically, view rate tables, self provision an AT&T Calling Plan or other CLASS services, conduct conference calls, or define a user profile for pointcast on a "ticker tape" that scrolls desired information on the videophone screen.

[0037] Performance transactions allows users via the videophone and its associated card swiper to enable users to perform transactions with security protection. These transactions include paying regular bills with paperless transactions, perform electronic banking including obtaining smart card cash in the home without the need to visit a bank or an ATM machine, conduct E-commerce, purchase products advertised on television via a synchronized ordering screen. The electronic bill payment scheme not only benefits the user but allows the service provider to obtain additional revenue by allowing those companies to outsource bill payments to AT&T.

[0038] Passive services can also be offered so that active customer responses are not required. These include advertising, providing electronic coupons, personalized news delivery services, and access to community news such as school closings. Providing an advertising feed directly to the customer premises equipment provides a new and potentially very large business opportunity to the local access network provider. Advertising can be displayed on the screen phone, whenever the videophone is not in active use. User profiles maintained on the network would enable the advertisements to target customer interests, geographic location, demographics, or some other criteria.

[0039] Providing electronic coupons is another passive service opportunity. The electronic coupon can be

displayed on the touch screen at appropriate times throughout the day (e.g., orange juice in the early morning) as "screen savers." By swiping their smart card customers can electronically collect such coupons and use them at the store without the inconvenience of cutting them out of newspapers, etc. At the same time AT&T participates in the coupon industry and has access to another revenue stream.

[0040] Delivery of personalized news leverages diverse content assists in the creation of user profiles. In addition, emergency broadcasts such as flash flood warnings, tornado, hurricane, etc., can be broadcast simultaneously while other transactions are being performed. This service could be offered as a public service.

[0041] The offering of interactive services include the combination of a graphics capable touch screen videophone, simultaneous voice and data capability, and a high speed data line to furnish a superior user interface than a traditional voice telephone and so enables a rich collection of new interactive services. These include multimedia enhanced voice calls, virtual PBX services, point and click conferencing, intelligent call management, access to the Internet, and a universal multimedia mailbox.

[0042] The multimedia enhances voice calls allows users to supplement voice calls with whiteboard graphics or text. The multimedia format can provide improved customer care, enhanced catalog ordering, interactive voice, and data response applications & info-on-demand,

support for work-at-home, virtual PBX services, point-and-click conferencing, intelligent call management, Internet access, and a universal mail box.

[0043] Work-at-home provides the capabilities of tying into private, corporate Intranets for secure and reliable connectivity with an employer, client or customer. Virtual PBX services provide POPs for message/call alerting and graphical call management using a touch interface for call setup/bridging capabilities. Point-and-Click conferencing provides a graphical user interfaces to initiate POTS calls. Intelligent call management provides an easy, specified instructions to direct call management including providing a personal registry and mobile manager for wireless connectivity, call scheduling, "call me back," and personal assistant functions. The universal multimedia mailbox supports voice, text, audio, images integrated with a common interface.

[0044] Figure 5 illustrates a diagram of the network server platform internal architecture. The network server platform 36 is connected into the SONET trunks 40 and 42 via a fiber distributed data interface (FDDI) 202 with the Stratus Continuum FTC 204, the information server / DBMS 206 and the HP K9000 28. The Stratus Continuum FTC 204 is a large computer that manages the switching and networking tasks. The information server / DBMS 206 contains database information regarding signaling, switching, dialing plans,

network configurations, customer information and called number information. The HP K9000 computer 208 manages the Stratus Continuum FTC and the information server / DBMS 206. The Stratus Continuum and HP K9000 computer types are merely descriptive of the type of computer that could be used to effectively operate the network server platform 36.

[0045] The NSP 36 is connected to a communications network illustrated by the SONET ring structure 195. Coupled to the SONET ring structure are other FMPs 193. In addition, NSP 36 is coupled to other NSPs such as NSP 191. This redundant interconnectivity provides a fault tolerant system and overall flexibility for coping with service interruption problems.

[0046] Figure 7 illustrates a block diagram of the NSP 36 consisting of devices and services used in the implementation of the new architecture. Connected to the SONET trunks 40 and 42 is a gateway 210. The gateway 210 might also function as the router 185 that was previously discussed. Located around the FDDI ring 202 are the management server 182, the information database server 183, and one or more application server clusters 184, as illustrated in Figure 6.

[0047] The connection manager 214 initiates and terminates the placement of telephone calls, while managing the services and messaging. In a typical scenario, the connection manager 214 automates the calling process. This automation involves the executing of computer commands to search records in the database server 218 to ensure that the customer is a subscriber to the desired service or that the called number is a subscriber to the desired service. In addition, the connection manager 214 uses the operations, administration, maintenance, and provisioning 216 to track billing information. After the connection manager 214 obtains the required authorization, it launches the application 212 from the application server 220.

[0048] The OAM&P server 182 contains OAM&P management information 216 consisting of data relating to configuration, capacity, fault, order, traffic activity, design, security, surveillance and testing of the network. The information/database server 183 contains specific customer information such as user profiles, authorization levels of service, provisioning and electronic commerce. The application server clusters 184 manage and track information regarding computer boot operations and initializations, call management, fault recognition and recovery, application binding, maintenance and design, application invoicing, craft interface enhancement, application downloads, translations, recent change and verify (RC/V), authorizations and registrations, configurations and performance statistics.

[0049] Figure 8 illustrates the software layer architecture for the application server 184 and the operation, administration and maintenance (OAM) server 182. In both the application server 184 and the OAM server 182, the software layer architecture is the same. The operating system kernel 250 contains a C application

programmable interface 252 for interfacing with communication, input/output and interprocess communication protocol (IPC). The data link, network, and transport layer contain middleware including the C applications 252, C++ wrappers 254 and the adaptive services layer 256. The C++ wrappers optimize the C library functions and the middleware puts intelligence into form object oriented programs in the transport layer to help applications route upwards and downwards in the protocol hierarchy. The session and transport layers contain service applications 260 and framework applications 258, respectively. The application layer contains the service/applications 262.

[0050] Figure 9 illustrates protocol hierarchy for the application server platform software architecture. The physical layer includes the operating system kernels 270 for fault tolerance, process/thread subsystems, communication subsystems, and virtual memory subsystems. The data link layer contains the following C application programmable interface sets 272: thread, stream, socket, name pipe, socket poll, dynamic link, memory map, and IPC. The network layer contains the operating system adaption layer 274, the thread manager, synch wrapper, spipe SAP, socket SAP, FIFO SAP, MEM MAP, and IPC wrapper. The transport layer contains the adaptive service executive 276 and the dispatch 278. The session layer contains the service acceptor 280, connector 282 and service handler 284. The presentation layer contains application program interface 286 and the application layer contains the traffic pipe management 288, the universal signal processing call processing system 290, new service applications 292, dynamic user profile management 294, user interfaces 296, and the OAM&P services 298. These protocols use a fault tolerant Unix language to make the transition between interfaces transparent.

[0051] Figure 10 illustrates the protocol hierarchy for the OAM&P server platform software architecture. The physical layer includes the operating system kernels 300 for fault tolerance, process/thread subsystems, communication subsystems, and virtual memory subsystems. The data link layer contains the following C application programmable interface sets 302: thread, stream, socket, name pipe, socket poll, dynamic link, memory map, and IPC. The network layer contains the operating system adaption layer 304, the thread manager, synch wrapper, spipe SAP, socket SAP, FIFO SAP, MEM MAP, and IPC wrapper. The transport layer contains the adaptive service executive 306 and the dispatch 308. The session layer contains the service acceptor 310, connector 312 and service handler 314. The presentation layer contains application program interface 316. The application layer contains the database management system (DBMS) 318, the OAM&P system services 320, the interactive user provisioning 322, craft interface 324 and the HP OAM 326.

[0052] The OSS interface applications 328 are supported by the distributed services access protocol 329.

The distributed services access protocol 329 is supported by the session layer distributed object services 330, the transport layer process services 332 and the network layer message manipulation and transport 334. These protocols also use a fault tolerant Unix language to make the transition between interfaces transparent.

[0053] Fig. 11 illustrates a diagram of a single NSP 36 connected to a plurality of FMPs that are in turn connected to a plurality of ISDs 22. The NSP 36 is connected to a communication network by trunk lines 40 and 42. By tying into the communication network, the NSPs 36 can communicate with each other and provide fault tolerant interaction should a particular NSP experience service problems. For a particular NSP 36, a plurality of FMPs 32 are registered with that NSP 36. The corresponding ISDs 22 connected to the registered FMPs 32 are also registered to the NSP 36. Because the NSP 36 recognizes the particular registered FMPs 32 and ISDs 22, caching frequently accessed information as well as developing user profiles can be stored at the NSP 36.

[0054] Figure 12 illustrates the protocol hierarchy between the FMP and the network. The SONET protocol 408 is used in the physical layer for both short term (option 1) and (long term option 2). In the short term, the data link layer is supported by TR303 [410]. Eventually, the ATM 412 protocol will replace TR 303 [410] in the data link layer. In the short term, the network layer is supported by Q.931 [414] for the transmission of signaling information and G.711 (PCM) or G.722 [416] will support the transmission of voice signals. In the long term, Q.2931 [418] will support signaling information and G.711 (PCM) or G.722 [420] will support the transmission of voice signals. In the long term, SAAL 422 and ATM adaption layer 1 (AAL1) 424 supports the signaling and voice traffic, respectively. The AAL is fully independent of the physical layer, and converts higher-layer information, such as data packets, into ATM cells for transmission across the ATM network. At the receiving end, the AAL converts the cells back into the higher-layer information.

[0055] Figure 13 illustrates the data protocol hierarchy between the FMP and the network. At the host-to-network layer, TVRC, SONET protocols 426 or ATM protocols 428 will be used for the transmission of data from the FMP 32 to the network. In the Internet layer, out-of-band signaling is performed by SAAL 430 and traffic is performed by AAL5 [432]. Also in the Internet layer, point-to-point 434 and point-to-point tunneling protocol 436 is used to transport traffic as well as IP 438. In the transport layer, traffic is supported by TCP 440.

[0056] Figure 14 illustrates the protocol hierarchy for voice services (option 1) employing end-to-end ATM. from the ISD 22 to the PSTN 46. The ISD 22 is connected to the FMP 32 by a self adaptive DSL 30 in the physical layer. The ISD 22, the FMP 32, ATM switch 449 and the local service office (LSO) 451 have their data link layer supported by ATM 444. The ISD 22 and the

LSO 451 have their network layer by AAL1 [446] and their transport layer supported by PCM 448. At the FMP 32, the data link layer is supported by ATM 444. Links from the ATM switch 449 to the FMP 32, the NSP 36 and the LSO 451, have the signaling aspects of these connections supported in the physical layer by Q.2931.

[0057] Figure 15 illustrates the protocol hierarchy for voice services (option 2) employing the TR-303 interface. The data link layer 454 in both the FMP 32 and the LSO 449 is supported by TR 303 across the local access network.

[0058] Figure 16 illustrates the protocol hierarchy for data services employing point-to-point over ATM from the ISD 22 to the Internet backbone 50. The ISD 22 is connected to the FMP 32 by a self adaptive DSL 30 in the host-to-network layer. The Internet layer at the ISD 22 is supported by IEEE 802.3 [466] and the transport layer is supported by IP 468. At the FMP 32, IEEE 802.3 [466] between the physical layer and the Internet layer for connections between the FMP 32 and the ISD 22. For connections between the FMP 32 and the ATM switch 449, Q.2931 signaling is used. Between the FMP 32 and the ISP access node 460, a permanent virtual circuit (PVC) 470 can be established to save bandwidth associated with circuit establishment and tear down in those situations where certain virtual circuits must exist all the time. When these conditions do not exist, a switched virtual circuit (SVC) 472 can be established to dynamically establish a circuit on demand.

[0059] Figure 17 illustrates the protocol hierarchy for data services using ATM signaling. Figure 17 is similar to Figure 16 in that both PVCs 470 and SVCs 472 can be established based on system requirements.

[0060] Figure 18 illustrates the virtual private data network "Extranet" between the FMP 32 and an access node 490 using point-to-point tunneling protocol. Point-to-point tunneling protocol wraps point-to-point packets in an IP format and uses a layer three protocol. The flexibility of point-to-point tunneling protocol allows the implementation to be client initiated or client transparent, but does require IP support. From the access node 490, users can connect to corporate private data networks 492 to create a secure connection between the customer services equipment and a private network.

[0061] Figure 19 illustrates the protocol hierarchy for establishing a point-to-point tunneling protocol from the customer services equipment to the private data network. The ISD 22 maintains a self adaptive DSL connection between the customer premises equipment and the FMP 32. Between the FMP 32 and the access node 490, data is sent along the ATM backbone via at least one ATM switch 449 in a switched virtual circuit (SVC) 472.

[0062] Figure 20 and 21 comprise service processing flow diagrams for the network server platform (NSP) of the present invention; Figure 20 shows from the time a user logs on to their personal computer (PC) or network computer (NC) to the time a menu list of accessible

services is displayed on their computer display; Figure 21 shows service processing from the time the user selects an available service to the time either service is allowed or denied.

[0063] Figure 20 and 21 comprise service processing flow diagrams for the network server platform (NSP) of the present invention. Figure 20 shows service processing by the NSP 907 from the time a user logs on to their personal computer (PC) or network computer (NC) 901 to the time a menu list of accessible services is displayed on the user's computer display. Figure 21 shows service processing from the time the user selects an available service to the time either service is allowed or denied. Referring briefly to Figure 1, the personal computer, network computer and other home devices CPE 10 interface to an Intelligent Services Director 22 shown in Figures 20 and 21 as ISD 903. Further details describing the operation of the ISD may be found in U.S. Application Serial No. (#32). At a local serving office (LSO) or wire center is located a facilities management platform 32 (Figure 1) shown in Figures 20 and 21 as FMP 905. Further details regarding the operation of FMP 905 may be obtained from reading U.S. Application Serial No. (#21). At a common carrier (toll carrier) point of presence according to Figure 1 is shown the network server platform 36 of the present invention referred to in Figures 20 and 21 as NSP 907. An information service provider may have Internet or dial-up or other accessible information services provided from anywhere in any network shown in Figure 1 and is alluded to but not further described in Figures 20 and 21 as ISP 909.

[0064] The service process is shown comprising steps 951 to 969. A key indicator and service process arrow are shown at the left of Figure 20 to show service processing flow over time. A user at step 951 logs on to their computer 901 and typically using a windows application and a mouse initiates a browser enabled applet for retrieving user services. For example, an icon may appear on the user's computer display for service launch. By clicking or otherwise selecting the icon, the user initiates the transmission of a request to network server platform 907 via step 953. The request message comprises the user's identity and address so that messages may be returned to the user and command data such as a one indicating a command for returning available services. In particular, the message will suggest that the services be retrieved using a separate thread. By thread is intended a term suggestive of a link but is in fact a virtual link that may be provided in various known ways and particularly requires a slow speed or small bandwidth of data transmission capability. Referring briefly to Figures 20 or 21, threads are not as bandwidth intensive, for example, as a stream (data stream) or pipe.

[0065] The network server platform 907 now must operate internal software algorithms for matching the identity of the user to available services. The services

may be services to which the user has subscribed on a pay basis or services that are free, for example, and available over the Internet. At step 955, a user service servlet fetches a user profile for the identified user and retrieves a list of services available to that specific user. In addition, new services that may have been provisioned via the OAM&P may be determined for eventual announcement to the user. This step is shown as step 957.

[0066] A low speed data thread having been determined, at step 959, the list of available and newly offered services customized for that user is provided to the user that initiated the request at step 951. Finally at step 961, a list of available services is displayed. The icon screen disappears and a new menu screen of listed available services is displayed for possible selection. These may comprise and are not limited to, for example, the availability of connection to a corporate LAN or WAN for telecommuting. A telecommuting application of the present invention is described in U.S. Application Serial No. (#28). Another application is information service provider (ISP) Internet access. An ISP access application is further described by U.S. Application Serial No. (#27). Another opportunity is for the user to view their service bill and make payments, etc. An NSP Integrated billing system is described in U.S. Application Serial No. (#30). Telephone directory for either personal or commercial (white or yellow pages) listings is also possible. The directory service application is further described by U.S. Application Serial No. (#29). Yet another service application is the availability of home entertainment such as digital audio and/or video program services via multicasting from a central network source. An NSP multicast application is described by U.S. Application Serial No. (#26). Other services are likewise possible in a new and unique, way via the Network Server Platform (NSP) of the present invention. The variety of the service opportunities are only limited by the imagination of the service provider.

[0067] Figure 22 shows a service processing flow diagram for providing a basic voice service via the Network Server Platform of the present invention wherein the user may identify the called party by audible name as an alternative to dialing digits. Figure 22 illustrates a systems and services process flow diagram for a basic voice service. Basic voice service is well known from a local phone company or local exchange carrier (LEC). What differentiates the present service flow process is that service is provided by a common toll carrier bypassing the LEC and the service may include voice or audible identification of the called party as an alternative to rotary or tone dialing. There are generally three steps to LEC dialing that are simulated here: 1) provision of dial tone to indicate that the carrier is ready to accept called party name or address identification (Steps 1051-1063), 2) name or address input, look-up and call setup (steps 1067-1071) and 3) call processing through to connection to a called party (steps 1073-

1079). Now the process will be described in further detail, particularly in the context of a voice dialed call.

[0068] Across the top of Figure 22 from left to right are shown the individual components of the system of the present invention which are actuated and utilized in the present voice service processing. The phone 1001 is a plain old telephone shown in Figure 1 as telephone 15 of CPE 10. The ISD 1003 refers to intelligent services director (ISD) 22 of Figure 1. The FMP 1005 refers to the facilities management platform (FMP) 32 of Figure 1. NSP 1007 refers to the Network Server Platform (NSP) 36 of Figure 1. SLC 1009 refers to subscriber loop carrier modified as necessary to provide call connect services and a voice carrying channel as required. LSO 1011 refers to the local serving office of a toll common carrier such as AT&T. "Other user" 1013 refers to the local exchange carrier or other termination for a called party's telephone.

[0069] At step 1051, a caller picks up the hand set of their telephone in order to release the switch-hook which typically provides a connection to local battery. The step of signaling of an off hook indication to ISD 1003 is represented by arrow 1053. The ISD 1003 of the present invention terminates the telephone and performs the task of providing local telephone battery power operation. The ISD 1003 recognizes that the user has gone off hook at step 1055 and selects a voice channel to FMP 1005. The voice channel is a typical low bandwidth voice channel and its allocation is shown as step 1057. Now the FMP 1005 signals the NSP 1007 and requests it to allocate a voice channel at step 1059. The NSP 1007 refers to its circuit provisioning opportunities and availabilities and obtains a subscriber loop carrier channel for connection to a local serving office 1011. The NSP 1007 also returns a message to the FMP that a voice channel has been allocated within step 1059 and FMP 1005 so signals the ISD 1003 at step 1061. The ISD 1003 provisions for the link from the SLC 1009 to the phone 1001. The subscriber loop carrier system 1009 either provides dialtone itself or couples with a dialtone generator at step 1063. The user at phone 1001 thus receives dialtone from a toll common carrier in a manner that simulates how the user would receive dialtone from a LEC in a conventional manner.

[0070] Once steps 1051-1063 have been performed, the user is ready to identify the called party. In a conventional manner, at step 1065, the user dials a number. The dialed tone or rotary dial pulse entries are converted by the ISD 1003 and transmitted as digital data for collection at SLC 1009. This dialed digit transfer is shown as step 1067. The collection of dialed digits via the SLC 1009 is shown as step 1069. Then, the call is set up via the local serving office 1011 at step 1011.

[0071] On the other hand, perhaps the touchtone dial is broken or otherwise refuses to operate or voice dialing is desired as a service feature. Voice dialing may be launched by any number of alternative means. One means would be for the SLC 1009 to await dialed digits

for a period of time and then allow for voice commands. Another means might be to immediately record voice received by the telephone mouth piece or microphone of telephone 1001. For example, the ISD 1003 may immediately or after a brief delay begin to digitize voice information, for example, via 64 kbps mu-law PCM data or other form of voice or audio coding/compression. The samples are then stored in a wave file of the ISD 1003 for subsequent transmission to the FMP 1005, for example, over a signaling channel. On receipt, the FMP 1005 forwards the voice data to the NSP 1007. The NSP 1007 may attempt to authenticate the request by ensuring that the subscriber or user has subscribed to the service or provides the service via, for example, a life-line emergency service. The NSP can determine the identity of the subscriber by looking at an address of an Internet Protocol (IP) field of a data message packet. The NSP 1007 can therefore reconstruct (if compressed) and interpret the information in the wave files of the ISD 1003 and take the appropriate action.

[0072] Let us assume that subscriber John wants to call a party Paul. Paul may already be identified in a personal directory for John by speech recognition circuitry as is known in the art by training the speech recognition circuitry. The NSP 1007 will attempt to determine who Paul is as defined by John in John's personal directory. A look-up table corresponds the spoken Paul to a directory number for Paul. Once the directory number for Paul has been determined by the NSP the equivalent of collecting dialed digits has been performed. The NSP 1007 can inform the FMP 1005 to set up a call to Paul's directory number. The FMP 1005 then may use a TR303 signaling or other interface to signal and set up a connection to Paul. The SLC 1009 receiving the directory number signaling from the FMP 1005 now is in the same position as it was at step 1069 of Figure 22.

[0073] Continuing now with Figure 22, steps 1071-1079, at step 1071, the SLC 1009 requests the LSO 1011 to select the appropriate ports to use for setting up the call to Paul. At step 1073 the local serving office will complete the regular voice call setup procedure. At step 1075, it rings the called party Paul. At step 1077, the local serving office 1011 detects user answer. Then a connection is established at step 1079 via the SLC channel 1009 between John and Paul.

[0074] It is important to note that the alternative digital or voice dialing service is being provided locally via the toll carrier's local serving office (LSO). There should be no need in the United States to pay for the Local Exchange Carrier (LEC) for providing such services. Similar services to voice dialing such as speed dialing, personal directory dialing and the like can now be made available locally by a toll common carrier according to the present invention.

[0075] Figure 23 is a service process flow diagram for showing how the NSP in concert with an FMP provides Internet service connectivity via, for example, an Internet Service Provider's point of presence (POP) using

AT&T's WorldNet Internet service as one example. Figure 23, illustrates another example of service connectivity by an NSP 36 as already generally described by Figures 20 and 21. In the application shown in Figure 23, any user may directly connect to an Internet service provider (ISP) at great bandwidth (bit rate) without having to connect via a local exchange carrier (LEC). The same convention as previously used with respect to Figure 10 is used here as well. Components of the system and service architecture are shown at the top including personal computer (PC) 1101, intelligent services director (ISD) 1103, facilities management platform (FMP) 1105 and network server platform (NSP) 1107. The Operations, Administration, Management and Provisioning server of the NSP 1107 is also shown as NSP OAM 1109. Finally, by way of example, a point of presence for an Internet service provider, namely AT&T's WorldNet service, is shown as WnetPOP 1111

[0076] As already described, bandwidth to the home or premises of a business may vary but may be in excess of 1 megahertz according to bandwidth allocation procedures followed by the ISD 1103 and FMP 1105. Thus, there is a great advantage in a user having access to the Internet connectivity feature shown in Figure 23 because the user has greater bandwidth availability and has immediate access to AT&T WorldNet, for example, via NSP 1107 bypassing the LEC.

[0077] Initially, the OAM&P server of the NSP 1109 provisions the Internet connectivity service by signaling and provisioning the FMP 1105 with address, routing and other data the FMP 1105 needs. Step 1151 is directed to configuring the FMP 1105 serving the user of PC 1101 for Internet service routing to, for example, AT&T WorldNet Internet Service point of presence 1111. As a result, the FMP 1105 updates its internal routing table of its memory with provisioned routing data for routing to Wnet POP 1111.

[0078] Assumed that a user has turned on their personal computer 1101 and wants to establish an Internet session. As already described, one of the services that may be offered the user as a menu display option is Internet service connectivity. The user clicks on or otherwise inputs their selection of Internet service connectivity. The personal computer 1101 via the ISD 1103 obtains immediate access to the already provisioned FMP 1105 at step 1157 as the user's Internet session begins. At step 1157, Internet protocol (IP) data packets are forwarded and returned via the FMP1105. The FMP 1105 now acts as a mini-server and performs steps 1159. The FMP 1105 looks up the user's packet header and compares the destination address against the routing table that was provisioned at step 1151. The routing table then provides routing data for routing the IP packets to, for example, AT&T WorldNet Internet service at Wnet POP 1111. Step 1161 suggests the routing of IP packets to the Wnet POP 1111 and an exchange of packets that follows via FMP 1105 to PC 1101. Note that the local exchange carrier is not involved and the

bandwidth and data rate for exchange of Internet IP packets may be the maximum bandwidth permissible by the facility between the FMP 1105 and the PC 1101. Figure 23 similarly describes the process of routing to other destinations of a routing table of FMP 1105 that has been provisioned by NSP OAM 1109. For example, besides serving as a gateway to the Internet, the NSP may provide a gateway to applets from a JAVA based server for such things as bill paying, utility meter reading, energy management, security services for any connected device (for example, a device at a customer premises (other than a personal computer) such as the VisionPhone described earlier or other device.

[0079] Figure 24 is a service process flow diagram for showing how the NSP in concert with an ISD provides a bill viewing and paying service via, for example, a billing server such as an AT&T billing server as one example. Figure 24, illustrates another example of service connectivity by an NSP as already generally described by Figures 20 and 21. In the application shown in Figure 24, any user may directly connect to a billing server that may be one for a utility, a bank, a credit card company or other creditor where an AT&T billing server is shown by way of example without having to connect via a local exchange carrier (LEC). The same convention as previously used with respect to Figure 22 is used here as well. Components of the system and service architecture are shown at the top including personal computer (PC) 1201, intelligent services director (ISD) 1203, facilities management platform (FMP) 1205 and network server platform (NSP) call processing server 1107. The Operations, Administration, Management and Provisioning server of the NSP is also shown as NSP OAM 1209 but is not otherwise described below. Finally, by way of example, a billing server is shown by way of example, namely an AT&T billing server 1211. One advantage of the present invention is that a billing server may comprise a clearing house for a plurality of bills. For example, an AT&T billing server 1211 may provide a bill viewing and payment opportunity for local phone service, toll phone service, Internet (for example, AT&T WorldNet service), digital audio and video program delivery services and other information and communication services.

[0080] As already described, bandwidth to the home or premises of a business may vary but may be in excess of 1 MHZ according to bandwidth allocation procedures followed by the ISD 1103 and FMP 1105. Nevertheless, a bill viewing and paying service does not require the bandwidth in either direction of data transmission as, for example, would be required for providing video conferencing. Referring to Figure 24, the user from their personal computer, intelligent telephone or video phone 1202 requests a billing viewing and paying service as already described generally by Figures 20 and 21 at step 1251. Typically the user has selected an icon (for bill viewing and paying services) on a display screen by clicking on the icon. The ISD 1203 in

response transmits a request message for the service to the NSP 1207 at step 1253. The message as already described must contain a service identifier, for example, BILLING. The NSP call process server 1207 responds to the message by looking to internal algorithms for billing services. In the internal algorithms it may be determined that a secure billing channel is required. As a result of the billing service look-up, then, the NSP CP 1207 downloads a secure viewing applet at step 1255 to the personal computer or other terminal 1201. The personal computer then may recognize that security is required for the service and may choose to secure, for example, by encryption or other means any future communications. The NSP 1207 and the PC 1201 must be sure that each other understands the security provisions put in place by each. Each device must know how to decrypt each other's communications by exchange any security keys and the like. Once the download is complete at step 1257, a transaction may be initiated. It may be assumed that communications within the AT&T network are secure, but communications over the local loop or other facility connecting the PC or other terminal 1201 with the NSP 1207 remote from the PC may not be as secure.

[0081] It may be assumed, by way of example, that a user has requested AT&T bill viewing and payment service. The transaction with the AT&T billing server then is initiated at step 1259 by the terminal 1101 signaling the NSP CP 1207. The interface with the AT&T billing server 1211 may be by any convenient method to the toll carrier service provider. Again, the channel is secure, within or outside the toll carrier network and may be provided with or without encryption security. At step 1263, the bill is requested and data returned at step 1265 to the NSP which converts the received data as necessary for eventual display or other use by the user. Preferably, at step 1267, the user will be able to interact with the bill viewing service by viewing any portion of the bill the user wants and may communicate and question any billing item of any service provider. Also, the user may arrange to pay the bill by providing, for example, AT&T universal or other credit card information or other payment option such as direct debit from a bank account.

[0082] Figures 25 and 26 each show service process flow diagrams for providing telecommuting services from the home; Figure 25 is a service process flow diagram for showing how the NSP 36 in concert with an ISD 22 provides a telecommuting service via, for example, an employer's office server using a frame relay backbone to interconnect the office server and a home terminal and Figure 26 shows a similar service process flow diagram for using the Internet to interconnect an office server and a home terminal.

[0083] Figures 25 and 26 each show service process flow diagrams for providing telecommuting services from the home. Figure 25 is a service process flow diagram for showing how the NSP 36 in concert with an

ISD 22 provides a telecommuting service via, for example, an employer's office server using a frame relay backbone to interconnect the office server and a home terminal. Figure 26 shows a similar service process flow diagram for using the Internet to interconnect an office server and a home terminal. Home/office telecommuting is yet a further example of service connectivity by an NSP as already generally described by Figures 20 and 21. In the application involving a frame relay backbone as shown in Figure 25 or in the Internet connect mode of operation shown in Figure 26, any user may directly connect to their employer's office server. The employee may connect to their office server without having to connect via a local exchange carrier (LEC). The same convention as previously used with respect to Figure 22 is used here as well. In Figure 25, components of the system and service architecture are shown at the top including personal computer (PC) 1301, intelligent services director (ISD) 1303, facilities management platform (FMP) 1305 and network server platform (NSP) 1307. In Figure 26, the same components are indicated prefaced by the figure number, for example, the facilities management platform is shown as FMP. In Figure 25, a frame relay point of presence is shown as FR POP 1309. In Figure 26, an Internet service provider point of presence is shown, for example, an AT&T WorldNet point of presence, as WNET POP 1409. In Figures 25 and 26, the employer office server is shown as Office SVR 1311 and 1411 respectively.

[0084] As already described, bandwidth to the home or premises of a business may vary but may be in excess of 1 megahertz according to bandwidth allocation procedures followed by the ISD 1303 or 1403 and FMP 1305 or 1405. In connections to the employer office server 1311/1411, it is desirable to achieve the greatest bandwidth or data rate possible. The employee would like to have the same access and data rate as if the employee were in fact at the location of the user's employer. In either connection of Figure 25 and 26, the maximum bandwidth may be achieved but may not be guaranteed in one case (Figure 26).

[0085] Now referring to Figure 25, the frame relay backbone approach to employee telecommuting will be discussed. While not particularly shown but suggested by Figure 1 is the access via the NSP 36 to a frame relay backbone network off ring 42. A frame relay POP 1309 is not shown but may be provided off, for example, a SONET OC-48 ring network 42. Now an employee user of the present network service actuates telecommuting service by selecting, for example, a telecommuting icon from a menu structure displayed as a result of the process of Figure 20. At step 1351, then, the user starts up the present telecommuting application by, for example, pointing to a telecommuting service icon and clicking or other selection means. It may be further assumed that the service may be identified by the service identifier "office". The service clicking and selection for an employer office connection is delivered to the ISD

1303 at step 1353. The ISD 1303 at step 1355 forwards an office service request message to NSP 1307 via FMP 1305. At step 1307, the network server platform performs a number of tasks. Firstly, the NSP 1307 validates the identity of the user forwarded to it by ISD 1303. The user having been validated by look up table, the user profile is retrieved showing what routing and other information is available for this user's request for LAN telecommuting service. The look-up process in NSP databases should show the accessibility to an office server 1311 associated with the user at personal computer or other terminal 1301 and, most importantly, that there exists a preconfigured connection between the FMP 1305 and the office server 1311 via a frame relay POP 1309. The NSP 1307 then provisions the FMP 1305 via step 1359 to provide resources such as LAN resources for reaching the office server 1311. Then a return message is provided by the FMP 1305 to the NSP 1307 acknowledging that the FMP is set up at step 1361. Once the NSP is satisfied that the FMP 1305 is ready, the NSP 1307 arranges at step 1363 to set up a private virtual circuit to the Office Server 1311 via FR POP 1309. Steps 1365 and 1367 show the establishment of a virtual circuit link between FR POP 1309 and Office SVR 1311. Once the PVC is set up, then an acknowledgment is returned by the FR POP 1309 to the NSP 1307 at step 1369. The NSP 1307 then forwards a service grant message to ISD 11303 at step 1371. Finally, the ISD 1303 signals the home terminal that the path is ready at step 1373. Now a communications link exists between the PC/ISD/FMP/FR POP/Office SVR. The user of terminal 1301 can begin to log in to the corporate LAN as if they were on site at step 1375. The connection is shown at step 1377 and assumes a high bandwidth connection at the maximum bandwidth the corporate LAN will allow.

[0086] Advantages of a frame relay POP mode of connection to an Office Server 1311 are that the connection is secure from intrusion and private to the user. Also, the bandwidth between the user and the corporate LAN is guaranteed. Of course, the guaranteed bandwidth comes at relatively high expense compared with Internet access and requires a preconfigured frame relay connection.

[0087] Referring now to Figure 26, an Internet connection to an employer office server 1411 will be described. First, as before, the user indicates a preference for obtaining a telecommuting service by actuating an input signal at their terminal 1401 at step 1451. Steps 1453 and 1455 are similar to steps 1353 and 1355 but for the fact that NSP 1307 has provisioned the FMP and so the ISD to arrange for an Internet connection to an Office SVR 1411 either as an alternative to a frame relay POP connection or in place of the frame relay mode. Consequently, at step 1457, the step proceeds as before but for the selection of a connection path which now involves an Internet connection path. Steps 1459 and 1461 proceed as before except that a PPTP protocol is

set up at step 1463 for data traffic to the office server. The FMP 1405 then tries out PPTP to and from the Office SVR 1411 via, for example, AT&T WNET POP 1409 at steps 1465 and 1467. If everything is ok, the FMP 1405 signals the NSP 1407 that the FMP is ready to communicate with the Office server 1411 via PPTP. The NSP replies by outputting a service grant to the ISD 1403 saying it is ok to begin telecommuting service via the Internet. At step 1473, the final step of the path to the terminal or PC 1401 is completed and the user can begin to log on to the corporate LAN at step 1475. Again, the maximum bandwidth is provided via Internet service that Internet service provides but the bandwidth cannot be guaranteed as another user at a premises where PC 1401 is located may take some bandwidth away. The service may be slow. Also, with Internet, there us a lot of packet overhead (extra bits that are not necessarily needed for information transfer). Yet, the connection will be complete and reasonably close in service quality to a user of a corporate LAN that is on site at step 1477. The Internet approach is inexpensive and requires minimal initial configuration.

[0088] Figure 27 is a service process flow diagram for showing how the NSP in concert with an ISD at a user's home and via an FMP serving that user provides white and yellow pages directory services including home shopping and dialing services.

[0089] Figure 27 illustrates another example of service connectivity by an NSP as already generally described by Figures 20 and 21. In the application shown in Figure 27, any user may directly access white (private) or yellow pages (commercial) directory services at required bandwidth (bit rate) without having to connect via a local exchange carrier (LEC). The same convention as previously used with respect to Figure 22 is used here as well. Components of the system and service architecture are shown at the top including intelligent terminal, video phone or personal computer (PC) 1501, intelligent services director (ISD) 1503, facilities management platform (FMP) 1505 and network

[0090] server platform (NSP) 1507. As already described, bandwidth to the home or premises of a business may vary but may be in excess of 1 megahertz according to bandwidth allocation procedures followed by the ISD 1503 and FMP 1505. Thus, there is a great advantage in a user having access to the directory services feature shown in Figure 27 because the user has greater bandwidth availability and the user may immediately access directory services, for example, via NSP 1107 bypassing the LEC, and additional services and connections may be provided via the NSP (also bypassing the LEC) for home shopping, banking by phone, obtaining directions to a destination and the like as will be further discussed below.

[0091] Initially, the OAM&P server of the NSP 1505 provisions the directory service availability by signaling and provisioning the FMP 1505 with its address, routing and other data the FMP 1505 needs. The NSP itself

1507 has already been described as comprising a large database of data that may provide according to the present application at least local directory (both telephony and Internet) address/directory number services. Moreover, the NSP comprises significant caching memory and access to remote NSP's and other directory databases from which it may obtain further directory data.

[0092] Initial step 1551 of the service process flow diagram of Figure 27 is directed to configuring the FMP 1505 to configure the ISD 1503 serving the user of PC 1501 for directory service routing to NSP 1507. As a result, the FMP 1505 updates its internal routing table of its memory with provisioned routing data for routing to NSP 1507 and for providing service via ISD 1503 to a particular user of terminal 1501.

[0093] Now, in step 1553, it may be assumed that a user has turned on their personal computer 1501 and wants to establish a directory session. As already described, one of the services that may be offered the user as a menu display option is directory service connectivity. The user clicks on or otherwise inputs their selection of directory service connectivity. The message forwarded as a result of the directory service can be the name, address or other indicia to be looked up. Also, a second column of the display may provide the desired output which may be directory number or Internet address but may also comprise, for example, directions for driving to a store nearest the user. The personal computer 1501 sends a lookup message with one or more of these requests to the ISD 1503 at step 1555. The ISD 1503 in turn obtains immediate access via the already provisioned FMP 1505 at step 1557 to the NSP 1507 where the local directory is located. The NSP 1507 now acts as an information database service provider and performs steps 1559. The NSP 1507 looks up the user's requested data and determines if it can provide the requested information itself. If NSP 1507 cannot provide the requested data look-up itself, it determines routing for a database having the requested information, collects the information and stores the information in cache memory for forwarding to the user along with any locally provided database information requested. Step 1561 suggests the return of the directory lookup result to the ISD 1561 for presentation to the user. Depending on the terminal, for example, the personal computer 1501, the ISD 1503 causes the result to be displayed at step 1563. Along with the result, the display may provide immediate dialing opportunity for a telephony directory number or immediate access to an Internet addressed web site.

[0094] For example, the user may wish to obtain a white pages listing for Tom Jones. The user may not know the city. The NSP 1507 may provide a directory service that identifies all individuals named Tom Jones in a geographical area such as the state of New York for possible review and selection. The user may continue to provide information until the selection process is nar-

rowed to the Tom Jones that the user wishes to locate. Once the result of the search is narrowed sufficiently to where the user may make a choice, the choice may include a hot spot for an immediate connection. Moreover, Tom Jones may be located, not only at home, but at his work phone, cellular phone, pager, personal computer, facsimile machine or other number or web site.

[0095] In another application, the user may be trying to locate a drug store nearest them. The user inputs the request. Because the NSP receives data regarding the user's identity, the NSP further has access to a user profile including a home address. Consequently, using appropriate algorithms known in the art, the NSP 1507 locates the nearest drug store, the next nearest and so on for the user to choose one. Moreover, the display may provide essential information input by the drug store such as hours of operation. The hours of operation may be used as a filter to eliminate possible drug stores that in fact are not presently open at the user's request. The user may select to call the drug store of their choice and/or obtain directions from their home to the drug store.

[0096] In accordance with the directory look-up feature, the user may make repeated requests for the same or additional information. Moreover, once the user receives the directory look-up result, the result may provide hot spots or clicking selection opportunity to directly access the directory look-up result, for example, by telephony or the Internet at the highest bandwidth permissible or desirable. Thus, the directory look-up may be the first step toward home shopping, bank from home and other services. Note that the local exchange carrier is not involved and the bandwidth and data rate for exchange of Internet IP packets may be the maximum bandwidth permissible by the facility between the FMP 1505 and the PC or other terminal 1501.

[0097] Figure 28 is a service process flow diagram for showing how the NSP in concert with an ISD at a user's home and via an FMP serving that user provides multicast audio and/or video program services or software, game and other program or information delivery services. Figure 28 illustrates another example of service connectivity by an NSP as already generally described by Figures 20 and 21. In Figures 20 and 21, the present service is indicated in shorthand by the suggestion that the present service is like BlockBuster Video (TM), being able to receive movies or video games at home without having to go to the store to bring home the video or other program for play on a player. In the application shown in Figure 16, any user may directly access multicast program services at required bandwidth (bit rate) without having to connect via a local exchange carrier (LEC). Pay-per-view, pay-per-listen, pay-per-play and other program delivery services may be provided from one or distributed sites from which the programs are multicast. Referring to Figure 1, briefly, the multicast programs are receivable at any NSP 36 within reach of the SONET ring network 42. Moreover, the NSP 36

comprises a database with program availability and routing information.

[0098] In describing the multicast program services application of Figure 28, the same convention as previously used with respect to Figure 10 is used here as well. Components of the system and service architecture are shown at the top including intelligent terminal, video phone or personal computer (PC) 1601, intelligent services director (ISD) 1603, facilities management platform (FMP) 1605 and network server platform (NSP) 1607.

[0099] As already described, bandwidth to the home or premises of a business may vary but may be in excess of 1 megahertz according to bandwidth allocation procedures followed by the ISD 1603 and FMP 1605. Thus, there is a great advantage in a user having access to the multicast program services feature shown in Figure 16 because 1) the user has greater bandwidth availability and 2) the user may immediately access multicast program services, for example, via NSP 1607 bypassing the LEC.

[0100] Initially, the OAM&P server of the NSP 1607 provisions the multicast program service availability by signaling and provisioning the FMP 1605 with its address, routing and other data the FMP 1605 needs. The NSP itself 1607 has already been described as comprising a large database of data that may provide according to the present application routing information needed for periodically receiving data from remote multicast server locations regarding availability to the user and routing information for receiving multicast programs. As is well known in the art, multicast audio and video programs may be provided in compressed format such as MPEG compressed format or other compression format. The compressed program is decompressed preferably at the terminal 1601. On the other hand, if the terminal is not so equipped, decompression algorithms may reside in the ISD 1603.

[0101] Initial step 1651 of the service process flow diagram of Figure 28 is directed to configuring the FMP 1605 to configure the ISD 1603 serving the user of terminal or PC 1601 for multicast program routing to NSP 1607. As a result, the FMP 1605 updates its internal routing table of its memory with provisioned routing data for routing to NSP 1607 and for providing multicast program services via ISD 1603 to a particular user of terminal 1601.

[0102] Now, in step 1653, it may be assumed that a user has turned on their personal computer or other terminal 1601 and wants to establish a multicast program session. As already described, one of the services that may be offered the user as a menu display option is a multicast program delivery service connectivity. The user clicks on or otherwise inputs their selection of multicast program service connectivity. The menu screen displayed as a result of the multicast program service can be tables of indicia to be looked up. For example, you know you want to see a movie starring Jimmy Stew-

art. You also know it is a Christmas movie. Using various selection algorithms within the design skills of one in the art, the selection may be narrowed to the well-known movie "It's a Wonderful Life" starring Jimmy Stewart about Christmas. Also, a second area of the display may provide the desired output which may be directory number or Internet address with information about the movie but may also comprise, for example, directions for driving to a movie theater nearest the user if the user wishes to see the movie at a theater in stead of at their home terminal.

[0103] At step 1653, the user makes a selection of a video or other program title. As already described the program title may comprise a movie title, an audio album or song title and the like by program, title and artist or a game program or software program for download. At step 1655, the program title selection is forwarded to the ISD 1603. The ISD 1603 then formats a requestService message describing the program to be delivered and service identifier data such as data representing a VIDEO service. The message is transmitted from the ISD 1603 via the FMP 1605 serving that ISD 1603 at step 1657 to NSP 1607.

[0104] At step 1659, the NSP 1607 validates the user and the requested service and obtains the user's profile from database memory. The user profile may provide the user's home address for locating a movie theater nearest them playing the desired movie or certain predetermined movie or other program preferences that can be used as a guide. Then, the NSP searches its database for movie or other program routing data to access the multicast program source and seek a download of the compressed program data.

[0105] Meanwhile, the NSP 1607 seeks the needed bandwidth for the program delivery service. Of course, audio program, software and game downloads may require less bandwidth than video. At steps 1661 and 1663, the NSP 1607 seeks to establish the necessary bandwidth at the FMP 1605 for receiving the needed resources. The FMP needs to assure a channel having the bandwidth required is available from the terminal or PC 1601 to the FMP 1605. The FMP 1605 then returns bandwidth and resource availability ok or not ok data to the NSP 1607.

[0106] If the movie is available on multicast and the bandwidth is available, then the NSP can issue a serviceGrant message for the desired video service to the ISD 1603 at step 1665. The ISD 1603 then signals the receiving device which may be a television, a recorder/player, a personal computer, a video phone, home theater center or other terminal or-collection of terminals 1601 that it is ready to provide the service at step 1667. The final play connection is shown at step 1669.

[0107] Figure 23 is a service process flow diagram for showing how the NSP in concert with an FMP provides Internet service connectivity via, for example, an Internet Service Provider's point of presence (POP) using

AT&T's WorldNet Internet service as one example. Figure 29 is a service process flow diagram for showing how the NSP may comprise cache memory and maintain a user profile such that the NSP may obtain information from various information service providers for forwarding and display to a user in accordance with their user profile.

[0108] Figure 23 illustrates another example of service connectivity by an NSP as already generally described by Figures 20 and 21. In the application shown in Figure 23, any user may directly connect to an Internet service provider (ISP) at great bandwidth (bit rate) without having to connect via a local exchange carrier (LEC). The same convention as previously used with respect to Figure 10 is used here as well. Components of the system and service architecture are shown at the top including personal computer (PC) 1101, intelligent services director (ISD) 1103, facilities management platform (FMP) 1105 and network server platform (NSP) 1107. The Operations, Administration, Management and Provisioning server of the NSP 1107 is also shown as NSP OAM 1109. Finally, by way of example, a point of presence for an Internet service provider, namely AT&T's WorldNet service, is shown as Wnet POP 1111.

[0109] As already described, bandwidth to the home or premises of a business may vary but may be in excess of 1 megahertz according to bandwidth allocation procedures followed by the ISD 1103 and FMP 1105. Thus, there is a great advantage in a user having access to the Internet connectivity feature shown in Figure 23 because the user has greater bandwidth availability and 2) immediate access to AT&T WorldNet, for example, via NSP 1107 bypassing the LEC.

[0110] Initially, the OAM&P server of the NSP 1109 provisions the Internet connectivity service by signaling and provisioning the FMP 1105 with address, routing and other data the FMP 1105 needs. Step 1151 is directed to configuring the FMP 1105 serving the user of PC 1101 for Internet service routing to, for example, AT&T WorldNet Internet Service point of presence 1111. As a result, the FMP 1105 updates its internal routing table of its memory with provisioned routing data for routing to Wnet POP 1111.

[0111] Now, it may be assumed that a user has turned on their personal computer 1101 and wants to establish an Internet session. As already described, one of the services that may be offered the user as a menu display option is Internet service connectivity. The user clicks on or otherwise inputs their selection of Internet service connectivity. The personal computer 1101 via the ISD 1103 obtains immediate access to the already provisioned FMP 1105 at step 1157 as the user's Internet session begins. At step 1157, Internet protocol (IP) data packets are forwarded and returned via the FMP 1105. The FMP 1105 now acts as a mini-server and performs steps 1159. The FMP 1105 looks up the user's packet header and compares the destination address against

the routing table that was provisioned at step 1151. The routing table then provides routing data for routing the IP packets to, for example, AT&T WorldNet Internet service at Wnet POP 1111. Step 1161 suggests the routing of IP packets to the Wnet POP 1111 and an exchange of packets that follows via FMP 1105 to PC 1101. Note that the local exchange carrier is not involved and the bandwidth and data rate for exchange of Internet IP packets may be the maximum bandwidth permissible by the facility between the FMP 1105 and the PC 1101. Figure 21 similarly describes the process of routing to other destinations of a routing table of FMP 1105 that has been provisioned by NSP OAM 1109. For example, besides serving as a gateway to the Internet, the NSP may provide a gateway to applets from a JAVA based server for such things as bill paying, utility meter reading, energy management, security services for any connected device (for example, a device at a customer premises (other than a personal computer) such as the VisionPhone described earlier or other device.

[0112] Referring now to Figure 29, there is shown yet another example of service connectivity by an NSP as already generally described by Figures 20 and 21. In the application shown in Figure 29, any user may enter and periodically update a user profile showing their interests and preferences. The NSP 1707 comprising significant cache memory can search for and obtain information directly related to the user entered preferences. When the user actuates their personal computer, the user may obtain the collected information that the NSP has collected on the user's behalf. The same convention as previously used with respect to Figure 10 is used here as well. Components of the system and service architecture are shown at the top including personal computer (PC) or network computer (NC) or other terminal 1701, intelligent services director (ISD) 1703, facilities management platform (FMP) 1705 and network server platform (NSP) 1707. Info #1 1709 and Info #2 1711 are shown by way of example as one or more information service providers that the NSP 1707 may access for information. Finally, by way of example, AT&T information content servers as a group are shown as AT&T Content Servers 1713.

[0113] At step 1751, the personal computer, intelligent terminal, video phone or other terminal 1701 performs system/service initialization. Without a user profile, the service will not be able to retrieve any relevant information. There is a startup via a user interface applet, for example, by clicking on a user profile icon. Then, the user is presented with a user profile display or other input means for inputting information contents of interest to the user. The contents ultimately may refer to channels whereby the information can be obtained, for example, stock market ticker or sports ticker channels. Likewise, the contents may simply define a preference such as to information directed to genealogical research of an ancestor or hobby or scientific interests or pursuits.

[0114] At step 1753, the user profile for selected contents (information channels) is transmitted via the ISD 1703 and FMP 1705 for storage at the NSP 1707. The NSP 1707 then updates the user profile at step 1755 that is presently stored in memory or initializes the user profile in memory. The NSP 1707 then, once the use profile is known, can begin to search for relevant information at any and all information sources available on SONET ring network 42 (Figure 1). The NSP 1707 then forwards an auto-start Info Receiver applet to the PC/NC 1701 for display, for example, as a menu selectable item or an icon or the like. Whenever the user accesses that applet, the collected information for their user profile is pushed to their terminal at step 1771.

[0115] However, prior to an information to terminal dump at step 1771, the NSP collects information from various sources at steps 1761, 1763 and 1765. The access to the information source may be via private line, shared line, Internet or telephony channels. For example, at step 1761 the information contents of Info #1 1709 relevant to the user profile is downloaded and stored in cache memory of NSP 1707 for that user to identify themselves and access. At step 1763, the information contents of Info #2 1711 relevant to the user profile is downloaded and stored in cache memory of NSP 1707 for the same user. Only two information sources are shown but many information sources may be queried and the query results downloaded to NSP 1707. Finally, via AT&T or other Internet service provider, the respective information content servers may be queried for relevant information and or channels (virtual or physical) realized and provided to NSP 1707. These may include stock market tickers, sports tickers, new tickers and the like of current interest. At either NSP 1707 or personal computer or network computer 1701, information filters may be used to only retrieve current data with respect to, for example, the stock portfolio or sports teams of interest to the user. Moreover, the NSP 1707 must periodically update the cache memory with newly received information relevant to the user's requests. A new information source may appear on the Internet or as a telephone listing or a new sports or other channel may be identified to NSP 1707 for polling. This is shown as step 1767.

[0116] In summary, then as shown at step 1769, the NSP 1707 caches contents from different sources (including from itself - for example - local directory listings and geographical location finding services). The NSP also polls contents from various sources to, for example, obtain updates or new information. At a user specified time interval or according to a user specified schedule as per their user profile, and according to a user specified priority ranking, the information may be ordered and delivered to the user via an information push at step 1771.

[0117] To illustrate the interaction between the various components of the instant invention, a voice dialing scenario will be described. When a user picks up the tele-

phone and dials a series of numbers, after a period of time in which no additional numbers are entered, the intelligent service director 22 will start digitizing the voice information into 64 Kbps μ -law PCM data. The samples are then stored in a wave file, which is subsequently transmitted to the facilities management platform 32 over a signaling channel. On receipt by the facilities management platform 32, the facilities management platform 32 will forward the information to the network server platform. The network server platform will attempt to authenticate the request by ensuring that the subscriber does indeed have a subscription to the voice dialing service.

[0118] The network server platform can determine the identity of the subscriber by looking at the address in the IP field of the packet. The network server platform 36 can therefore interpret the information in the wave files and take the appropriate action. Let us assume that a first user wanted to call a second user. The network server platform 36 attempt to determine who the second user is as defined by the first user. Once the telephone number for the second user has been determined the network server platform 36 will inform the facilities management platform 32 to set up a call to the second user. The facilities management platform 32 will then transmit a signal over the trunk lines requesting the second users local office to inform the NSP 36 the appropriate ports to use for setting up the call. The facilities management platform 32 has its own DTMF and tone generator which is used for signaling.

[0119] Note that there is a significant advantage implicit in the design. The voice dialing service is being provided locally and there is no need to pay for the local exchange carrier (LEC) for providing such a service. Similar services, such as speed dialing, that the LEC provides can now can be made available locally.

[0120] When an incoming call arrives from the PSTN, the facilities management platform 32 will obtain the signaling information from the modified digital loop carrier. The information will be dispatched over the signaling channel to the NSP 36. The NSP 36 will instruct the FMP 32 with information regarding call set up, connection and termination. On receiving this message, the FMP 32 will send the appropriate signaling message to the ISD 22. The ISD 22 knows the phones that are in use and those that are available for service.

[0121] While exemplary systems and methods embodying the present invention are shown by way of example, it will be understood, of course, that the invention is not limited to these embodiments. Modifications may be made by those skilled in the art, particularly in light of the foregoing teachings. For example, each of the elements of the aforementioned embodiments may be utilized alone or in combination with elements of the other embodiments.

[0122] Where technical features mentioned in any claim are followed by reference signs, those reference signs have been included for the sole purpose of

increasing the intelligibility of the claims and accordingly, such reference signs do not have any limiting effect on the scope of each element identified by way of example by such reference signs.

Claims

1. A systems management server for controlling user access to a plurality of communication networks, comprising:
 - a router providing a gateway connection between said systems management server and said communication networks along at least one trunk line;
 - an applications server coupled to said router along fiber distributed data interface (FDDI) ring;
 - a database server for storing information supporting operation of said systems management server; coupled along said fiber distributed data interface ring; and
 - an operations, administration, maintenance, and provision server coupled to said fiber distributed data interface ring for supporting operation of said user access to said communications network.
2. The systems management server described in Claim 1, where said trunk line connection said routes to said communication networks operates using SONET protocol.
3. The systems management server described in Claim 1, where said trunk line connecting said routes to said communication networks operates using a TR303 protocol.
4. The systems management server described in Claim 1, where said communication networks is a SS7 network.
5. The systems management server described in Claim 1, where said communication network is a public switched telephone network.
6. The systems management server described in Claim 1, where said communication network is a private Intranet.
7. The systems management server described in Claim 1, where said communication network is an Internet.
8. A system management server for controlling user access to a plurality of communication networks comprising:
 - a router providing a gateway connection between said systems management server and said communication networks along at least one trunk line;
 - an applications server coupled to said router along fiber distributed data interface (FDDI) ring;
 - a database server for storing information supporting operation of said systems management server; coupled along said fiber distributed data interface ring; and
 - an operations, administration, maintenance, and provision server coupled to said fiber distributed data interface ring for supporting operation of said user access to said communications network.
 - a connection manager coupled along said fiber distributed data interface ring supporting launching of applications stored in said applications server;
 - and said connection manager capable of supporting said operations, administration; maintenance and provisioning server.
9. The systems management server described in Claim 8, where said trunk line connecting said routes to said communication networks operates using a SONET protocol.
10. The systems management server described in Claim 8, where said trunk line connecting said routes to said communication networks operates using a TR303 protocol.
11. The systems management server described in Claim 8, where said communication networks is an SS7 network.
12. The systems management server described in Claim 8, where said communication network is a public switched telephone network.
13. The systems management server described in Claim 8, where said communication network is a private Intranet.
14. The systems management server described in Claim 8, where said communication network is an Internet.
15. A method for providing user access to a plurality of communication networks comprising the steps of:
 - receiving a signal from an access module containing information regarding a request to connect said user access to said communication network;
 - verifying said request to connect said user to

said communication network for
 authorization to initiate said connection by a
 systems management server;
 initiating or denying said user access if said
 user access is granted, launching by said sys- 5
 tem management server of applications sup-
 porting said user access; and
 launching operations; administration; mainte-
 nance, and provisioning tools to support said
 user access. 10

- 16. A method for providing access to a user from sig-
 nals sent from a plurality of a communication net-
 work, comprising the steps of:

15
 receiving said signal by a systems manage-
 ment server from said communication network
 where said signal contains information regard-
 ing setting up a connection between said user
 serviced by said systems management server 20
 and said communication network.
 processing said signal by said systems man-
 agement server to determine if said user is
 authorized and available for said connection;
 and if said user is authorized and available for 25
 said connection; said systems management
 server setting up said connection by sending
 said signal to an access module supporting
 said user. 30

15

20

25

30

35

40

45

50

55

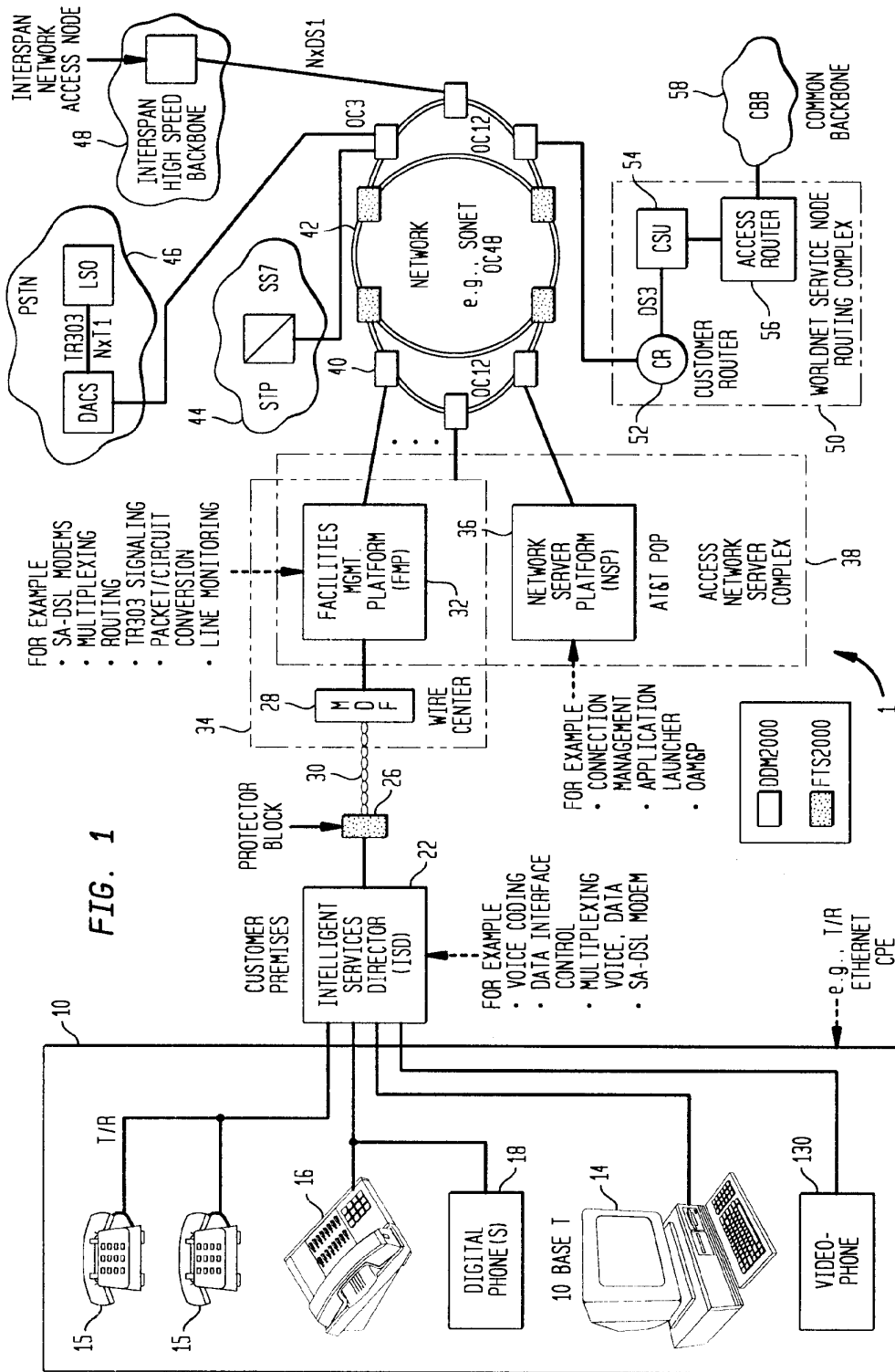
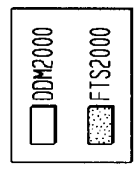


FIG. 1

- FOR EXAMPLE:
- SA-DSL MODEMS
 - MULTIPLEXING
 - TR303 SIGNALING
 - PACKET/CIRCUIT CONVERSION
 - LINE MONITORING

- FOR EXAMPLE:
- VOICE CODING
 - DATA INTERFACE CONTROL
 - MULTIPLEXING
 - VOICE DATA
 - SA-DSL MODEM

- FOR EXAMPLE:
- CONNECTION MANAGEMENT
 - APPLICATION LAUNCHER
 - OAM&P



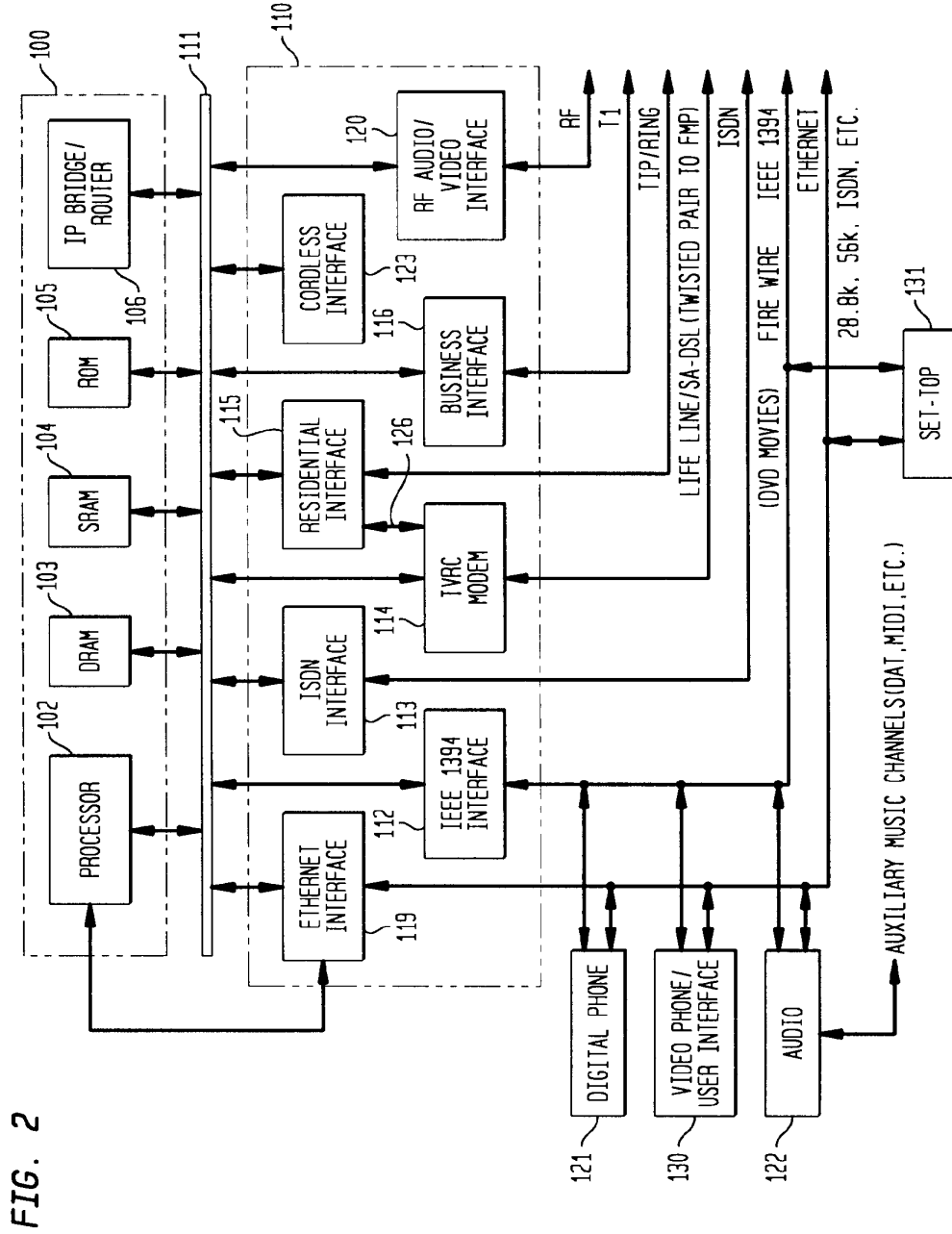


FIG. 2

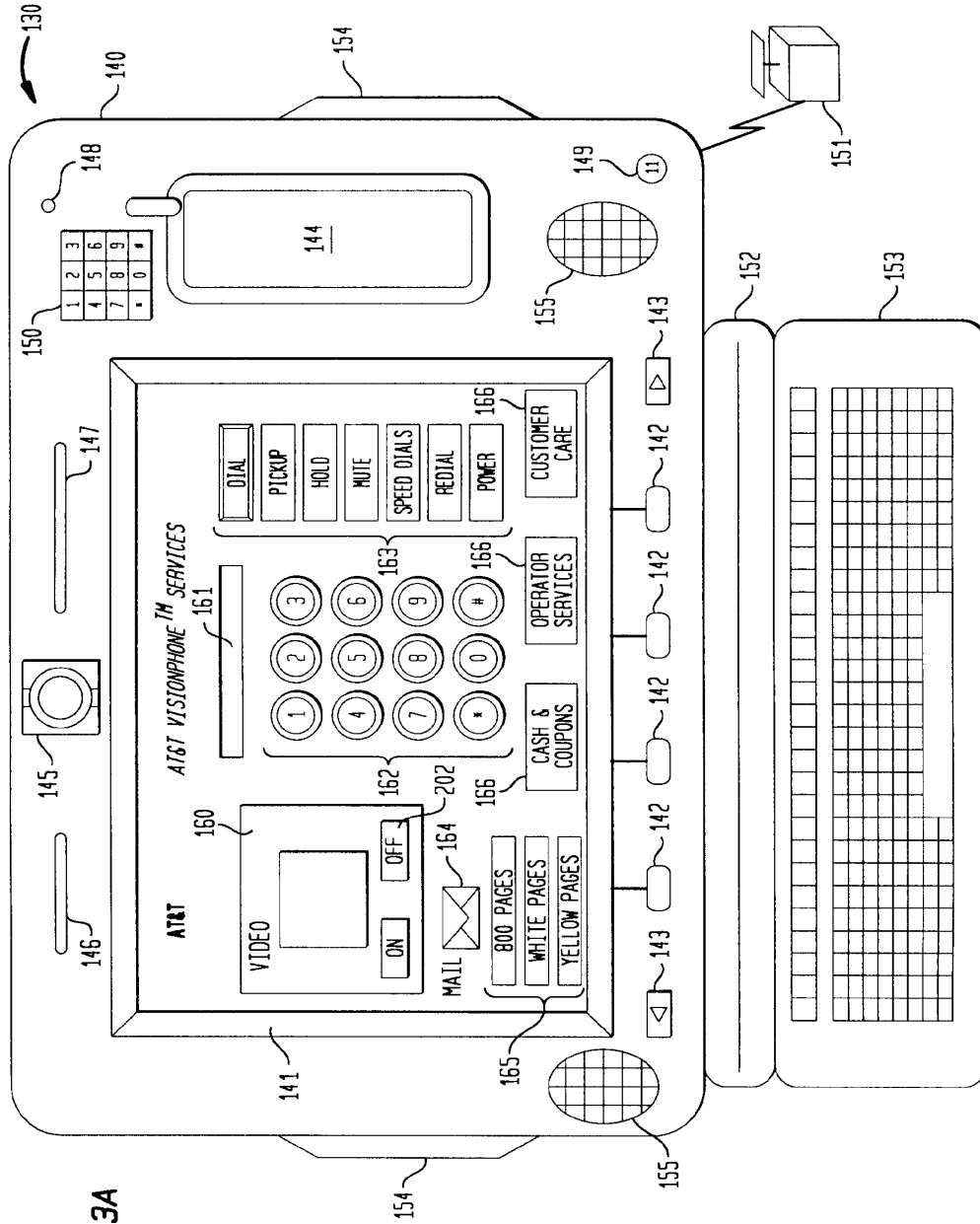
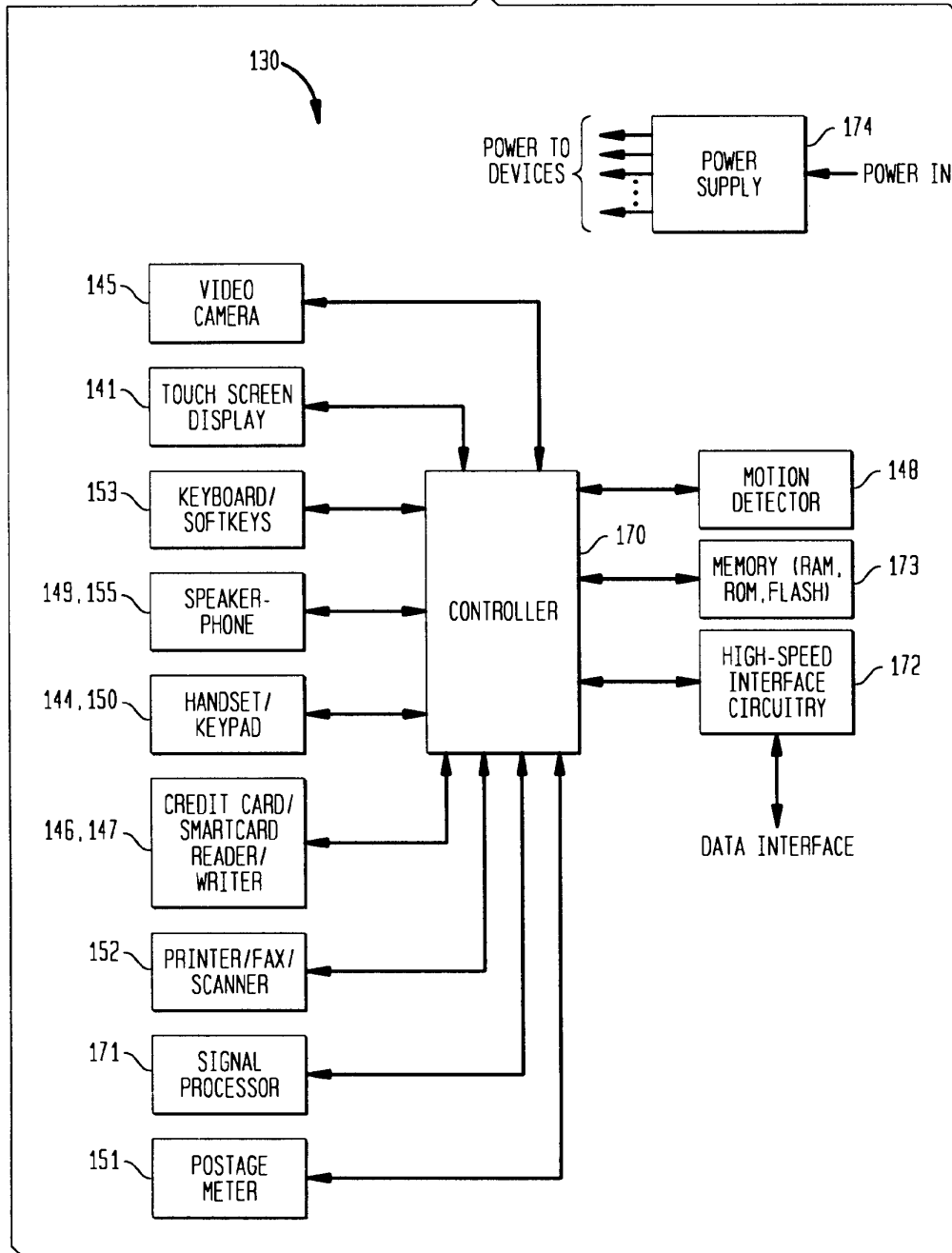


FIG. 3A

FIG. 3B



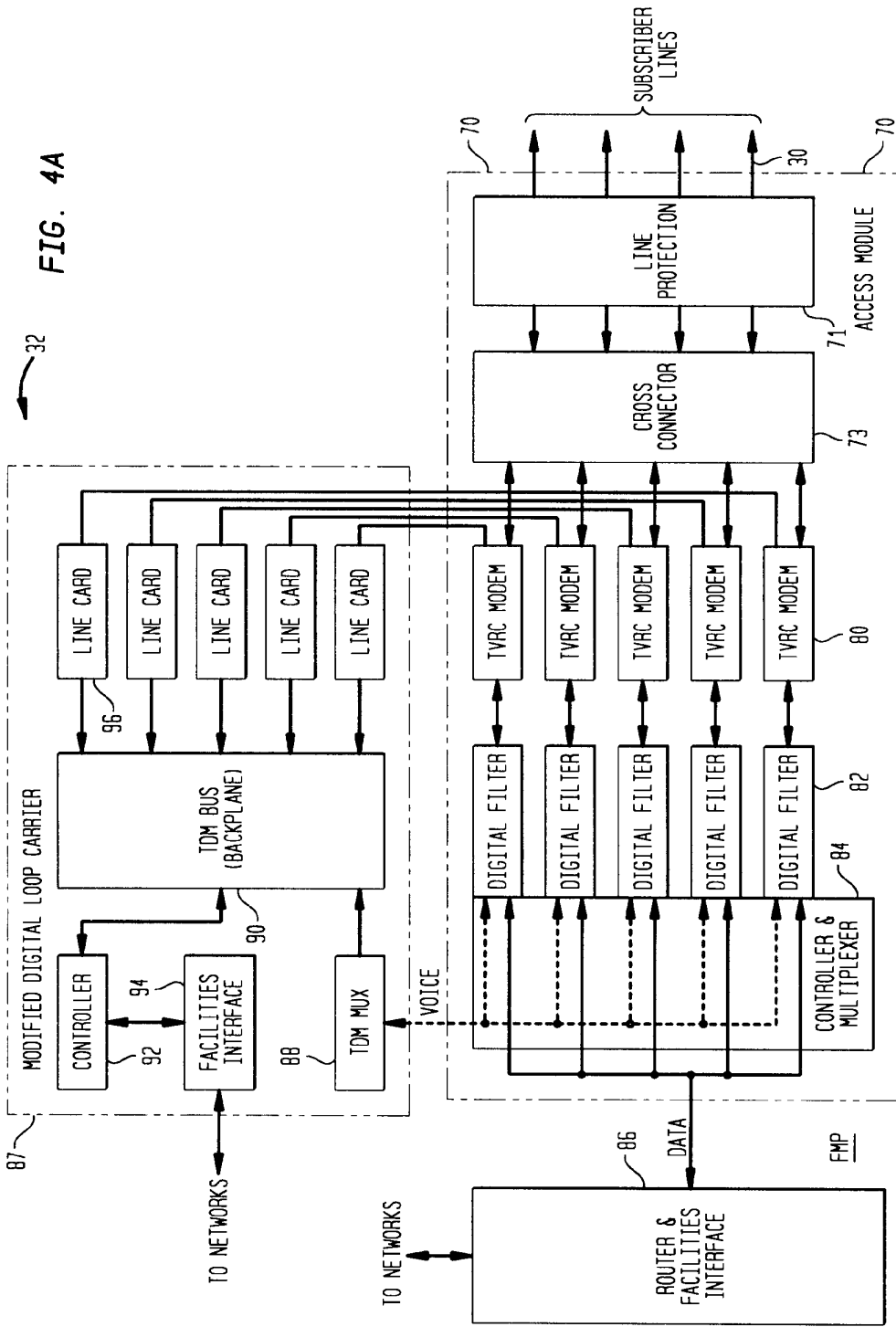
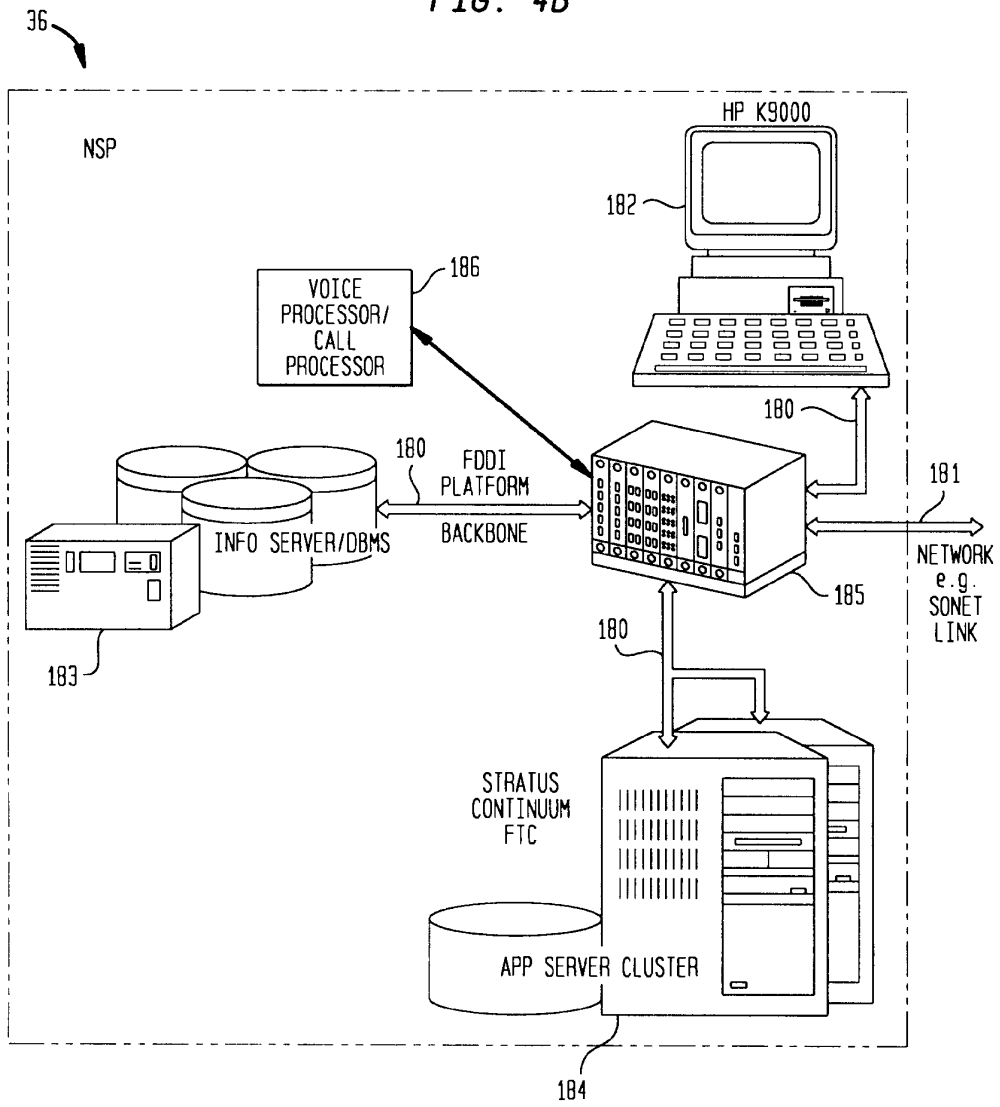


FIG. 4B



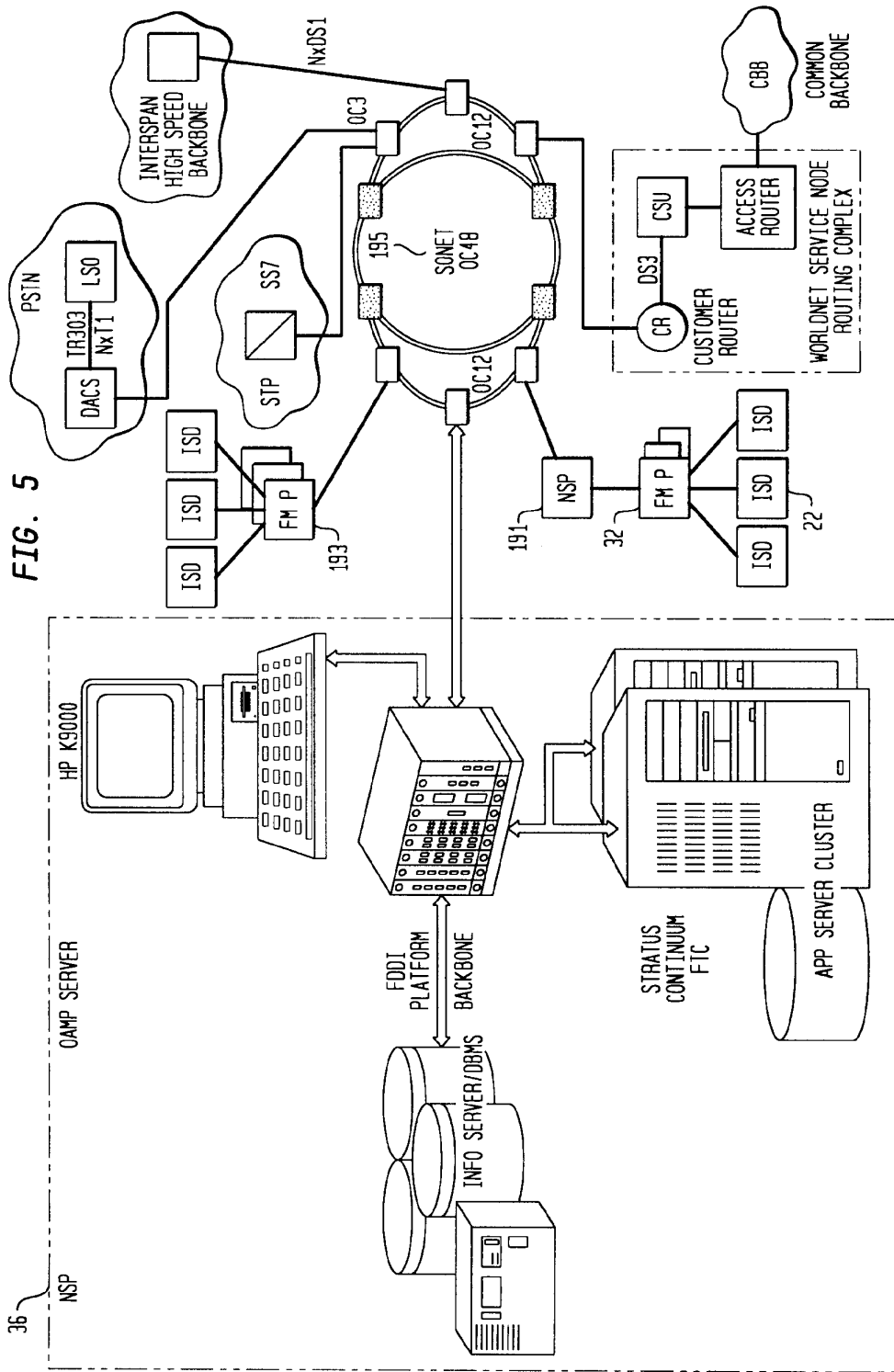


FIG. 5

FIG. 6

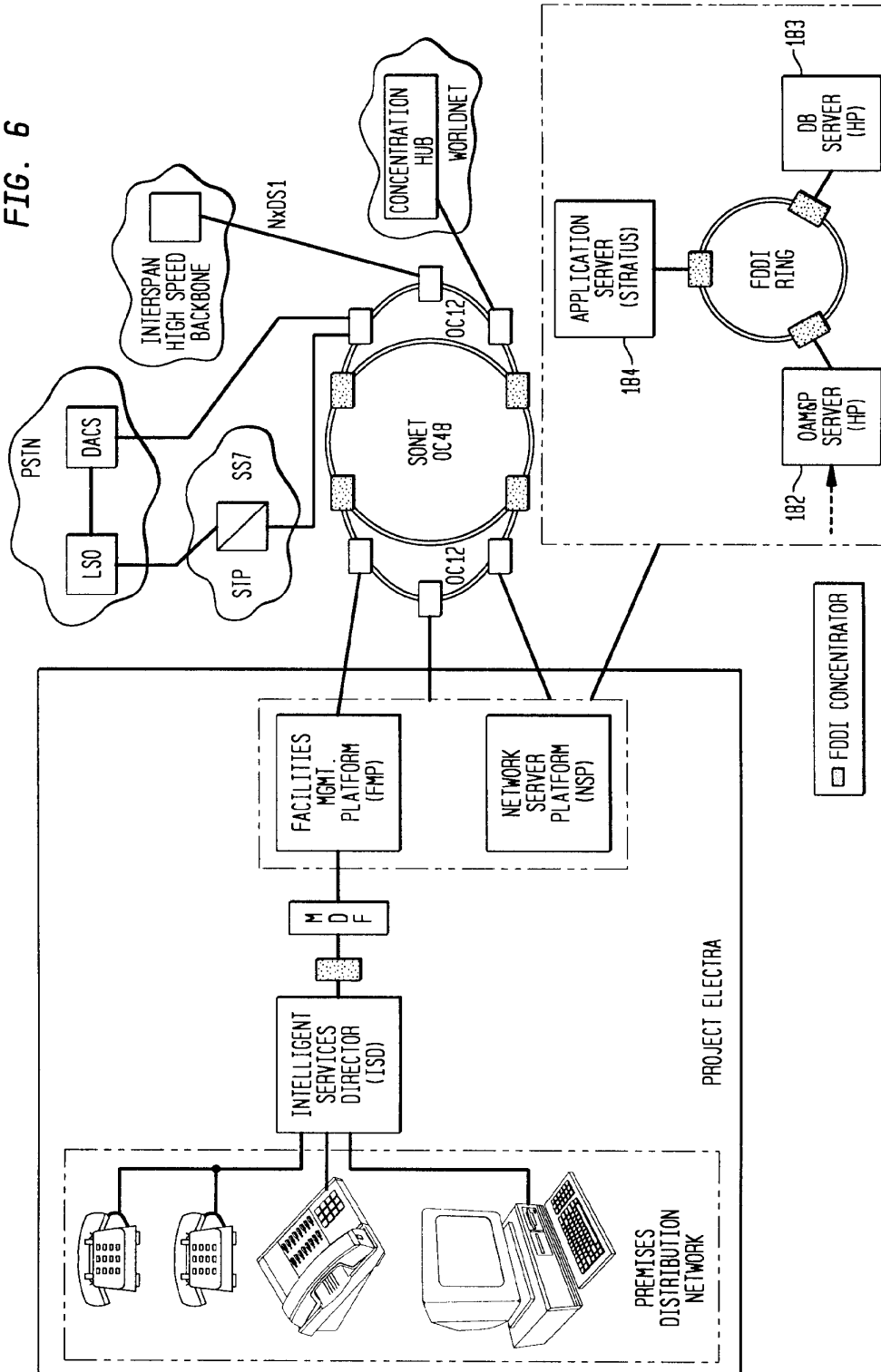


FIG. 7

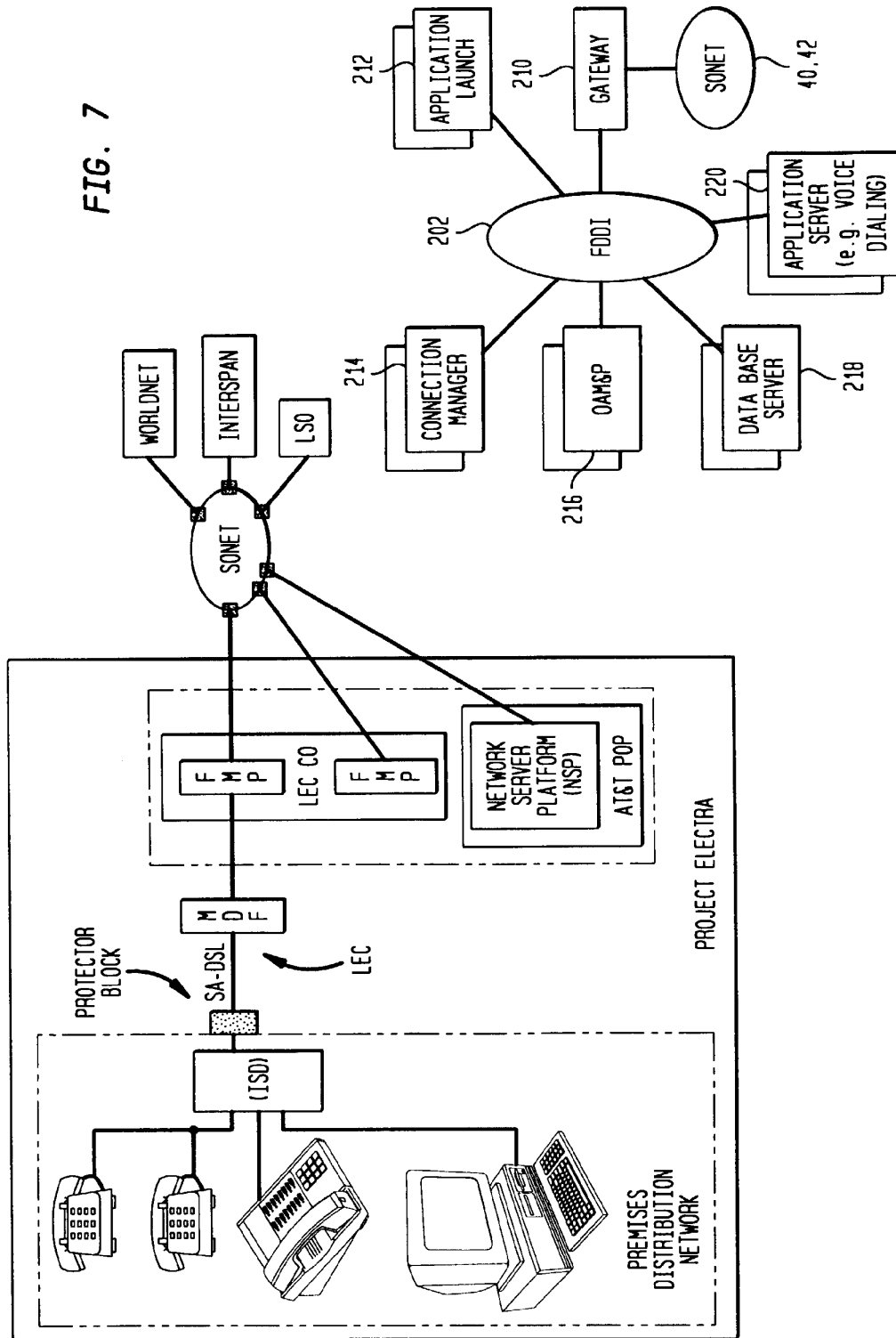


FIG. 8

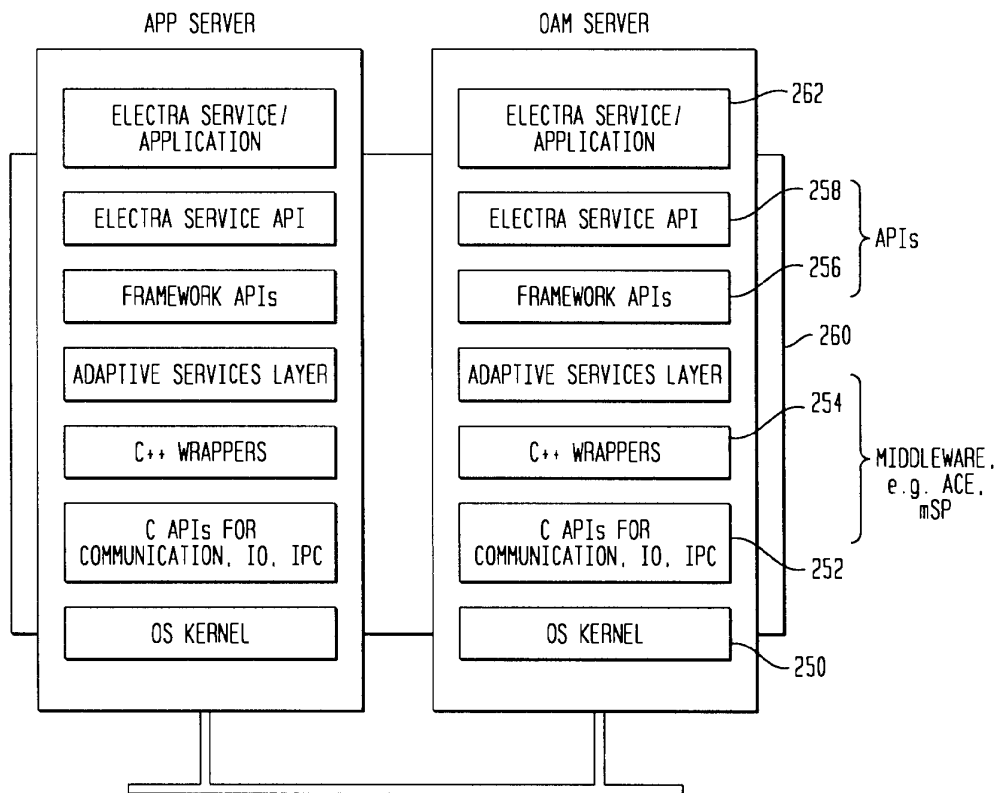


FIG. 9

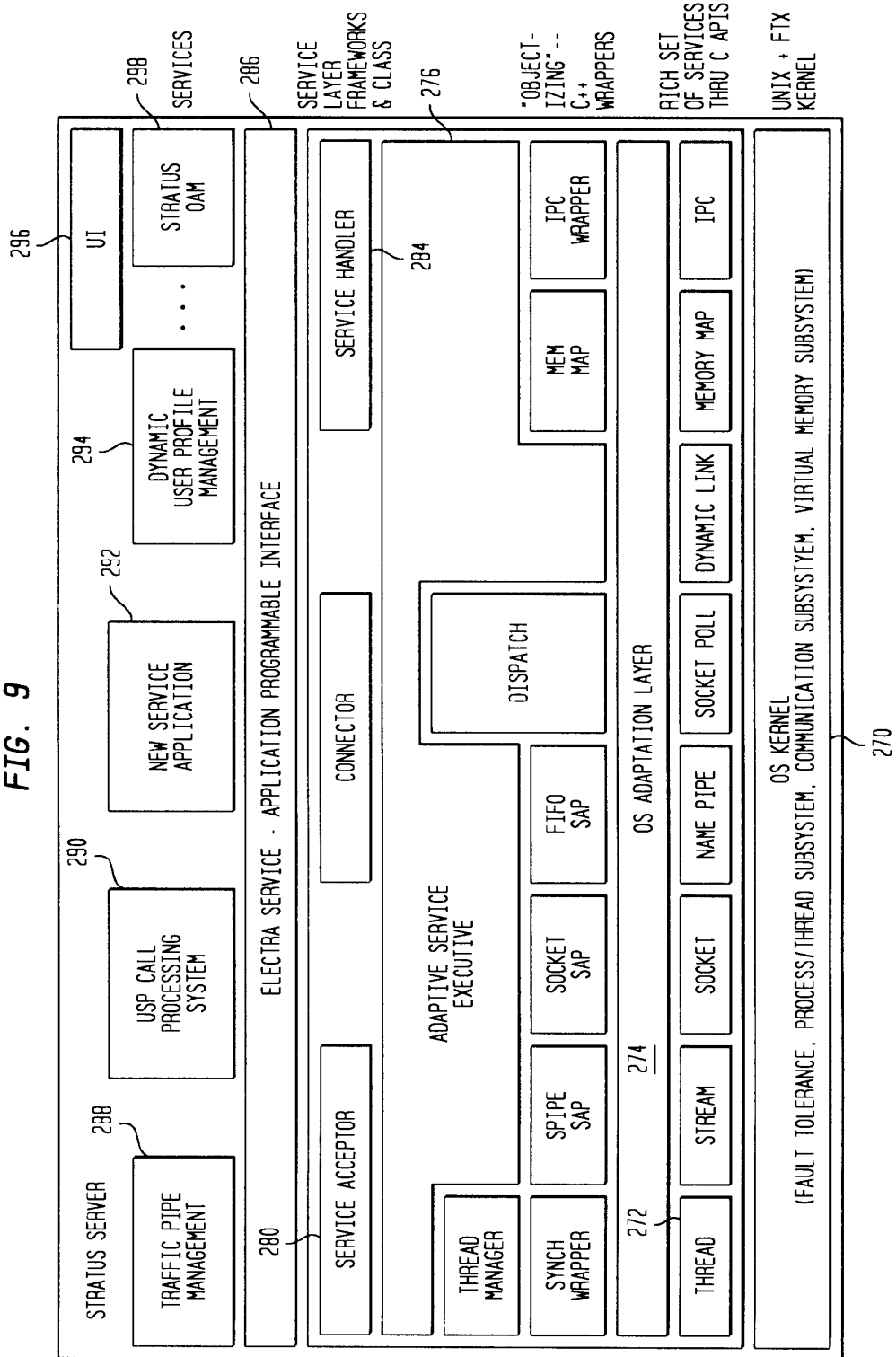


FIG. 10

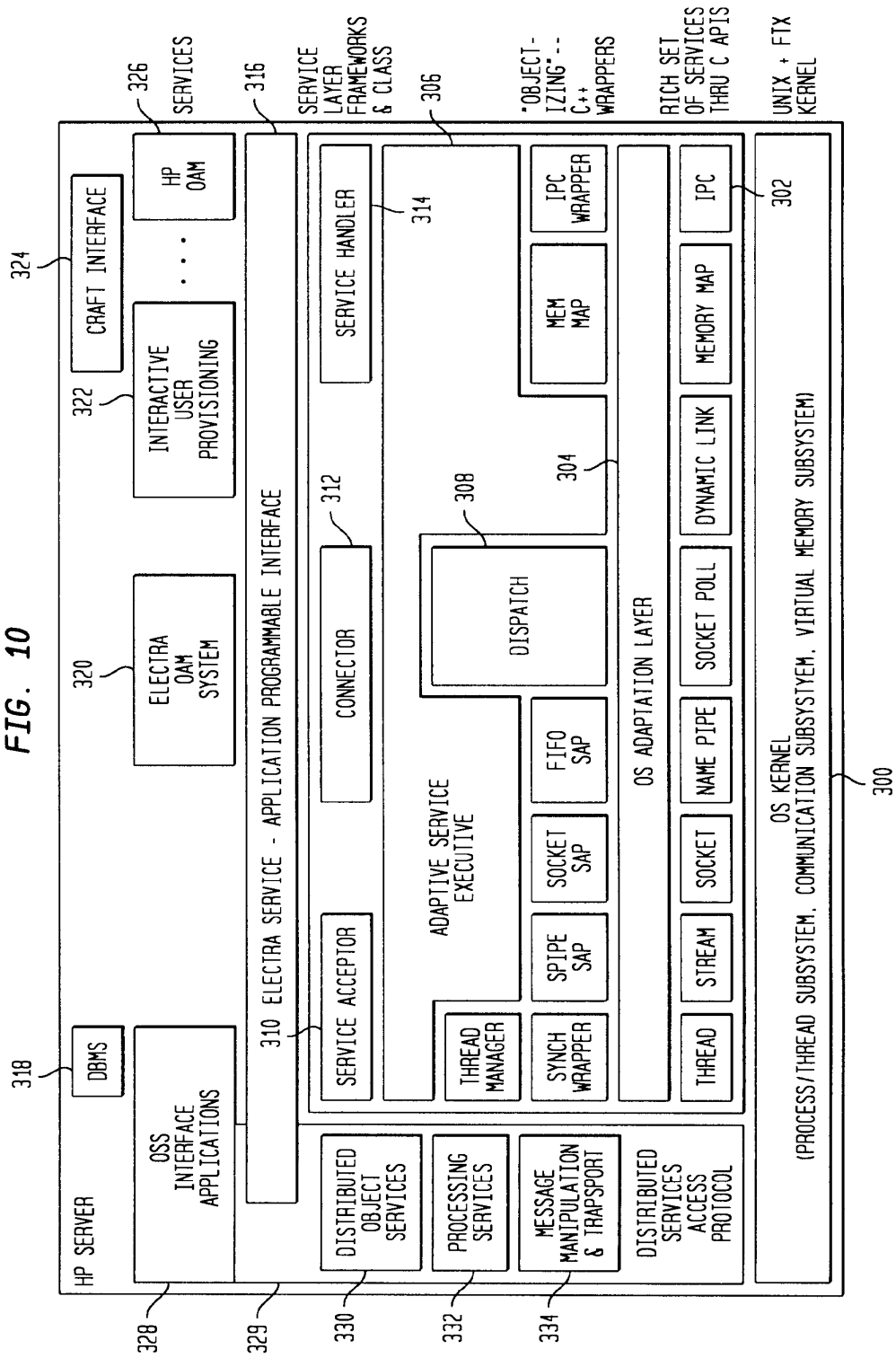


FIG. 11

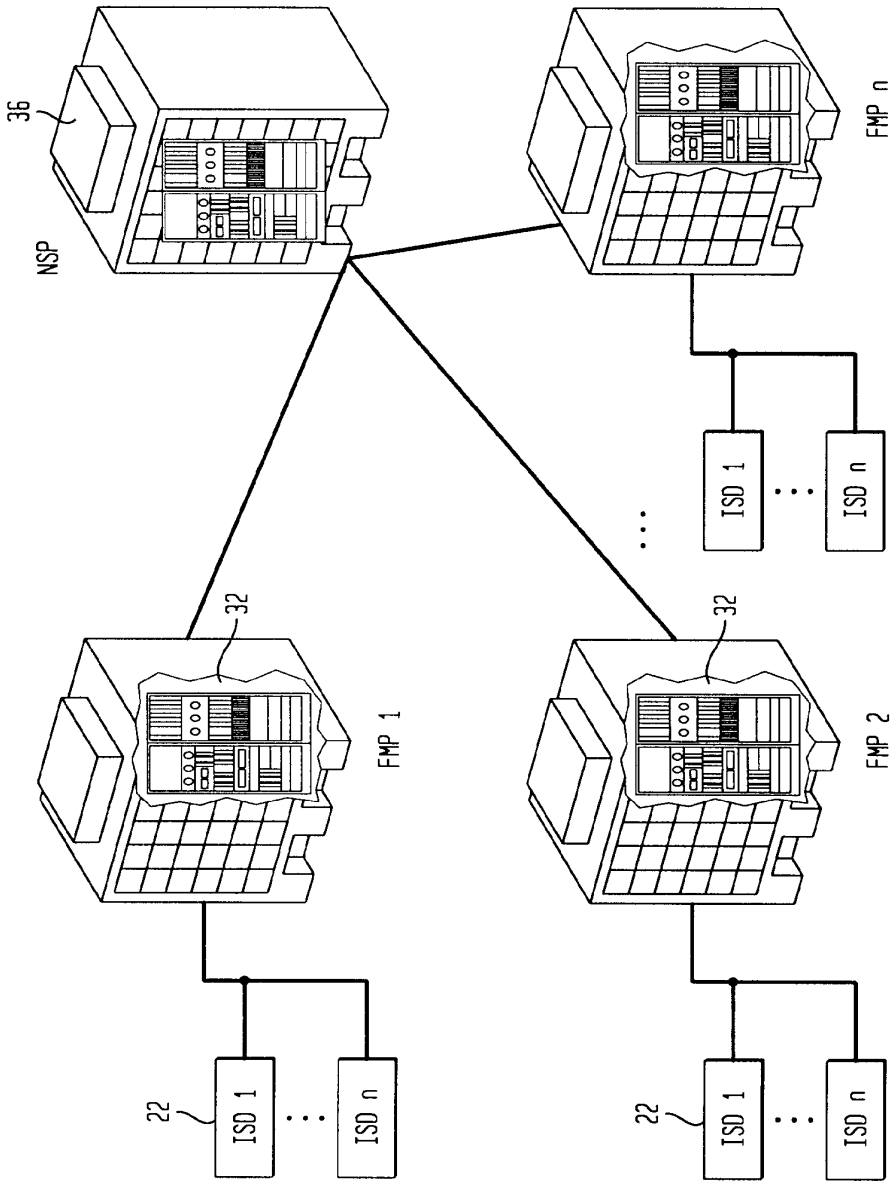
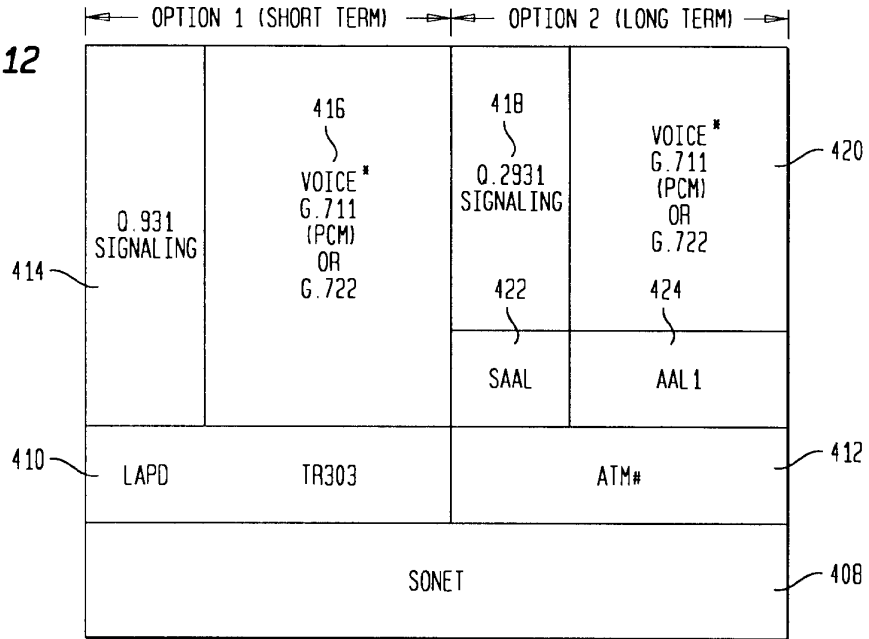
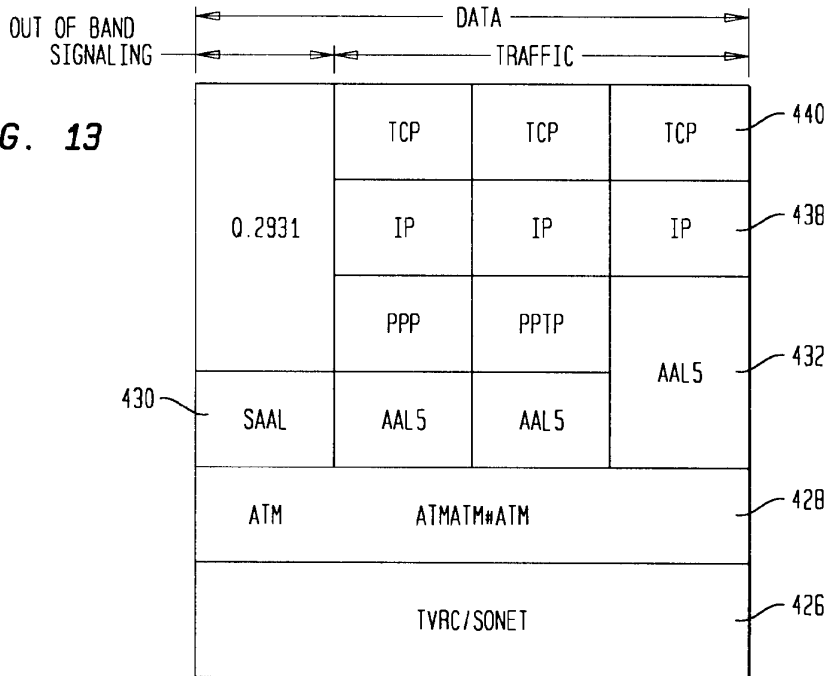


FIG. 12



* AN ALTERNATIVE OPTION IS IN-BAND SIGNALING
 # OTHER ALTERNATIVE OPTIONS WILL BE CONSIDERED

FIG. 13



* AN ALTERNATIVE OPTION IS IN-BAND SIGNALING
 # OTHER ALTERNATIVE OPTIONS WILL BE CONSIDERED

FIG. 14

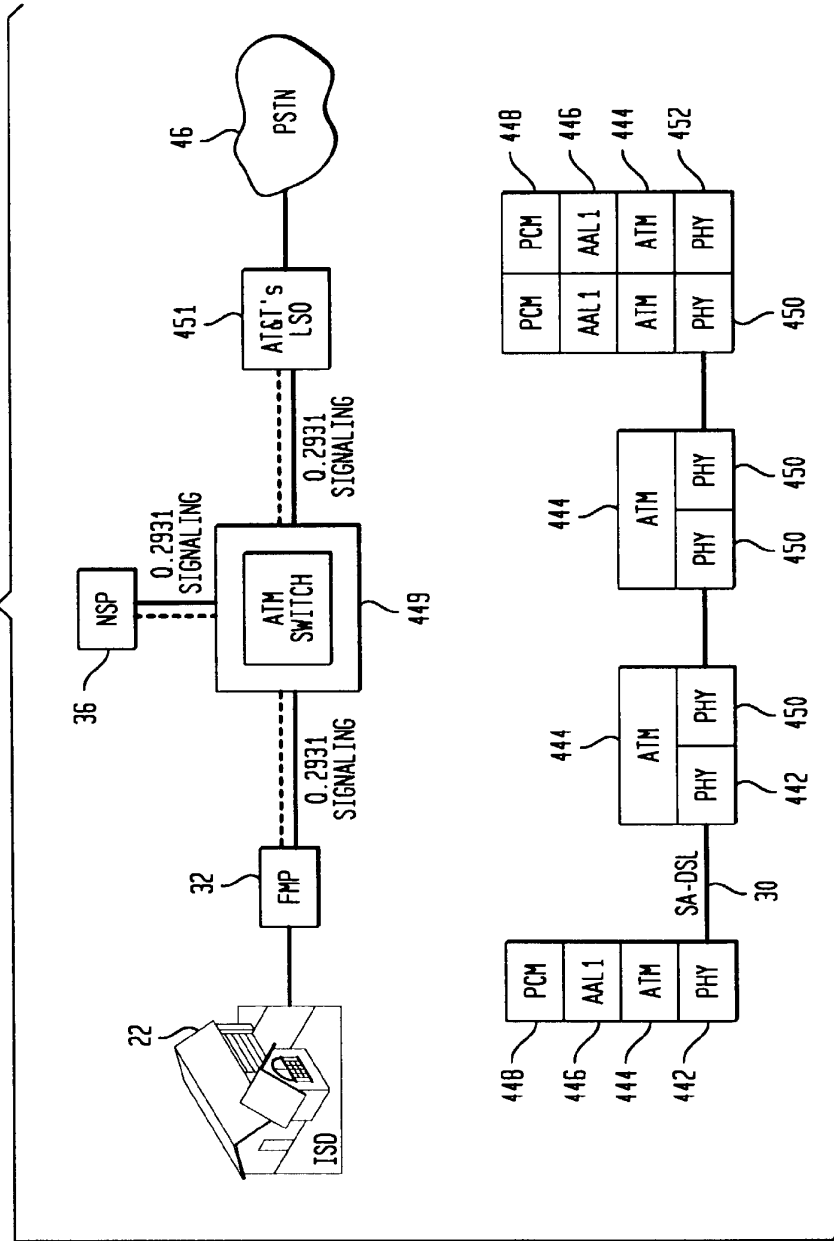


FIG. 15

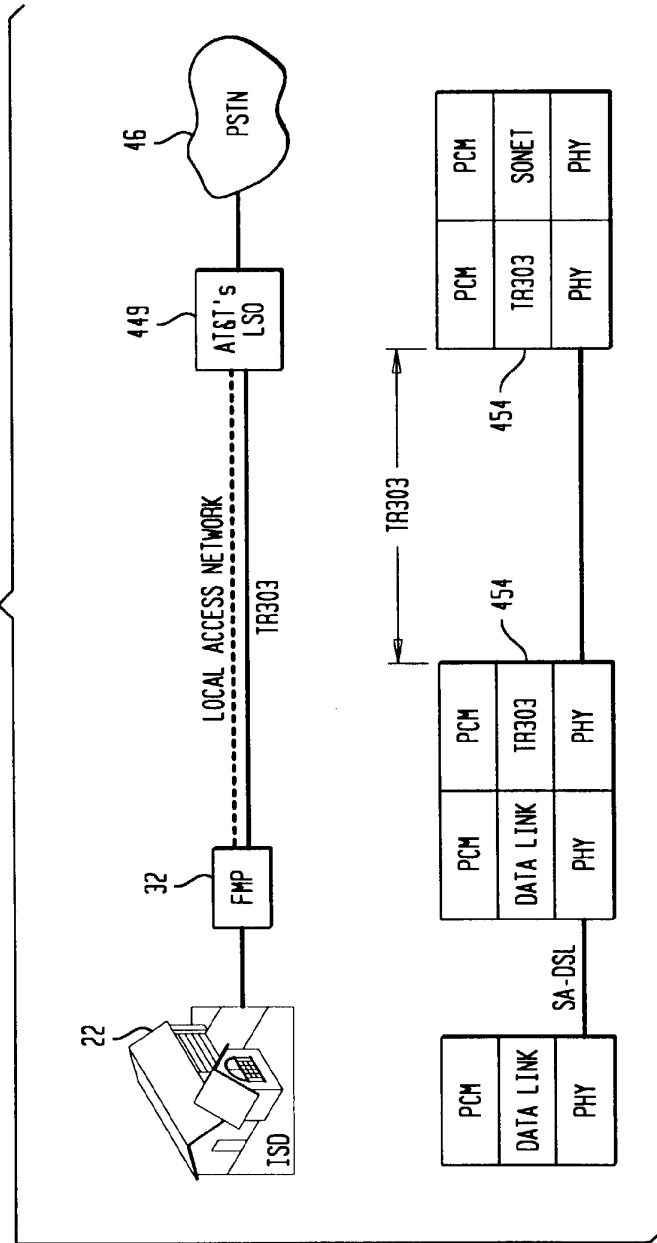


FIG. 16

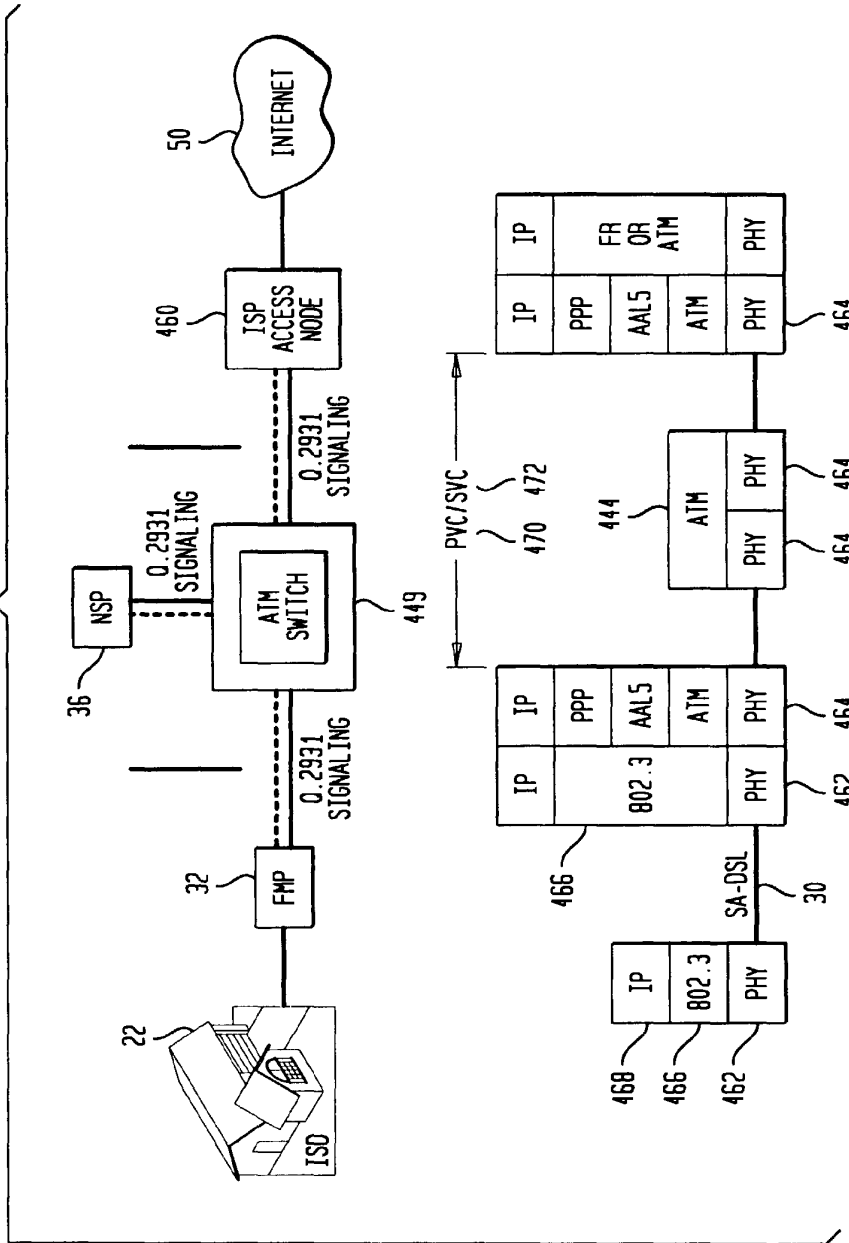


FIG. 17

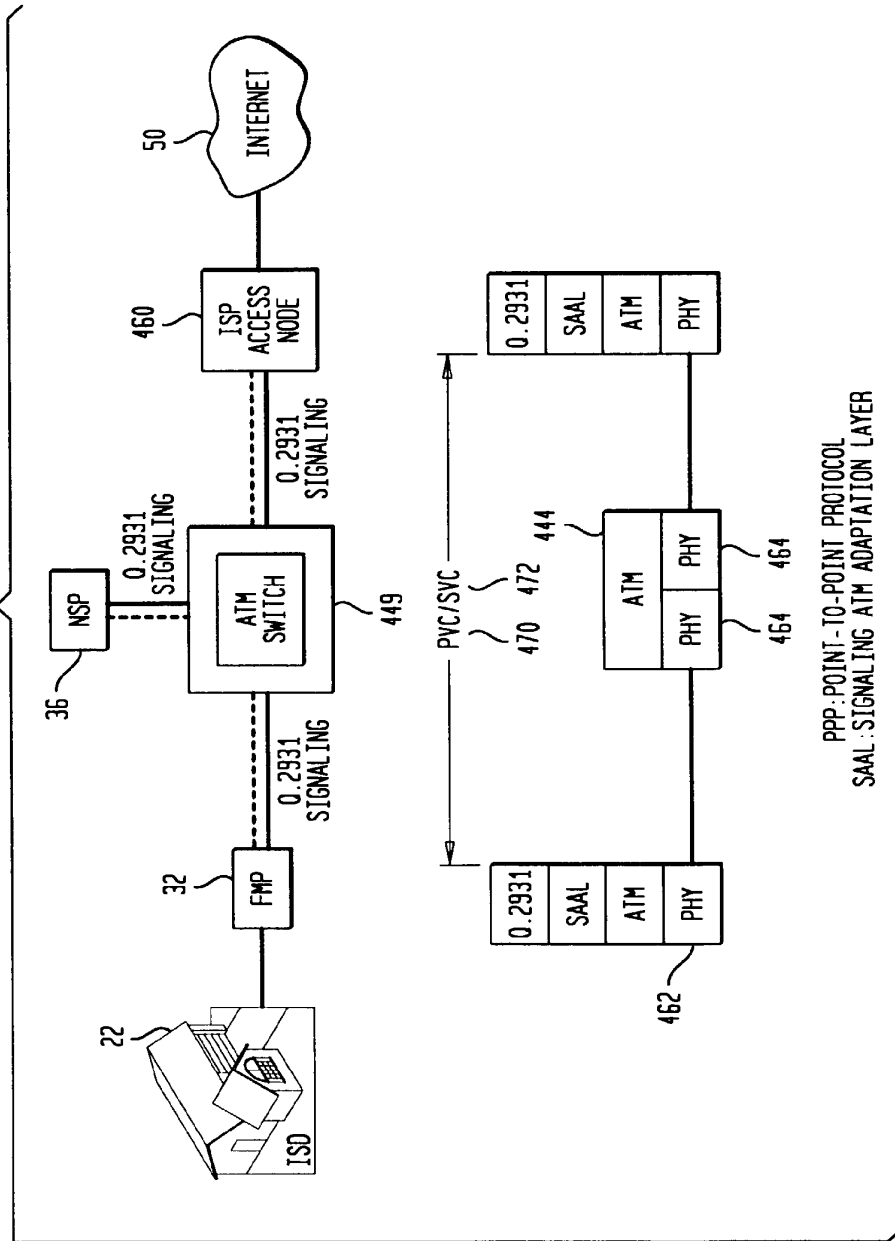


FIG. 18

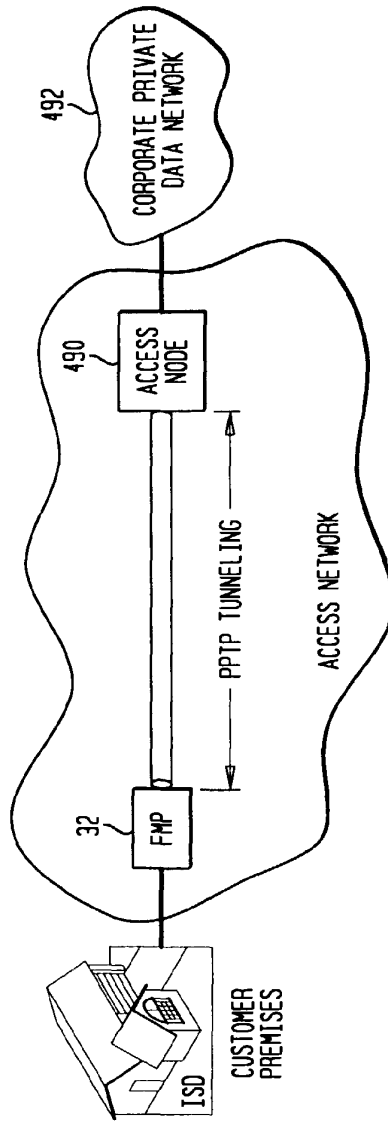
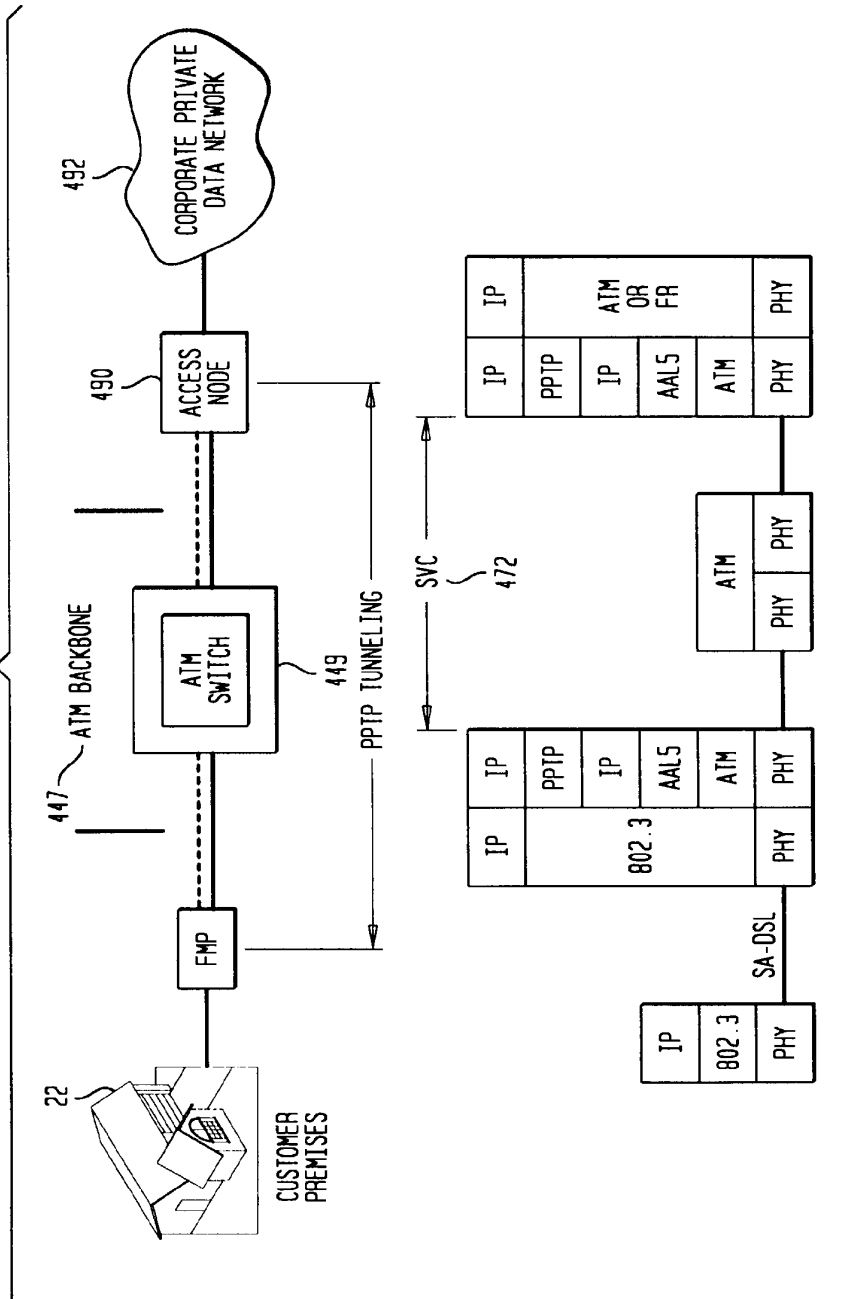


FIG. 19



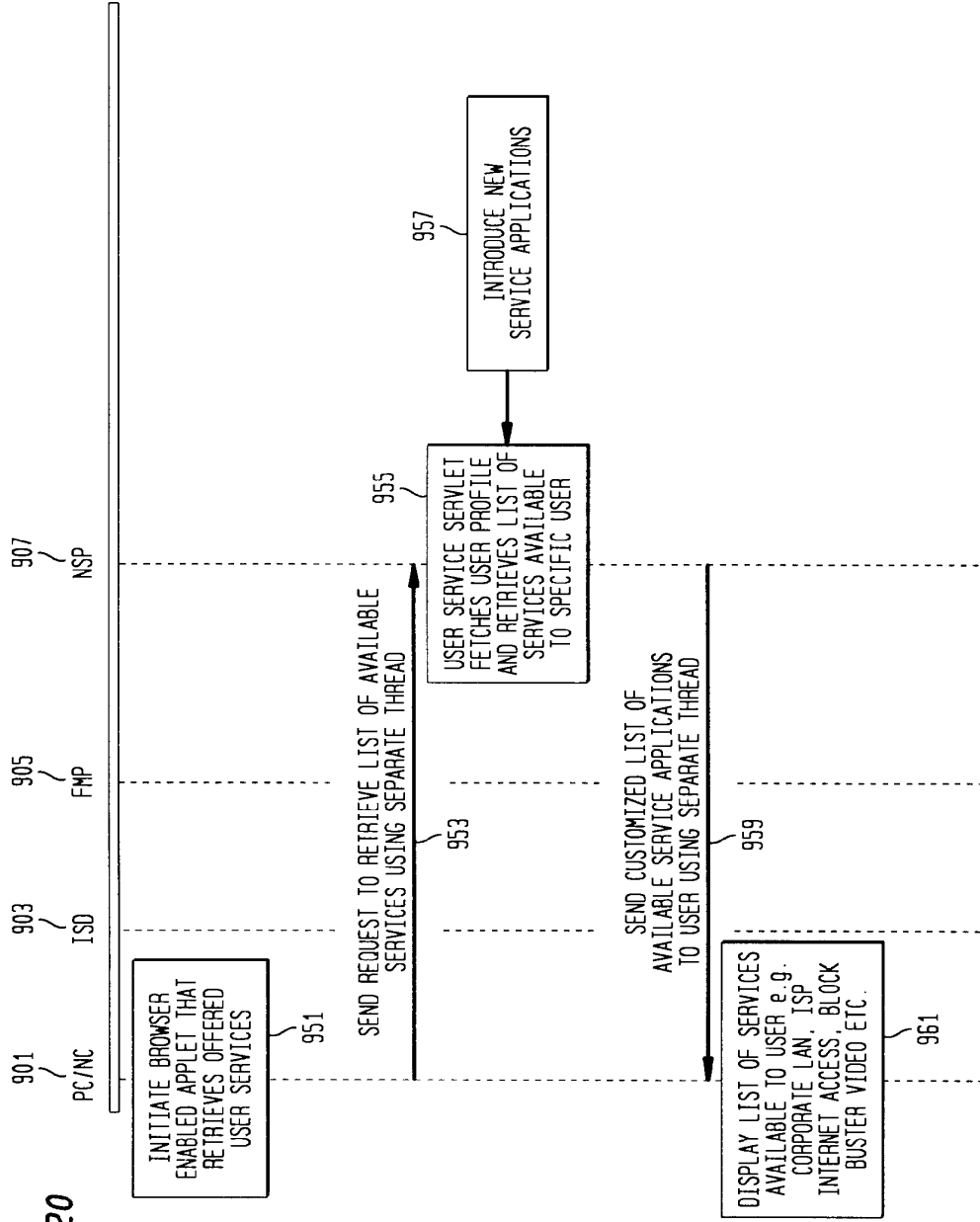


FIG. 20

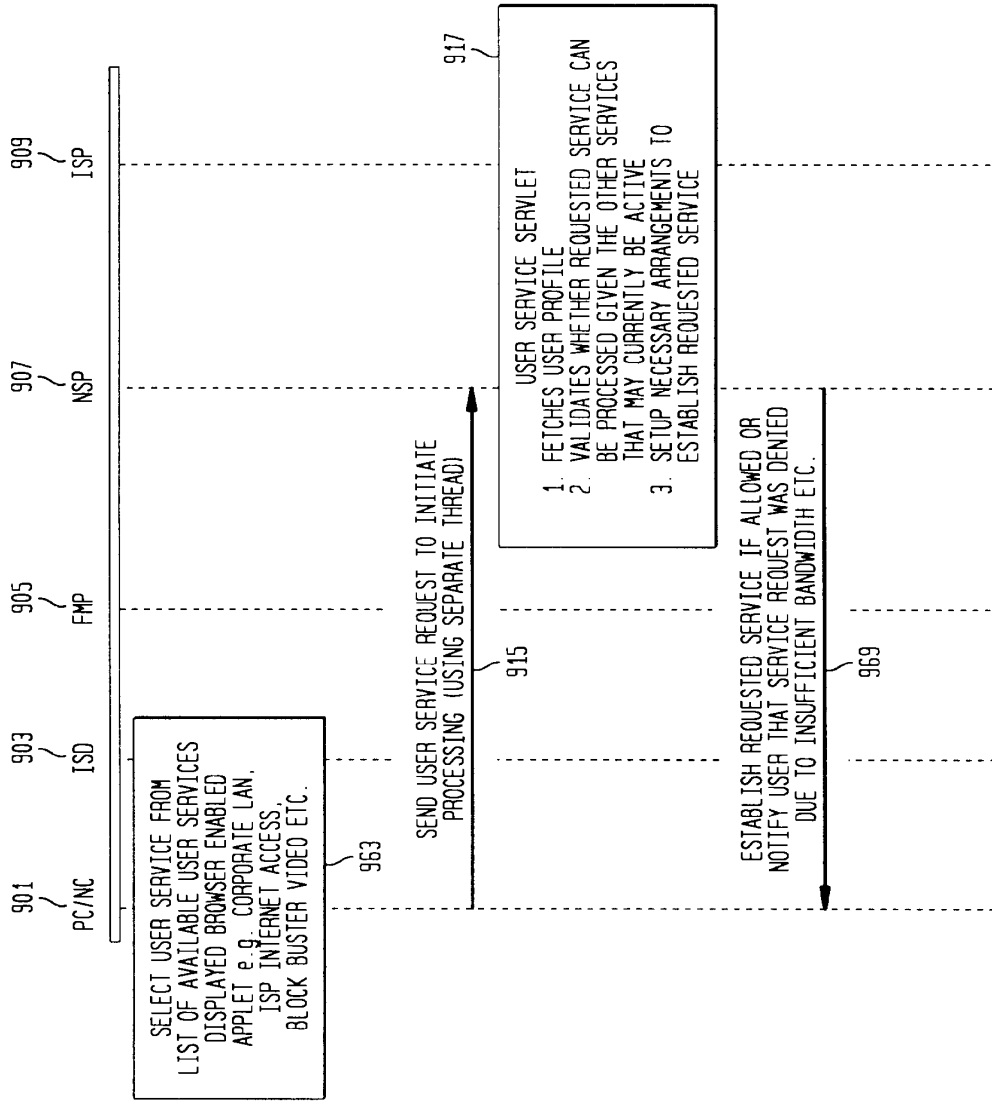


FIG. 21

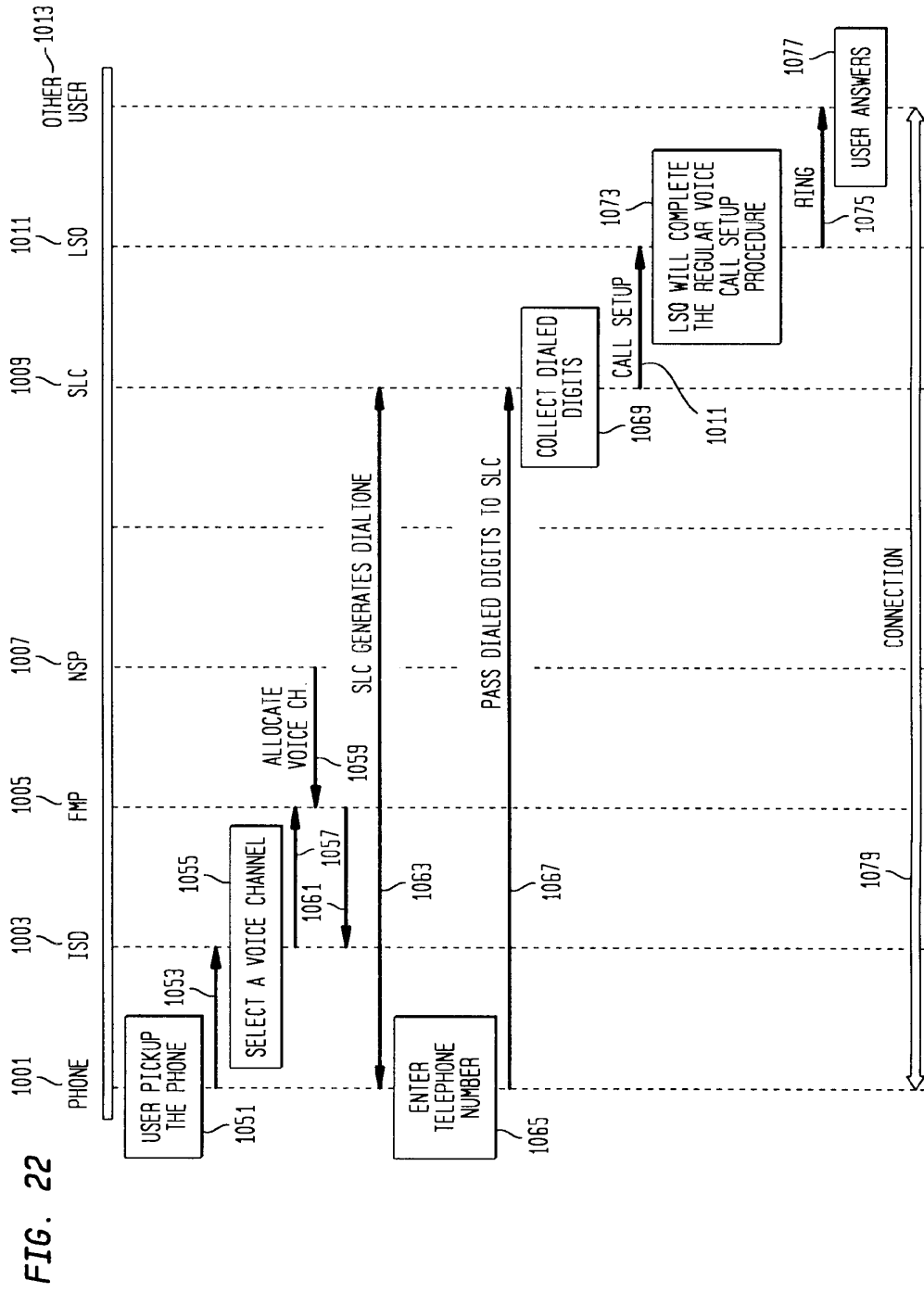
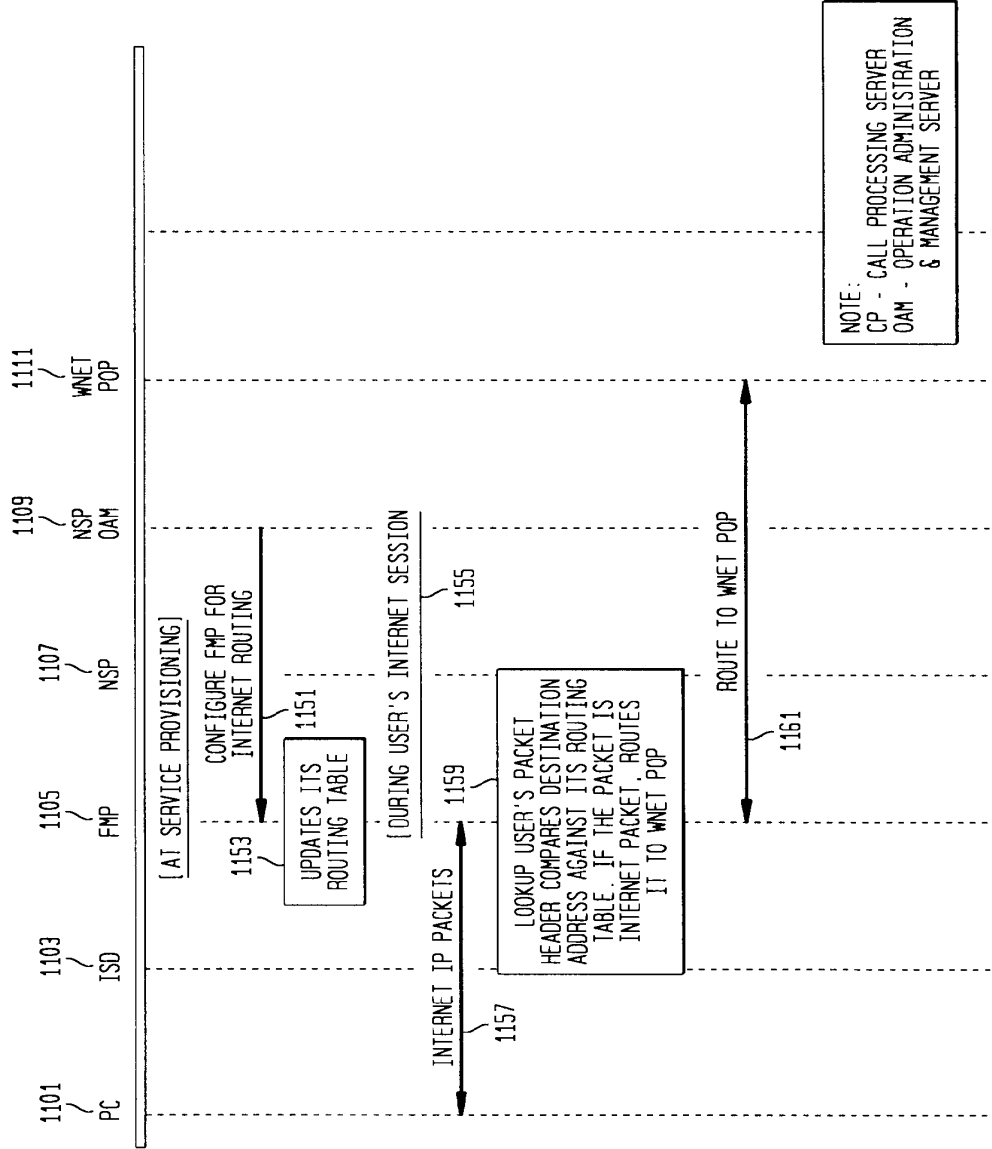


FIG. 22

FIG. 23



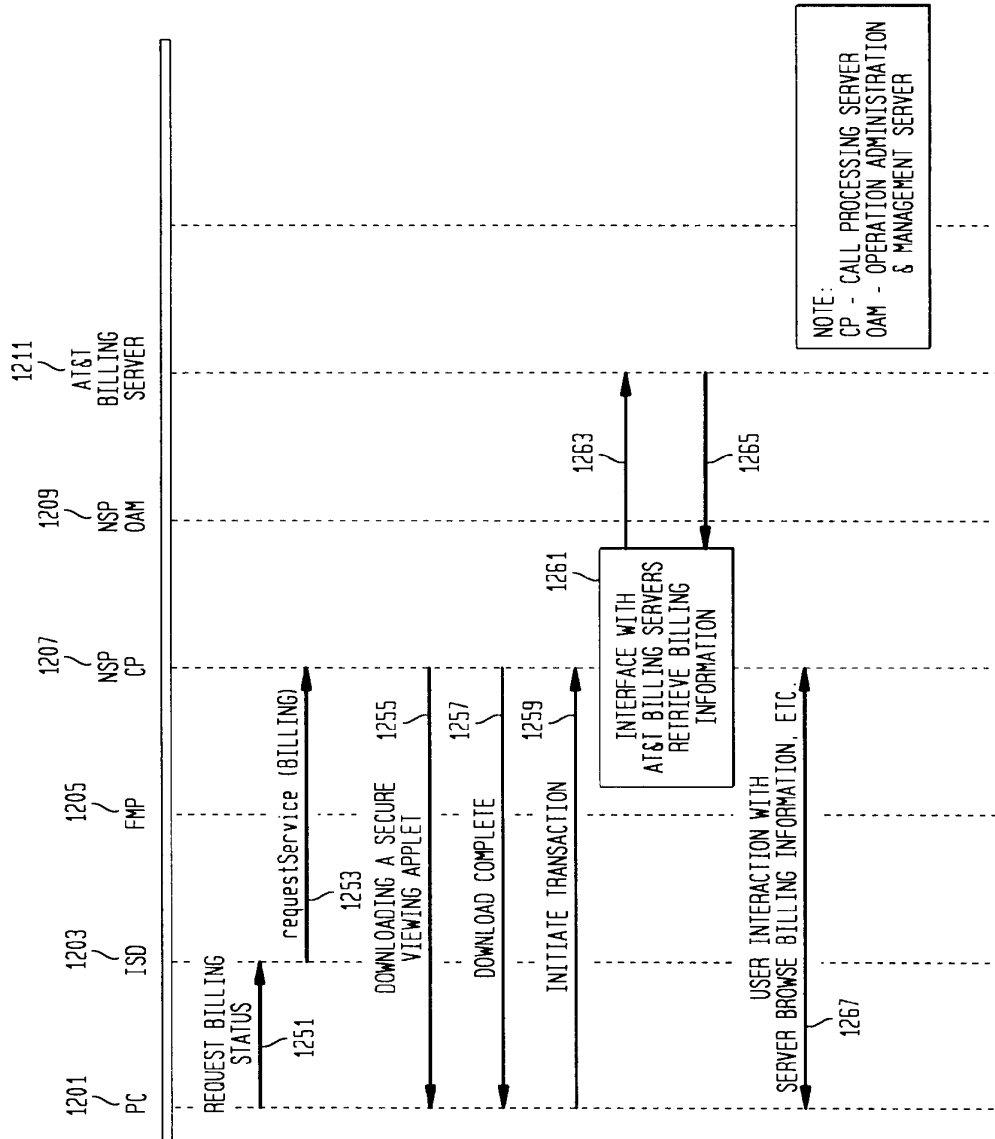


FIG. 24

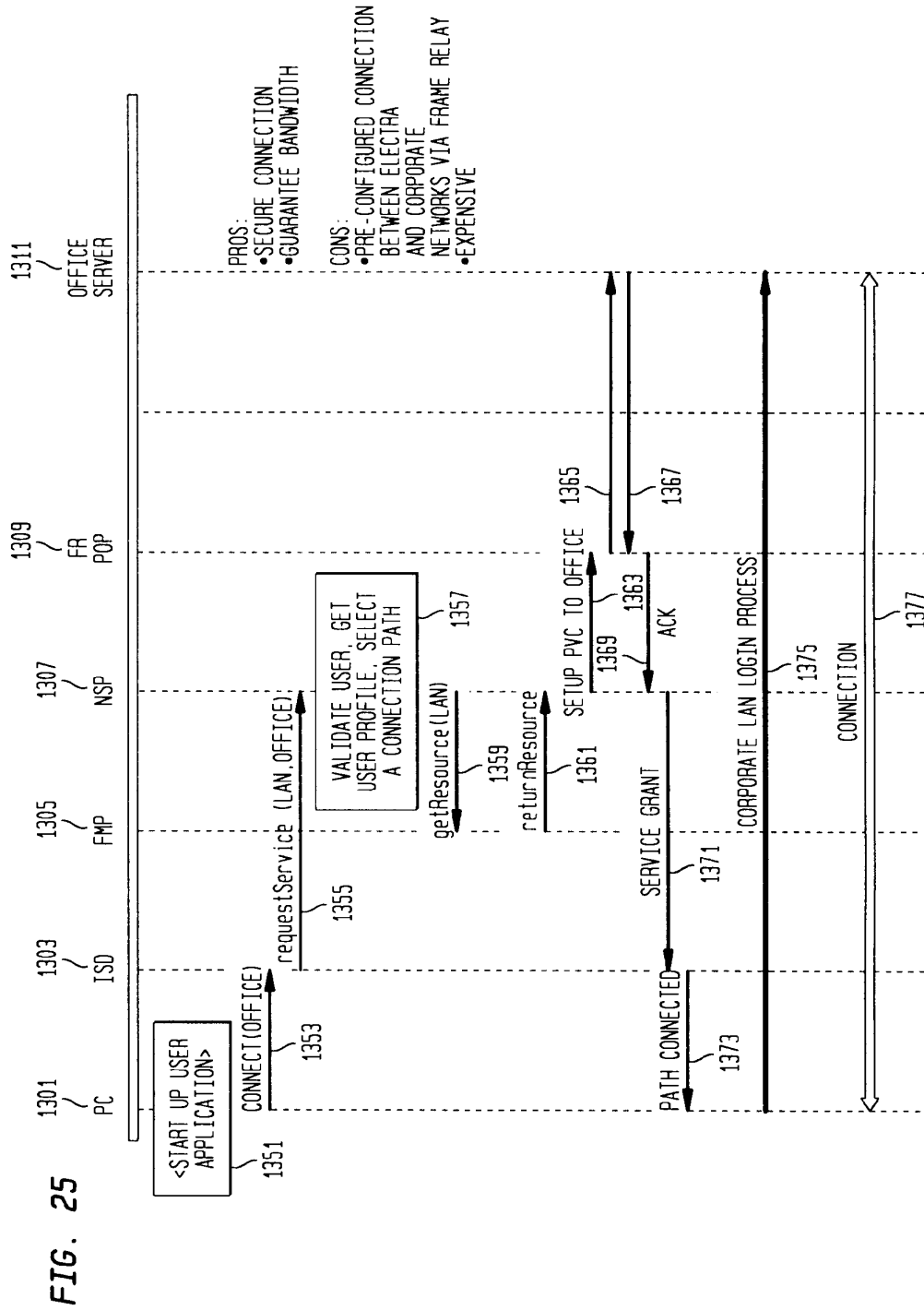


FIG. 26

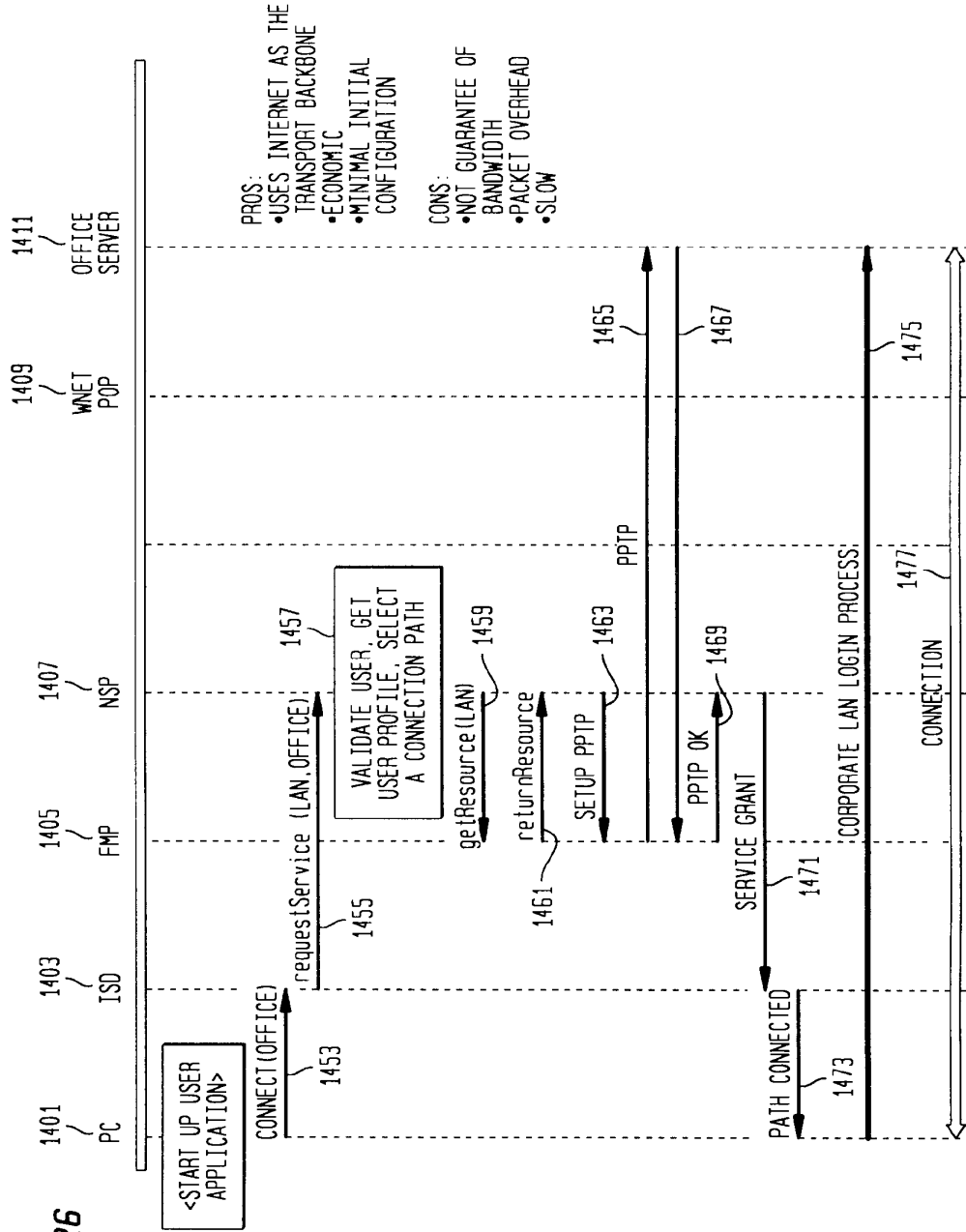


FIG. 27

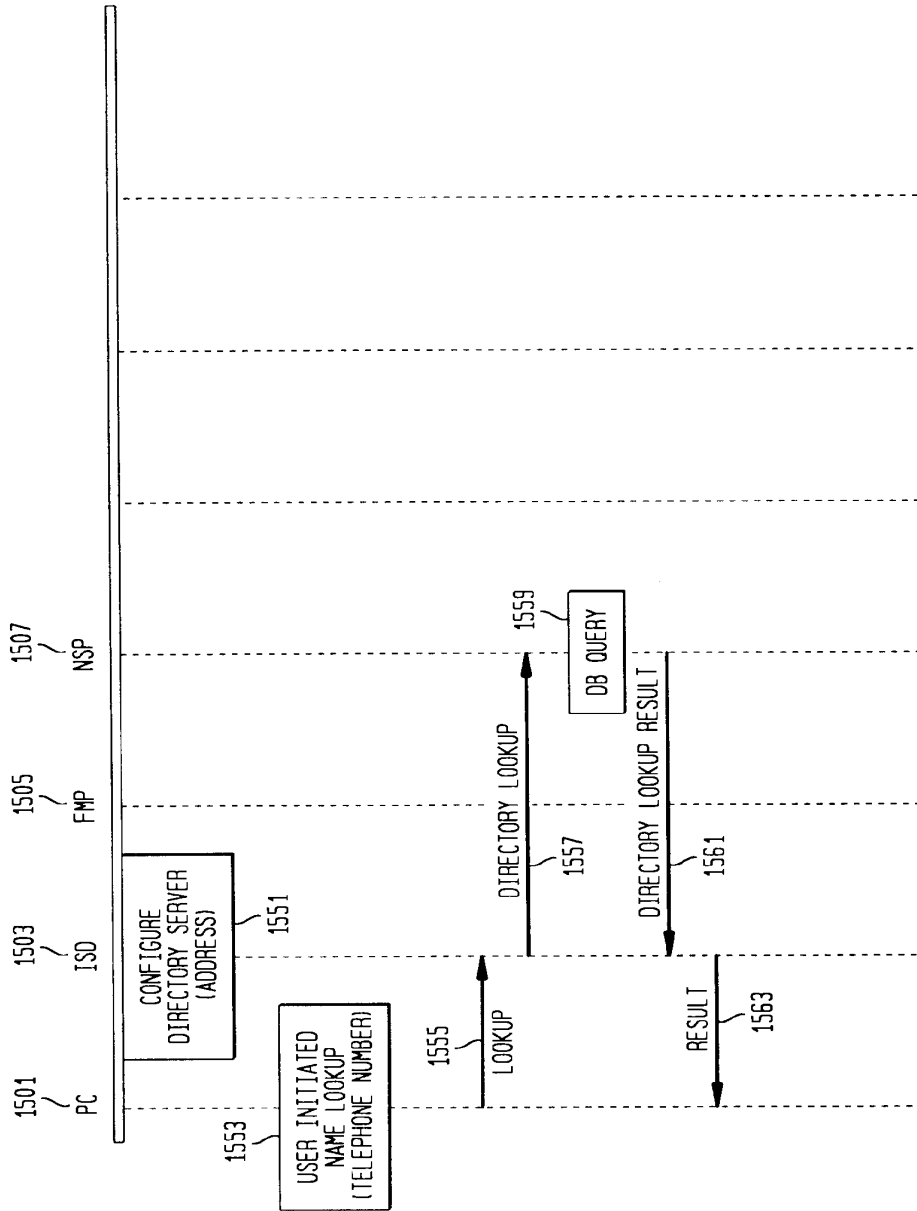
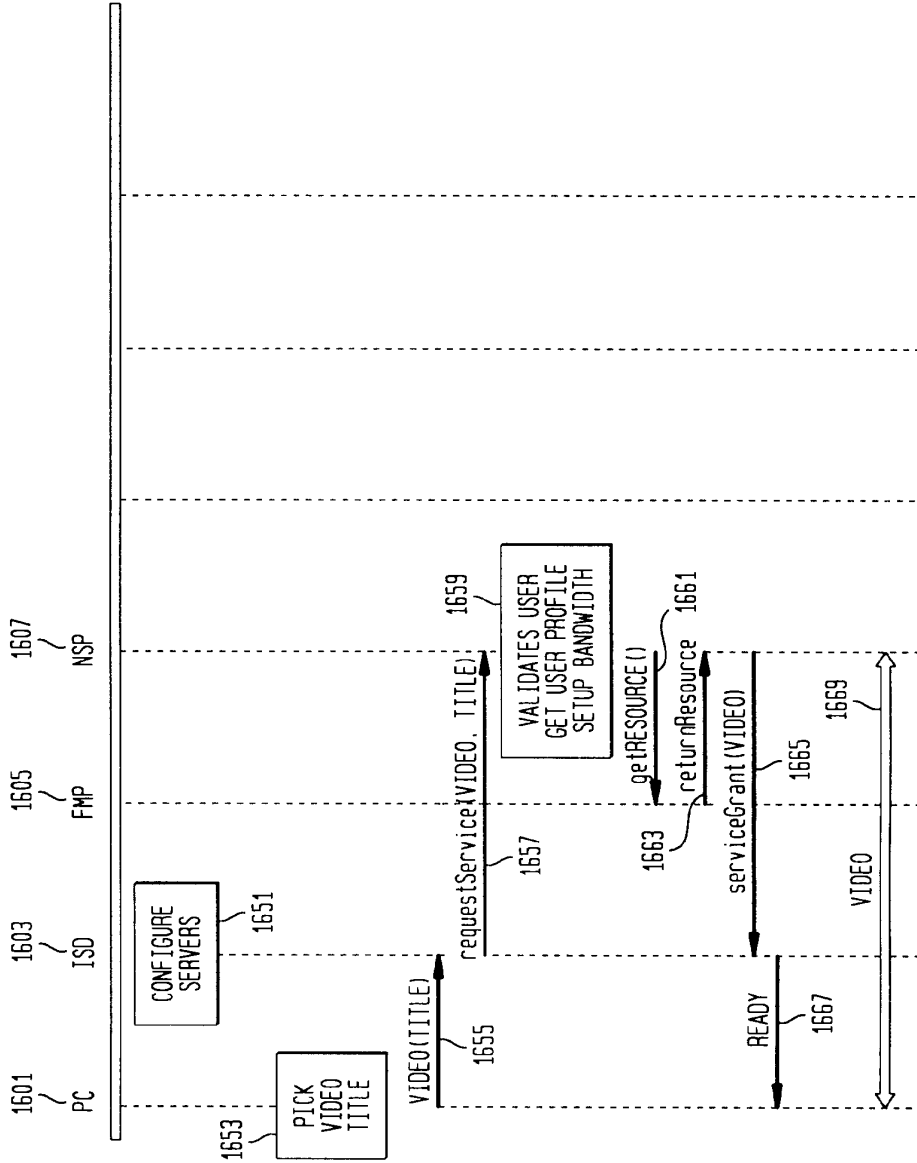
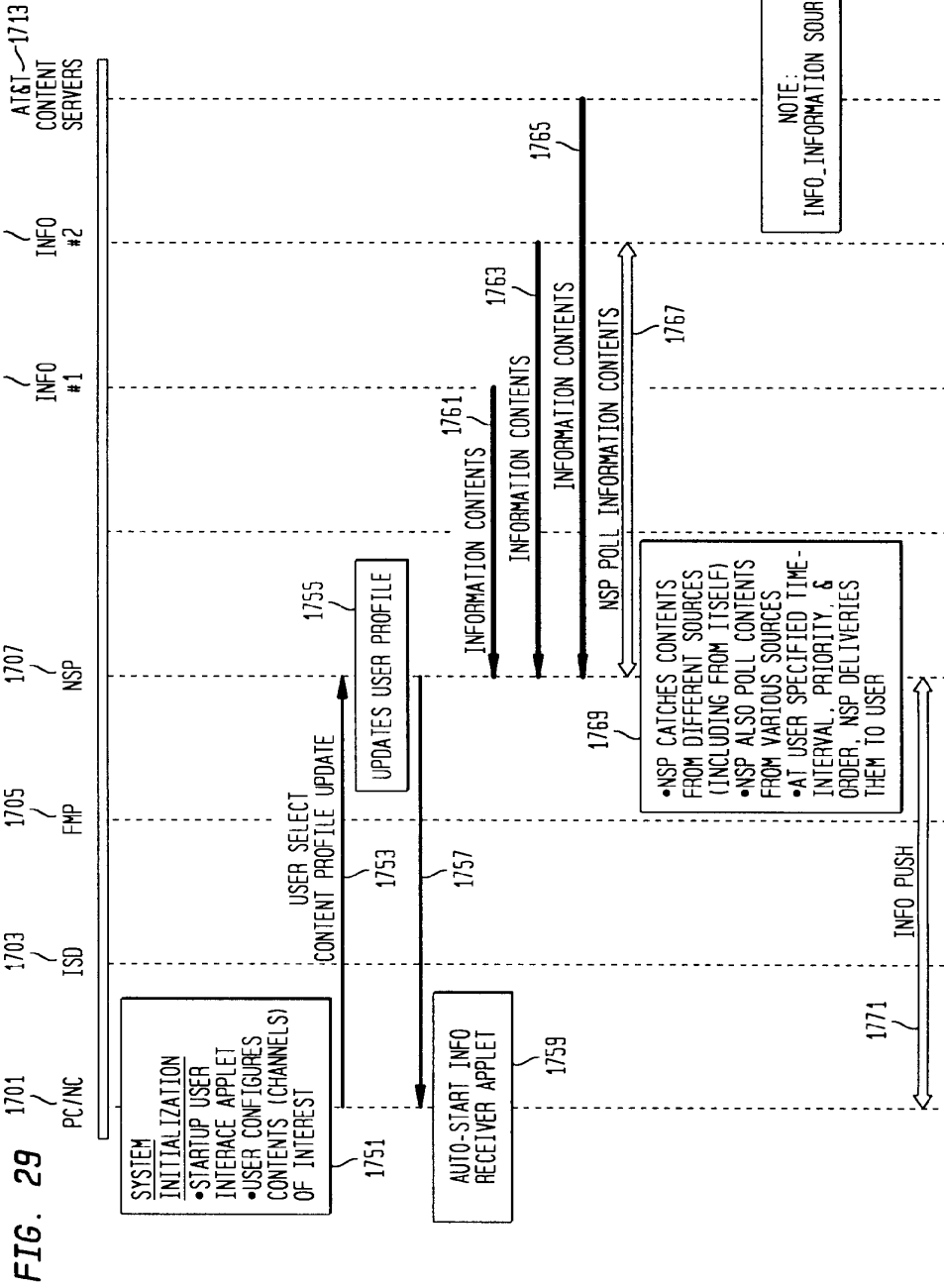


FIG. 28







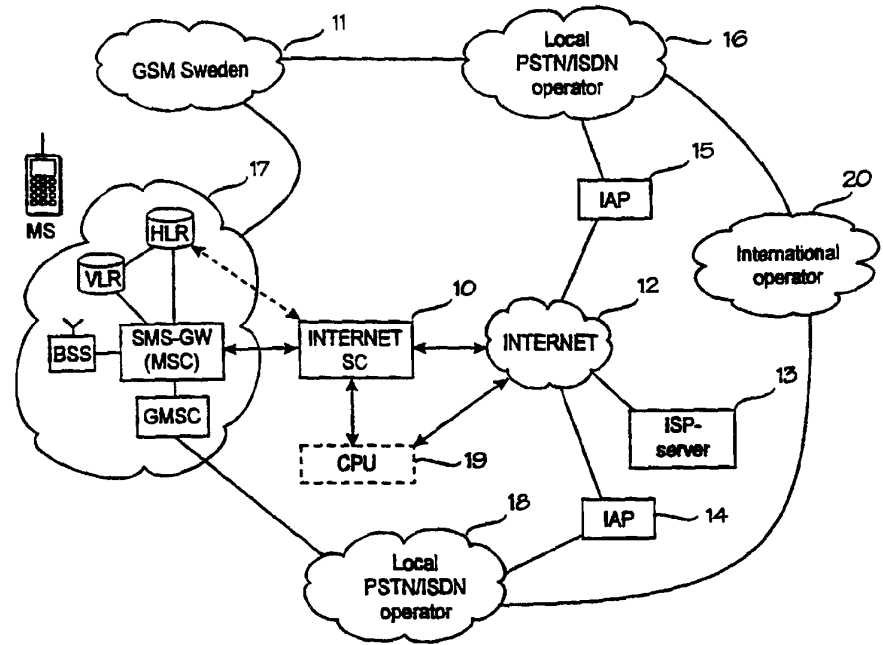
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁶ : H04Q 7/38, H04L 12/28</p>	<p>A3</p>	<p>(11) International Publication Number: WO 99/16263 (43) International Publication Date: 1 April 1999 (01.04.99)</p>
<p>(21) International Application Number: PCT/FI98/00724 (22) International Filing Date: 15 September 1998 (15.09.98) (30) Priority Data: 973737 19 September 1997 (19.09.97) FI (71) Applicant (for all designated States except US): NOKIA TELECOMMUNICATIONS OY [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI). (72) Inventors; and (75) Inventors/Applicants (for US only): TARNANEN, Teemu [FI/FI]; Kaskipuunkaari 5 C 6, FIN-02340 Espoo (FI). MOSLEMIE, Abbas [FI/FI]; Pajalahdentie 4 A 9, FIN-00200 Helsinki (FI). (74) Agent: KOLSTER OY AB; Iso Roobertinkatu 23, P.O. Box 148, FIN-00121 Helsinki (FI).</p>	<p>(81) Designated States: AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published With international search report. (88) Date of publication of the international search report: 20 May 1999 (20.05.99)</p>	

(54) Title: UPDATING OF INTERNET ACCESS POINT SETTINGS IN A MOBILE COMMUNICATION SYSTEM

(57) Abstract

A digital mobile communication system is provided with a facility by means of which it can establish a connection to the Internet network (12) via an Internet access point (14, 15). IAP settings needed for establishing a connection are stored in a mobile station (MS). When a mobile station (MS) roams, the closest point may, however, change, and IAP settings should be updated in the mobile station (MS). The invention comprises dividing the mobile communication system into IAP areas, which are given preferred IAPs. An IAP area may be e.g. a mobile communication network (11, 17). Mobile communication networks broadcast system information on the basis of which a mobile station may detect that the IAP area has changed and start a procedure for updating IAP settings.



Updating may comprise retrieval of IAP settings from a special server (13) in the network maintained by an Internet service provider. Retrieval can be done e.g. via a short message service center (10). In one embodiment the mobile communication network broadcasts messages giving recommended IAP settings to mobile stations.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI 98/00724

A. CLASSIFICATION OF SUBJECT MATTER		
IPC6: H04Q 7/38, H04L 12/28 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols)		
IPC6: H04L, H04J, H04B, H04Q		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
SE,DK,FI,NO classes as above		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
WPIL, EDOC		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5533026 A (HAMID AHMADI ET AL), 2 July 1996 (02.07.96), column 1, line 39 - line 40; column 2, line 14 - line 17; column 6, line 20 - line 65, abstract --	1-19
X	US 5095480 A (PETER R. FENNER), 10 March 1992 (10.03.92), column 1, line 59 - column 2, line 4; column 8, line 21 - line 65 --	1-19
X	EP 0696117 A2 (INTERNATIONAL BUSINESS MCHINES CORPORATION), 7 February 1996 (07.02.96), abstract --	1-19
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
11 March 1999		18-03-1999
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86		Authorized officer Malin Gullstrand Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI 98/00724

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0695058 A2 (INTERNATIONAL BUSINESS MACHINES CORPORATION), 31 January 1996 (31.01.96), abstract ----- -----	1-19

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT
Information on patent family members

02/02/99

International application No.

PCT/FI 98/00724

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5533026 A	02/07/96	CA 2170786 A CZ 9702656 A EP 0813800 A JP 8274792 A PL 321754 A WO 9627994 A	07/09/96 13/05/98 29/12/97 18/10/96 22/12/97 12/09/96
US 5095480 A	10/03/92	US 5842224 A US 5860136 A	24/11/98 12/01/99
EP 0696117 A2	07/02/96	CA 2129200 A JP 8065304 A US 5654959 A	30/01/96 08/03/96 05/08/97
EP 0695058 A2	31/01/96	CA 2129193 A JP 8065305 A US 5594731 A	30/01/96 08/03/96 14/01/97

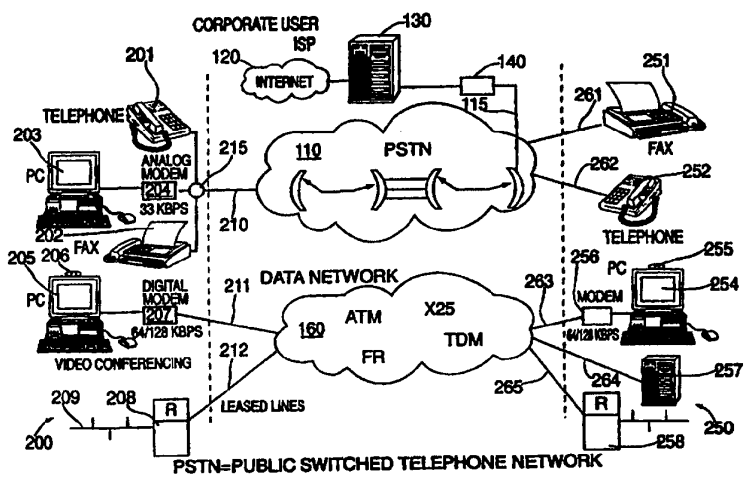
Form PCT/ISA/210 (patent family annex) (July 1992)



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁶ : H04M</p>	<p>A2</p>	<p>(11) International Publication Number: WO 99/51005 (43) International Publication Date: 7 October 1999 (07.10.99)</p>
<p>(21) International Application Number: PCT/US99/06917 (22) International Filing Date: 30 March 1999 (30.03.99) (30) Priority Data: 60/080,099 31 March 1998 (31.03.98) US (71) Applicant: TRANSACCESS CORP. [US/US]; 5th floor, 300 East 42nd Street, New York, NY 10017 (US). (72) Inventor: HEUMANN, Seily; 2nd floor, Avenida das Nações Unidas, 18.605, CEP-04795-902 São Paulo, SP (BR). (74) Agent: AUFRICHTIG, Peter, D.; Aufrichtig Stein & Aufrichtig, P.C., 5th floor, 300 East 42nd Street, New York, NY 10017 (US).</p>		<p>(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).</p> <p>Published <i>Without international search report and to be republished upon receipt of that report.</i></p>

(54) Title: MULTI-SERVICE ACCESS SWITCHED SYSTEM



(57) Abstract

A multi-service access switched system which provides for the simultaneous use of the telephone for voice communications and for transfer of data over public communication and switching systems, increases the transmission speed for data access to a level permitting the use of video conferencing, relieves the congestion in the voice telephone network by simultaneously diverting the computer data video conferencing data to the high speed data network and accessing data networks employing TDM, X.25, Frame Relay and ATM without the need for the installation of a new pair of telephone wires or a pair of digital modems while diverting voice signals through existing telephone company switch systems.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

MULTI-SERVICE ACCESS SWITCHED SYSTEM**BACKGROUND OF THE INVENTION**

The invention is generally directed to a multi-service access switched system which allows simultaneous use of the telephone lines for voice and data communications, increases transmission speed to provide enhanced services, relieves voice telephone network congestion and provides access to high speed data networks using protocols such as TDM, X.25, Frame Relay and ATM without the need for the installation of a new pair of telephone wires.

In the early 1990's the socio-economic evolution of the industrialized nations has helped these countries to enter the era of information. The foundation of this information era is the knowledge-based industry. The industrial period which is coming to an end was characterized by heavy use of machines which basically replaced and supplemented man's physical efforts. An industrial worker is a typical symbol of this period.

During the last twenty years the increasing use of computers has replaced not only the physical effort of human beings but the mental efforts of human beings through the use of powerful tools to organize people's lives and their personal objectives. These computers, interfacing with various electromechanical and combustion driven machinery have in a brief period revolutionized the quality of life and nature of communications, particularly in the first world.

If we consider the computer as the principal tool of this new era, information is its raw material. However, information by itself has no value if it cannot be adequately accessed by people from a remote source, regardless of the distance between the user and the source. In this process of accessing, analyzing, distributing and acting upon information the telecommunications industry has been and will continue to play a fundamental role.

Until the early 1970's the information carried by the public telecommunication systems was almost exclusively in the form of voice signals known now as telephony. From that time forward, as the exponential growth in the use of computers has proceeded there has been a similar explosive rise in the demand for the transmission of data. As there was a perceived explosive even increasing rise in the demand for data transmission in the early 1970's, today there is an ever increasing interest in the transmission of higher bandwidth signals, such as video conferencing, videophones and multi-media communication. As a result, an important characteristic of current communication networks is the need and the ability to allow voice, music, data and video signals to share the same networks as basic telephony.

The constant pressure to implement more reliable, multimedia-compliant and less expensive networks with every increasing bandwidth capacities has applied substantial pressure to force the data transmission for the communications services

to be completely digital in nature rather than the existing analog and hybrid analog/digital systems. As time progresses the conversion of the last segments of the telecommunications networks to a digital form will be extended even to include the replacement of the copper wires, which physically connect the customer's premises with the local telephone exchange, with optical fiber cabling or other digitally oriented physical mediums. In this way, the entire networks from end to end will be digital. The telephony conversion from the analog speech to the digital signal and vice versa will be performed by the telephony instruments themselves.

With the decreasing costs of computer related equipment and telecommunication services the need for ever increasing high speed access to computer data networks and the Internet have increased beyond the days when only big corporations required telecommunications access beyond conventional telephony. The world wide popularity and success of the Internet is a prime example of this demand for a reliable inexpensive multimedia-compliant digital network. This popularity has included small firms, residential users, educational institutions and created new business opportunities spawned by the Internet and requiring ever increasing digital communication requirements.

The concept of a equal access to a multiplicity of services in a telecommunications network and to date, in particular the Internet, has brought about a need for an enormous

increase in the bandwidth in the requirements for residential, commercial, industrial or corporate customers of the current telephony based telecommunications networks.

To satisfy all these current and anticipated requirements the characteristics of network which must be implemented within the next several decades can be established. The network must be a multimedia and multi-service network and the switching functions in the network will be an Asynchronous Transfer Mode (ATM) type. Presently, the principal parameters of such a network are in the process of being defined and the network will be known as a Broadband Integrated Services Digital Network (BISDN).

It is possible to distinguish between two principal and distinct phenomena in the evolutionary process towards BISDN services. First, we observe that the linking of trunk lines which, in most cases, are made of fiber optics and that the multiplexing equipment in these trunk lines follow the SDH hierarchy exactly in the same way as it will be used in BISDN networks.

The second phenomenon that is observed is that the links between the digital central offices and the customer premises are still in the form of copper cables exactly as they were in the early days when the public telephone switching networks were implemented. However, if we now consider the total investment in a public telephone network which would include

switching equipment and trunk lines it is clear that the highest percentage of the investment was and continues to be consumed by the physical links between the local exchanges and the customer premises. The cost of replacing the copper cables with optical fiber, within a short or medium time frame, is prohibitively expensive. It is also apparent that the cost of replacing the Stored Program Switches-T (Digital Switches) by Asynchronous Transfer Mode (ATM) switches within a short time frame is also prohibitively expensive except in limited applications.

One solution to this problem would be a gradual migration of all networks toward BISDN. One way to achieve this gradual migration would be to stop using any more copper cables for future connections to customer premises. The capacity of the present copper cable installed base would be increased by utilizing digital carrier and multichannel modems until a new demand for yet wider bandwidth justifies the cost of the replacement of copper cables with optical fiber. This replacement of copper cables with fiber optics at the beginning will be restricted to medium and heavy telecommunication users whose volume of bandwidth justifies economically the conversion to fiber optic connections.

Added to this apparent increasing need for bandwidth and traditional telephony and data transmission requirements is the overwhelmingly expanding bandwidth requirements of the Internet. As more and more people access the Internet, the volume

of bandwidth absorbed likewise expands. This adds more complexity to the plethora of already existing problems affecting the telecommunications networks without adequate time to undertake large scale physical plant changes. The explosive success of the Internet has brought, to the small and light user, the possibility of accessing information sources of all types which could not previously have been imagined. The Internet has cause a complex problem to the telecommunications network. This problem relates to the threat of serious congestion in the switching systems in local exchanges which were not designed to handle this extra demand on the network. In addition to the problem of the Internet affecting the switches at the local exchanges, the small or home user often has a unique problem of his or her own because of use of a single telephone line which does not permit the simultaneous use of the line for both voice and data. Generally, it is one or the other. When a user accesses the Internet it has to establish a connection to the user's Internet service provider (ISP). The user cannot either receive or place telephone calls. This problem of a single line is compounded with the bad quality of lines through which the customer accesses data networks using an analog modem resulting in a low-speed communication full of errors. Other interesting and useful services such as video conferencing, video telephone, e-commerce, video surveillance, telemetry and Frame Relay and the like add to the temptation and pressure on the customer to

implement these services. This further burdens the limited bandwidth available between the customer and the local exchange.

As a result, these problems call for an urgent solution which is based on two basic premises. First of these two premises is that the solution must utilize the existing copper cables connecting the local exchange with the customer's premises. The second premise demands that the solution also relieve congestion at the switches of telephone companies' central offices which were not designed to handle either the length or the bandwidth of the new data and videophone call demand.

Accordingly, there is a need for an improved telecommunications system which can provide increased volume telecommunication service to end users with existing copper cables while relieving congestion at telephone company central switching offices.

SUMMARY OF THE INVENTION

The invention is generally directed to a multi-service access switched system which provides for the simultaneous use of the telephone for voice communications and for transfer of data over public communication and switching systems, increases the transmission speed for data access to a level permitting the use of video conferencing, relieves the congestion in the voice telephone network by simultaneously diverting the computer data video conferencing data to the high speed data network and

accessing data networks employing TDM, X.25, Frame Relay and ATM without the need for the installation of a new pair of telephone wires or a pair of digital modems while diverting voice signals through existing telephone company switch systems.

Another object of the invention is to provide an improved multi-service access switched system which includes a multi-service access terminal installed at the customer premises and a multi-service access switch concentrator installed at the central office of a telephone company.

Still another object of the invention is to provide an improved multi-service access switched system which provides for a customer to transmit both telephony and data over a single telephone connection.

Still a further object of the invention is to provide an improved multi-service access switch system which provides a multi-service access switch concentrator at a central switching office to support multi-channel telephony and data communications on a simultaneous basis over the existing copper wire connection between the customer and the central office.

Yet another object of the invention is to provide an improved multi-service access switch system which allows a migration from current narrow band ISDN technology to ISDN broad band (i.e. ATM and other new systems) technology with speeds from 2 Mbps up to at least 2.5 Gbps.

Still yet a further object of the invention is to provide an improved multi-service access switched system in which data is efficiently directed by the central office and is piped to the fastest and most efficient network so that data need not clog the analog telephony transmissions.

Yet still another object of the invention is to provide an improved multi-service access terminal installed at the customer's premises which provides both a standard analog telephone line and a digital port without the need for a digital modem.

A further object of the invention is to provide an improved telephone and data system which provides the ability to bundle groups of users' voice and data transmissions for pre-switching processing outside of traditional control of full switching centers so that increased speed and reduced load on telephone company switching equipment is achieved.

Still other objects and advantages of the invention will, in part, be obvious and will, in part, be apparent from the specification.

The invention accordingly comprises the features of construction, combinations of elements, and arrangements of parts which will be exemplified in the constructions hereinafter set forth, and the scope of the invention will be indicated in the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

For a fuller understanding of the invention, reference is had to the following description taken in connection with the accompanying drawings, in which:

Fig. 1 is a flow chart diagram showing the flow of telecommunications transmission by a small office or home office user;

Fig. 2 is a flow chart diagram showing the telecommunications uses by a corporate user;

Fig. 3 is a block diagram of a multi-service access terminal constructed in accordance with a preferred embodiment of the invention;

Fig. 4 is a block diagram of a multi-service access concentrator constructed in accordance with a preferred embodiment of the invention;

Fig. 5A is a block diagram of a line interface module constructed in accordance with a preferred embodiment of the invention;

Fig. 5B is another block diagram of a line interface module constructed in accordance with a preferred embodiment of the invention;

Fig. 6 is a block diagram of a switch and control module constructed in accordance with a preferred embodiment of the invention;

Fig. 7 is a block diagram of a data network interface module constructed in accordance with a preferred embodiment of the invention;

Fig. 8 is a block diagram of the software breakdown of a multi-service access terminal constructed in accordance with a preferred embodiment of the invention;

Fig. 9A is a block diagram showing the implementation of the software in connection with a SCM module for use with an analog R2 protocol constructed in accordance with a preferred embodiment of the invention;

Fig. 9B is a block diagram showing the implementation of the software in connection with a SCM module for use with an analog R2D protocol constructed in accordance with a preferred embodiment of the invention;

Fig. 9C is a block diagram showing the implementation of the software in connection with a SCM module for use with an analog V5.1 protocol constructed in accordance with a preferred embodiment of the invention;

Fig. 10 is a block diagram of an analog interface module constructed in accordance with a preferred embodiment of the invention;

Fig. 11A is a block diagram of a management control module constructed in accordance with a preferred embodiment of the invention;

Fig. 11B is another block diagram of a management control module constructed in accordance with a preferred embodiment of the invention;

Fig. 12 is a block diagram of the multi access service system constructed in accordance with a preferred embodiment of the invention;

Fig. 13 is a block diagram of the multi-service access concentrator, including each of the various components, constructed in accordance with a preferred embodiment of the invention;

Fig. 14 is a block diagram showing the implementation of the software in connection with a DNIM - Frame Relay module constructed in accordance with a preferred embodiment of the invention;

Fig. 15 is a block diagram showing the implementation of the software in connection with a DNIM - ATM module constructed in accordance with a preferred embodiment of the invention;

Fig. 16 is a block diagram showing the implementation of the software in connection with a MCM module constructed in accordance with a preferred embodiment of the invention;

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The recent commercialization and surprising popularity of the Internet has resulted in extraordinarily high volume of data traffic through public switch telephone networks (PSTN).

The telephone lines, when utilized for the transfer of data or access to the Internet are kept busy for much longer times than for voice telephone connections and time sharing of the telephone lines is not possible as is the case with the standard voice based telephone communication. Traditionally, the central offices were not designed for sustaining connections for extremely long durations. Besides accessing the Internet, small offices in homes and small office environments use the telephone lines of the PSTNs for transfer of large computer files, for holding video conferences and for surfing the Internet.

Reference is made to Fig. 1 in which a block diagram of the small office/home office (SOHO) user configures telecommunications usage in connection with the public switch telephone network in accordance with the prior art. The PSTN 110 is accessed by the small office and home office users 70 and 50, respectively, through standard analog telephone lines 111, 112, 113 and 114. User 50, generally a home office user, has only a single telephone line access 55 with a switch 56 for allocating incoming calls to either telephone 51, fax machine 52 or personal computer 53 through an analog modem 54. Analog modem 54 is shown as a separate box but may conveniently be a component of the personal computer 53. When the home office user has an outgoing connection on the telephone line, the single telephone line prohibits any inward or outward use of the fax machine 52 or the telecommunications capacity of personal computer 53. The

connection is made through the PSTN to the designated location. To the extent that the connection is to the Internet, generally through an Internet Service Provider (ISP), the ISP has a server 130 which is connected to the Internet 120 in accordance with conventional server technology and the server 130 is connected to the PSTN and through the PSTN to the user by a series of analog modems 140 which are connected through a telephone line 115 to the PSTN.

Small office user 70 is shown as having telephone 71, fax machine 72 and personal computer 73 with an analog modem 74. However, this configuration includes a separate, dedicated telephone line, 112, 113 and 114, for each of the three separate forms of telecommunication. Obviously, there may be multiple lines for each of the forms of communications based upon capacity needs.

The traditional volume estimates by the PSTNs have been based upon purely voice based telecommunications. As fax machines developed, telephone calls and data bandwidth requirements increased substantially. However, these loads were manageable by the PSTNs. However, as SOHO users began to use the Internet for e-mail, web surfing and large file data transmission, even the smaller users began to keep Internet access lines open for hours at a time or even continuously around the clock. This use of telephone lines has caused congestion in the central office switching systems and brings them almost to

a point of collapse. Furthermore, the analog telephone lines restrict the transfer of data to about 10,000 bits per second.

The second problem which affects the user of a telephone system is the fact that, having only a single telephone line as in the user 50 shown in Fig. 1, the customer can only use his telephone to call or to be called if at that particular time he does not use his computer modem to access the Internet or to transfer a data file or transmit a fax. It also follows that if the user wishes to use access to the Internet or any online data base he cannot make or receive a telephone call at the same time without adding an additional line of service.

Reference is next made to Fig. 2 wherein a block diagram of the connections of corporate users for telecommunications in accordance with the prior art is depicted, like reference numerals representing like elements. A corporate user 200 is connected to the PSTN 110 by a series of lines 210 through a PBX or similar switch 215 which distributes the available telephone lines among telephones 201, personal computers 203 with analog modems 204 and fax machines 202. In addition, video conferencing can be done through personal computers 205 with cameras 206 through digital modems 207 connected to a data network 160 through an analog line 211. In addition, a router 208 is connected to a digital data network such as one using ATM, X.25, Frame Relay and TDM through leased

lines 212. The internal connections 209 to router 208 can include personal computers, mini computers, mainframes and the like. For the telecommunications needs which go through the PSTN 110, analog lines are general used and connection to Internet 120 is similarly through the PSTN 110. Connections to the data network 160 are digitally oriented to increase the bandwidth availability. Similarly, connections can be made to a corporate user 250 having independent lines 261 and 262 for fax machines 251 and telephones 252. Likewise, the user can have video conferencing capabilities, including a computer 254, camera 255 and modem 256 coupled directly to the data network 160 through line 263. Also, a network server 257 can be connected to the data network or to other locations for the company or customer and vendor servers through data network 160. Finally, leased lines with a router 258 can access data network 160 through leased lines 265. Access to a data communications network 160 demands a dedicated telephone cable and a pair of high speed (64,000 or 128,000 bits per second) modems. This line being dedicated, has a high initial installation expense and a high monthly maintenance charge as well. Furthermore, it should be known that the service offered by such dedicated connection is for a point-to-point configuration. It is generally not possible to "dial" any other physical or virtual address whenever it is needed to do so.

The multi-service access switched system constructed in accordance with a preferred embodiment of the invention satisfies four major challenges for accessing the public telecommunication systems. First, it provides for simultaneous use of the telephone line for voice communication and for transfer of data, including the Internet over public data communications networks and voice switching systems. Second, the transmission speed for data access is increased from the present 10,000 bits per second to at least 64,000 to 128,000 bits per second, permitting the use of video conferencing. Third, the congestion in the voice telephone network is relieved by simultaneously diverting the computer data and video conferencing traffic to a high-speed data network, rather than the PSTN. Fourth, access to data networks employing TDM, X.25, Frame Relay and ATM is achieved without the need for the installation of a new pair of telephone wires or a pair of digital modems.

In contrast to the present access systems which basically offer a point-to-point service over private lines, the multi access service switched system lets the user address (dial) his information to any physical or virtual address as need be or be called from any physical or virtual address.

The system, in accordance with a preferred embodiment of the invention, consists of two components. The first is a multi-service access terminal (MAT) installed at the customer premises and the other is a multi-service access concentrator

switch (MAC) installed at the central office of a telephone company. A block diagram of the MAT, found at the customer's site, is shown in Fig. 3 and a block diagram of the multi-service access terminal concentrator (MAC) is shown in Fig. 4. There is an ST port which can connect any ISDN device.

Reference is made to Fig. 3. The MAT 300 includes a microprocessor 301, line interface 302, signalling component 303, digital to analog converter 304, 2 Mbps bus 305, digital port 306 and analog port 307. The user connects phone line 310 to the central office directly into the MAT 300. The telephone 320 is connected to analog port 307 and computer 330 is connected directly to digital port 306. The MAT 300 is installed at the customer premises, residence or small office. The two ports 306, 307 are digitized, synchronized and multiplexed with the information being transported over the same telephone line but now in the form of two digital channels, each of which is a totally independent, 64,000 per bits per second bi-directional and synchronous channel (B channel). A third 16,000 bit per second channel, designated as a D channel, carries the signalling (dialing) information about the first two channels described above. The D channel can also carry other information such as the number of a credit card using X.25 protocols, for example, which can enter in a signalling port 311.

An important characteristic is that it is possible to combine the two synchronous 64 Kbps channels into one 128 Kbps

channel for transmission of data when the telephone line is not being utilized. However, when a telephone call is made or received, the 128 Kbps channel reverts to the initial two separate 64 Kbps channels.

At the central office the Multiservice Access Concentrator (MAC) connects to wires coming from either 105 or 180 customers in current preferred embodiments of the invention. The telephone number of each individual customer remains unchanged. Physically, the MAC holds, in a current preferred embodiment, 12 cards for interfacing with the customers, three cards for cross-connecting, two cards for interfacing with the data network, one card for management and two for power supplies (one of which acts as a hot standby).

Reference is next made to Figs. 4 and 13, wherein a physical diagram and block diagram of a MAC, generally indicated as 400, is shown. Fig. 4 shows the redundant power supplies 401, 402. As better seen in Fig. 13, MAC includes seven U-interface modules (line interface modules) 403, each of which has 15 ports so that the MAC 400 can deal with 105 customers. The MAC 400 shown in Figs. 4 and 14 is configured for 105 customers but with additional U-interface module capacity can be expanded to 180 incoming lines. The U-interface modules are also known as line interface modules (LIM). Next, there are a series of switching and control modules (SCM) 404. In addition to switching and control module 404 there is a management and control module 406

(shown as a box without attachments, but actually with connections to each of the other modules and buses for control purposes), data network interface module 407 and analog interface modules 408. In one preferred embodiment the MAC 400 physically holds eighteen cards for interfacing with customers, one card for management and two cards for power supply 401, 402 (one as a hot standby). Cross-connection cards 440 are shown in Fig. 4. The double headed arrows in Fig. 13 represent buses.

Reference is next made to Figs. 5A and 5B wherein a circuit diagram and block diagram of a line interface module 403 are shown. As better seen in Fig. 5B, each module is designed to receive input from 15 subscriber lines, each of which includes two B data lines and one D signal channel. The telephone line which carries two digital channels is connected to the concentrator (MAC) 400. The function of the concentrator is the reverse of the MAT 300, which is found at the customer's premises. In other words, the MAC demultiplexes the two digital channels and sends the telephone channel, in an analog form, to the proper terminal of the central office voice switch. This functionality is implemented initially at the line interface module 403 which interfaces with the incoming telephone line. This module with the U-interface receives the two 64 Kbps channels (B channels) and the 16 Kbps signalling channel (D channel). In one single printed circuit board, in a preferred embodiment, up to 15 of these interface components are combined

into a line interface module (LIM) 403. U interface 501 combines two B channels on a 4 Mbps bus and has two outputs, one serial and one for the D channel (also serial). The 15 components on one single card can multiplex information from 15 users forming a block of 15 X 2 B channels or, in other words, thirty channels at one port and another block of 15 D channels at another port. A serial communication port (SCP) bus architecture links U interface components 501 with the management and control module (MCM) 406. Each user on U line 502 is connected to interface 501 where it is demultiplexed and then added to the other U line inputs. Wave controls FOB 503 establish a 4 Mbits/s control signal from the MCM unit. The U interface 501 outputs the demultiplexed D channel signals on the DCH OUT line to the SCM 404. As seen in Fig. 5B, a 20 Mbits/s clock is used to demultiplex the U-channels by the channel interfaces 501. U select and D circuit transmissions block 507, collects each of the D channels, as well as orders the channels by selecting the data signals from the various U lines. The control signals include the SCPEN input (SPIEN) 508 from MCM 406. The U select and D circuit transmission box 507 outputs fifteen D channel signals to an SCM 404. A D channel out signal from a U interface 501 is shown. In fact, each interface 501 has a separate output line which is attached to U select and D circuit transmission box 507. A SCPEN selection box 510 shows the line which enters each U interface 501 to control the interface demultiplexing process.

This serial control port enable signal orders the selection process among the U channel interface boxes (1-15) 501.

Reference is next made to Fig. 6 wherein a switching and control module 404 constructed in accordance with a preferred embodiment of the invention is depicted. The information from the two blocks linked as described above, is sent, through the back plane (electrical connector), to a switching control module (card) 404. Switching control module 404 consists of two switch matrices 601, 602 and a microprocessor 603. Each of switching matrices 601, 602 is composed of two 4 Mbps ports which combine at each port a block of 60 channels (30 B1 and B2 channels). The 60 channels arriving, each at 4 Mbps, originally grouped from two line interface modules, are forwarded to four 2 Mbps ports. These two Mbps ports carry: 30 voice channels digitized at 64 Kbps from LIM 1 and LIM 2; 15 128 Kbps data channels from LIM 1; and 15 data channels from LIM 2; and 30 signalling channels at 64 Kbps for the voice channels. Another 4 Mbps bus enters the SCM from four LIM 403 and carries 60 D channels to the microprocessor 603. The block containing 30 channels for voice and R2 or V.5.2 signalling may be interfaced directly with the trunk port of the Stored Program Switch (digital switch) at the central office, simplifying the cabling between the multi access switched system and the central office switch. This is the digital interface option to connect the MAC to the voice switch.

The microprocessor has the double function of controlling the two switching matrices 601, 602 and at the same time converting the Q.931 protocol of the D channel signalling information into Q.933 (Frame Relay) or Q.2931 (ATM) signalling protocols. The microprocessor also provides the management information and the information on the configuration of the matrices through a 10 Base-T Ethernet port to the management control module 406. The microprocessor 603 is also responsible for D channel signalling conversion to R2 or V.5 on the digital interface. In addition, each of switching matrices 601, 602 outputs through Framers DS 2154 transmission blocks 605 and are framed either by E1 Framed G. 703 2 Mbits/s boxes for Voice 606 or for Video Conference 607. Microprocessor 603, which, in a preferred embodiment, is a Motorola 860T, is connected to 60D channels at port TDMA, an SPI bus 612 (to be connected to the AIM), an output port TDMB which is connected to V.35/36 Electrical Drivers 608 with X25 protocol, a 10/100 Base T 609, which is connected in turn to LXT 970 Ethernet Drivers 610 with a TCP/IP for Management input 611.

Figs. 9A, 9B and 9C depict the breakdown of the software operations of the SCM module in connection with analog R2, R2D and V5.1 line protocols.

The 30 128 Kbps channels used for transmission of data or video conference transmission are now combined and sent over 4 Mbps buses to the module which interfaces with the data network

of the network provider. This module is known as the Data Network Interface Module (DNIM), 407 shown in detail in Fig. 7. Data Network Interface Module 407 is composed of two microprocessors 701, 702 which serve the function of receiving at each two 4 Mbps blocks consisting of 60 channels (30 B1 + B2) with the information on data from 30 users' LIM 1 and 30 users' LIM 2.

Data signals, when generated by a video conference, are sent to a deterministic network (TDM) and then on to the video conference service providers. If the data channels are to be fed to a switched packet network of Frame Relay or ATM type, those channels are pre-formatted (packaged) to Frame Relay or ATM protocols at data network interface module (DNIM) 407. DNIM 407 consists of two microprocessors 701, 702. Each serves the function of receiving two 4 Mbps blocks consisting of 60 channels (30 B1 + B2) which would be information or data from 30 users' LIM 1 and 30 users' LIM 2. These blocks of channels arrive at microprocessor 701 or 702 and each processes the corresponding data packets conforming to the Frame Relay or ATM protocols at this level. The interfunctionality between the D channel protocol and the Frame Relay and ATM headers are performed at the main microprocessor here by software. In a preferred embodiment microprocessor 705 which controls the operation of the DNIM is a Motorola 860 SR. The programming and memory for the microprocessor 802 is found in PROM 707 and DRAM 706. The data

is then sent through Framers 711, 712 to an E1 line either with Frame Relay or ATM network protocols. Alternatively, data to be sent to the Internet utilizes the 33 MHZ system I/O bus 714 to SCCI Ethernet Port 713.

The addressing (dialing) function is implemented by correct handling of information contained in a D channel such as the called number, the number of the calling party, busy tone, dial tone and other commonly known signals. All of this information is reformatted from channel D protocols to the respective headers for Frame Relay or ATM for call set up procedures. For each call these data packets are sent to physical or virtual addresses through high-speed networks.

Reference is next made to Figs. 14 and 15 wherein a software breakdown of the DNIM module in connection with Frame Relay and ATM networks in accordance with preferred embodiments of the invention are depicted.

Reference is next made to Fig. 8 which shows the implementation of software and reformatting (routing) on the user side. These virtual addresses include other users of the network or the providers of the Internet access, Intranet, video conferencing and other users or data providers. These networks can be connected to other domestic or international networks as well as described below.

If the voice switch interface of the central office happens to be analog, a different module designated as an analog

interface module (AIM) 408 shown in Fig. 10 is utilized. The AIM 408 basically consists of a demultiplexer of 30 voice channels (B channels) and demultiplexer of the signalling channels (D channels) and fifteen digital/analog converters followed by fifteen analog line interfaces to which the ports of the signalling channel demultiplexer are connected. This signalling is a reproduction of the signalling initiated by a MAT user in the first place.

Reference is next made to Figs. 11A and 11B wherein a management and control module generally indicated as 406 is depicted. The management control module is utilized for the management of other modules contained in the MAC 400 and also receives error and failure signals. The management and control module 406 consists of a clock decision module 1102, wave control generator 1103, which connects to other modules, a microprocessor 1105 and a the serial port (RS-232) SCC2 which is used for local management. The Ethernet port 1107 of this module connects to all other microprocessors of the system. The serial control port (SCC2) controls the U-interfaces of the line interface modules 403. The management and control module 406 is able to do a "loop-back" for identification of the failures, alter configurations if needed and provide data for billing purposes. Clock decision module 1102 improves each of the 2 Mbits/s clocks and selects a master clock for use by all components, splitting the clock speed as required by other components in block 1103.

The host computer line on the Ethernet port 1107 allows control of the overall system by a remote controller, either at the physical site or through the Internet.

Reference is next made to Fig. 12 wherein a diagrammatic view of two setups incorporating the multi-service access switched system constructed in accordance with preferred embodiments of the invention are depicted. On the left side of Fig. 12 a multi-service access terminal 300 is used to connect a large office configuration including telephones 51, card readers 221, faxes 52, video phone personal computers 205 with cameras 206 and a series of personal computers configured in a LAN 222 to the central office and, in particular, to a multi-service access concentrator 400 which directs the signal either to the PSTN 110 or to the data network 160. Similarly, on the right side of Fig. 13 a smaller installation in which telephone 51 and personal computer 53 are connected through a multi-service access terminal 300 to a multi-service access concentrator 400 which acts as a gateway with both the PSTN 110 and data network 160 for access to the Internet and video conferencing through high-speed data networks and to and from data connected to a data network by leased lines.

Reference is next made to Fig. 13 wherein an overall block diagram of the MAC 400, in accordance with a preferred embodiment of the invention, is depicted, like elements being represented by like reference numerals. MAC 400 includes seven

LIM modules 403, two SCM modules 404, a DNIM module 407, a MCM module 406 and seven AIM modules 408 coupled together with various buses. The LIM modules are shown in Figs. 5A and 5B. The SCM modules are shown in Fig. 6. The DNIM module is shown in detail Fig. 7. The AIM modules are shown in Fig. 10 and the MCM module is shown in Fig. 11.

Reference is next made to Fig. 9 wherein the software breakdown for the MAC 400 is shown. Software breakdown includes interfaces, protocol changes and connections for the two B channels and one D channel, as well as a telephone, fax input and a digital ISDN and X25 connectors and a PC connector.

Reference is next made to Fig. 10 wherein a block diagram of the AIM module 408, in accordance with a preferred embodiment of the invention, is depicted. AIM 408 is coupled to the SCM 404 through a 2 Mbps TDM bus for voice 491 and essentially demultiplexes the TDM signal through use of PCM filter codes 1003 and central office interface circuits 1004 in accordance with conventional practice. A wave control selection is performed under wave control generator 1103 found in the MCM 406. A microprocessor 1005 controls the local activity within AIM 408. In practice there are 15 separate parallel circuits for dealing with each of the 15 user inputs under the selection of the wave control generator 1103 controlled by MCM 406.

Reference is next made to Fig. 16 in which a block diagram of the software breakdown of the MCM module constructed

in accordance with a preferred embodiment of the invention is depicted.

There are additional applications for the Multi-Service Access Switched System. As stated before, the MAT is always installed at the user's premises, but the MAC can reside at the Central Office main building or at a POP (point of presence). One possible location for the MAC is inside a cabinet that is installed at the curb. This cabinet is known as an "optical cabinet" as it is linked to the network provider which can be the ILEC (Incumbent Local Exchange Company) or a CLEC (Competitive Local Exchange Company) through a pair of fiber optical cable. The technology employed is FTTL - Fiber To The Loop. In this application the Multi-Service Access Switched System is actually part of the access side of the network and the MAC can be connected to the subscriber over a copper pair in two different ways.

One way is a connection as described in the initial part of the patent application through the "U" interface with the MAT. The other possibility is to connect the same "U" interface with a PCM-4 and provide a voice service to four subscribers with voice compression 2:1 or with a PCM-2 and provide a voice service to two subscribers without the voice compression. The PCM-2 and PCM-4 technologies are a relatively old technique to multiplex respectively two and four subscribers over one single pair of copper wires and is not part of this patent application. In

accordance with the invention each shelf can handle 180 MAT subscribers and the Central Office interface requires 6 E1 for voice and 2 E1 for the data channels. An E1 line is an international standard high bandwidth line similar to the US T1 lines. These E1 are normally transported into the fiber via a PDH or SDH multiplexer. If a PCM-2 or PCM-4 connection is used then the capacity is expanded to 360 or 720 users per shelf. These are low cost solutions to access the voice and data networks.

Another application of Multi-Service Access Switched System is to place the MAC at the Cable Distribution Frame of a condominium or a business offices building. In this case MAC keeps the same analog interface through the AIM board to the Central Office as if it were at the Central Office premises, but the data channels or video-conference signals go directly to the data network of any network provider e.g. an ISP via a high speed local link. This architecture uses the existing cable infrastructure, so the new service can be turned on as soon as the MAC shelf is installed.

A third possible application is to use the Multi-Service Access Switched System as part of the process to digitize the Telephone Plant in countries or regions where the major Central Office switches are still analog. These analog switches cannot provide important new services such as caller party identification, call forwarding, automatic billing, hold and many

others provided by computer-controlled switches. The average capacity of an analog switch is 10,000 subscribers, which can be completely replaced with the MAC with a MAT terminal – in which case ISDN services are provided – or with a PCM-2 or PCM-4 terminal and link the trunk interface with an existing digital switch.

The savings in ground space is greater than 10:1 and the cost per terminal is about half of the current average cost. By using IN (Intelligent Network) signaling the existing subscribers can keep their same phone number although connecting to a new Central Office switch.

As described above, the multi-service access switch system solves the four challenges posed by the current extraordinary increases in demand for capacity of the public telecommunications systems. The multi-service access switched system allows for simultaneous use of telephone for voice communications and for transfer of data. It allows for the increase of transmission speeds for data access from the present limited band width transmission to a much high speed transmission. Congestion in the voice telephone network is relieved by simultaneously diverting computer data and video conferencing traffic to high speed digital data networks rather than the public switched telephone networks. Finally, access to data networks employing new high-speed communication protocols, including TDM, X.25, Frame Relay and ATM without the need for the

installation of a new pair of telephone wires or digital modems is enabled.

The capacity of the system can be easily stepped up on the multi-service access concentrator components either by the use of multiple components based upon subscriber volume or by increased miniaturization and concentration of components.

Accordingly, an improved multi-service access switched system based upon the use of customer based multiple access terminals and central office multiple access concentrators which provide for the more efficient utilization of available bandwidth of existing wiring and simultaneous voice and data transmissions which are allocated by the central office multi-service access concentrator so that data and video conferencing transmissions are dealt with by high-speed data networks thereby freeing the PSTN from excessive data loading is provided.

It will thus be seen that the objects set forth above, among those made apparent in the proceeding description, are efficiently obtained and, since certain changes may be made in the above constructions and processes without departing from the spirit and scope of the invention, it is intended that all matter contained in the above description or shown in the accompanied drawings shall be interpreted as illustrative, and not in the limiting sense.

It will also be understood that the following Claims are intended to cover all of the generic and specific features

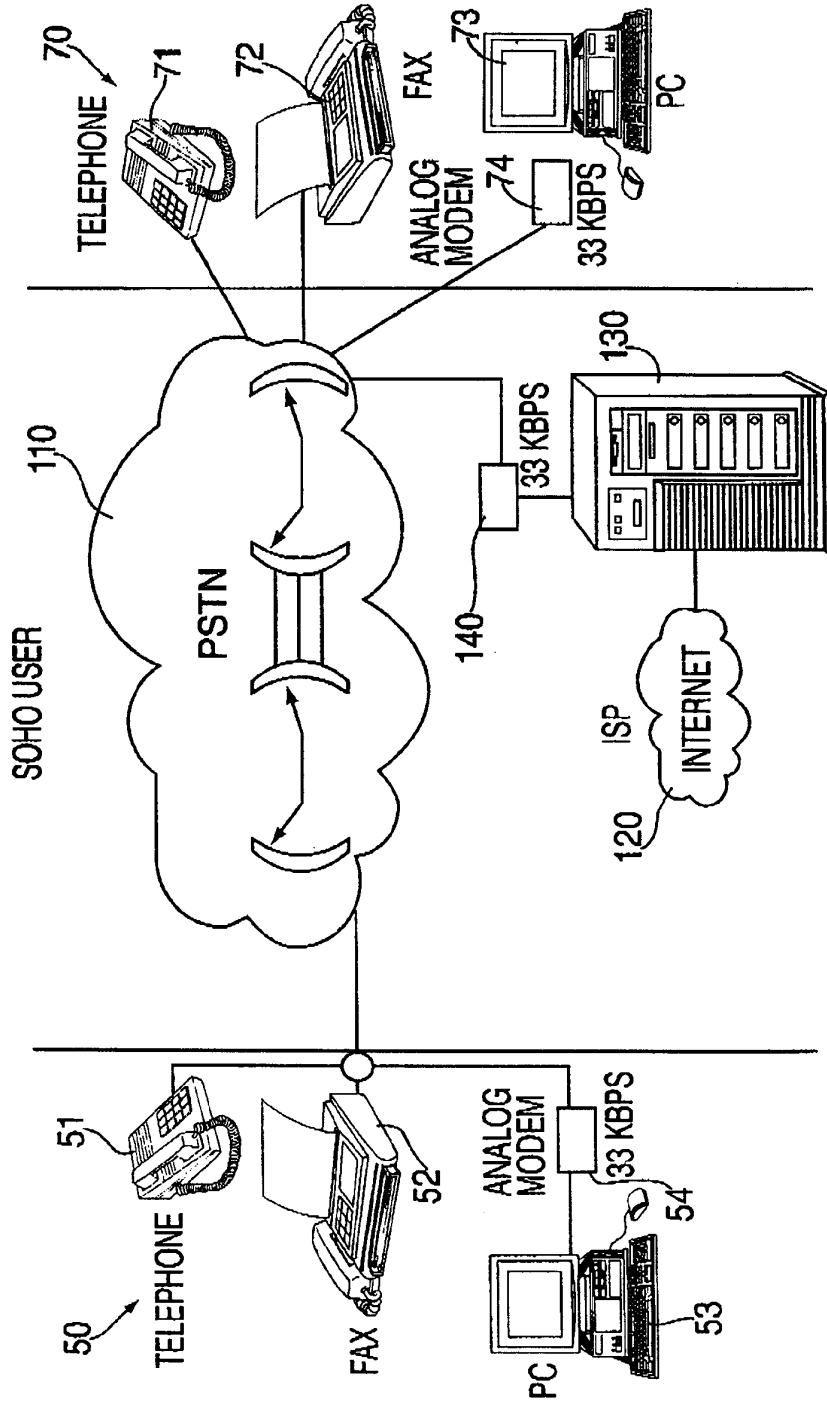
of the invention, herein described and all statements of the scope of the invention which, as a matter of language, might be said to fall therebetween.

C L A I M S

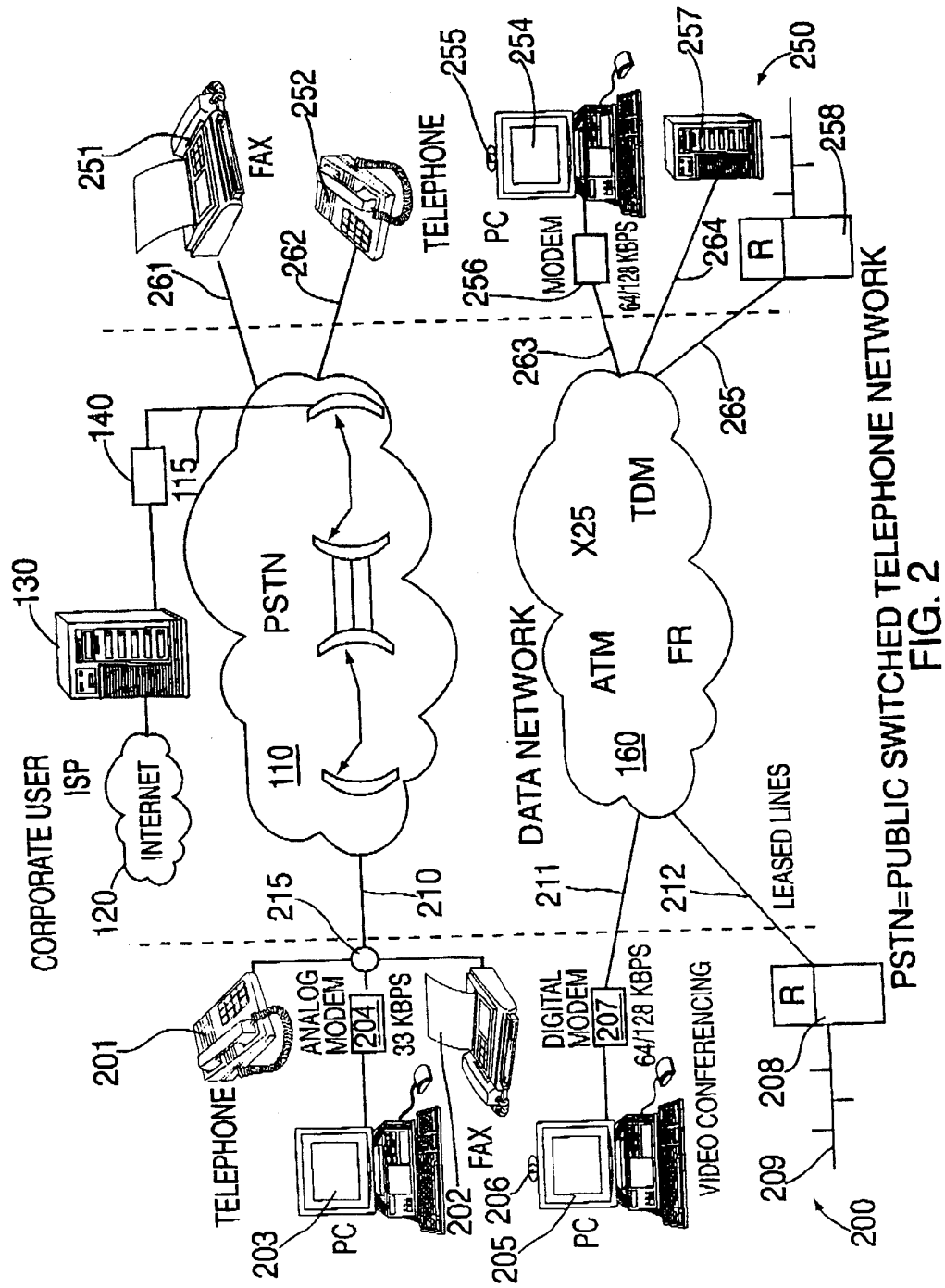
1. A multi-service access switched system for providing simultaneous voice and data, comprising:

a multi-service access terminal unit coupled to a user's telephone and data processing equipment; and

multi-service access concentrator means for receiving the output of a plurality of multi access terminal units and directing the voice components of the transmission to a public switch telephone network and the data components of the transmission to a separate data network.



PSTN=PUBLIC SWITCHED TELEPHONE NETWORK
FIG. 1



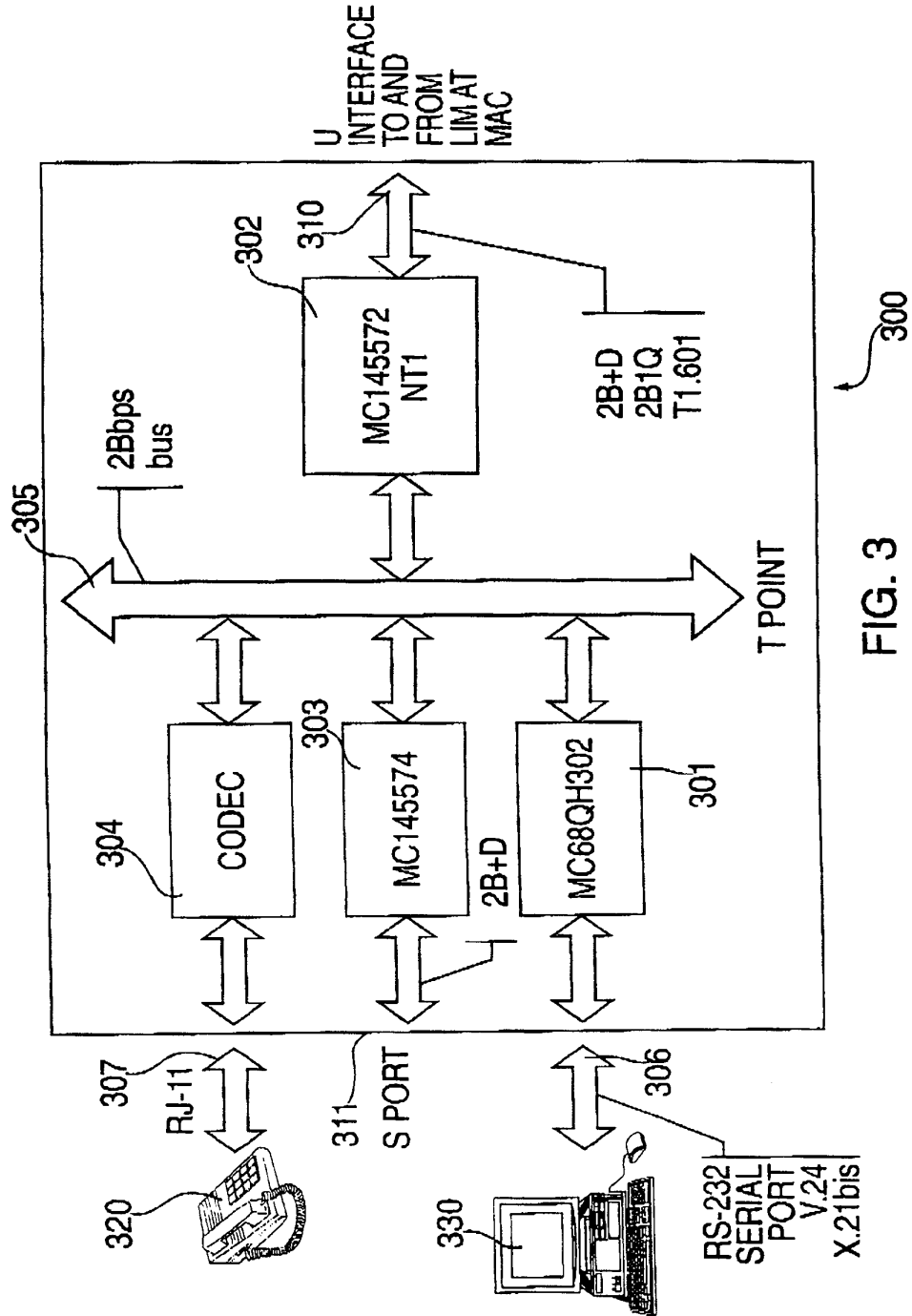
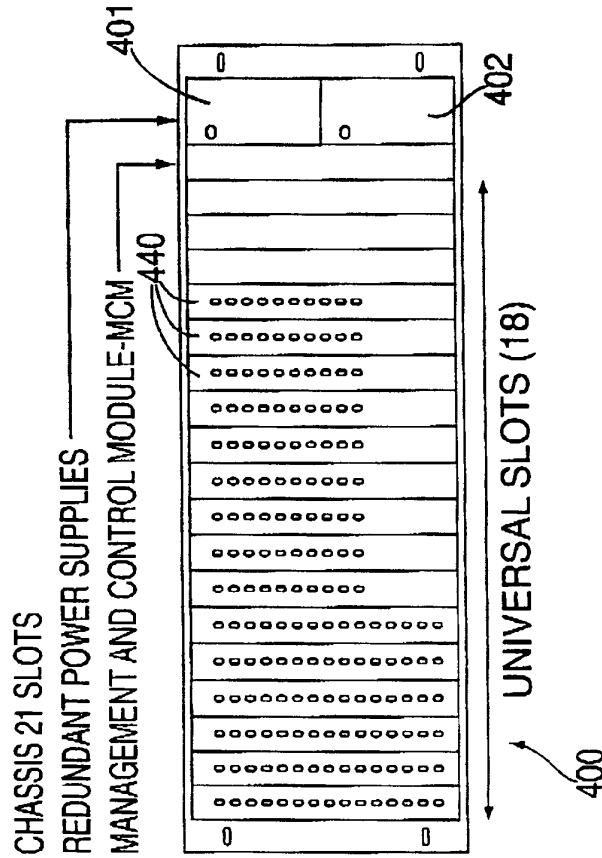


FIG. 3

M@SS
MAC-MULTISERVICE ACCESS CONCENTRATOR



UNIVERSAL SLOTS		NO. PORTS
TYPE		
LINE INTERFACE MODULE-LIM		15
ANALOG INTERFACE MODULE-AIM		15
SWITCHING AND CONTROL MODULE-SCM		60
DATA NETWORK INTERFACE MODULE-DNIM (FR OR ATM)	SUBSCRIBERS	1ATM E1 / 1FR E1
ATM E3 MODULE	FUTURE	FUTURE
FR E3 MODULE	FUTURE	FUTURE

FIG. 4

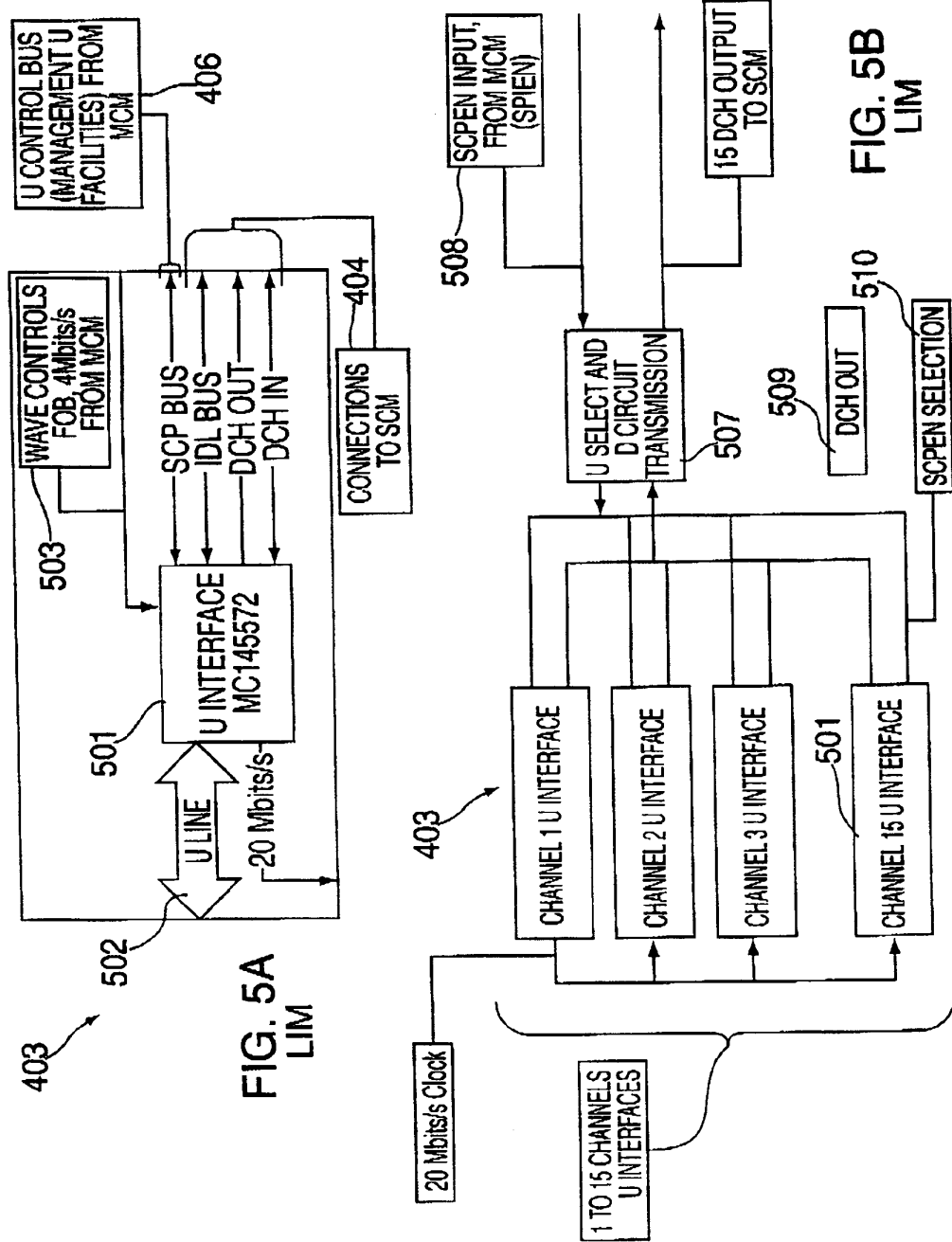


FIG. 5A
LIM

FIG. 5B
LIM

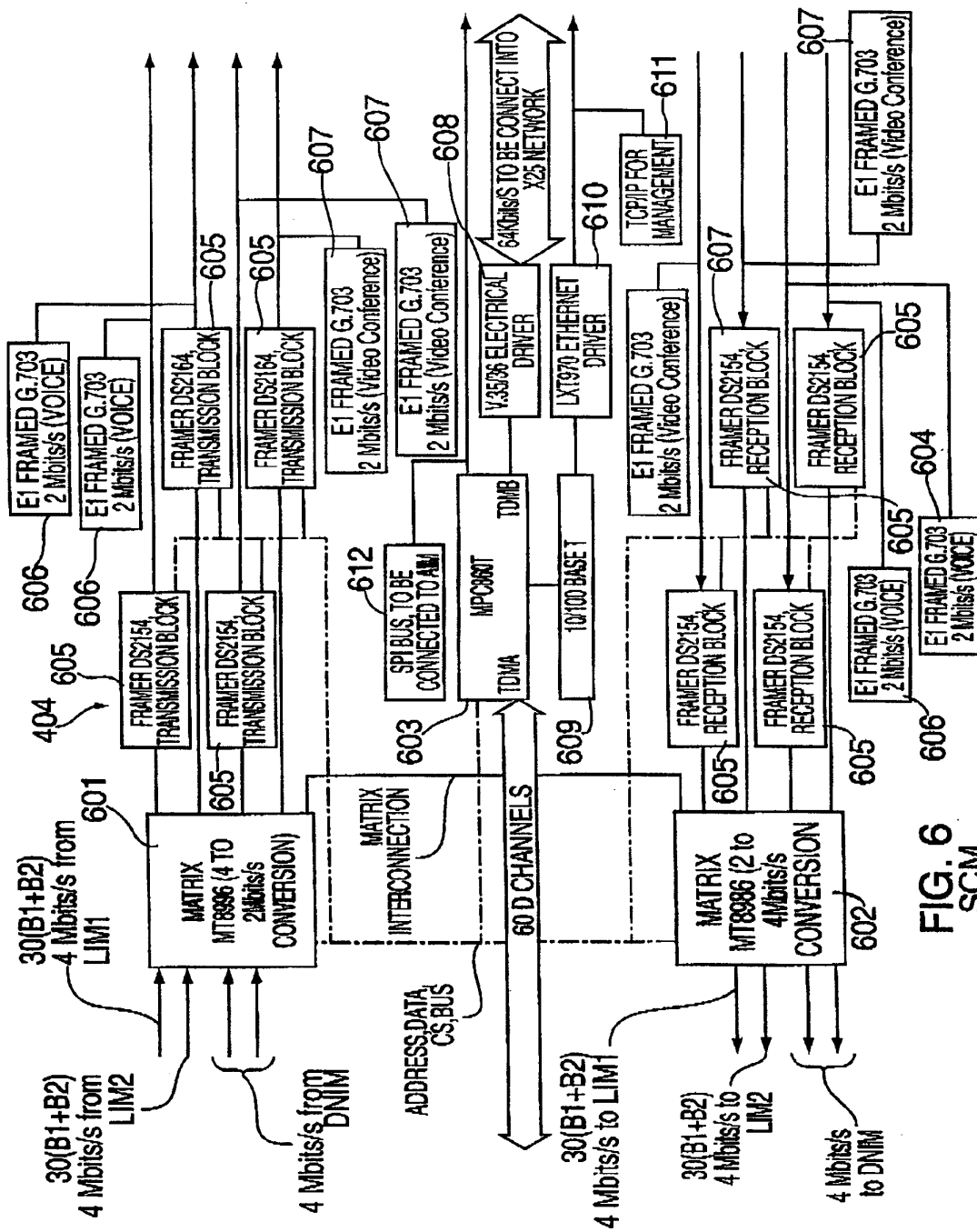


FIG. 6
SCM

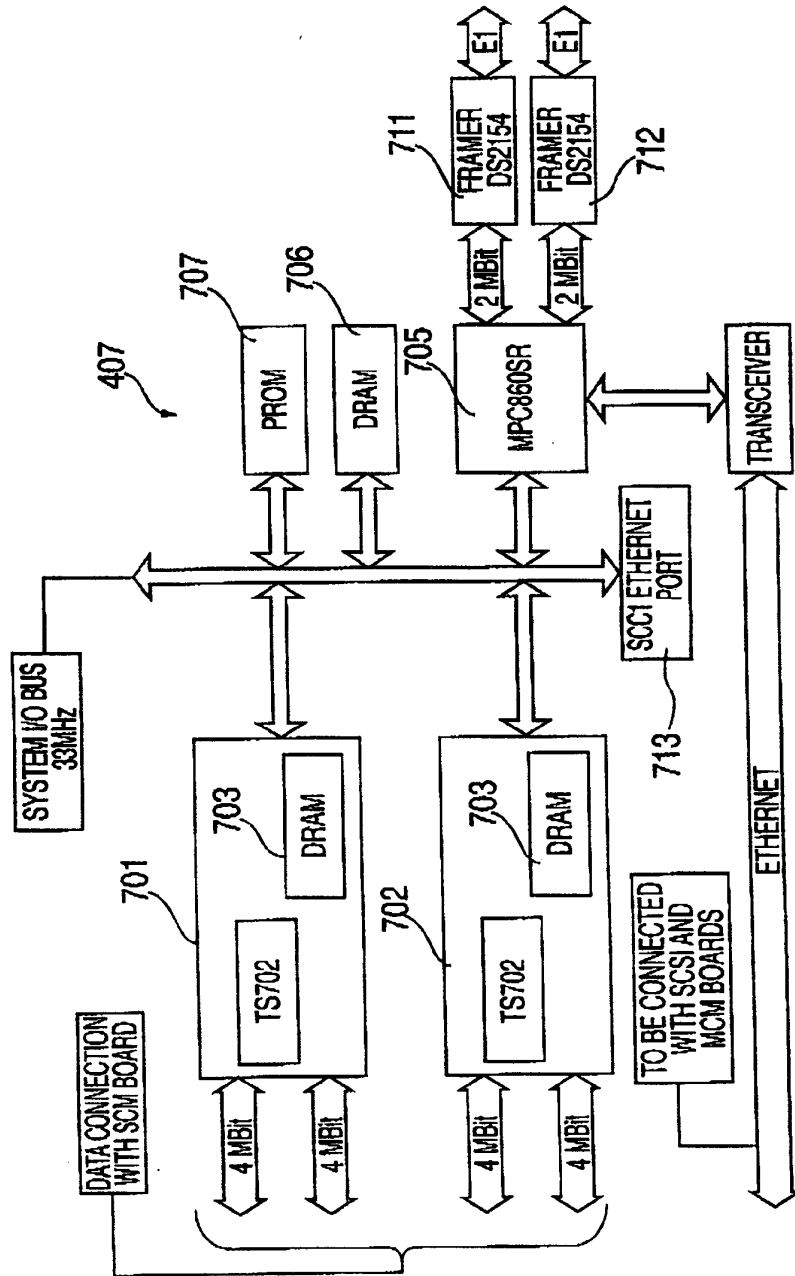


FIG. 7
DNIM

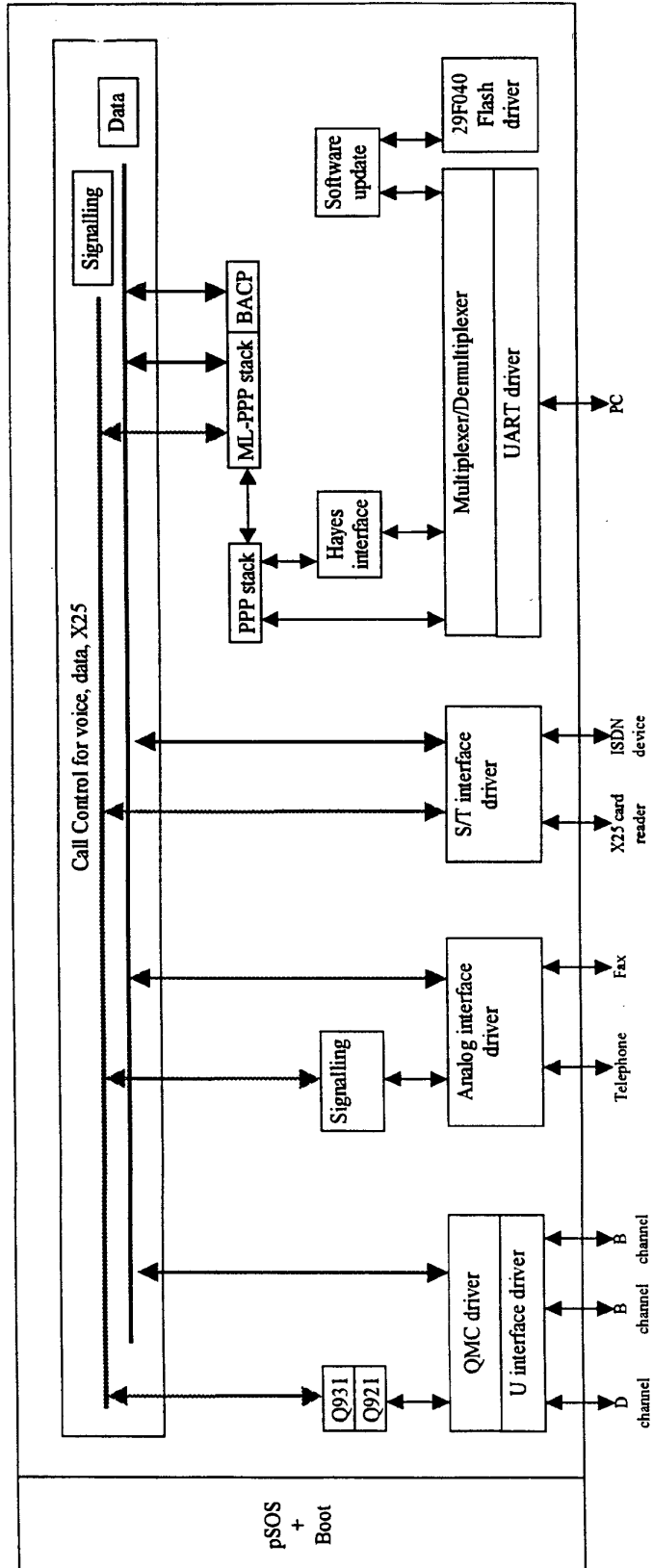


FIG. 8

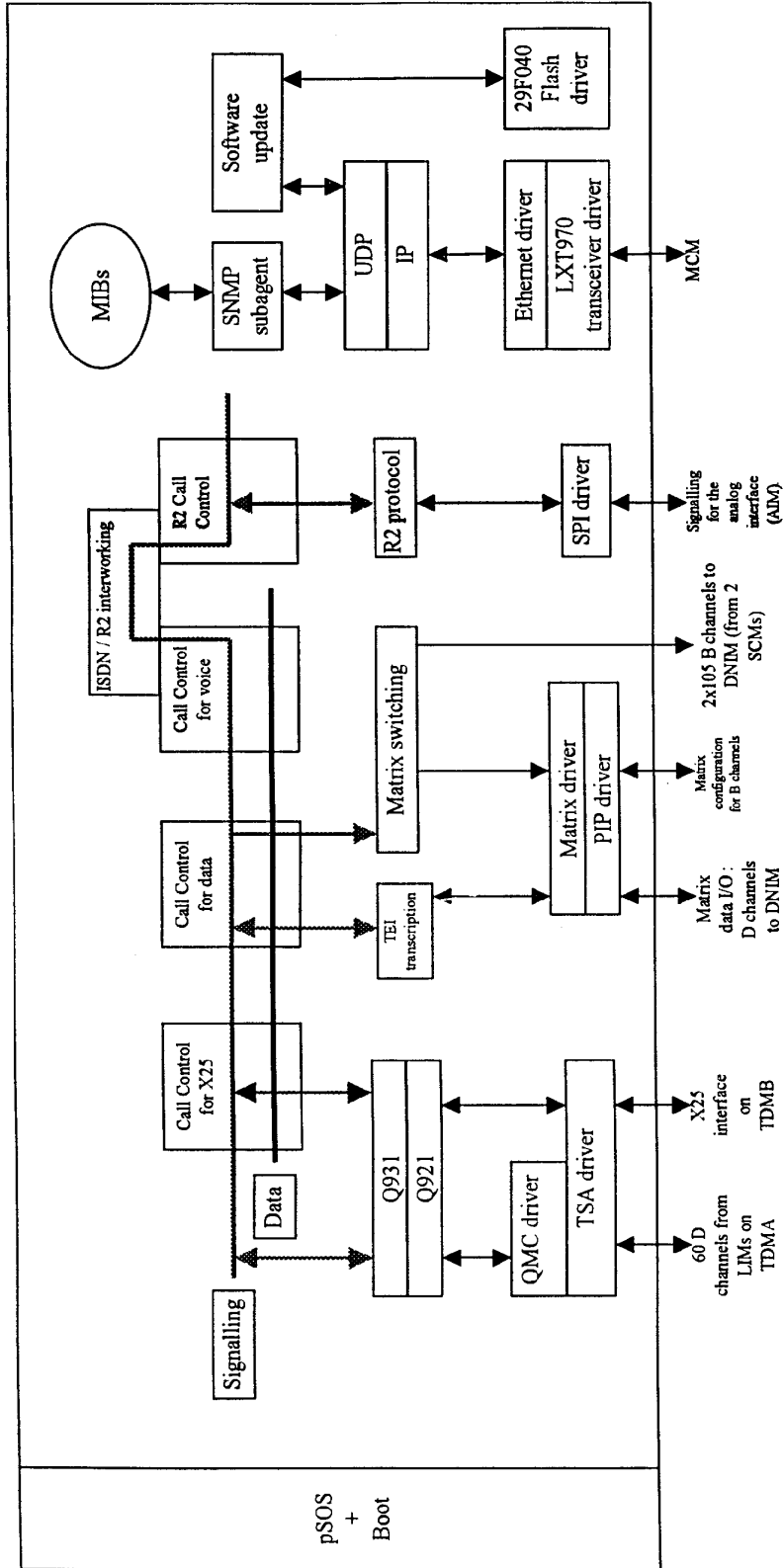


FIG. 9a

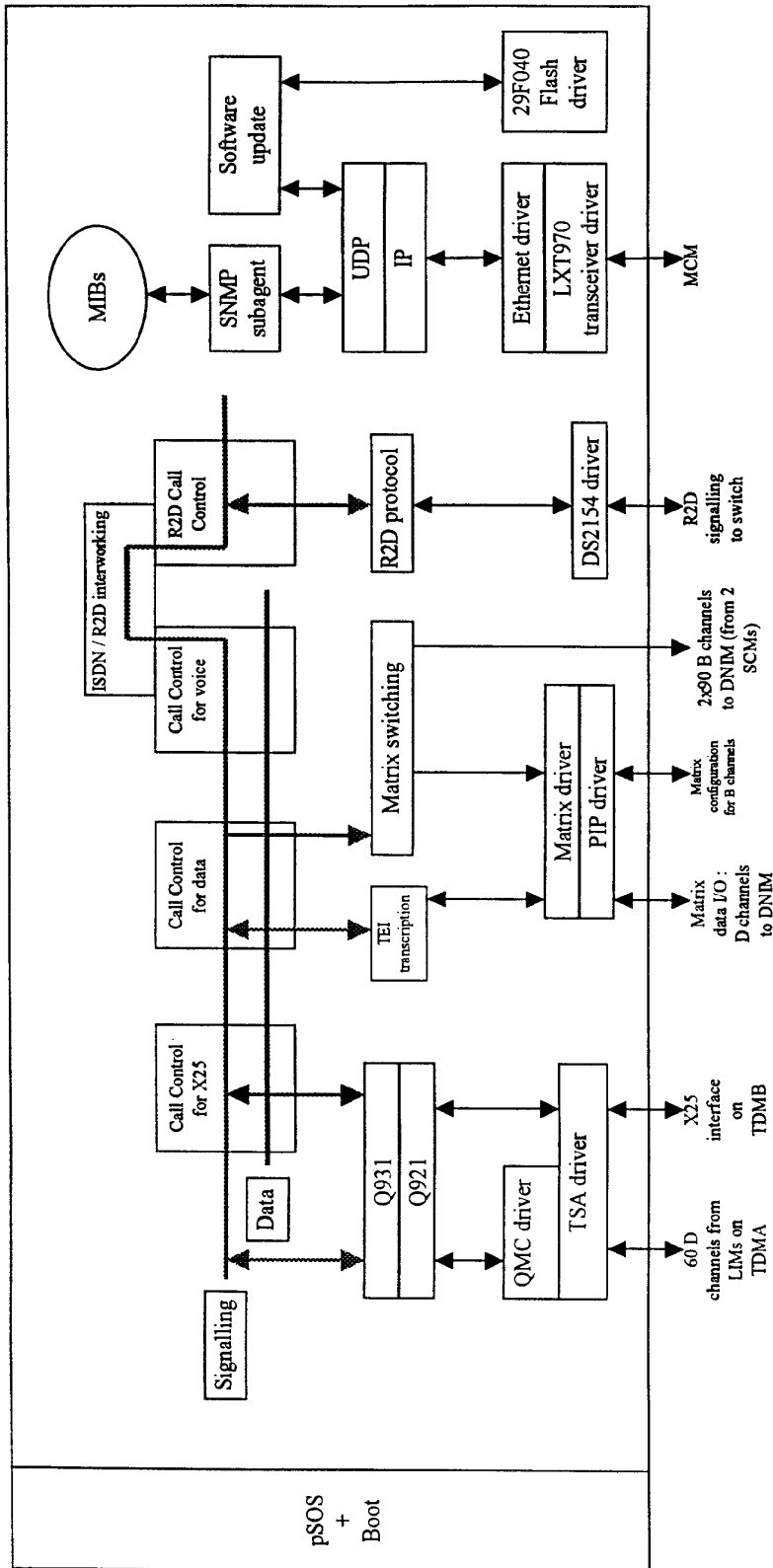


FIG. 9b

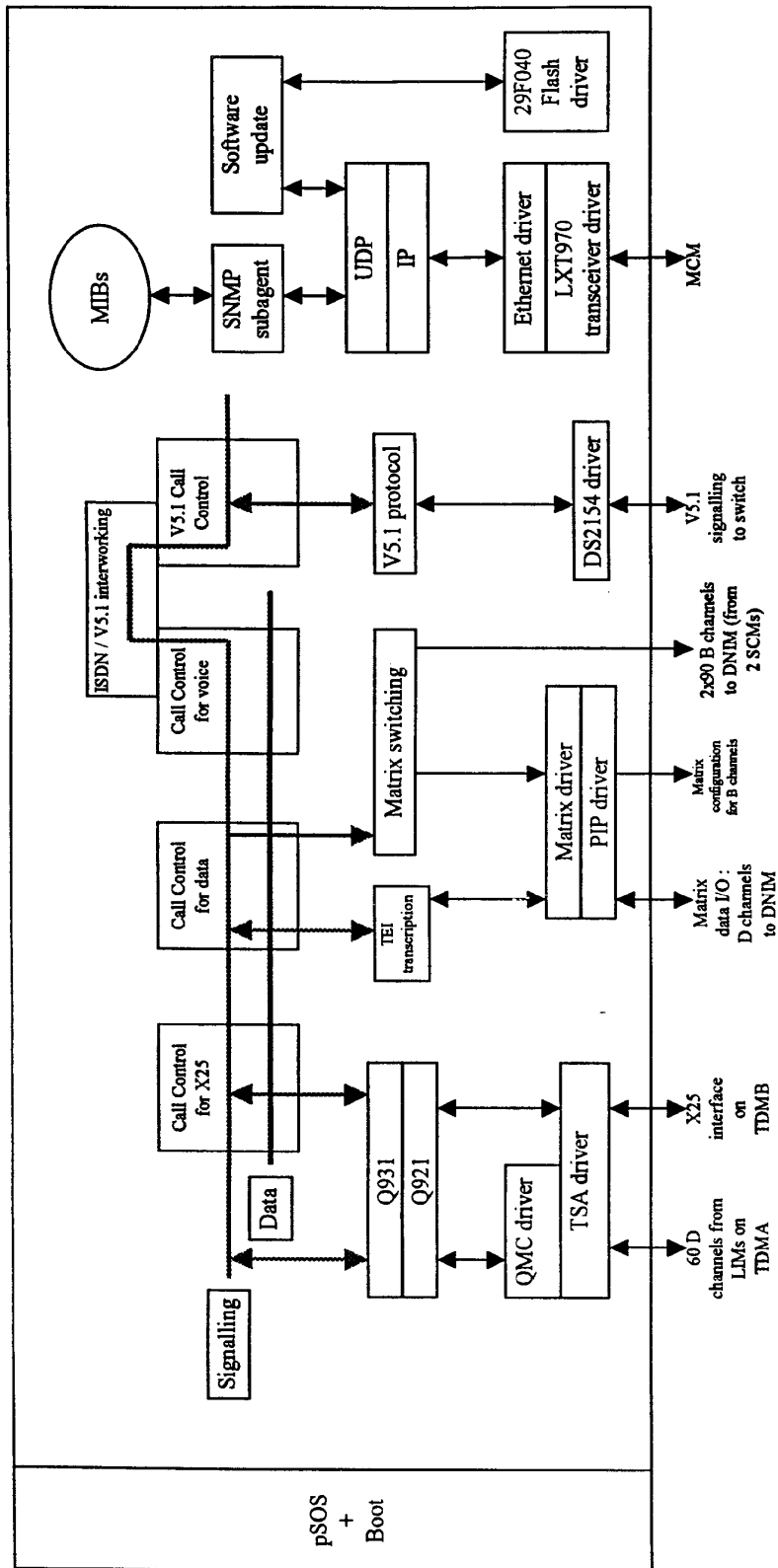


FIG. 9c

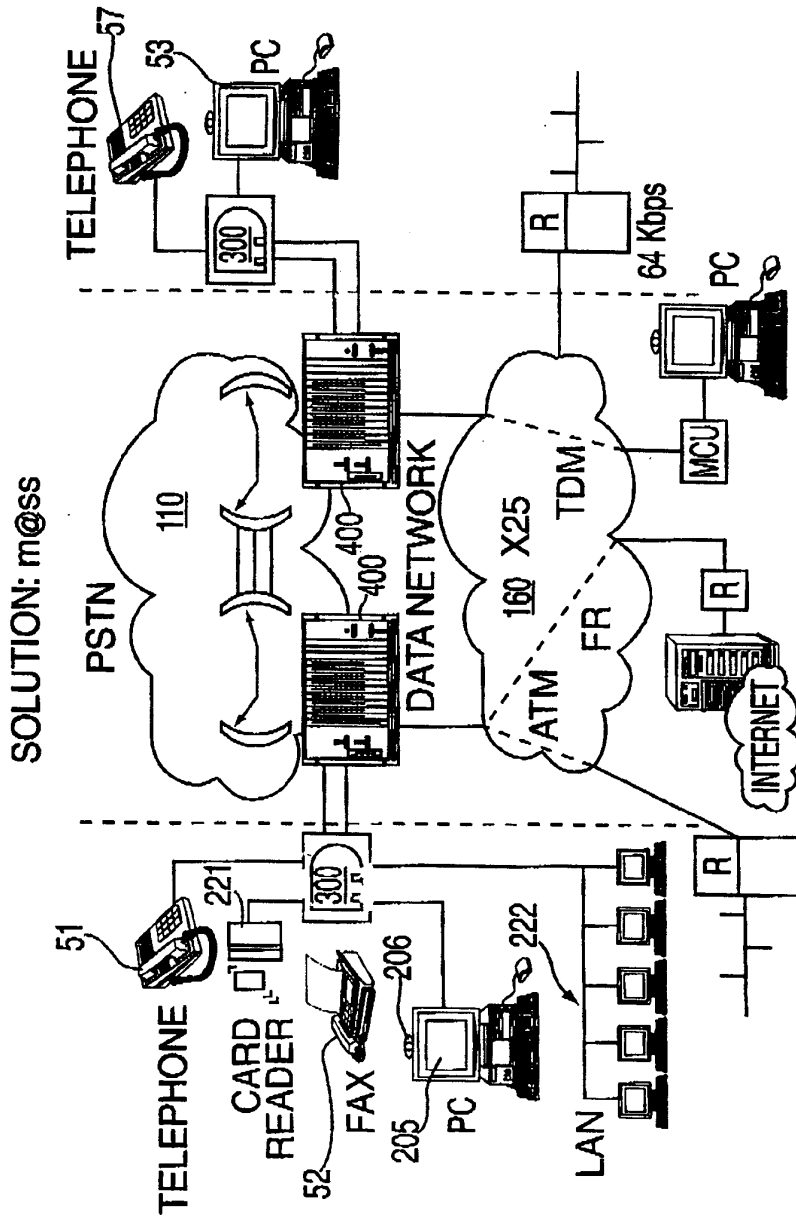


FIG. 12

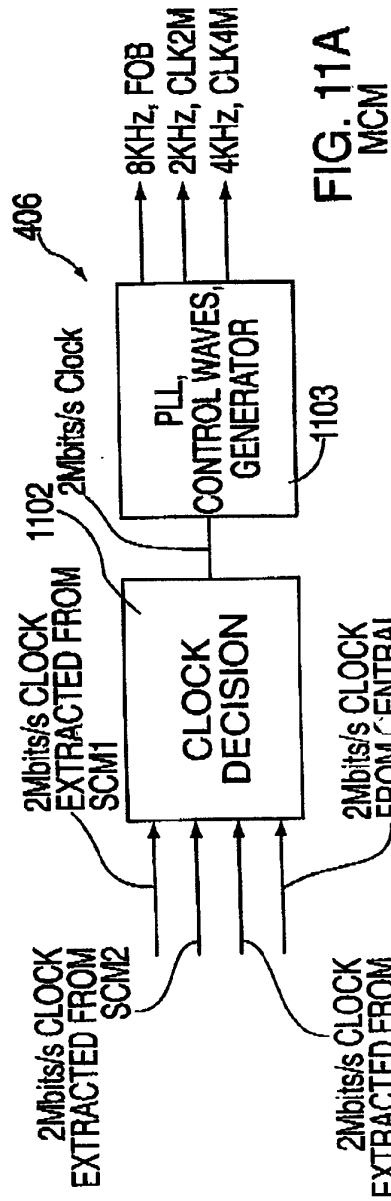


FIG. 11A MCM

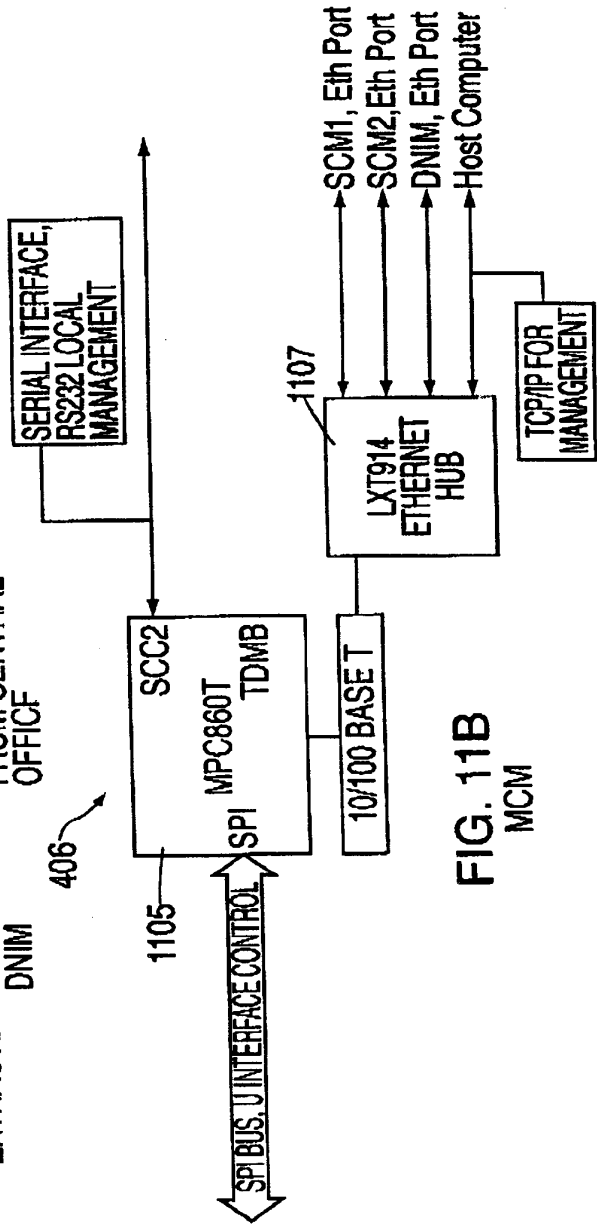


FIG. 11B MCM

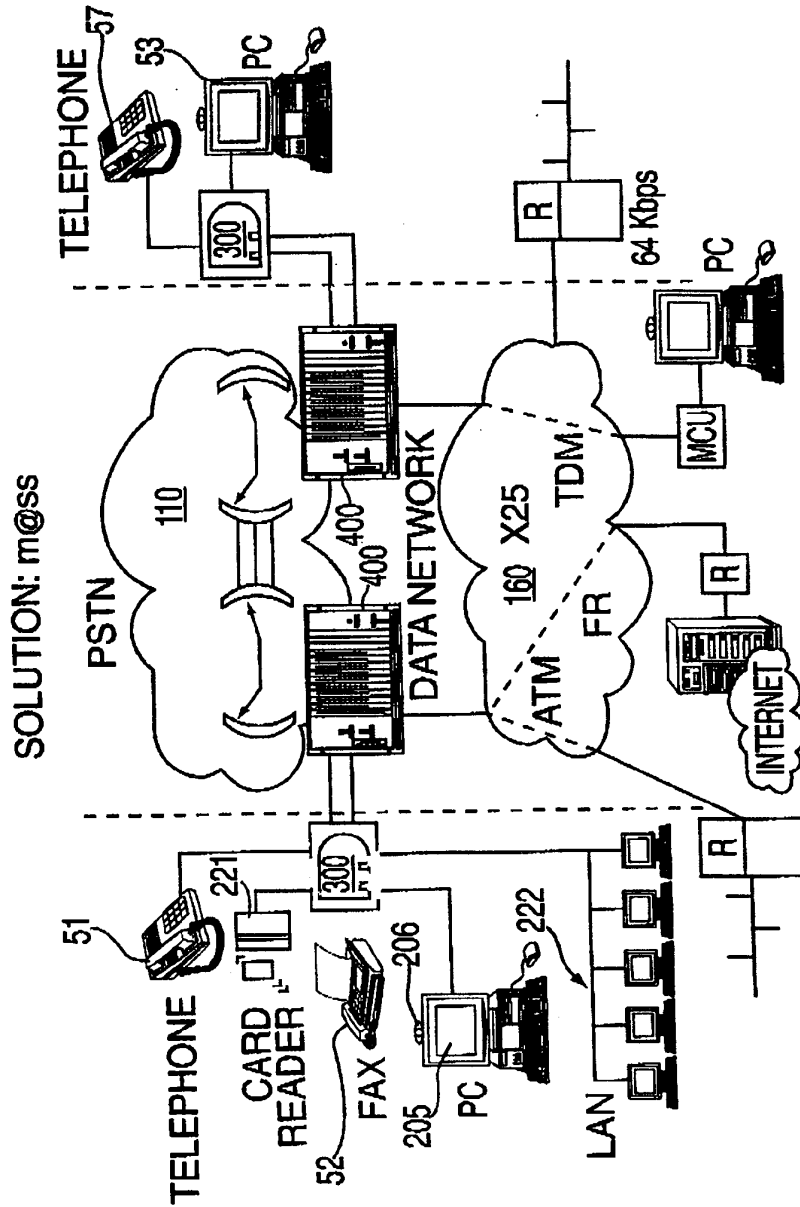


FIG. 12

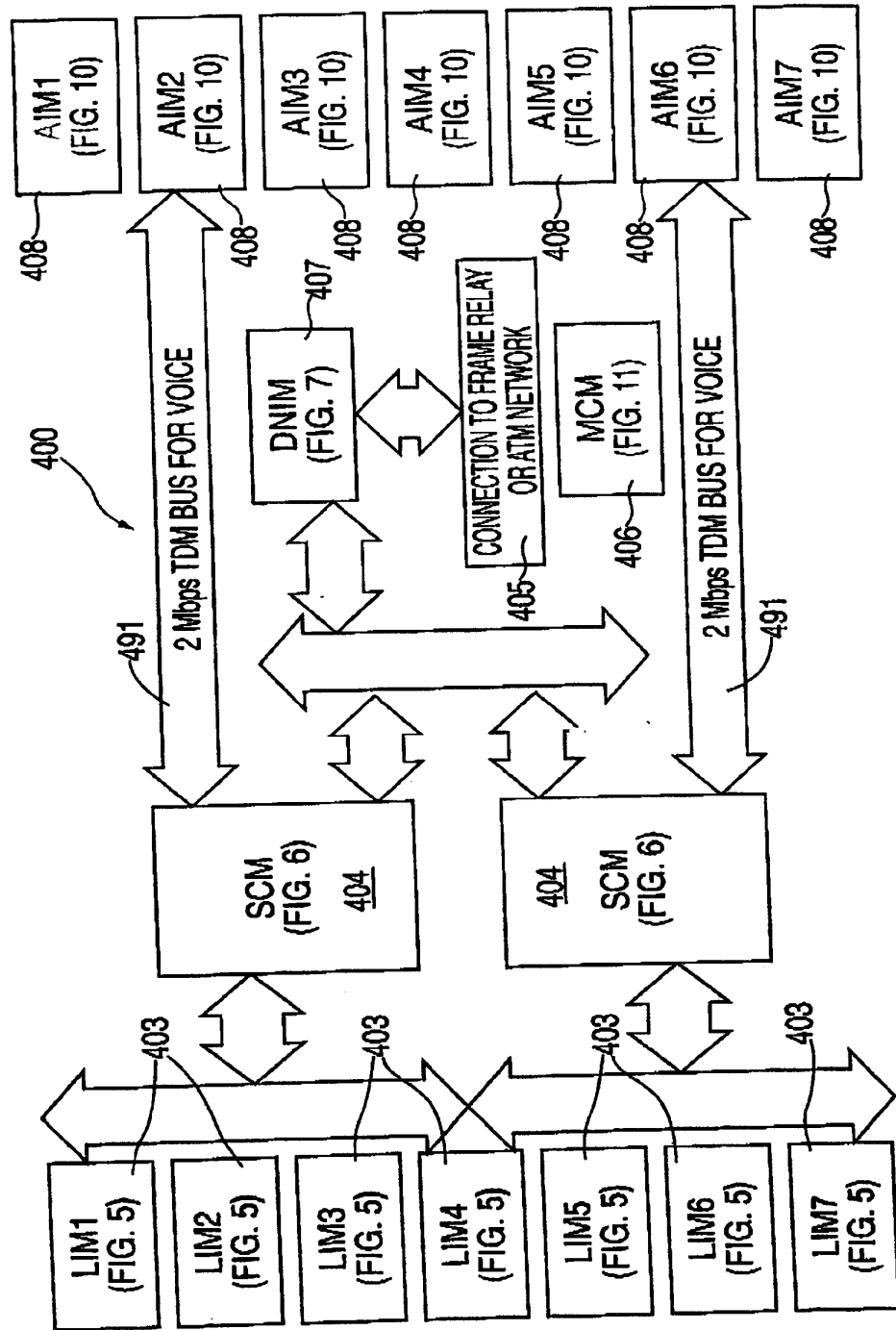


FIG. 13

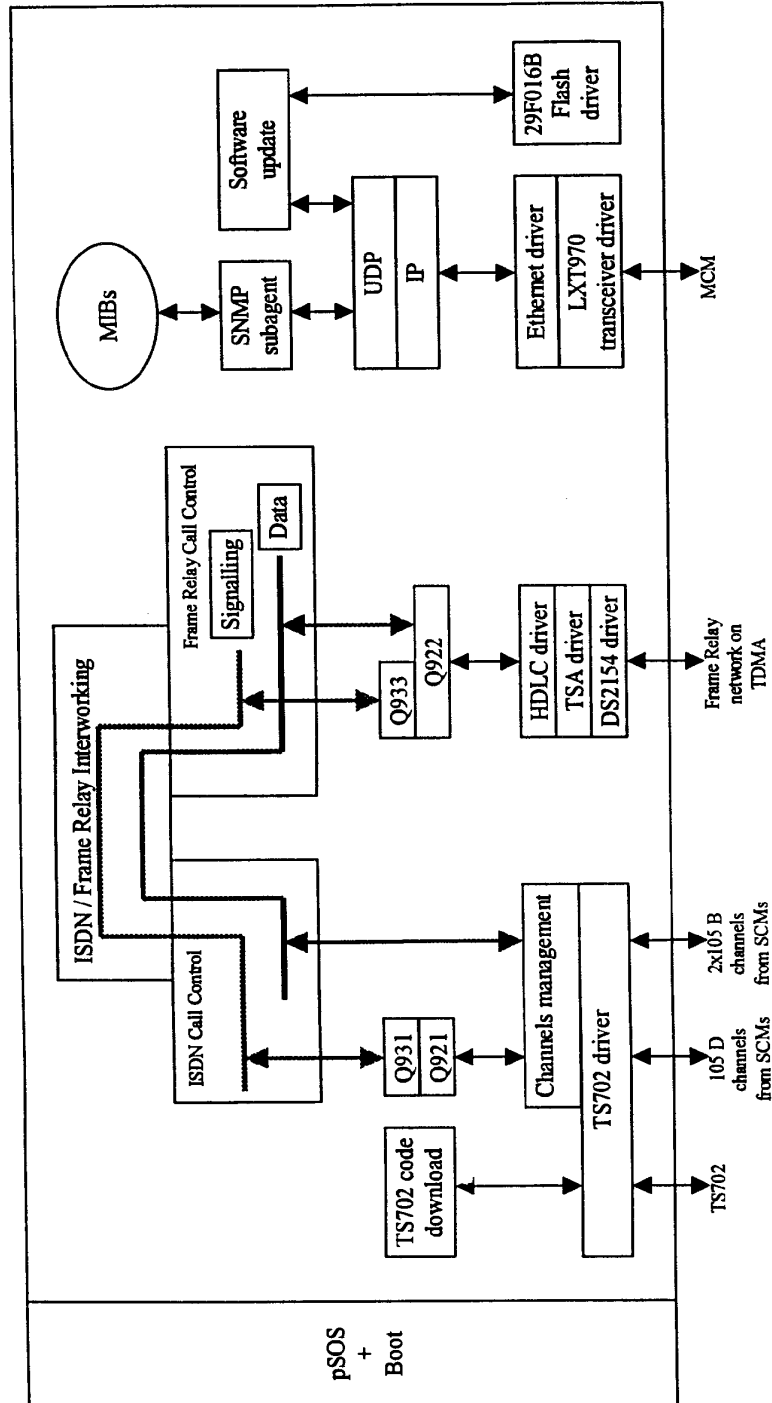


FIG. 14

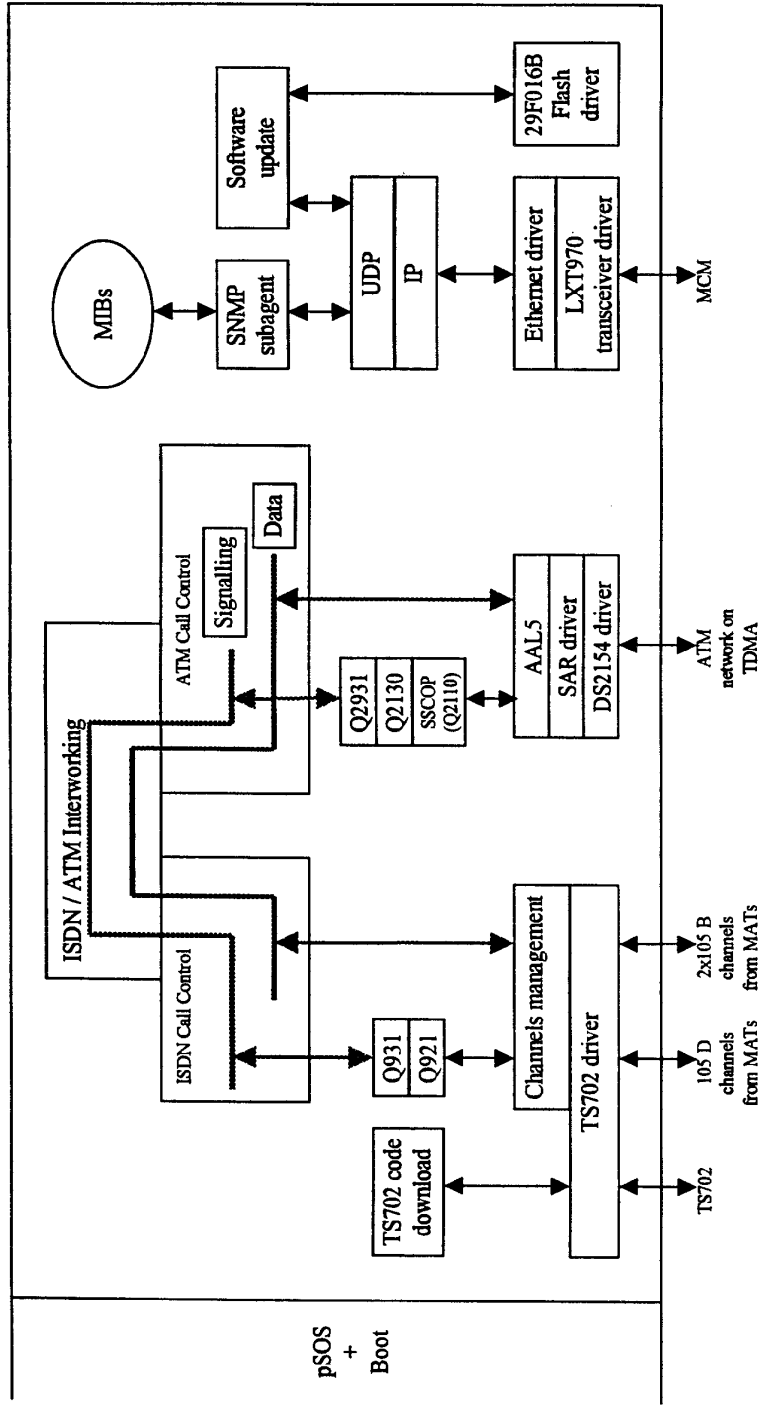


FIG. 15

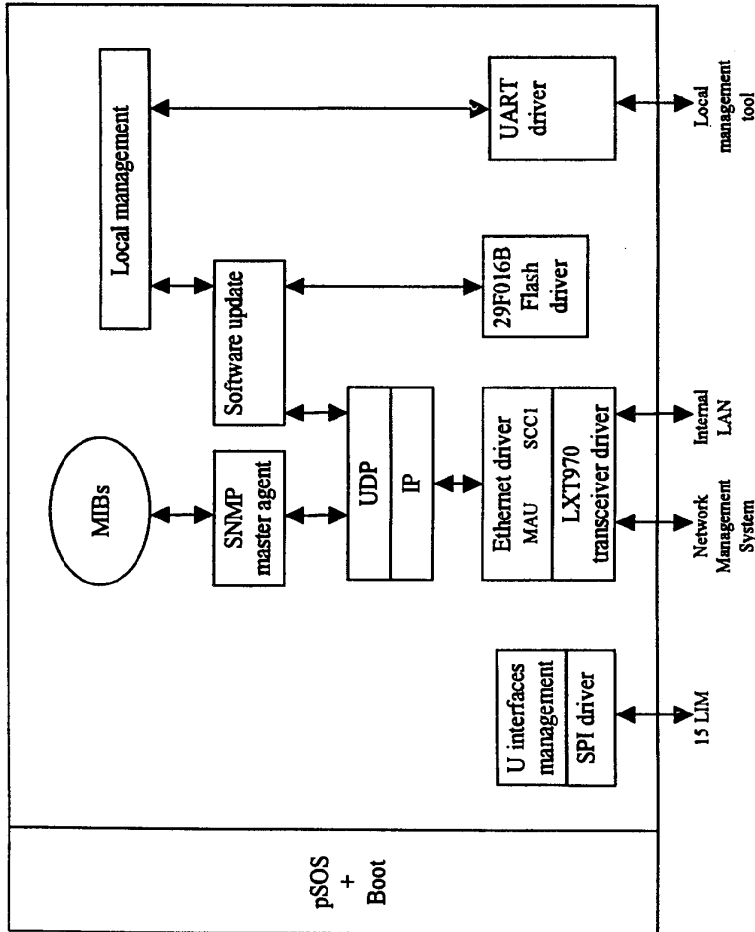


FIG. 16

(12) **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3:
24.11.1999 Bulletin 1999/47

(51) Int Cl.®: **H04M 3/30, H04M 1/24**

(43) Date of publication A2:
15.05.1996 Bulletin 1996/20

(21) Application number: **95308134.6**

(22) Date of filing: **14.11.1995**

(84) Designated Contracting States:
AT BE CH DE ES FR GB IE IT LI NL SE

- Schillaci, Onofrio
 Camarillo, California 93010 (US)
- Rischpater, Raymond William
 Felton, California 95018 (US)

(30) Priority: **14.11.1994 US 340083**

(71) Applicant: **HARRIS CORPORATION**
Melbourne, FL 32919 (US)

(74) Representative: **van Berlyn, Ronald Gilbert**
23, Centre Heights
London NW3 6JG (GB)

(72) Inventors:
 • **Horton, Michael D.**
Ojai, California 93023 (US)

(54) **Trouble-shooting system for telephone system**

(57) A trouble-shooting mechanism is incorporated into a telephone service technician's portable computer unit, to enable a craftsman, to respond to a trouble ticket. By analyzing multiple sources of information, including user inputs from the craftsman, parametric data embedded in the trouble ticket, test data obtained through the execution of local tests, and remote test data, the trouble-shooting mechanism derives and suggests a problem solving strategy that is appears accurate. The system architecture includes a trouble-shooting application engine, and an associated set of databases, one of which is a knowledge database, and the other of which is a shared, parameter database. The knowledge database contains rules and static parameters which define the characteristics and behavior of the application engine. These rule sets and information are telephone line trouble-shooting specific.

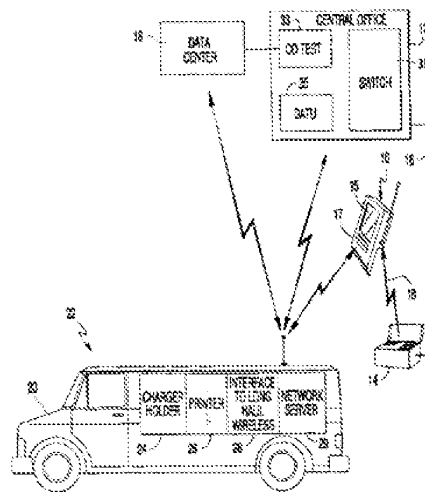


FIG. 1

EP 0 712 227 A3



European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 95 30 8134

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	US 4 922 516 A (BUTLER MYRON C ET AL) 1 May 1990 (1990-05-01) * abstract * * column 7, line 6 - column 8, line 6 *	1, 6, 8	H04M3/30 H04M1/24
A	US 4 841 560 A (CHAN AARON ET AL) 26 June 1989 (1989-06-26)		
A	US 4 977 399 A (PARK DANIEL J ET AL) 11 December 1990 (1990-12-11)		
			TECHNICAL FIELD SEARCHED (Int.Cl.6)
			H04M
The present search report has been drawn up for all claims			
Place of search		Date of completion of the search	Examiner
THE HAGUE		4 October 1999	Megalou, M
CATEGORY OF CITED DOCUMENTS			
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, not published on, or after the filing date C : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	

EPO FORM 1503 (08/83) (P.02/00.1)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 95 30 8134

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on the European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

G4-10-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4922516 A	01-05-1990	US 4837811 A	06-06-1989
		CA 1299788 A	28-04-1992
		EP 0326365 A	02-08-1989
US 4841560 A	20-06-1989	CA 1294076 A	07-01-1992
		EP 0335956 A	11-10-1989
		GB 2217954 A, B	01-11-1989
		IN 179646 A	25-04-1992
		WO 8903622 A	20-04-1989
US 4977399 A	11-12-1990	AU 4223689 A	05-03-1990
		EP 0428619 A	29-05-1991
		JP 4501791 T	26-03-1992
		WO 9001855 A	22-02-1990

EPO Patent Register

For more details about this annex, see Official Journal of the European Patent Office, No. 12/92

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication: 07.07.2004 Bulletin 2004/28 (51) Int. Cl.7: **H04Q 7/38**

(21) Application number: **02360383.0**

(22) Date of filing: **30.12.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
IE IT LI LU MC NL PT SE SI SK TR
 Designated Extension States:
AL LT LV MK RO

- Egler, Wolfgang, Dr.
70734 Fellbach (DE)
- Berg, Markus, Dipl.-Ing.
70176 Stuttgart (DE)
- Ebmeyer, Jürgen, Dipl.-Ing.
70619 Stuttgart (DE)

(71) Applicant: **EVOLIUM S.A.S.**
75008 Paris (FR)

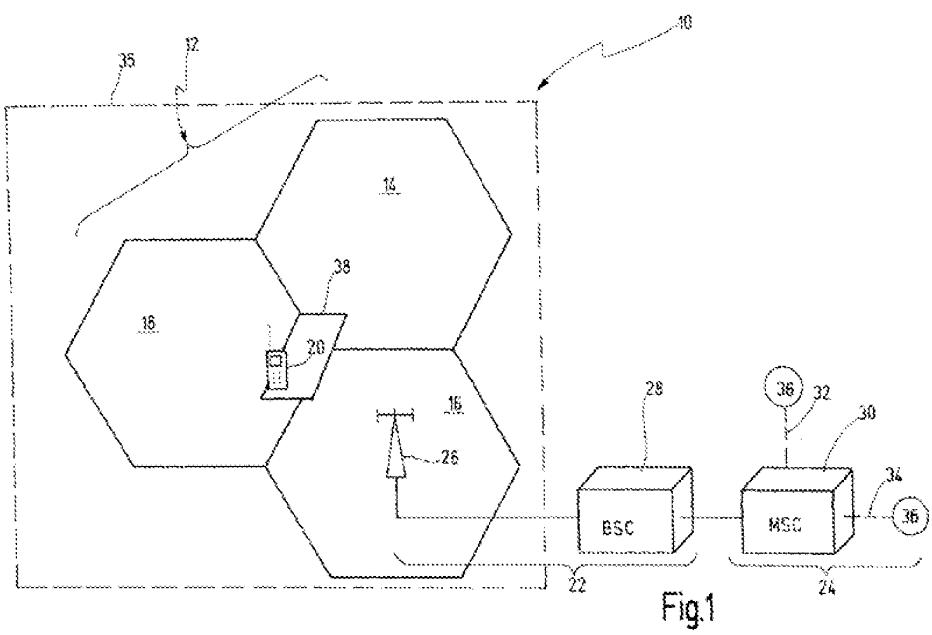
(74) Representative:
Dreiss, Fuhlendorf, Steimle & Becker
Patentanwälte,
Postfach 10 37 62
70032 Stuttgart (DE)

(72) Inventors:
 • Allerborn, Wilhelm, Dipl.-Ing.
71254 Ditzingen (DE)

(54) **Location based call barring**

(57) Disclosed are network elements (30, 40, 44) involved in the transmission of service requests between a mobile access terminal (20) of a first category assigned to a communication network (24), and the communication network (24), the network elements (30, 40, 44) imposing location dependent restrictions on service

requests concerning said mobile access terminal (20), the locations being covered by said mobile communication network (24). The network elements are characterized in that the network elements (30, 40, 44) bar forwarding service requests to or from the mobile access terminal (20) when the position of the mobile access terminal (20) is in a predetermined area (38).



EP 1 435 749 A1

Description

[0001] The present invention relates to Network elements involved in the transmission of service requests (i.e. mobile originating calls (MOC) or terminating calls (MTC), short messages, etc.) between a mobile access terminal of a first category assigned to a communication network, and the communication network, the network elements imposing location dependent restrictions on service requests concerning said mobile access terminal, the locations being covered by said mobile communication network.

[0002] Further, the present invention relates to a method of imposing location based restrictions on service requests of a mobile access terminal of a first category assigned to a mobile communication network, the locations being covered by said mobile communication network.

[0003] Such network elements and such a method are known from EP 891 110 A1.

[0004] According to this document, mobile stations like handsets could cause disturbance at electronic equipment, thereby endangering human lives in a sensitive environment. To avoid such disturbances, the use of mobile access terminals like mobile phones is sometimes not allowed at certain places, for example inside planes during parts of a flight and inside hospitals. To prevent being dependent upon the user's decency, the possible use of said handset could be deactivated by transmitting a deactivation signal from a base station to the handset, which deactivation signal either only deactivates said use for a predefined time-interval, or deactivates said use all the time until an activation signal originating from said base station has been received by said handset.

[0005] However, in order to obey such a deactivation signal, the mobile access terminals need a particular design, which has not been implemented up to now. Accordingly, all mobile access terminals that are presently in use would not follow such a deactivation signal, thereby rendering the function useless for the lifetime of the existing mobile access terminals.

[0006] Further, each and every future mobile access terminal had to show the particular design, thereby increasing manufacturing expenditure.

[0007] Even further, since the functionality would at least partially be located in the mobile access terminal, manipulations and malfunctions of relatively few concerned mobile access terminals may affect the usefulness of such a functionality adversely.

[0008] It is in view of the prior art outlined above the objective of the invention to provide for a functionality that prevents a mobile access terminal from causing disturbance, that does not rely on a particular design of the mobile access terminal, thereby, also including older mobile access terminals that are already in use, and that is less prone to manipulation and malfunction.

[0009] These objective is achieved by network ele-

ments as mentioned at the outset, wherein the network elements bar forwarding service requests to or from the mobile access terminal when the position of the mobile access terminal is in a predetermined area.

[0010] Further, these objectives are achieved by a method as mentioned at the outset, the method comprising the step of barring forwarding service requests to or from the mobile access terminal when the position of the mobile access terminal is in a predetermined area.

[0011] The Location Based Call Barring according to the invention allows to bar all service requests (i.e. mobile originating calls (MOC) or terminating calls (MTC), short messages, etc.) of a mobile access terminal if this mobile access terminal is roaming in a predetermined or pre-defined area, hereafter also referred to as the barred area. Thereby, possible disturbances of a mobile access terminal at sensitive locations can be effectively avoided. It is an important advantage of the inventive functionality that even the utilization of mobile phones that are already in use will be affected, since the new functionality applies to each and every standard compliant mobile phone.

[0012] The inventive functionality applies to all mobile subscribers roaming in the barred area, with the exception of specific subscribers or categories of subscribers as described below. Specific subscribers may have an "override category" in their profile, i.e. they are allowed to override location based call barring. There may be an exception list (mobile subscribers who are exempted from barring, e.g. police, fire brigades, priority subscribers, a specific subscriber class, or a list of specific individual subscribers).

[0013] In order to facilitate implementation, the network elements comprise preferably a mobile switching center MSC, a gateway mobile location center GMLC and, facultatively, a service control point SCP.

[0014] It is this combination of network elements that allow for an implementation of the inventive functionality without establishing a need for additional equipment.

[0015] Recent cellular systems include location service LCS and related technologies, and many architectures, protocols and procedures are still in development, such as logical LCS architecture, signalling protocol and interfaces, network location procedures and positioning procedures. The LCS referred to in accordance with the present invention is logically implemented on the GSM structure through the addition of one network node, the Gateway Mobile Location Center GMLC. However, the invention is not limited to the GSM structure and may be implemented in other network architectures like UMTS, CDM... The Gateway Mobile Location Center GMLC used in GSM contains functionality required to support LCS.

[0016] It is, particularly, preferred that the mobile communication network comprises at least two cells and that at least one of said cells overlaps said predetermined area.

[0017] Accordingly, the "barred area" can be within

one cell, or it can belong to two or more cells. It can also be part of more than one location area, which may be controlled by one or more BSCs and even MSCs. Hence, the borders of a barred area need not match the borders of a cell.

[0018] Preferably, when the mobile access terminal is in one of the overlapping cells, the mobile access terminal's location is determined using standard positioning methods to achieve a position information of decreased resolution, thus enabling the network elements to check whether the mobile access terminal is in the predetermined area or not.

[0019] As a resulting advantage it is not mandatory for the network to obtain highly resolved position data permanently for a potentially large number of mobile access terminals roaming inside a cell and, therefore, being potentially present at the barred area. Instead, the highly resolved localization is only implemented when needed. Hence, potential strain on the system resulting from establishing position data for a plurality of mobile access terminals at a time can be avoided. Since the accuracy of the position determination depends also on the capabilities of the concerned mobile access terminal, an exact localization might be difficult. If only a low accuracy is available (or only the Cell-ID can be determined e.g. for old mobiles), the wider area (up to the whole cell) may be barred or, alternatively, barring does not take place, depending on service options.

[0020] It is, further, preferred that the barring of forwarding service requests is activated and/or deactivated by an instance (client), e.g. deactivated by a client via said gateway mobile location center GMLC, which checks and confirms or refuses the client's respective authority.

[0021] It is, even further, preferred, that said gateway mobile location center GMLC activates a cell based intelligent network IN trigger in the network elements.

[0022] This feature allows a more subscriber dependent implementation.

[0023] Additionally, it is preferred, that the predetermined area is subscriber specific.

[0024] A subscriber specific location barring offers additional advantages like enhanced privacy at home and less disturbance at work, if desired. Such a functionality would apply to a specific subscriber who has subscribed to this service. The barring may depend on the called party number in case of mobile originated calls or on the calling party number in case of mobile terminated calls, date and time. Such a functionality could be designated as a location based call screening. As an example, mobile terminating calls may be inhibited from specified parties (e.g. no business calls when at home). Alternatively, mobile terminating calls are only allowed from specified parties (e.g. only business calls when at work, except calls from specified party). In other words: Business related calls could be barred when the subscriber is at home. Likewise, only work-related calls could be forwarded to an office.

[0025] Since service requests to or from a mobile access terminal can be particularly disturbing at a church, a cinema, a graveyard, a hospital, a theatre, an opera, a school and/or a restaurant, it is preferred that the predetermined area is the area of at least one of these locations.

[0026] It is, further, preferred to implement the method such that the above mentioned effects of the above mentioned network elements appear.

[0027] Further advantages can be taken from the description and the enclosed drawings.

[0028] It is to be understood that the features mentioned above and those yet to be explained below can be used not only in the respective combinations indicated, but also in other combinations or in isolation, without leaving the scope of the present invention.

[0029] Embodiments of the invention are shown in the drawings and will be explained in more detail in the description below. In the drawings:

Fig. 1 shows, schematically, a barred area overlapping cells of a mobile communication network;

Fig. 2 depicts, schematically, a first example scenario for implementing the present invention;

Fig. 3 shows, also schematically, a second example scenario for implementing the present invention; and

Fig. 4 depicts a third example scenario of the present invention, also in schematic form.

[0030] In Figure 1, a mobile communication system is designated in its entirety by identification reference 10. Mobile communication system 10 covers a cluster 12 of cells, each cell being defined by the range of coverage of a respective transceiver. In Figure 1, cells 14, 16 and 18 are part of cluster 12 that is covered by mobile communication system 10. In general, however, cluster 12 of mobile communication system 10 covers a significantly larger number of cells.

[0031] In general, mobile communication system 10 may be divided into three subsystems, namely into a mobile system 20, a base station system 22 and a network and switching system 24. Mobile system 20 is embodied by any mobile access terminal, e.g. by a mobile phone. The base station system 22 connects the mobile switching center with several mobile systems 20, although only one mobile system 20 is shown in Figure 1. The base station system 22 comprises a transmitter and a receiver in a base transceiver station BTS 26, and a base station controller BSC 28. Base station controller 28 handles, inter alia, the handover between several cells that are controlled by the concerned base station controller 28. Each base station system 22 comprises only one base station controller 28 but, in general, sev-

eral base transceiver stations 26. Again, only one BTS 26 is depicted, ass being representative for a plurality of BTSs

[0032] The network and switching system 24 switches, on the one hand, radio links in the GSM over great distances, e.g. between subscribers in different countries and, on the other hand, radio links between mobile subscribers in GSM and other networks like PSDN and ISDN. The mobile switching center 30 forms the center component of a network and switching system 24. Mobile switching center 30 switches between several connected base station systems 28. Further, mobile switching center 30 is connected to other network elements 36, e.g. other mobile switching centers. Dashed lines 32, 34 represent such connections. As is generally known, a mobile switching center 30 is connected to four data bases, namely to a home location register HLR, to an authentication center AOC, to a visitor location register VLR and, to an equipment identity register EIR.

[0033] The HLR administers the mobile subscribers that are allocated to a certain network and switching system. The HLR stores the locations of the allocated mobile systems/subscribers as well as the services that may be utilized by a particular subscriber. The VLR contains information concerning the locations of mobile subscribers that are not allocated to a particular network and switching system, but that are temporarily located in an area covered by the particular network and switching system.

[0034] In Figure 1, identification reference 38 designates a pre-defined area in which all service requests of a mobile system 20 should be barred, if the mobile system 20 is roaming in the pre-defined area 38. Accordingly, pre-defined area 38 may also be designated as a barred area 38. Barred area 38 may, for instance, be a church, a cinema, a grave yard, a hospital, a theatre, an opera, a school and/or a restaurant. However, this enumeration is meant to list examples only and, therefore, not meant to be complete. Instead, barred area 38 may be allocated to each area, in which service requests to or from a mobile system 20 roaming in barred area 38 would be potentially disturbing.

[0035] Of course, the barring of service requests may take place only temporarily. For instance, service requests may be barred during a presentation in a cinema, theatre, etc. or during a funeral, when the barred area 38 is a grave yard. As is generally known, the term service request may relate to mobile originating calls (MOC) or terminating calls (MTC) and/or short messages, etc. of a mobile station 20.

[0036] The barring of service requests is controlled by the mobile switching center 30 which blocks all service requests of a mobile system 20 which is roaming in the barred area 38. Barred area 38 may be within one cell or may overlap with two or more cells. It can also be part of more than one location area 35, which may be controlled by one or more base station controllers and mobile switching centers.

[0037] If a mobile system 20 requests a service request (MOC, MTC, ...) while roaming in one of the concerned cells, the location of the mobile system 20 is determined, using standard positioning methods. In figure 1, barred area 38 overlaps cells 14, 16 and 18. Accordingly, these cells are concerned. In other words, if a mobile system 20 roaming in one of these cells requests a service, the location of that particular mobile system 20 is determined with a higher resolution in order to be able to check whether mobile system 20 is within barred area 38 or not. If the position of mobile system 20 is within barred area 38, the service request of mobile system 20 is denied.

[0038] The location determination (location estimate) may be performed by a position calculation function located in the mobile system 20 or in the network 24. Position calculation functions a per se known. See, for instance, third generation partnership project; technical specification 3GPP TS 44.018 (2002-09). Further relevant 3GPP standards are: TS36PP23.071, Location Services (LCS); Service Description, Stage 1; TS 36PP23.071, Functional Stage 2 Description of Location Services. According to the specification mentioned first, several position calculation functionalities exist.

This specification mentions four position calculation functionalities, abbreviated as TA (timing advance between a mobile station and its serving base transceiver station), TOA (time of arrival position mechanism), E-OTD (enhanced observed time difference) and GPS (global positioning system positioning mechanism).

[0039] For example, in the E-OTD, the mobile system measures relative time of arrival of the signals from several base transceiver stations. The position of the mobile station is then determined by deducing the geometrical components of the time delays to a mobile station from the base transceiver station. Measurements are performed by the mobile station without any additional hardware. For more details, references is made to the above mentioned specifications, which are incorporated by reference herein. It should be noted, that the invention relates to a functionality of location based call barring rather than to a particular functionality of determining a location.

[0040] Figure 2 shows, schematically, a first example scenario for implementing the present invention. In this first example scenario, the mobile switching center 36 of figure 1 communicates with a gateway mobile location center 40, which is connected to a client 42. The gateway mobile location center GMLC 40 contains functionality required to support localizations. In one public land mobile network PLMN, there may be more than one GMLC. The barring functionality can be activated/deactivated by client 42 via GMLC 40. The authorization of client 42 to activate the barring is verified by the GMLC. The GMLC contains the relevant data like:

The clients which are authorized to activate the location based barring;

the related area description (e.g. geographic coordinates);

the allowed service options (e.g. an exception list).

[0041] The exception list may comprise mobile subscribers who are exempted from barring, e.g. the police, fire brigades, priority subscribers or a list of specific individual subscribers. Except for these exempted subscribers, the barring functionality applies to all mobile subscribers roaming in the barred area. Specific subscribers may have an override category in their profile enabling them to override location based call barring. In the first example scenario according to figure 2 client 42 activates location based call barring via GMLC 40. GMLC 40 then verifies the authorization of client 42 and determines the related cells. The related cells may include cell 16 in figure 2. Afterwards, GMLC 40 activates the service in the related mobile switching center 36. Mobile switching center 36 stores a list of the concerned cells, which include, in the example shown in figure 2, cell 16.

[0042] After being activated, a location based call barring may be invoked by a mobile subscriber roaming in one of the concerned cells. For instance, mobile system 20 tries to originate a call or receive a mobile terminating call. Cell 16, in which mobile system 20 is roaming, is known to the mobile switching center 36. Mobile switching center 36 determines that a barred area 38 belongs to this cell 16. Accordingly, mobile switching center 36 initiates a position determination concerning mobile system 20.

[0043] As has already been mentioned, standard position determination methods as disclosed in the above mentioned 3GPP specifications may be used. Once the position of mobile system 20 in cell 16 is known, mobile switching center 30 sends the position data and the relevant mobile system 20 data to GMLC 40.

[0044] The relevant mobile system 20 data include all data that is relevant for barring determination, e.g. the identity of the subscriber, potentially an override category, etc. GMLC 40 then checks whether mobile system 20 is within barred area 38 or not, and checks whether the call shall be barred or not. The result is given back to mobile switching center 30, which then denies or allows the call accordingly.

[0045] In the second example scenario according to figure 3, an additional service control point 44 is provided. Figure 3 represents an intelligent network (IN) based solution, in which the barring condition is verified by the service control point SCP44. This method allows a more subscriber dependant behaviour. In telecommunication systems, the intelligent network (IN) architecture, in which subscriber services are stored as service logics in a service node (SCP), is the preferred way to provide enhanced subscriber services.

[0046] IN services are defined by the service provider who loads the service logics into a service logic data base in a service node such as a service control point 11.

[0047] In the structure of figure 3, client 42 activates a location based call barring via GMLC 40, which verifies the authorization of client 42 and determines the related cells. Then, GMLC 40 activates a call based IN trigger in the related mobile switching center 30. Mobile switching center 30 activates the call based IN trigger. The service is also activated in service control point 44. As an alternative, the service activation may also be implemented directly in service control point 44, without involvement of GMLC 40.

[0048] Afterwards the activated service may be invoked by a subscriber (mobile system 20) roaming in one of the concerned cells, e.g. cell 16, by trying to originate a call or receiving a mobile terminating call. In this case, mobile switching center 30 determines that a call based IN trigger is activated for this cell. Accordingly, mobile switching center 30 triggers an IN service towards service control point 44. Service control point 44 requests a position of mobile system 20 via GMLC 40, using a standard positioning method. The position result is then returned to service control point 44 via GMLC 40. Service control point 44 decides whether the call is allowed or must be denied. The result is given back from service control point 44 to mobile switching center 40. Accordingly, mobile switching center 30 denies or allows the call.

[0049] In figure 4, a fourth example scenario is depicted, in which a subscriber specific location call barring is implemented. In the structure of figure 4, the location based call barring/screening-service is activated in service control point 44 by the subscriber himself. This may be done by a standard service user interaction tools, for instant via the internet, WAP, SMS, etc. The authorization of the subscriber is checked by a service control point 44. Service control point 44 then activates the subscriber specific IN trigger in mobile switching center 30.

[0050] If not activated, the IN service is triggered for all calls of the respective subscriber. After having been activated, the location based call barring may be invoked by the concerned subscriber trying to originate a call or receiving a mobile terminating call. Mobile switching center 30 then triggers an IN service toward service control point 44. In response, service control point 44 requests the position of mobile system 20, that is the mobile system allocated to the concerned subscriber, via GMLC 40 using standard position methods as outlined above. The position result is then returned to service control point 44 via GMLC 40. Service control point 44 then decides whether the call is allowed or as to be denied. The respective result is then given back from service control point 44 to mobile switching center 30. Mobile switching center 30 denies or allows the call accordingly.

Claims

1. Network elements (30, 40, 44) involved in the transmission of service requests between a mobile access terminal (20) of a first category assigned to a communication network (24), and the communication network (24), the network elements (30, 40, 44) imposing location dependent restrictions on service requests concerning said mobile access terminal (20), the locations being covered by said mobile communication network (24), **characterized in that** the network elements (30, 40, 44) bar forwarding service requests to or from the mobile access terminal (20) when the position of the mobile access terminal (20) is in a predetermined area (38).
2. The network elements (30, 40, 44) of claim 1, **characterized by** comprising a mobile switching center MSC (30), a gateway mobile location center GMLC (40) and, facultatively, a service control point SCP (44).
3. The network elements (30, 40, 44) of claim 2, **characterized in that** the communication network (24) comprises at least two cells (14, 16, 18) and that at least one of said cells (14, 16, 18) overlaps said predetermined area (38).
4. The network elements (30, 40, 44) of claim 3, **characterized in that**, when the mobile access terminal (20) is in one of the overlapping cells (14, 16, 18), the mobile access terminal's (20) location is determined using standard positioning methods to achieve a position information of higher resolution, enabling the network elements (30, 40, 44) to check whether the mobile access terminal (20) is in the predetermined area (38) or not.
5. The network elements (30, 40, 44) of claim, **characterized in that** the barring of forwarding service requests is activated and/or deactivated by an instance (client) (42), e.g. deactivated by a client (42) via said gateway mobile location center GMLC (40), which checks and confirms or refuses the client's (40) respective authority.
6. The network elements of claim 5, **characterized in that** said the gateway mobile location center GMLC (40) activates a cell based intelligent network IN trigger in the network elements (30, 40, 44).
7. The network elements (30, 40, 44) of claim 7, **characterized in that** the predetermined area (38) is subscriber specific.
8. The network elements (30, 40, 44) of claim 1, **characterized in that** said predetermined area (38) is the area of at least one of a church, a cinema, a graveyard, a hospital, a theatre, an opera, a school and/or a restaurant.
9. Method of imposing location based restrictions on service requests of a mobile access terminal (20) of a first category assigned to a communication network (24), the locations being covered by said communication network (24), **characterized by** the step of barring forwarding service requests to or from the mobile access terminal (20) when the position of the mobile access terminal (20) is in a predetermined area (38).
10. The method of claim 9, **characterized by** handling the network elements (30, 40, 44) of any of claims 2 to 7 such that the effects featured in these claims appear.

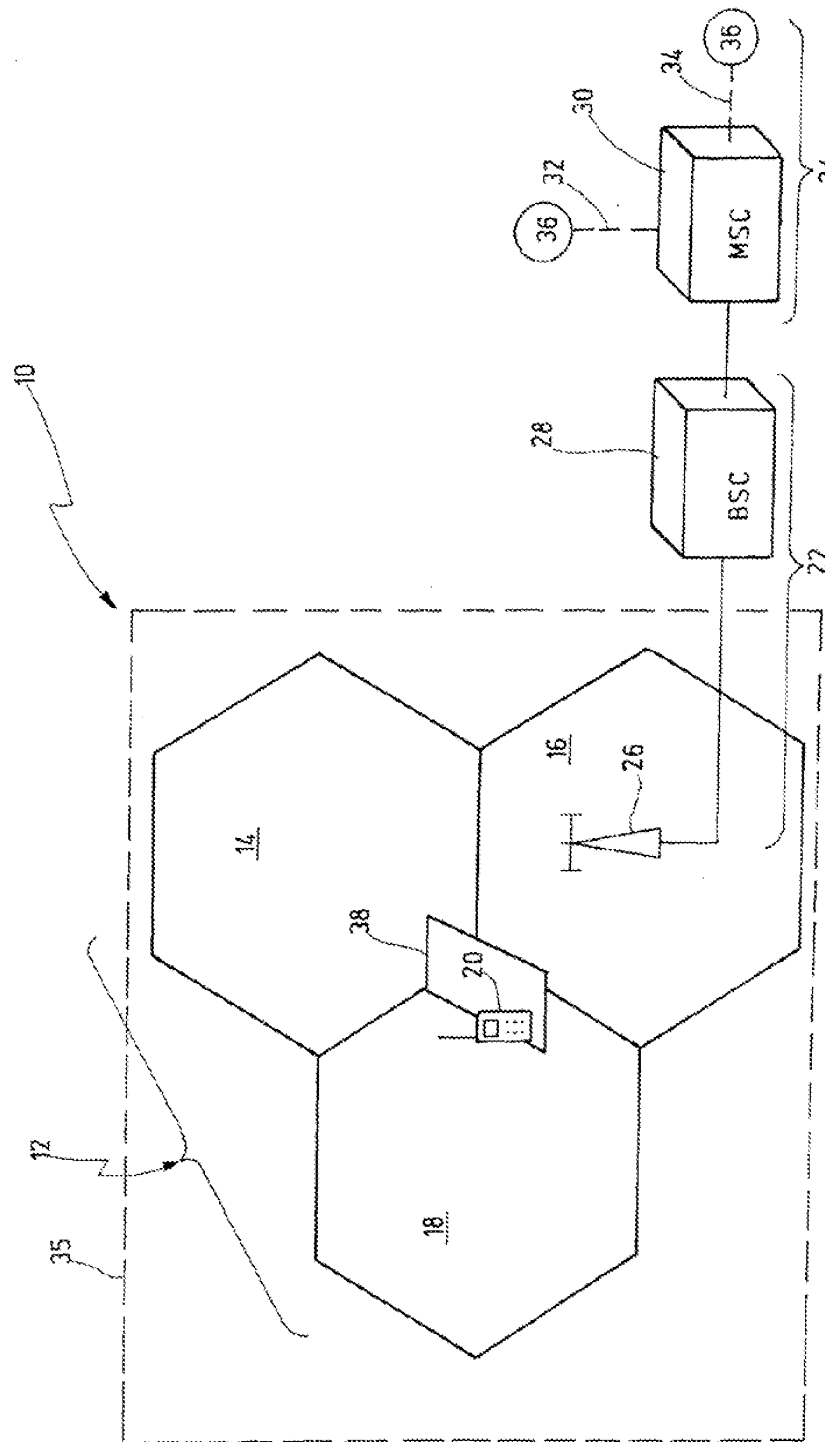


Fig.1

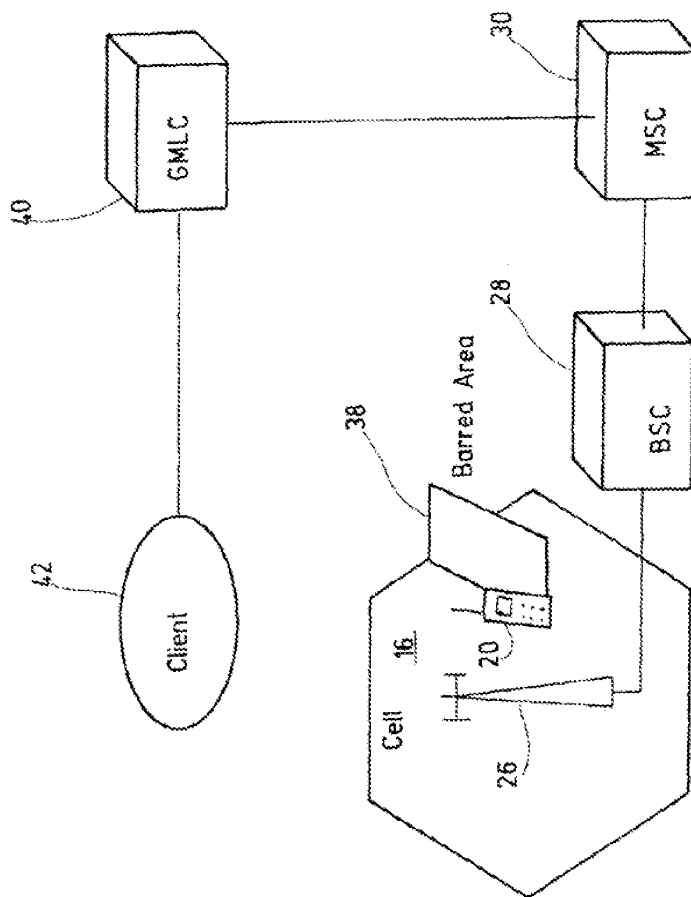


Fig.2

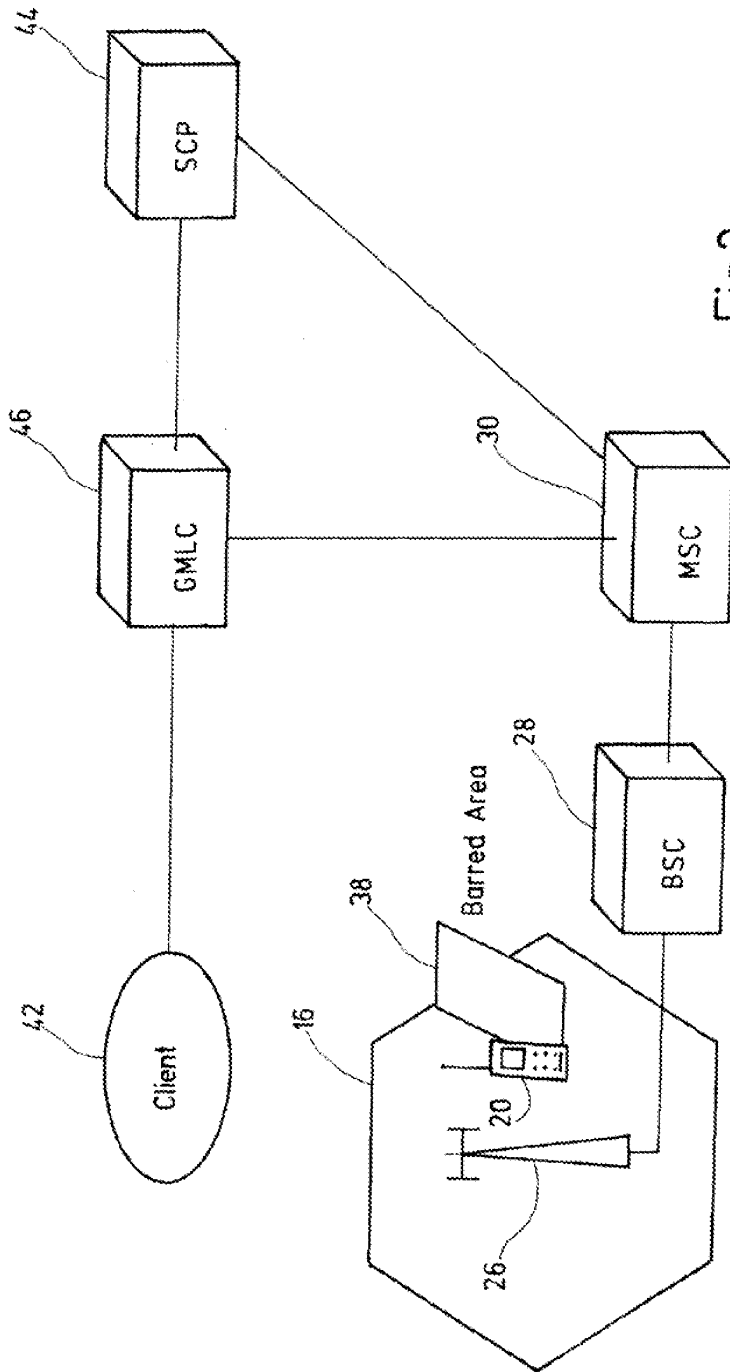
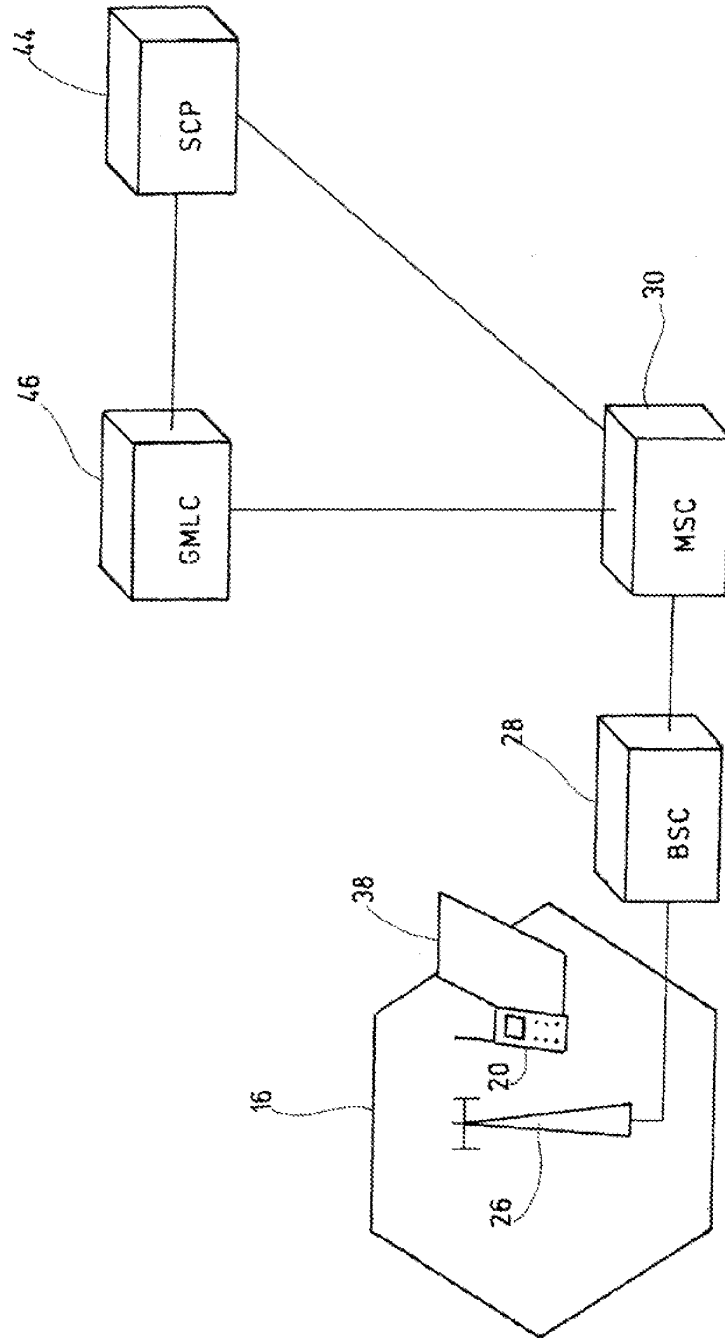


Fig.3





EUROPEAN SEARCH REPORT

Application Number
EP 02 36 0383

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 5 594 947 A (GRUBE GARY W ET AL) 14 January 1997 (1997-01-14) * column 2, line 38 - column 3, line 46 * ---	1-10	H04Q7/38
X	US 5 778 304 A (GRUBE GARY W ET AL) 7 July 1998 (1998-07-07) * column 2, line 41 - column 4, line 8 * ---	1-10	
X	WO 99 55102 A (ISRAELI GIL ; TE ENI BEN (IL); NETLINE COMMUNICATIONS TECHNOL (IL)) 28 October 1999 (1999-10-28) * page 3, line 11 - page 4, line 14 * * page 12, line 27 - page 13, line 20 * ---	1-4,8-10	
X	US 2001/031631 A1 (PITTS ROBERT L) 18 October 2001 (2001-10-18) * paragraphs [0023],[0044]-[0050] * ---	1,3,5, 8-10	
X	US 6 233 447 B1 (TOMOIKE HIROYUKI) 15 May 2001 (2001-05-15) * column 2, line 37 - column 3, line 27 * -----	1-3,5,6, 9,10	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04Q
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 28 May 2003	Examiner Weinmiller, J
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	

EP 02 36 0383 A1

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 02 36 0383

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on the European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

28-05-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5594947 A	14-01-1997	DE 69523901 D1 EP 0749667 A1 WO 9524809 A1	20-12-2001 27-12-1996 14-09-1995
US 5778304 A	07-07-1998	NONE	
WO 9955102 A	28-10-1999	AU 3343799 A EP 1074156 A1 WO 9955102 A1	08-11-1999 07-02-2001 28-10-1999
US 2001031631 A1	18-10-2001	NONE	
US 6233447 B1	15-05-2001	JP 2940526 B2 JP 11069420 A	25-08-1999 09-03-1999

EPO FORM 1938

For more details about this annex, see Official Journal of the European Patent Office, No. 12/82

EP1445923A1

Publication Title:

Operation limiting technique for a camera-equipped mobile communication terminal

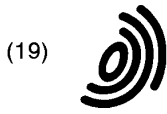
Abstract:

Abstract of EP 1445923

(A1) A camera-equipped mobile communication terminal allows its own camera functions to be selectively inhibited according to camera-function inhibition flags included in a camera-function limiting signal broadcast by a radio station or based on GPS-measured location and camera-function inhibition flags for each operation-limited area. Appropriate function limitations on the camera-equipped mobile communication terminal and necessary function permissions can be made depending on situations or occasions.

Courtesy of <http://v3.espacenet.com>

This Patent PDF Generated by Patent Fetcher(R), a service of Stroke of Color, Inc.



(19)

Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 1 445 923 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
11.08.2004 Bulletin 2004/33

(51) Int Cl.7: H04M 1/725

(21) Application number: 04002319.4

(22) Date of filing: 03.02.2004

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HU IE IT LI LU MC NL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(72) Inventor: Hayashi, Hideyuki, c/o NEC Corporation
Tokyo (JP)

(74) Representative:
von Samson-Himmelstjerna, Friedrich R.,
Dipl.-Phys. et al
SAMSON & PARTNER
Widenmayerstrasse 5
80538 München (DE)

(30) Priority: 04.02.2003 JP 2003027586
02.12.2003 JP 2003403515

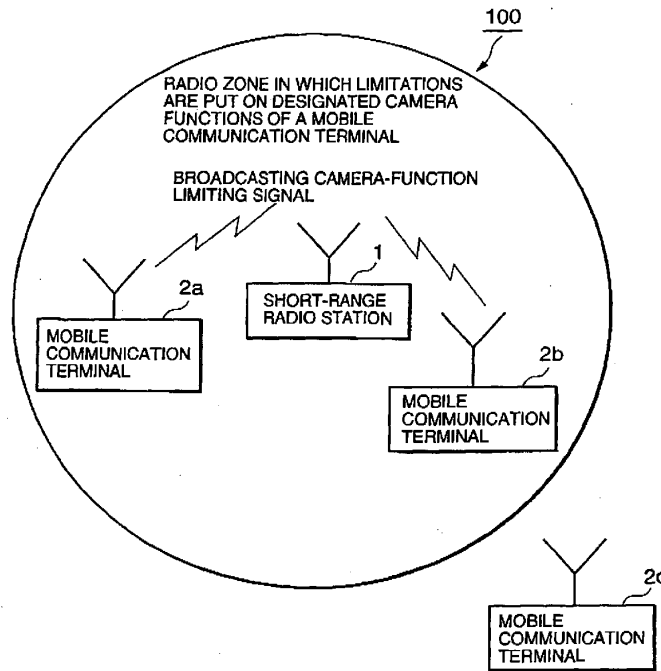
(71) Applicant: NEC CORPORATION
Tokyo (JP)

(54) Operation limiting technique for a camera-equipped mobile communication terminal

(57) A camera-equipped mobile communication terminal allows its own camera functions to be selectively inhibited according to camera-function inhibition flags included in a camera-function limiting signal broadcast by a radio station or based on GPS-measured location

and camera-function inhibition flags for each operation-limited area. Appropriate function limitations on the camera-equipped mobile communication terminal and necessary function permissions can be made depending on situations or occasions.

FIG. 1



EP 1 445 923 A1

Description

[0001] The present invention relates to a mobile communication terminal equipped with a camera such as a digital still camera or a digital video camera and in particular to an operation limiting system and method for putting operation-limitations on the camera-equipped mobile communication terminal.

[0002] With the widespread use of mobile telephone terminals equipped with digital still/video camera, there have arisen various camera-related problems, for example, an invasion of privacy and photo/video shooting in an area where cameras are prohibited from use. Accordingly, there have been proposed various techniques of solving such problems.

[0003] Japanese Patent Application Unexamined Publication No. 11-261674 discloses a camera-equipped portable telephone terminal which can be set to an inhibition mode of shooting with a flash or making a beep depending on whether the terminal is located near a control station or within a radio zone formed by the control station.

[0004] Japanese Patent Application Unexamined Publication No. P2000-152217A discloses a mobile video telephone terminal, which can be surely inhibited from capturing, storing or transmitting any image in the vicinity of a shooting-inhibition signal transmitter.

[0005] Contrarily, there are cases where video telephone function is needed, for example, in emergency. Japanese Patent Application Unexamined Publication No. P2002-252683A discloses a mobile telephone terminal having a video telephone function, which can be automatically set to a video telephone mode when an emergency communication request is detected.

[0006] However, the conventional techniques uniformly put function limitations on mobile telephones located in the place. Accordingly, there are cases where the photo/video shooting and telecommunication functions of a camera-equipped mobile telephone terminal are remarkably impaired. In addition, it is true that the video telephone function or the like is needed in emergency.

[0007] An object of the present invention is to provide a camera-equipped mobile communication terminal and its operation limiting system and method, which allow appropriate function limitations on camera-equipped mobile communication terminals and necessary function permissions depending on situations or occasions.

[0008] According to the present invention, a system for limiting a plurality of camera functions in a mobile communication terminal equipped with a camera, includes: at least one operation-limited area, wherein the mobile communication terminal is allowed to determine whether the mobile communication terminal is located within an operation-limited area; a memory storing camera-function limitation data for each of the at least one operation-limited area, the camera-function limitation data indicating selective inhibition of the plurality of cam-

era functions; and a camera function controller for selectively inhibiting the plurality of camera functions depending on camera-function limitation data corresponding to an operation-limited area in which the mobile communication terminal is located.

[0009] The camera function controller preferably releases an inhibited camera function when a predetermined condition is satisfied.

[0010] According to an aspect of the present invention, each of the at least one operation-limited area is substantially defined by radio propagation of a camera-function limiting signal broadcast by a radio station, the camera-function limiting signal including the camera-function limitation data, wherein the mobile communication terminal comprises a radio receiver for receiving the camera-function limiting signal from the radio station.

[0011] The system may further include: an emergency communication detector for detecting occurrence of an emergency communication to inform the camera function controller of the occurrence of the emergency communication, wherein, when informed of the occurrence of the emergency communication in a case of inhibition of a predetermined camera function, the camera function controller releases the inhibition of the predetermined camera function.

[0012] The predetermined camera function is preferably a video telephone function.

[0013] The system may further include: a face image memory for previously registering a face image of each authorized user, wherein, when an input image picked up by the camera matches a face image registered in the face image memory in a case of inhibition of a predetermined camera function, the camera function controller releases the inhibition of the predetermined camera function.

[0014] The system may further include: an emergency communication detector for detecting occurrence of an emergency communication to inform the camera function controller of the occurrence of the emergency communication; and a face image memory for previously registering a face image of each authorized user, wherein, in one of cases where the camera function controller is informed of the occurrence of the emergency communication in a case of inhibition of a predetermined camera function and where an input image picked up by the camera matches a face image registered in the face image memory in a case of inhibition of the predetermined camera function, the camera function controller releases the inhibition of the predetermined camera function.

[0015] The radio station may transmit the camera-function limiting signal in a short-range radio communication scheme, which is different from a radio communication scheme of the mobile communication terminal. In an embodiment, the short-range radio communication scheme may be one of Bluetooth^(R), UWB (Ultra Wide Band), and wireless LAN.

[0016] According to another aspect of the present in-

vention, each of the at least one operation-limited area is determined by the mobile communication terminal, wherein the mobile communication terminal includes: a location detector for detecting a location of the mobile communication terminal; an operation-limited area memory storing operation-limited area location data; and an area decision section for searching the operation-limited area memory for a detected location of the mobile communication terminal to determine whether the mobile communication terminal is located within an operation-limited area.

[0017] The location detector may be a GPS positioning section for receiving global positioning system (GPS) signals to detect the location of the mobile communication terminal.

[0018] The camera functions may include image pick-up function, auto-focusing and zooming function, strobe function, shutter-sound generating function, and video telephone function.

[0019] According to the present invention, a method for limiting a plurality of camera functions in a mobile communication terminal equipped with a camera, comprising: preparing at least one operation-limited area, wherein the mobile communication terminal is allowed to determine whether the mobile communication terminal is located within an operation-limited area; storing camera-function limitation data for each of the at least one operation-limited area, the camera-function limitation data indicating selective inhibition of the plurality of camera functions; and selectively inhibiting the plurality of camera functions depending on camera-function limitation data corresponding to an operation-limited area in which the mobile communication terminal is located.

[0020] According to the present invention, a mobile communication terminal which is equipped with a camera and has a plurality of camera functions, includes: a radio receiver for receiving a camera-function limiting signal from a radio station; a signal decoder for decoding the camera-function limiting signal to produce camera-function limitation data indicating selective inhibition of the plurality of camera functions; and a camera function controller for selectively inhibiting the plurality of camera functions depending on camera-function limitation data.

[0021] The camera function controller may release an inhibited camera function when a predetermined condition is satisfied.

[0022] According to the present invention, a mobile communication terminal which is equipped with a camera and has a plurality of camera functions, includes: a location detector for detecting a location of the mobile communication terminal; a memory storing camera-function limitation data for each of at least one operation-limited area, wherein the camera-function limitation data indicates selective inhibition of the plurality of camera functions; an area decision section for searching the operation-limited area memory for a detected location of the mobile communication terminal to determine whether the mobile communication terminal is located

within an operation-limited area; and a camera function controller for selectively inhibiting the plurality of camera functions depending on camera-function limitation data corresponding to a found operation-limited area.

[0023] As described above, the camera functions of a camera-equipped mobile communication terminal are selectively inhibited 1) by a camera-function limiting signal broadcast by a radio station installed at a predetermined location or 2) based on location information detected by the GPS system, predetermined operation-limited area data and camera-function inhibition data.

[0024] Installation of a radio station, especially a short-range radio station, at a desired location can provide a relatively small operation-limited area, resulting in cost-effective and reasonable operation-limitation of camera functions. Similarly, in the case of using the GPS system, the location of a mobile communication terminal can be accurately measured without the need of radio stations for operation limitation, allowing cost-effective and reasonable operation-limitation of camera functions.

[0025] In addition, a camera function, which is prohibited or inappropriate around the predetermined location or in the detected operation-limited area, can be automatically inhibited without any dependence on user's good manners. On the other hand, a camera function, which is not prohibited or can be made without any problem, can be normally operated. In this manner, only inappropriate camera functions are inhibited and other camera functions are permitted, achieving compulsory but reasonable operation limitation of camera functions.

[0026] In addition, an inhibited camera function can be made active again when a predetermined condition is satisfied, for example, an emergency occurs and/or a user is authenticated, resulting in enhanced convenience of the mobile communication terminal for users.

Fig. 1 is a diagram showing a network system employing an operation limiting system according to a first embodiment of the present invention;

Fig. 2 is a block diagram showing a short-range radio station used in the operation limiting system according to the first embodiment of the present invention;

Fig. 3 is a schematic block diagram showing a function structure of a camera-equipped mobile communication terminal used in the operation limiting system according to the first embodiment;

Fig. 4A is a diagram showing a function inhibition operation in the operation limiting system according to the first embodiment;

Fig. 4B is a diagram showing a format of an operation-limitation packet used in the operation limiting system according to the first embodiment;

Fig. 4C is a diagram showing an example of operation inhibition and permission flags set in the operation-limitation packet of Fig. 4B;

Fig. 5 is a flowchart showing a function inhibition operation in the operation limiting system according to the first embodiment;

Fig. 6 is a schematic block diagram showing a function structure of a camera-equipped mobile communication terminal used in an operation limiting system according to a second embodiment of the present invention;

Fig. 7 is a flowchart showing a function inhibition operation in the operation limiting system according to the second embodiment;

Fig. 8 is a schematic block diagram showing a function structure of a camera-equipped mobile communication terminal used in an operation limiting system according to a third embodiment of the present invention;

Fig. 9 is a flowchart showing a function inhibition operation in the operation limiting system according to the third embodiment;

Fig. 10 is a schematic block diagram showing a function structure of a camera-equipped mobile communication terminal used in an operation limiting system according to a fourth embodiment of the present invention;

Fig. 11 is a diagram showing a network system employing an operation limiting system according to a fifth embodiment of the present invention;

Fig. 12 is a schematic block diagram showing a function structure of a camera-equipped mobile communication terminal used in an operation limiting system according to the fifth embodiment of the present invention;

Fig. 13 is a diagram showing an example of contents of operation limitation data and operation limited areas in the camera-equipped mobile communication terminal according to the fifth embodiment of the present invention;

Fig. 14 is a flowchart showing a function inhibition operation in the operation limiting system according to the fifth embodiment;

Fig. 15 is a schematic block diagram showing a function structure of a camera-equipped mobile communication terminal used in an operation limiting system according to a sixth embodiment of the

present invention;

Fig. 16 is a schematic block diagram showing a function structure of a camera-equipped mobile communication terminal used in an operation limiting system according to a seventh embodiment of the present invention;

Fig. 17 is a schematic block diagram showing a function structure of a camera-equipped mobile communication terminal used in an operation limiting system according to an eighth embodiment of the present invention; and

Fig. 18 is a block diagram showing a camera-equipped mobile communication terminal used in an operation limiting system according to a ninth embodiment of the present invention.

20 1. First embodiment

System configuration

[0027] Referring to Fig. 1, an operation limiting system according to a first embodiment of the present invention is provided with a radio station for each geographical area where the camera functions of a camera-equipped mobile communication terminal are selectively inhibited from use. Here, it is assumed that the radio station is a short-range radio station 1 and is further assumed for the sake of simplicity that the short-range radio station 1 defines an operation-limitation radio zone 100 and a plurality of mobile communication terminals (here, 2a and 2b) are located within the radio zone 100 and a mobile communication terminal is located out of the radio zone 100. As described later, the mobile communication terminals 2a and 2b within the radio zone 100 are inhibited from operating the designated camera-related functions and the mobile communication terminal 2c out of the radio zone 100 is not inhibited.

[0028] The operation-limitation radio zone 100 of the short-range radio station 1 is, for example, about 10 meters in radius. The mobile communication terminals 2a-2c are typically a camera-equipped mobile telephone terminal.

Short-range radio station

[0029] As shown in Fig. 2, the short-range radio station 1 includes a man-machine interface 11, an operation-limitation data memory 12, a camera-function limiting signal generator 13 and a short-range radio transmitter 14. The man-machine interface 11 may be formed by an input device such as a keypad and a display such as a LCD. The operation-limitation data memory 12 is composed of a plurality of registers, which store operation-limitation data inputted through the man-machine interface 11. The operation-limitation data may be com-

posed of a string of control flags.

[0030] The camera-function limiting signal generator 13 generates a camera-function limiting signal from the string of control flags stored in the operation-limitation data memory 12. The camera-function limiting signal may be a packet composed of a header and a payload including a set of control flags. The short-range radio transmitter 14 broadcasts the camera-function limiting signal with a relatively small transmission power at predetermined time intervals in a predetermined short-range radio transmission system such as Bluetooth (Registered TM), UMB (Ultra Wide Band) or Wireless LAN standard. In Fig. 1, the mobile communication terminals 2a and 2b within the radio zone 100 can receive the broadcast camera-function limiting signal and the mobile communication terminal 2c out of the radio zone 100 cannot substantially receive it.

Mobile communication terminal

[0031] Each of the mobile communication terminals (here, 2a-2c) has the same function block structure. Hereinafter, for simplicity, each mobile communication terminal is referred to as a mobile communication terminal 2.

[0032] As shown in Fig. 3, the mobile communication terminal 2 is provided with a camera section composed of an image pickup device unit 21, a lens unit 22, and a strobe device 23. The image pickup device unit 21 includes an image sensor such as CCD sensor, CMOS sensor or the like, which may be used for video and photograph shooting. The lens unit 22 includes a set of lenses allowing focusing and zooming. The strobe device 23 emits a strobe light when photo-shooting. A shutter-sound generator 24 generates a shutter sound when shooting so as to avoid stealing a camera shot. A display controller 25 controls a display such as a liquid crystal display device (LCD), which is usually provided on a main body of the terminal 2.

[0033] The mobile communication terminal 2 is further provided with an operation section 26 such as a keypad to enter data or instructions. A mobile communication system 27 including a radio communication controller 271 is provided to perform predetermined mobile communication operations.

[0034] A camera function controller 28, which may be implemented in a program-controlled processor (not shown), controls the above-described camera section, the shutter-sound generator 24 and the display controller 25 depending on a camera-function limiting signal received from the short-range radio station 1. The camera function controller 28 controls the camera section to capture still/video images, which are output as an image signal to the mobile communication system 27. The captured image can be superimposed on another image received from the other party and the combined image is displayed on the display device.

[0035] The mobile communication terminal 2 is further

provided with a signal decoder 29 and a short-range radio receiver 30. The short-range radio receiver 30 receives a camera-function limiting signal from the short-range radio station 1 and the signal decoder 29 decodes the received camera-function limiting signal to output camera function control flags to the camera function controller 28. When no camera-function limiting signal is received, the signal decoder 29 notifies the camera function controller 28 of no signal. As described later, the camera function controller 28 selectively inhibits the camera functions including image pickup, focusing/zooming, flashing, shutter-sound generating, and the likes, depending on the camera function control flags.

15 Camera-function limiting signal

[0036] Taking a system of Fig. 1 as an example, the camera-function limiting signal will be described in detail.

20 **[0037]** Referring to Fig. 4A, the short-range radio station 2 broadcasts the camera-function limiting signal. The mobile communication terminals 2a and 2b within the radio zone 100 can receive the broadcast camera-function limiting signal. However, the mobile communication terminal 2c out of the radio zone 100 cannot substantially receive it. Accordingly, for only the mobile communication terminals 2a and 2b within the radio zone 100, camera functions designated by the received camera-function limiting signal are inhibited from operation.

30 **[0038]** As shown in Fig. 4B, the camera-function limiting signal is typically a packet composed of a header and a payload including a plurality of camera-function control flags. For example, the camera-function control flags include an image pickup inhibition flag IF, an auto-focusing/zooming inhibition flag AZ, a strobe inhibition flag ST, a shutter-sound inhibition flag SS, a display/TV (video telephone) inhibition flag DSPL and, if necessary, other operation inhibition flags. In this example, the camera-function control flags are initially reset to 0s.

35 **[0039]** An example of the camera-function control flags is shown in Fig. 4C. In this example, the control flags are set to IP=0, AZ=1, ST=1, SS=1 and DSPL=0, where 1 indicates inhibition and 0 indicates permission. Therefore, the auto-focusing/zooming function, the strobe function and the shutter-sound generating function are all inhibited and the image pickup function and the display/TV (video telephone) function are permitted. In this manner, by selectively setting the camera-function control flags to 1, an arbitrary one or any combination of the camera functions can be inhibited.

40 **[0040]** Alternatively, different codes each identifying predetermined camera functions may be written into the payload of the packet. In this case, the signal decoder 29 outputs camera-function control flags set to 1 corresponding to codes written in the payload.

Operation limitation mode

[0041] As described above, the operation limitation mode in the mobile communication terminal 2 includes the following inhibition modes:

- Inhibition of all camera functions: image capturing of the image pickup device unit 21 and image displaying of the display device are fully inhibited. At places such as crowded public trains, museums or research laboratories, for example, all camera functions including photography and video shoot should be inhibited from use. In the above example, such a complete inhibition mode is active when all the camera-function control flags are set to 1s.
- Inhibition of auto-focussing and zooming functions:

lens movement of the lens unit 22 for focusing and zooming up/down is inhibited. At public places where zoom-up shooting is not appropriate, for example, the auto-focussing and zooming functions should be inhibited from use. In the above example, such an auto-focus/zoom inhibition mode is active when the auto-focusing/zooming inhibition flag AZ is set to 1.

- Inhibition of strobe function: flashing of the strobe device 23 is inhibited. At places such as museums, movie theaters or zoological gardens where the taking of photographs using a strobe light is forbidden or inappropriate, for example, the strobe function should be inhibited from use. In the above example, such a strobe inhibition mode is active when the strobe inhibition flag ST is set to 1.
- Inhibition of shutter-sound generating function:

shutter-sound generation of the shutter-sound generator 24 is inhibited. In the above example, such a shutter-sound inhibition mode is active when the shutter-sound inhibition flag SS is set to 1.

- Inhibition of display/TV (video telephone) function: image displaying control of the display controller 25 is inhibited. At places such as museums or movie theaters, for example, the display/TV (video telephone) function should be inhibited from use. In the above example, such a video telephone inhibition mode is active when display/TV (video telephone) inhibition flag DSPL is set to 1.

Camera-function limiting operation

[0042] As described above, when the short-range radio receiver 30 has received the camera-function limiting signal from the short-range radio station 1, the signal decoder 29 decodes the received camera-function limiting signal to output the camera-Function control flags

as shown in Fig. 4B to the camera function controller 28.

[0043] As shown in Fig. 5, the camera function controller 28 determines whether the camera-function control signal has been received (step S101). When having received the camera-function control flags from the signal decoder 29 (YES in step S101), the camera function controller 28 checks the camera-function control flags to set corresponding limitation modes as described before (steps S102 and S103-S107).

[0044] More specifically, when the image pickup inhibition flag IP = 1, the camera function controller 28 inhibits the image pickup device unit 21 from capturing images (step S103). When the auto-focusing/zooming inhibition flag AZ = 1, the camera function controller 28 inhibits the lens unit 22 from auto-focusing and zooming (step S104). When the strobe inhibition flag ST = 1, the camera function controller 28 inhibits the strobe device 23 from flashing (step S105). When the shutter-sound inhibition flag SS = 1, the camera function controller 28 inhibits the shutter-sound generator 24 from shutter-sound generation (step S106). When the display/TV (video telephone) inhibition flag DSPL = 1, the camera function controller 28 inhibits the display controller 25 from image/video displaying (step S107).

[0045] In this manner, the camera function controller 28 repeatedly performs the steps S101-S107 at regular intervals as long as the camera-function control signal is received. When the mobile communication terminal leaves the operation-limitation radio zone 100 and thereby no camera-function control signal is received (NO in step S101), the camera function controller 28 resets all the camera-function control flags to 0 and returns to the normal operation (step S108).

35 2. Second embodiment

[0046] As described above, a mobile communication terminal 2 can be set to a designated operation limitation state depending on the camera-function limiting signal received from the short-range radio station 1. In addition, a mobile communication terminal 2 according to a second embodiment of the present invention also has a limitation releasing function of selectively releasing the limitations of designated operations depending on whether an emergency communication is needed. The camera-function limiting signal broadcast by the short-range radio station 1 may be set so that such a limitation releasing function is permitted.

[0047] As shown in Fig. 6, the mobile communication terminal 2 according to the second embodiment is further provided with an emergency communication detector 272 in the mobile communication system 27. Blocks similar to those previously described with reference to Fig. 3 are denoted by the same reference numerals and descriptions of the similar blocks will be omitted.

[0048] The emergency communication detector 272 determines whether an emergency communication is requested by a user operating a ten-key of the operation

section 26. For example, when the user makes an emergency call such as a 911/999 call, the emergency communication detector 272 detects such an emergency communication request and notifies the camera-function controller 28 of occurrence of emergency. In response to the occurrence of emergency, the camera-function controller 28, even in the case of operation limitation mode, sets the current operation limitation mode to a predetermined emergency operation mode. Even when all camera functions have been inhibited, one or more predetermined camera function can be made active by resetting corresponding operation control flags to 0. For example, when all of IP, AZ, ST, SS and DSPL are 1s, the camera-function controller 28, when detecting an emergency, resets the image pickup control flag IP and the display/TV (video telephone) operation control flag DSPL to 0s to permit the use of TV telephone function.

[0049] The emergency operation mode preferably enables at least a TV (video) telephone function from the viewpoint of the amount of information necessary for emergency communication. One or more camera functions other than the TV (video telephone) telephone function, for example, a photograph shooting function, may be selectively made active.

[0050] Referring to Fig. 7, the camera function controller 28 determines whether an emergency communication is detected (step S201). When having detected the emergency communication (YES in step S201), the camera function controller 28 resets predetermined operation control flags to 0 so that the current operation mode is changed to the emergency operation mode (step S202). When no emergency communication is detected (NO in step S201), the above-described steps S101-S108 are performed.

3. Third embodiment

[0051] A mobile communication terminal 2 according to a third embodiment of the present invention also has a limitation releasing function of selectively releasing the limitations of designated operations depending on whether a captured face matches a previously registered face. The camera-function limiting signal broadcast by the short-range radio station 1 may be set so that such a limitation releasing function is permitted.

[0052] As shown in Fig. 8, the mobile communication terminal 2 according to the third embodiment is further provided with a face recognizer 31 and a face image database 32. Blocks similar to those previously described with reference to Fig. 3 are denoted by the same reference numerals and descriptions of the similar blocks will be omitted.

[0053] The face image database 32 stores face image data of authorized users. The face images are captured through the camera function of the mobile communication terminal 2 and the captured face image data are registered into the face image database 32 through the

face recognizer 31. When a user wishes to use a specific camera function (e.g. TV telephone function), the face of the user is captured by the camera function and the face recognizer 31 determines whether the captured face matches one of the registered faces. When a match is found, the camera function controller 28 makes the TV telephone function active even in the case of the display/TV (video telephone) function inhibition.

[0054] In Fig. 9, the camera function controller 28 performs operation limitation controls as described in the steps S101-S107 of Fig. 5. In the case where the limitation mode settings have been completed, the face recognizer 31 determines whether the captured face matches one of the registered faces (step S301). If no match is found (NO in step S301), the steps S101-S107 are repeatedly performed as described before. If a match is found (YES in step S301), the face recognizer 31 notifies the camera function controller 28 that the present user is an authorized user. The camera function controller 28, even in the case of the display/TV (video telephone) function inhibition, resets the display/TV (video telephone) control flag DSPL to 0 to permit the authorized user to use the TV telephone function (step S302).

4. Fourth embodiment

[0055] A mobile communication terminal 2 according to a fourth embodiment of the present invention also has a limitation releasing function of selectively releasing the limitations of designated operations depending on whether an emergency communication is needed or whether a captured face matches a previously registered face. The camera-function limiting signal broadcast by the short-range radio station 1 may be set so that such a limitation releasing function is permitted.

[0056] As shown in Fig. 10, the mobile communication terminal 2 according to the third embodiment is further provided with an emergency communication detector 272 in the mobile communication system 27, a face recognizer 31, and a face image database 32. Blocks similar to those previously described with reference to Fig. 3 are denoted by the same reference numerals and descriptions of the similar blocks will be omitted.

[0057] It is assumed that the camera-function limiting signal broadcast by the short-range radio station 1 is set so that, even in the case of display/TV (video telephone) function inhibition, the TV telephone function is permitted when an emergency occurs or when the face of an authorized user is transmitted to the other party. In this case, even when all of AZ, ST, SS and DSPL are 1s, the camera-function controller 28, when detecting an emergency or when the captured face matches one of the registered faces, resets the display/TV (video telephone) inhibition flag DSPL to 0 to permit the use of TV telephone function. Since the detailed operations of the fourth embodiment are similar to those described in the second and third embodiments, the detailed descrip-

tions are omitted.

5. Fifth embodiment

System configuration

[0058] In the above first to fourth embodiments, an operation limited geographical area is determined by the radio propagation of the camera-function limiting signal from the short-range radio station 1. However, the present invention is not limited to these embodiments. According to a fifth embodiment of the present invention, positioning information obtained from GPS (Global Positioning System) satellites are used to determine the location of a mobile communication terminal 2, thereby determining whether the mobile communication terminal 2 is located in a predetermined operation limited geographical area where the camera functions of a camera-equipped mobile communication terminal are selectively inhibited from use.

[0059] Referring to Fig. 11, an operation limiting system according to the fifth embodiment is provided with four or more GPS satellites and a plurality of camera-equipped mobile communication terminals, each of which is provided with a GPS receiver and a location calculator. Further, each of the mobile communication terminals stores operation-limitation area information, which is used to determine whether the mobile communication terminal 2 is located in an operation limitation area. Here, it is assumed for the sake of simplicity that an operation-limitation area 100x is previously set in each mobile communication terminal and a plurality of mobile communication terminals (here, 200a and 200b) are located within the operation-limitation area 100x and a mobile communication terminal 200c is located out of the operation-limitation area 100x. As described later, the mobile communication terminals 200a and 200b within the operation-limitation area 100x are inhibited from operating the designated camera-related functions and the mobile communication terminal 200c out of the operation-limitation area 100x is not inhibited. Since the operation-limitation area 100x is determined by location information such as latitude and longitude, its size has no upper limit but a lower limit determined by the positioning resolution of the GPS system.

[0060] In the case where a mobile communication terminal is located inside a building or the like and thereby cannot receive GPS positioning signals, a relay station for GPS positioning may be installed in a building so that mobile communication terminals inside the building can receive GPS location data through the mobile communication channel.

Mobile communication terminal

[0061] Each of the mobile communication terminals (here, 200a-200c) has the same function block structure. Hereinafter, for simplicity, each mobile communi-

cation terminal is referred to as a mobile communication terminal 200.

[0062] As shown in Fig. 12, the mobile communication terminal 200 is provided with a camera section composed of an image pickup device unit 21, a lens unit 22, and a strobe device 23. The image pickup device unit 21 includes an image sensor such as CCD sensor, CMOS sensor or the like, which may be used for video and photograph shooting. The lens unit 22 includes a set of lenses allowing focusing and zooming. The strobe device 23 emits a strobe light when photo-shooting. A shutter-sound generator 24 generates a shutter sound when shooting so as to avoid stealing a camera shot. A display controller 25 controls a display such as a liquid crystal display device (LCD), which is usually provided on a main body of the terminal 200.

[0063] The mobile communication terminal 200 is further provided with an operation section 26 such as a keypad to enter data or instructions. A mobile communication system 27 including a radio communication controller 271 is provided to perform predetermined mobile communication operations.

[0064] A camera function controller 28, which may be implemented in a program-controlled processor (not shown), controls the above-described camera section, the shutter-sound generator 24 and the display controller 25 depending on whether the mobile communication terminal 200 is located in a predetermined operation limitation area, which will be described later. The camera function controller 28 controls the camera section to capture still/video images, which are output as an image signal to the mobile communication system 27. The captured image can be superimposed on another image received from the other party and the combined image is displayed on the display device (not shown).

[0065] The mobile communication terminal 200 is further provided with a GPS positioning section 41 composed of a GPS receiver 41a and a location information calculator 41b, an operation limitation data memory 42, an operation limited area memory 43, and an area decision section 44.

[0066] The GPS receiver 41a receives positioning information from the GPS satellites to output it to the location information calculator 41b. The location information calculator 41b calculates location information of the mobile communication terminal 200 from the positioning information to output it to the area decision section 44.

[0067] The operation limitation data memory 42 stores operation-limitation data including camera function control flags for each operation limited area. The operation limited area memory 43 stores location data (e. g. latitude and longitude) of each operation limited area. Since the operation-limitation data are associated with each of the operation limited areas, the operation limitation data memory 42 and the operation limited area memory 43 may be combined to a single memory.

[0068] The area decision section 44, when receiving the location information from the location information

calculator 41b, searches the operation limited area memory 43 for an operation limited area in which the mobile communication terminal 200 is now located. A found operation limited area is output to the camera function controller 28. The camera function controller 28 searches the operation limitation data memory 42 for camera function control flags corresponding to the found operation limited area. As described later, the camera function controller 28 selectively inhibits the camera functions including image pickup, focusing/zooming, flashing, shutter-sound generating, and the likes, depending on the camera function control flags.

[0069] As described before, in the case where the operation limitation data memory 42 and the operation limited area memory 43 may be combined to a single memory, the area decision section 44 is incorporated in the camera function controller 28.

[0070] Referring to Fig. 13, a combined memory of the operation limitation data memory 42 and the operation limited area memory 43 contains camera function control flags (IP, AZ, ST, SS, DSPL) for each of operation limited areas (A1, A2, ...).

[0071] As shown in Fig. 13, the camera-function control flags include an image pickup inhibition flag IP, an auto-focusing/zooming inhibition flag AZ, a strobe inhibition flag ST, a shutter-sound inhibition flag SS, a display/TV (video telephone) inhibition flag DSPL and, if necessary, other operation inhibition flags.

[0072] In this example, the operation limited area A1 is set to IP=1, AZ=1, ST=1, SS=1 and DSPL=1, where 1 indicates inhibition and 0 indicates permission. Therefore, all camera functions: the image pickup function, the auto-focusing/zooming function, the strobe function, the shutter-sound generating function and the display/TV (video telephone) function, are inhibited. In contrast, the operation limited area A2 is set to IP=0, AZ=1, ST=1, SS=0 and DSPL=0. Therefore, although the auto-focusing/zooming function and the strobe function are both inhibited, the image pickup function, the shutter-sound generating function and the display/TV (video telephone) function are permitted. In this manner, by selectively setting the camera-function control flags to 1 for each operation limited area, an arbitrary one or any combination of the camera functions can be inhibited in each operation limited area.

Operation limitation mode

[0073] As described above, the operation limitation mode in the mobile communication terminal 200 includes the following inhibition modes:

- Inhibition of all camera functions: image capturing of the image pickup device unit 21 and image displaying of the display device are entirely inhibited. At places such as crowded public trains, museums or research laboratories, for example, all camera functions including photography and video shoot

should be inhibited from use. In the above example, such a complete inhibition mode is active when all the camera-function control flags are set to 1s.

- Inhibition of auto-focussing and zooming functions:

lens movement of the lens unit 22 for focusing and zooming up/down is inhibited. At public places where zoom-up shooting is not appropriate, for example, the auto-focussing and zooming functions should be inhibited from use. In the above example, such an auto-focus/zoom inhibition mode is active when the auto-focusing/zooming inhibition flag AZ is set to 1.

- Inhibition of strobe function: flashing of the strobe device 23 is inhibited. At places such as museums, movie theaters or zoological gardens where the taking of photographs using a strobe light is forbidden or inappropriate, for example, the strobe function should be inhibited from use. In the above example, such a strobe inhibition mode is active when the strobe inhibition flag ST is set to 1.

- Inhibition of shutter-sound generating function:

shutter-sound generation of the shutter-sound generator 24 is inhibited. In the above example, such a shutter-sound inhibition mode is active when the shutter-sound inhibition flag SS is set to 1.

- Inhibition of display/TV (video) function: image displaying control of the display controller 25 is inhibited. At places such as museums or movie theaters, for example, the display/TV(video) function should be inhibited from use. In the above example, such a display/TV (video telephone) inhibition mode is active when display/TV (video telephone) inhibition flag DSPL is set to 1.

Camera-function limiting operation

[0074] It is assumed that the operation limitation data memory 42 and the operation limited area memory 43 are combined to a single memory as shown in Fig. 13 and the area decision section 44. is incorporated in the camera function controller 28.

[0075] As shown in Fig. 14, the camera function controller 28 inputs location information from the location information calculator 41b (step S401). Thereafter, the camera function controller 28 searches the combined memory as shown in Fig. 13 for an operation limited area in which the location information is included (step S402). When a match is found, that is, the mobile communication terminal 200 is located in an operation limited area (YES in step S402), the camera function controller 28 reads camera function control flags corresponding to the found operation limited area and checks the camera function control flags to set corresponding limitation

modes as described before (steps S102 and S103-S107).

[0076] More specifically, when the image pickup inhibition flag IP = 1, the camera function controller 28 inhibits the image pickup device unit 21 from capturing images (step S103). When the auto-focusing/zooming inhibition flag AZ = 1, the camera function controller 28 inhibits the lens unit 22 from auto-focusing and zooming (step S104). When the strobe inhibition flag ST = 1, the camera function controller 28 inhibits the strobe device 23 from flashing (step S105). When the shutter-sound inhibition flag SS = 1, the camera function controller 28 inhibits the shutter-sound generator 24 from shutter-sound generation (step S106). When the display/TV (video telephone) inhibition flag DSPL = 1, the camera function controller 28 inhibits the display controller 25 from image/video displaying (step S107).

[0077] When it is determined that the location information gets out of an operation limited area, that is, the mobile communication terminal 200 leaves the operation limited area (NO in step S402), the camera function controller 28 resets all the camera-function control flags to 0 and returns to the normal operation (step S403). In this manner, the camera function controller 28 repeatedly performs the steps S401, S401 and S102-S107 at regular intervals.

6. Sixth embodiment

[0078] As described above, a mobile communication terminal 200 can be set to a designated operation limitation state depending on whether the location obtained by the GPS system falls into an operation limitation area stored in the operation limited area memory 43. In addition, a mobile communication terminal 200 according to a sixth embodiment of the present invention also has a limitation releasing function of selectively releasing the limitations of designated operations depending on whether an emergency communication is needed.

[0079] As shown in Fig. 15, the mobile communication terminal 200 according to the sixth embodiment is further provided with an emergency communication detector 272 in the mobile communication system 27. Blocks similar to those previously described with reference to Fig. 12 are denoted by the same reference numerals and descriptions of the similar blocks will be omitted.

[0080] The emergency communication detector 272 determines whether an emergency communication is requested by a user operating a ten-key of the operation section 26. For example, when the user makes an emergency call such as a 911/999 call, the emergency communication detector 272 detects such an emergency communication request and notifies the camera-function controller 28 of occurrence of emergency. In response to the occurrence of emergency, the camera-function controller 28, even in the case of operation limitation mode, sets the current operation limitation mode to a predetermined emergency operation mode. Even

when all camera functions have been inhibited, one or more predetermined camera function is made active by resetting corresponding operation control flags to 0. For example, when all of IP, AZ, ST, SS and DSPL are 1s, the camera-function controller 28, when detecting an emergency, resets the image pickup control flag IP and the display/TV (video telephone) operation control flag DSPL to 0s to permit the use of TV telephone function.

[0081] The emergency operation mode preferably enables at least a TV (video) telephone function from the viewpoint of the amount of information necessary for emergency communication. One or more camera functions other than the TV (video) telephone function, for example, a photograph shooting function, may be selectively made active.

[0082] An operation limitation releasing control of the sixth embodiment is basically similar to that of the second embodiment as shown in Fig. 7. As shown in Fig. 7, the camera function controller 28 determines whether an emergency communication is detected (step S201). When having detected the emergency communication (YES in step S201), the camera function controller 28 resets predetermined operation control flags to 0 so that the current operation mode is changed to the emergency operation mode (step S202). When no emergency communication is detected (NO in step S201), the above-described steps S101-S108 are performed.

7. Seventh embodiment

[0083] A mobile communication terminal 200 according to a seventh embodiment of the present invention also has a limitation releasing function of selectively releasing the limitations of designated operations depending on whether a captured face matches a previously registered face.

[0084] As shown in Fig. 16, the mobile communication terminal 200 according to the seventh embodiment is further provided with a face recognizer 31 and a face image database 32. Blocks similar to those previously described with reference to Fig. 12 are denoted by the same reference numerals and descriptions of the similar blocks will be omitted.

[0085] The face image database 32 stores face image data of authorized users. The face images are captured through the camera function of the mobile communication terminal 2 and the captured face image data are registered into the face image database 32 through the face recognizer 31. When a user wishes to use a specific camera function (e.g. TV telephone function), the face of the user is captured by the camera function and the face recognizer 31 determines whether the captured face matches one of the registered faces. When a match is found, the camera function controller 28 makes the TV telephone function active even in the case of the display/TV function inhibition.

[0086] An operation limitation releasing control of the seventh embodiment is basically similar to that of the

third embodiment as shown in Fig. 9. As shown in Fig. 9, the camera function controller 28 performs operation limitation controls as described in the steps S101-S108. In the case where the limitation mode settings have been completed, the face recognizer 31 determines whether the captured face matches one of the registered faces. If no match is found, the steps S101-S108 are repeatedly performed as described before. If a match is found, the face recognizer 31 notifies the camera function controller 28 that the present user is an authorized user. The camera function controller 28, even in the case of the display/TV function inhibition, resets the display/TV (video telephone) inhibition flag DSPL to 0 to permit the authorized user to use the TV telephone function.

8. Eighth embodiment

[0087] A mobile communication terminal 200 according to an eighth embodiment of the present invention also has a limitation releasing function of selectively releasing the limitations of designated operations depending on whether an emergency communication is needed or whether a captured face matches a previously registered face.

[0088] As shown in Fig. 17, the mobile communication terminal 200 according to the eighth embodiment is further provided with an emergency communication detector 272 in the mobile communication system 27, a face recognizer 31, and a face image database 32. Blocks similar to those previously described with reference to Fig. 3 are denoted by the same reference numerals and descriptions of the similar blocks will be omitted.

[0089] As described above, even in the case of display/TV function inhibition, the TV telephone function is permitted when an emergency occurs or when the face of an authorized user is transmitted to the other party. More specifically, even when all of AZ, ST, SS and DSPL are 1s, the camera-function controller 28, when detecting an emergency or when the captured face matches one of the registered faces, resets the display/TV (video telephone) inhibition flag DSPL to 0 to permit the use of TV telephone function. Since the detailed operations of the eighth embodiment are similar to those described in the sixth and seventh embodiments, the detailed descriptions are omitted.

9. Ninth embodiment

[0090] As shown in Fig. 18, the first to fourth embodiments of the present invention can be applied to a mobile telephone terminal having a video-telephone function. Blocks similar to those previously described with reference to Fig. 3 are denoted by the same reference numerals and descriptions of the similar blocks will be omitted.

[0091] The mobile telephone terminal according to a ninth embodiment of the present invention is provided

with a radio-frequency (RF) system 501, a baseband processor 502, an audio CODEC 503, a speaker (telephone receiver), and a microphone (telephone transmitter), which are used for telephone conversation. The mobile telephone terminal is further provided with a sound generator 506 and a speaker 507, which can be used as the shutter-sound generator 24 under the control of a microprocessor 508.

[0092] The microprocessor 508 is a program-controlled processor, which executes at least one of control programs stored in a program memory 509 using a random access memory 513. The control programs include a mobile telephone controller 510, a camera function controller 511, a signal decoder 512 and other necessary programs.

[0093] The display controller 25 controls a LCD device 516 under control of the microprocessor 508. The lens unit 22, the image pickup device 21 and the strobe device 23 are controlled by a camera controller 514 under control of the microprocessor 508. Image data captured by the image pickup device 21 is processed by an image processor 515 under control of the microprocessor 508. The captured image data is displayed on the LCD device 516 and is transmitted to the party on the other end through the RF system 501 and the baseband processor 502.

[0094] The short-range radio receiver 30 receives a camera-function limiting signal from the short-range radio station 1 and the received camera-function limiting signal is decoded to produce camera-function control flags by the signal decoder 512 running on the microprocessor 508. According to the camera-function control flags, as described before, the camera function controller 511 inhibits designated camera functions.

[0095] In addition, as described in the second to fourth embodiments, an inhibited camera function (e.g. the video-telephone function) can be made active when an emergency occurs or when a captured face matches a registered face.

[0096] The fifth to eighth embodiments of the present invention can be also applied to a mobile telephone terminal having a video-telephone function. In this case, the mobile telephone terminal is equipped with the GPS receiver in place of the short-range radio receiver 30 of Fig. 18. Since the operation of the GPS-equipped mobile telephone terminal is similar to that of the fifth to eighth embodiments, the descriptions are omitted.

50 Claims

1. A system for limiting a plurality of camera functions in a mobile communication terminal (2, 200) equipped with a camera, comprising:

at least one operation-limited area (100, 100x),

wherein the mobile communication terminal is al-

lowed to determine whether the mobile communication terminal is located within an operation-limited area;

characterized by comprising:

a memory (12, 42, 43) storing camera-function limitation data for each of the at least one operation-limited area, the camera-function limitation data indicating selective inhibition of the plurality of camera functions; and
 a camera function controller (28) for selectively inhibiting the plurality of camera functions depending on camera-function limitation data corresponding to an operation-limited area in which the mobile communication terminal is located.

2. The system according to claim 1, wherein the camera function controller releases an inhibited camera function when a predetermined condition is satisfied.

3. The system according to claim 1, wherein each of the at least one operation-limited area is substantially defined by radio propagation of a camera-function limiting signal broadcast by a radio station (1) installed at a predetermined location, the camera-function limiting signal including the camera-function limitation data,

wherein the mobile communication terminal comprises a radio receiver for receiving the camera-function limiting signal from the radio station.

4. The system according to claim 3, further comprising:

an emergency communication detector (272) for detecting occurrence of an emergency communication to inform the camera function controller of the occurrence of the emergency communication,

wherein, when informed of the occurrence of the emergency communication in a case of inhibition of a predetermined camera function, the camera function controller releases the inhibition of the predetermined camera function.

5. The system according to claim 3, further comprising:

a face image memory (32) for previously registering a face image of each authorized user,

wherein, when an input image picked up by the camera matches a face image registered in the face image memory in a case of inhibition of a predetermined camera function, the camera function

controller releases the inhibition of the predetermined camera function.

6. The system according to claim 3, further comprising:

an emergency communication detector (272) for detecting occurrence of an emergency communication to inform the camera function controller of the occurrence of the emergency communication; and
 a face image memory (32) for previously registering a face image of each authorized user,

wherein, in one of cases where the camera function controller is informed of the occurrence of the emergency communication in a case of inhibition of a predetermined camera function and where an input image picked up by the camera matches a face image registered in the face image memory in a case of inhibition of the predetermined camera function, the camera function controller releases the inhibition of the predetermined camera function.

7. The system according to any of claims 4-6, wherein the predetermined camera function is a video telephone function.

8. The system according to claim 3, wherein the radio station broadcasts the camera-function limiting signal in a short-range radio communication scheme, which is different from a radio communication scheme of the mobile communication terminal.

9. The system according to claim 1, wherein each of the at least one operation-limited area is determined by the mobile communication terminal, wherein the mobile communication terminal comprises:

a location detector (41) for detecting a location of the mobile communication terminal;
 an operation-limited area memory (43) storing operation-limited area location data; and
 an area decision section (44) for searching the operation-limited area memory for a detected location of the mobile communication terminal to determine whether the mobile communication terminal is located within an operation-limited area.

10. The system according to claim 9, further comprising:

an emergency communication detector (272) for detecting occurrence of an emergency communication to inform the camera function controller of the occurrence of the emergency communication

munication,

wherein, when informed of the occurrence of the emergency communication in a case of inhibition of a predetermined camera function, the camera function controller releases the inhibition of the predetermined camera function.

11. The system according to claim 9, further comprising:

a face image memory (32) for previously registering a face image of each authorized user,

wherein, when an input image picked up by the camera matches a face image registered in the face image memory in a case of inhibition of a predetermined camera function, the camera function controller releases the inhibition of the predetermined camera function.

12. The system according to claim 9, further comprising:

an emergency communication detector (272) for detecting occurrence of an emergency communication to inform the camera function controller of the occurrence of the emergency communication; and

a face image memory (32) for previously registering a face image of each authorized user,

wherein, in one of cases where the camera function controller is informed of the occurrence of the emergency communication in a case of inhibition of a predetermined camera function and where an input image picked up by the camera matches a face image registered in the face image memory in a case of inhibition of the predetermined camera function, the camera function controller releases the inhibition of the predetermined camera function.

13. The system according to any of claims 10-12, wherein the predetermined camera function is a video telephone function.

14. The system according to claim 9, wherein the location detector is a GPS positioning section for receiving global positioning system (GPS) signals to detect the location of the mobile communication terminal.

15. The system according to claim 1, wherein the camera functions include image pickup function, auto-focusing and zooming function, strobe function, shutter-sound generating function, and video telephone function.

16. A method for limiting a plurality of camera functions in a mobile communication terminal equipped with a camera, comprising:

preparing at least one operation-limited area,

wherein the mobile communication terminal is allowed to determine whether the mobile communication terminal is located within an operation-limited area;

characterized by comprising:

storing camera-function limitation data for each of the at least one operation-limited area, the camera-function limitation data indicating selective inhibition of the plurality of camera functions; and

selectively inhibiting the plurality of camera functions depending on camera-function limitation data corresponding to an operation-limited area in which the mobile communication terminal is located.

17. The method according to claim 16, further comprising:

releasing an inhibited camera function when a predetermined condition is satisfied.

18. The method according to claim 16, wherein each of the at least one operation-limited area is substantially defined by the mobile communication terminal receiving a camera-function limiting signal from a radio station, the camera-function limiting signal including the camera-function limitation data.

19. The method according to claim 16, wherein each of the at least one operation-limited area is determined by the mobile communication terminal

detecting a location of the mobile communication terminal;

storing operation-limited area location data; and

searching the operation-limited area memory for a detected location of the mobile communication terminal to determine whether the mobile communication terminal is located within an operation-limited area.

20. A mobile communication terminal which is equipped with a camera and has a plurality of camera functions,

characterized by comprising:

a radio receiver (30) for receiving a camera-function limiting signal from a radio station installed at a predetermined location;

a signal decoder (29) for decoding the camera-

function limiting signal to produce camera-function limitation data indicating selective inhibition of the plurality of camera functions; and a camera function controller (28) for selectively inhibiting the plurality of camera functions depending on camera-function limitation data.

21. The mobile communication terminal according to claim 20, wherein the camera function controller releases an inhibited camera function when a predetermined condition is satisfied.

22. The mobile communication terminal according to claim 20, further comprising:

an emergency communication detector for detecting occurrence of an emergency communication to inform the camera function controller of the occurrence of the emergency communication,

wherein, when informed of the occurrence of the emergency communication in a case of inhibition of a predetermined camera function, the camera function controller releases the inhibition of the predetermined camera function.

23. The mobile communication terminal according to claim 20, further comprising:

a face image memory for previously registering a face image of each authorized user,

wherein, when an input image picked up by the camera matches a face image registered in the face image memory in a case of inhibition of a predetermined camera function, the camera function controller releases the inhibition of the predetermined camera function.

24. The mobile communication terminal according to claim 20, further comprising:

an emergency communication detector for detecting occurrence of an emergency communication to inform the camera function controller of the occurrence of the emergency communication; and

a face image memory for previously registering a face image of each authorized user,

wherein, in one of cases where the camera function controller is informed of the occurrence of the emergency communication in a case of inhibition of a predetermined camera function and where an input image picked up by the camera matches a face image registered in the face image memory in a case of inhibition of the predetermined camera

function, the camera function controller releases the inhibition of the predetermined camera function.

25. The mobile communication terminal according to any of claims 22-24, wherein the predetermined camera function is a video telephone function.

26. The mobile communication terminal according to claim 20, wherein the radio station transmits the camera-function limiting signal in a short-range radio communication scheme, which is different from a radio communication scheme of the mobile communication terminal.

27. A mobile communication terminal which is equipped with a camera and has a plurality of camera functions, comprising:

a location detector (41) for detecting a location of the mobile communication terminal;

characterized by comprising:

a memory (42, 43) storing camera-function limitation data for each of at least one operation-limited area,

wherein the camera-function limitation data indicates selective inhibition of the plurality of camera functions;

an area decision section (44) for searching the operation-limited area memory for a detected location of the mobile communication terminal to determine whether the mobile communication terminal is located within an operation-limited area; and

a camera function controller (28) for selectively inhibiting the plurality of camera functions depending on camera-function limitation data corresponding to a found operation-limited area.

28. The mobile communication terminal according to claim 27, wherein the camera function controller releases an inhibited camera function when a predetermined condition is satisfied.

29. The mobile communication terminal according to claim 27, further comprising:

an emergency communication detector for detecting occurrence of an emergency communication to inform the camera function controller of the occurrence of the emergency communication,

wherein, when informed of the occurrence of the emergency communication in a case of inhibition of a predetermined camera function, the camera function controller releases the inhibition of the

predetermined camera function.

- 30. The mobile communication terminal according to claim 27, further comprising:

5

- a face image memory for previously registering a face image of each authorized user,

- wherein, when an input image picked up by the camera matches a face image registered in the face image memory in a case of inhibition of a predetermined camera function, the camera function controller releases the inhibition of the predetermined camera function.

10

15

- 31. The mobile communication terminal according to claim 27, further comprising:

- an emergency communication detector for detecting occurrence of an emergency communication to inform the camera function controller of the occurrence of the emergency communication; and

20

- a face image memory for previously registering a face image of each authorized user,

25

- wherein, in one of cases where the camera function controller is informed of the occurrence of the emergency communication in a case of inhibition of a predetermined camera function and where an input image picked up by the camera matches a face image registered in the face image memory in a case of inhibition of the predetermined camera function, the camera function controller releases the inhibition of the predetermined camera function.

30

35

- 32. The mobile communication terminal according to any of claims 29-31, wherein the predetermined camera function is a video telephone function.

40

- 33. The mobile communication terminal according to claim 27, wherein the location detector is a GPS positioning section for receiving global positioning system (GPS) signals to detect the location of the mobile communication terminal.

45

50

55

FIG. 1

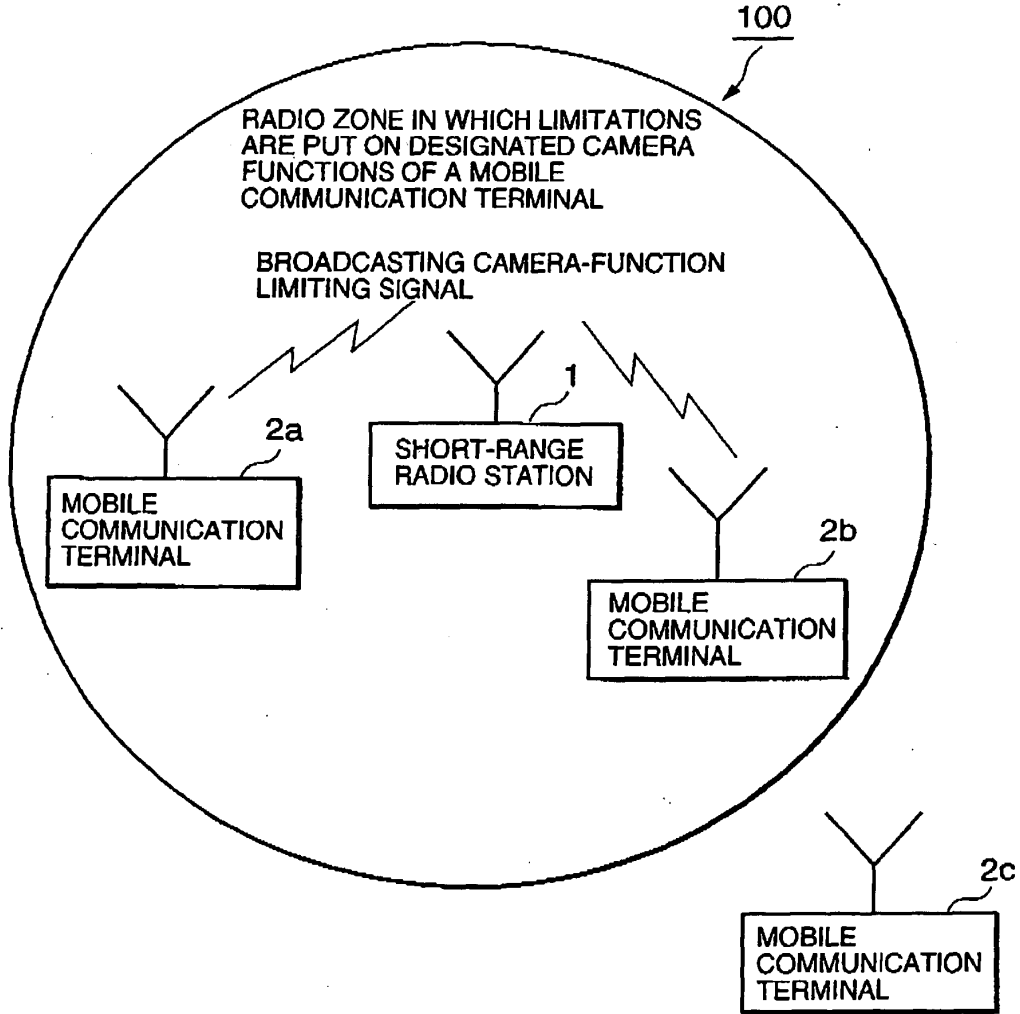


FIG. 2

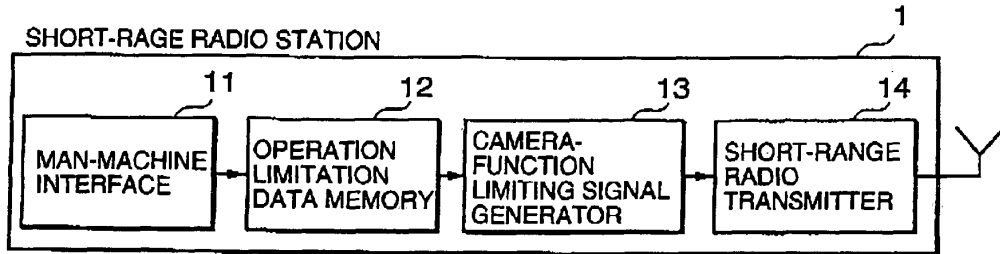


FIG. 3

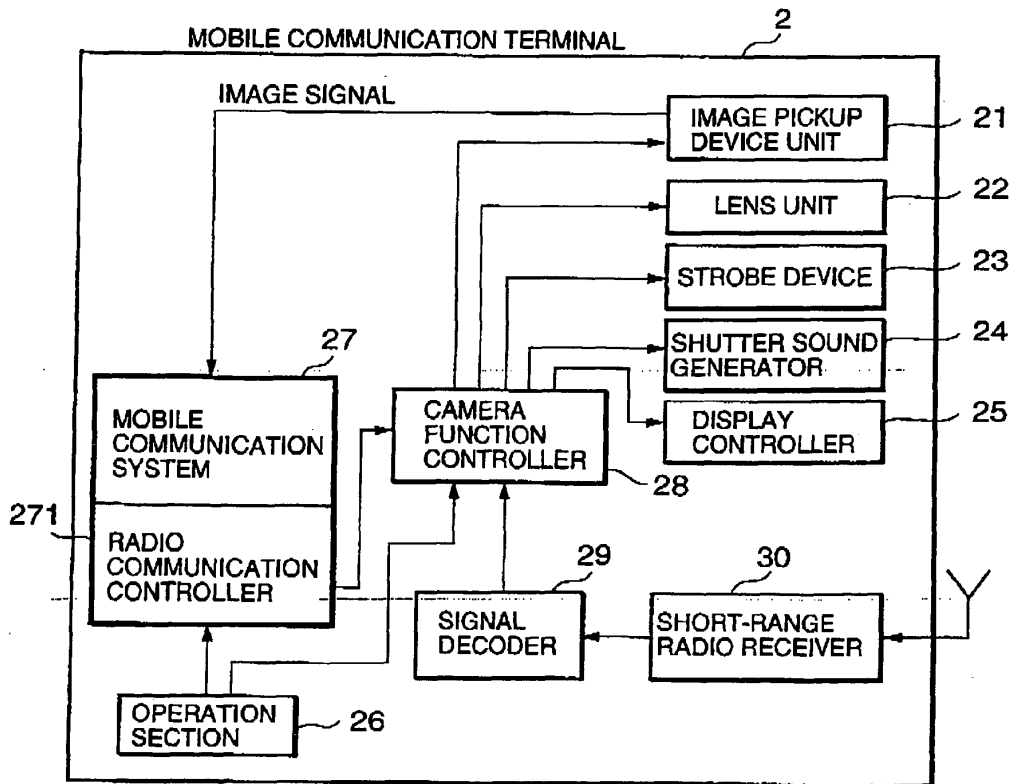


FIG. 4A

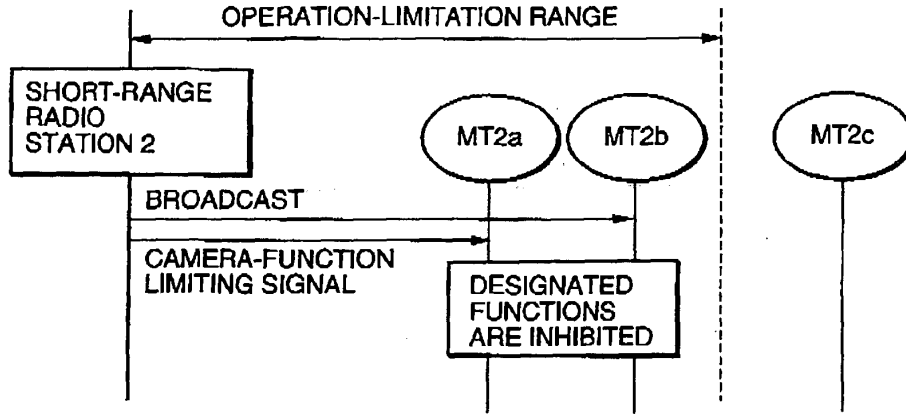


FIG. 4B

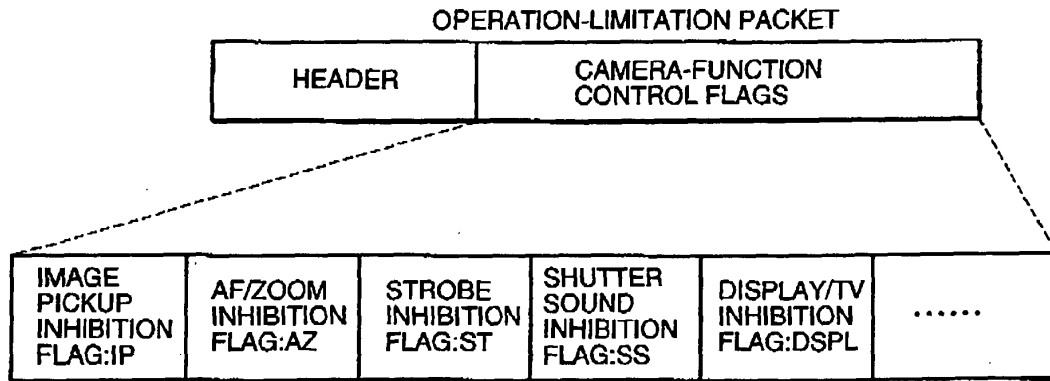


FIG. 4C

IP	AZ	ST	SS	DSPL
0	1	1	1	0

{ 1 : INHIBITED
0 : PERMITTED }

FIG. 5

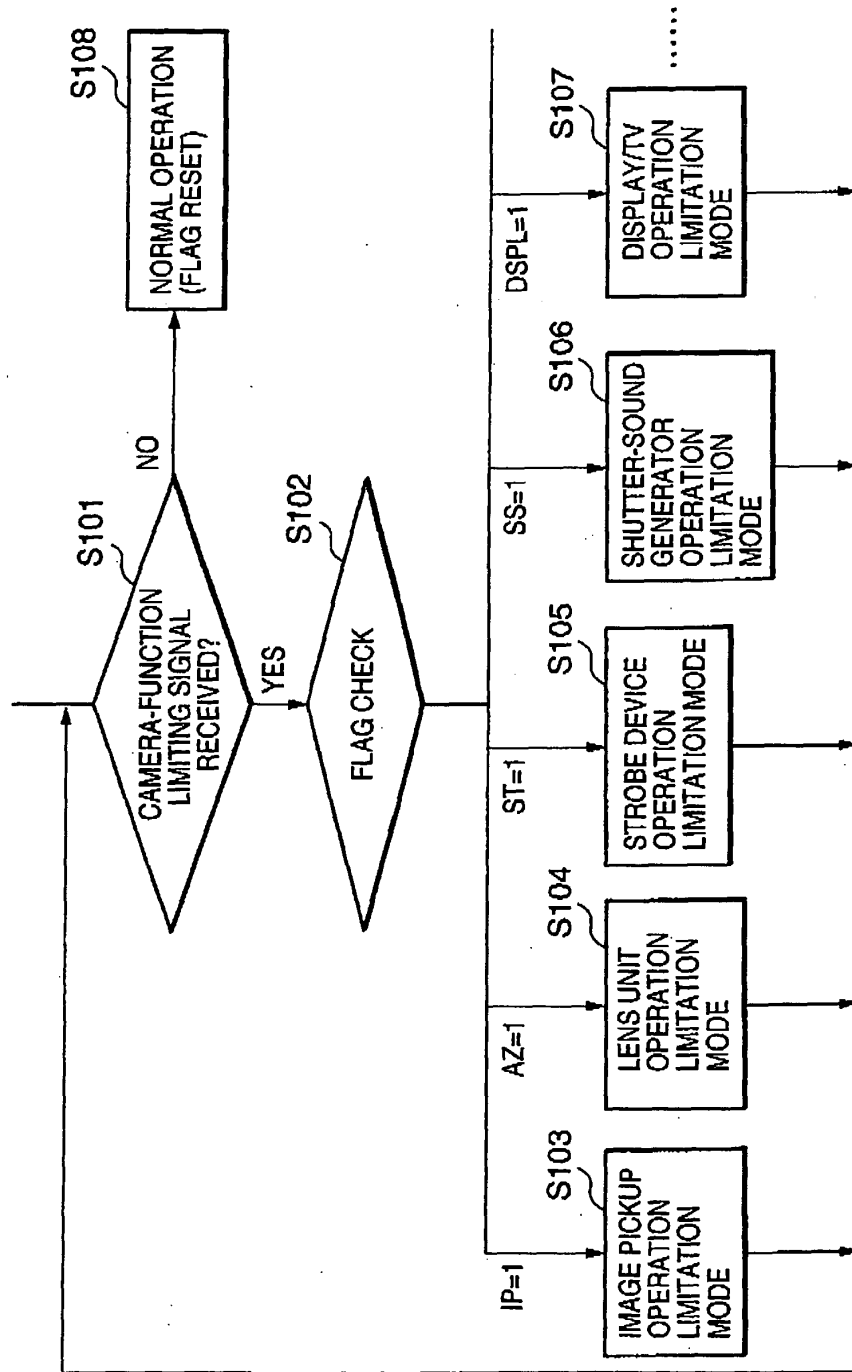


FIG. 6

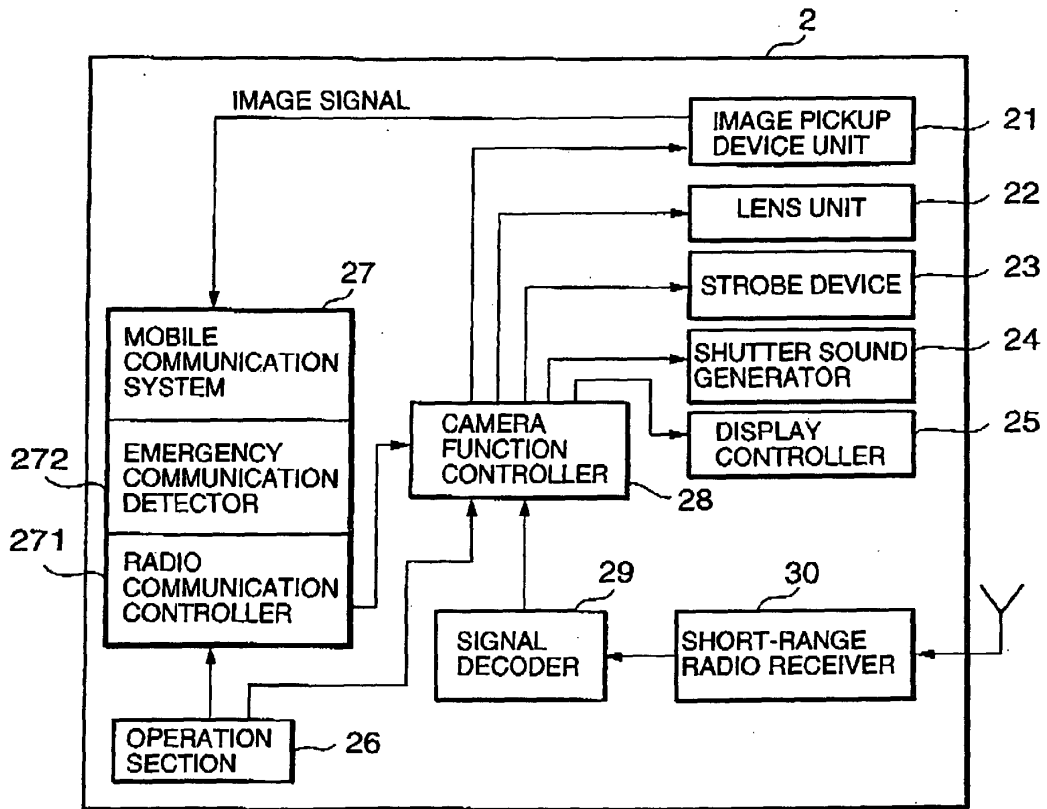


FIG. 7

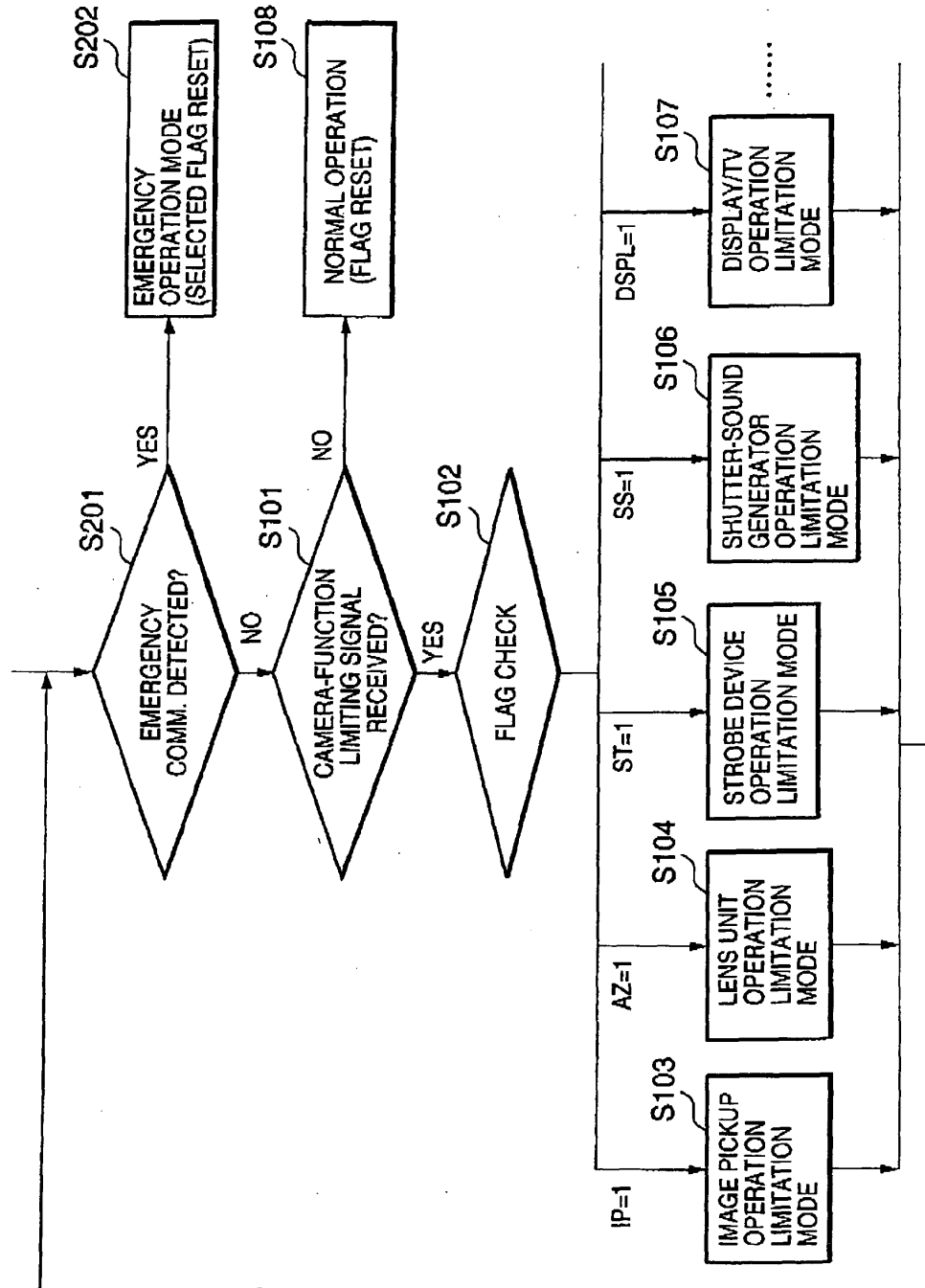


FIG. 8

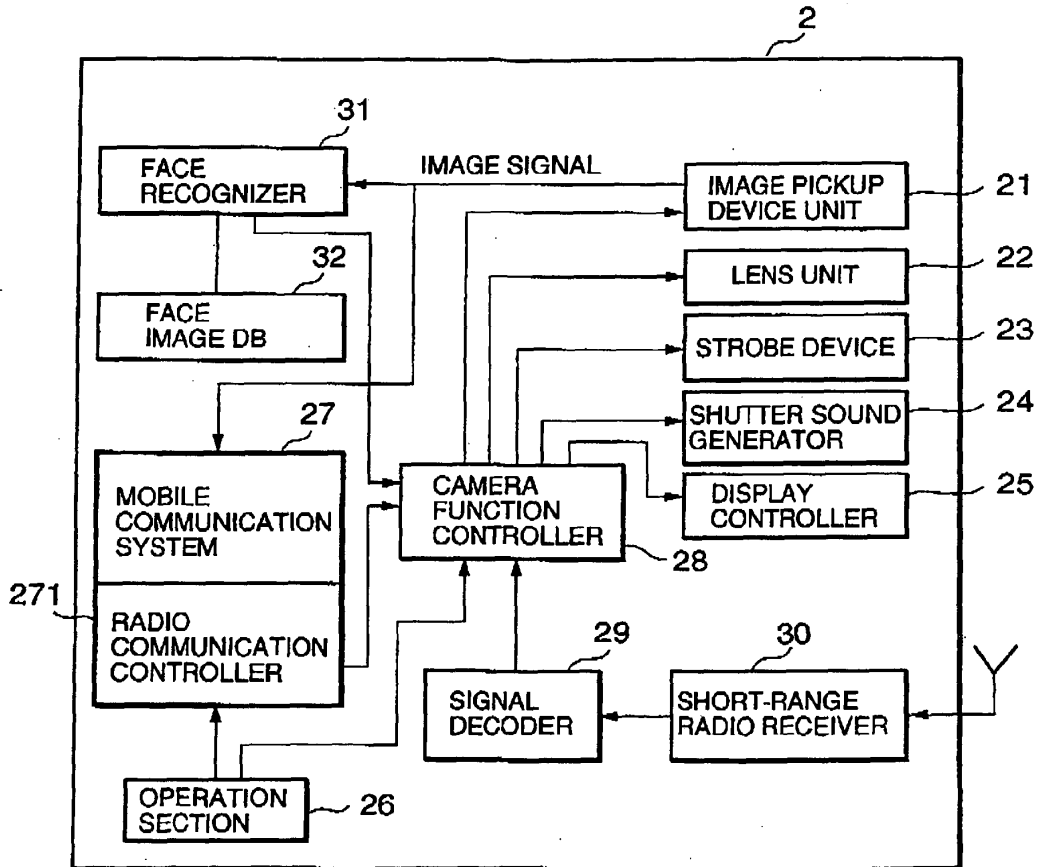


FIG. 9

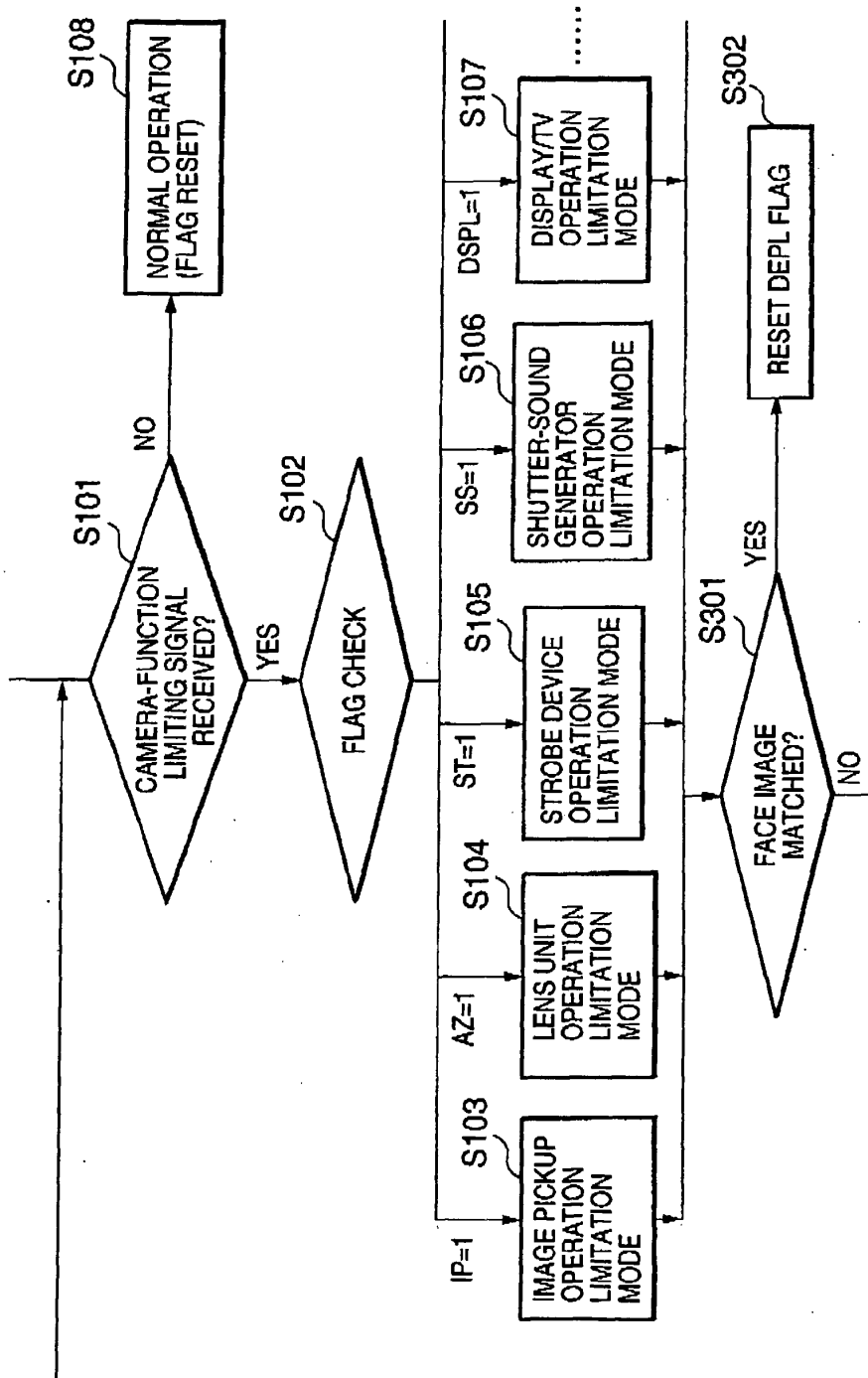


FIG. 10

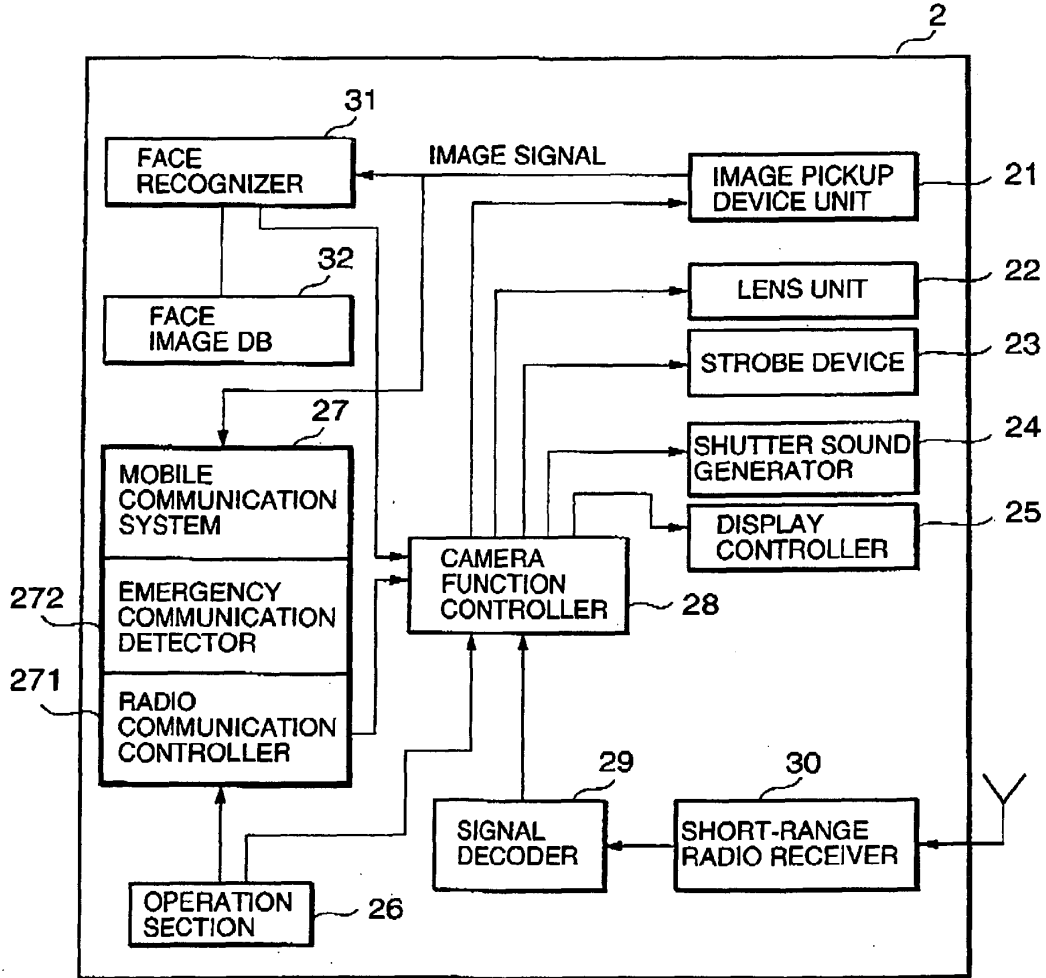


FIG. 11

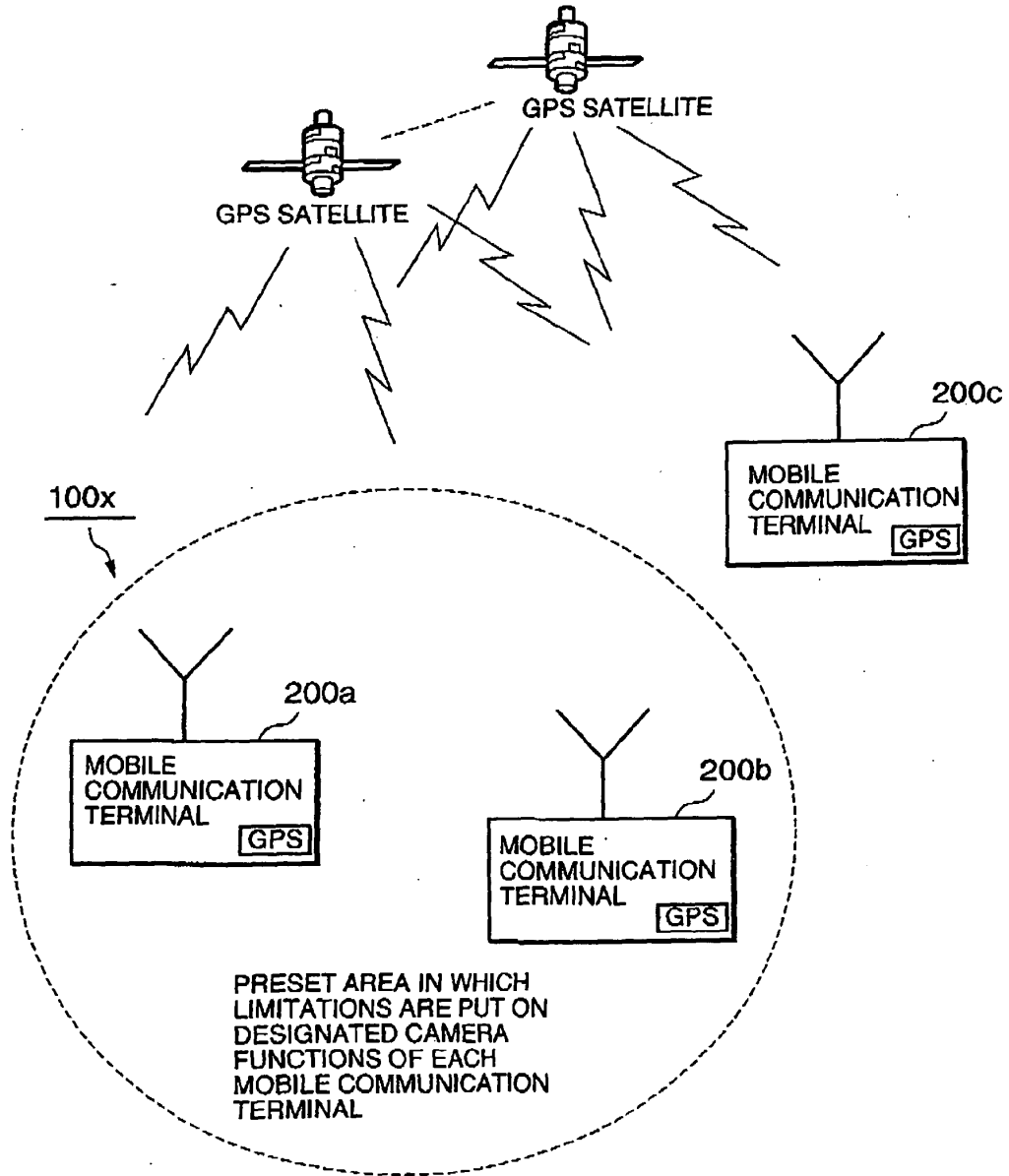


FIG. 12

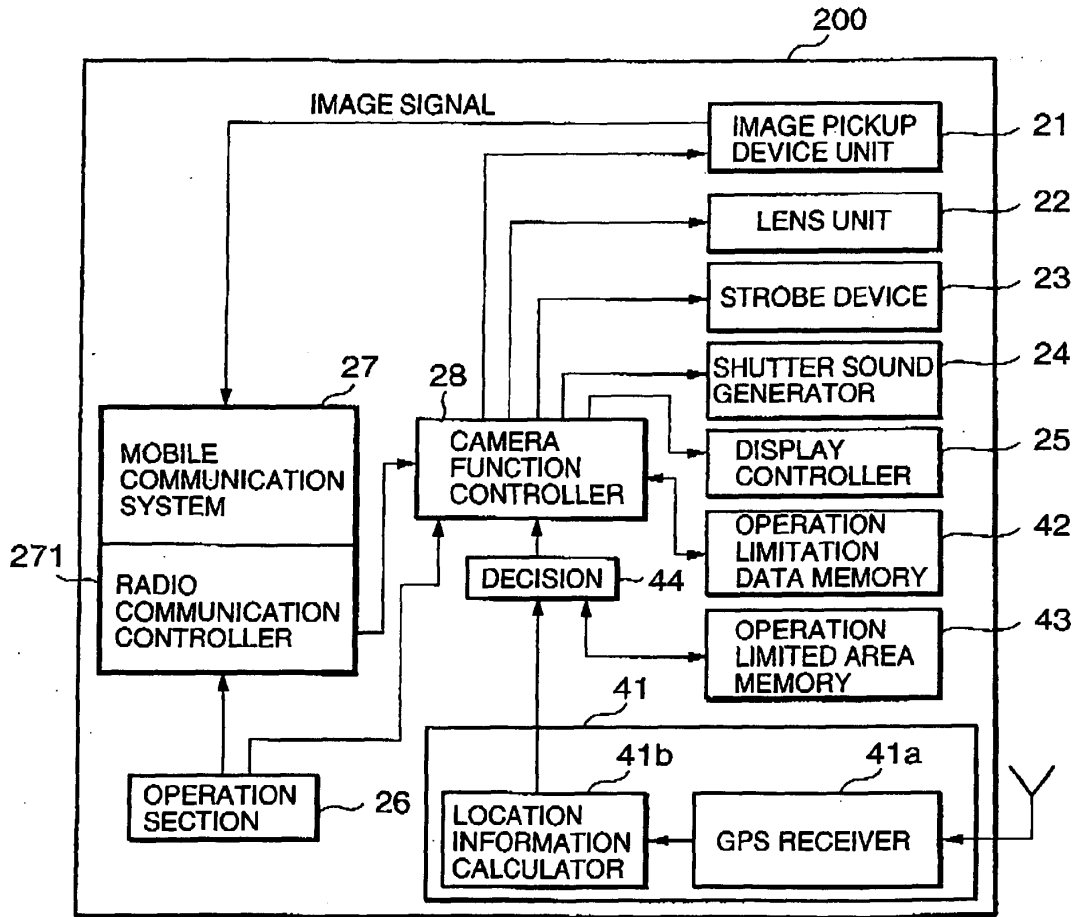


FIG. 13

42,43

OPERATION LIMITED AREA	IMAGE PICKUP INHIBITION (IP)	AF/ZOOM INHIBITION (AZ)	STROBE INHIBITION (ST)	SHUTTER SOUND INHIBITION (SS)	DISPLAY/TV INHIBITION (DSPL)
A ₁	1	1	1	1	1
A ₂	0	1	1	0	0
⋮	⋮	⋮	⋮	⋮	⋮

(1: INHIBITED
0: PERMITTED)

FIG. 14

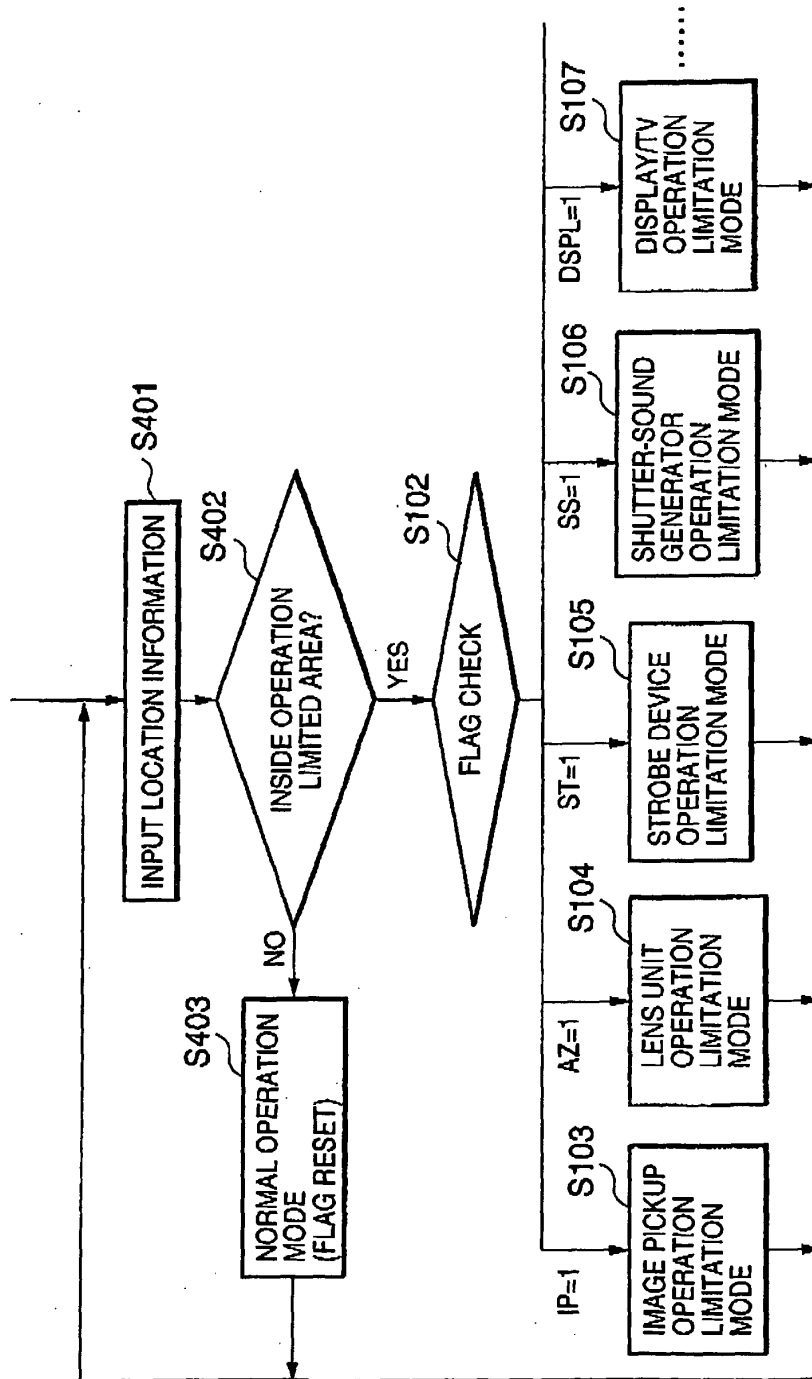


FIG. 15

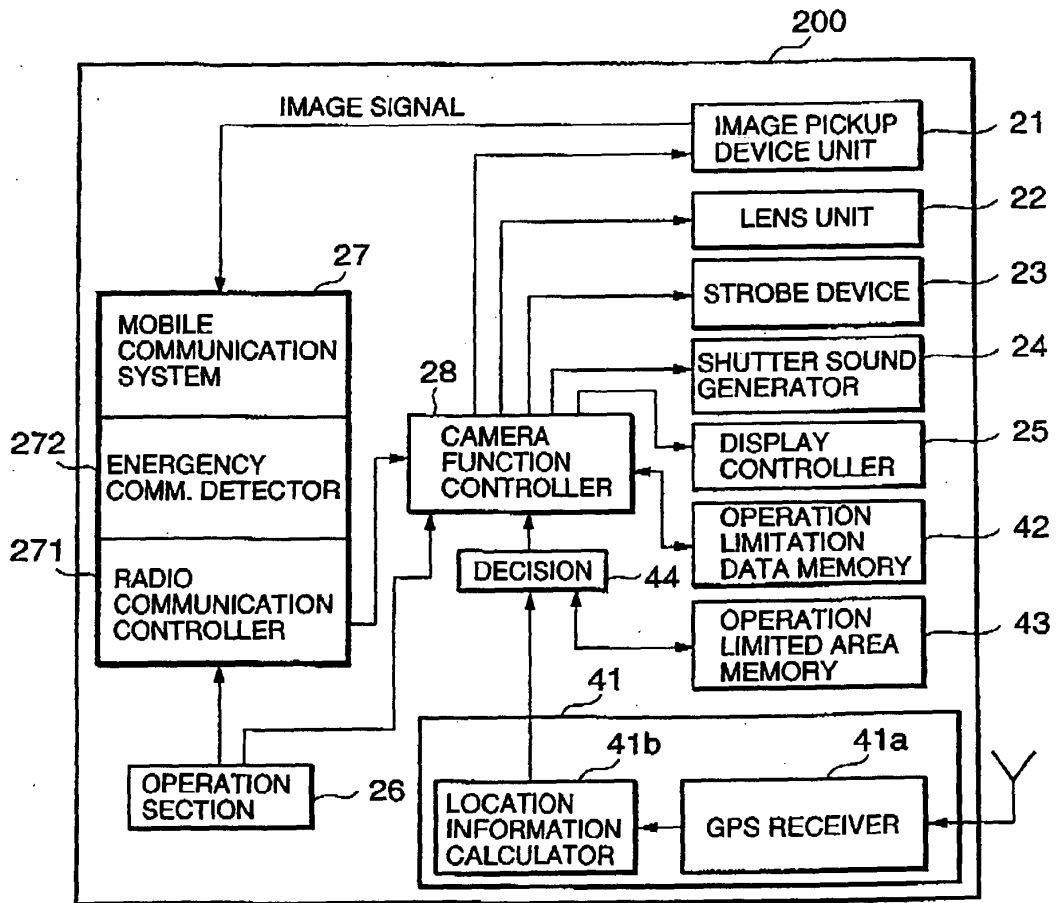


FIG. 16

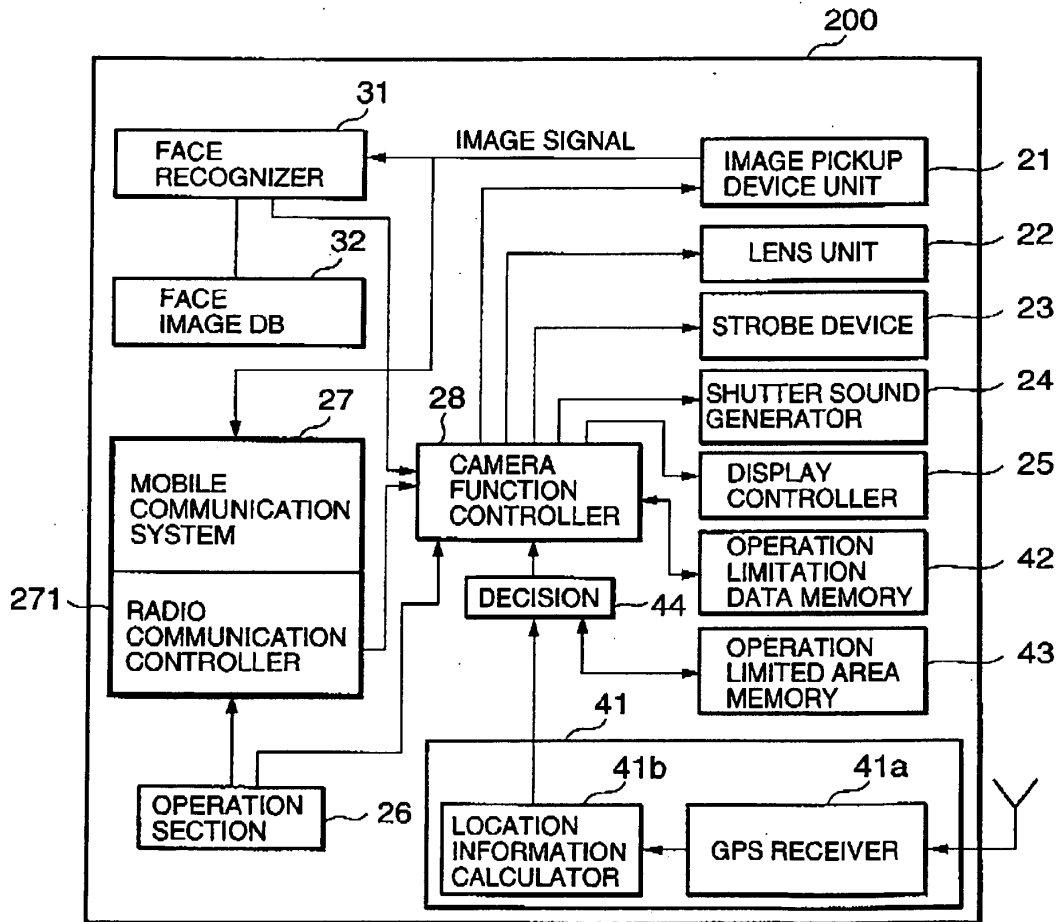
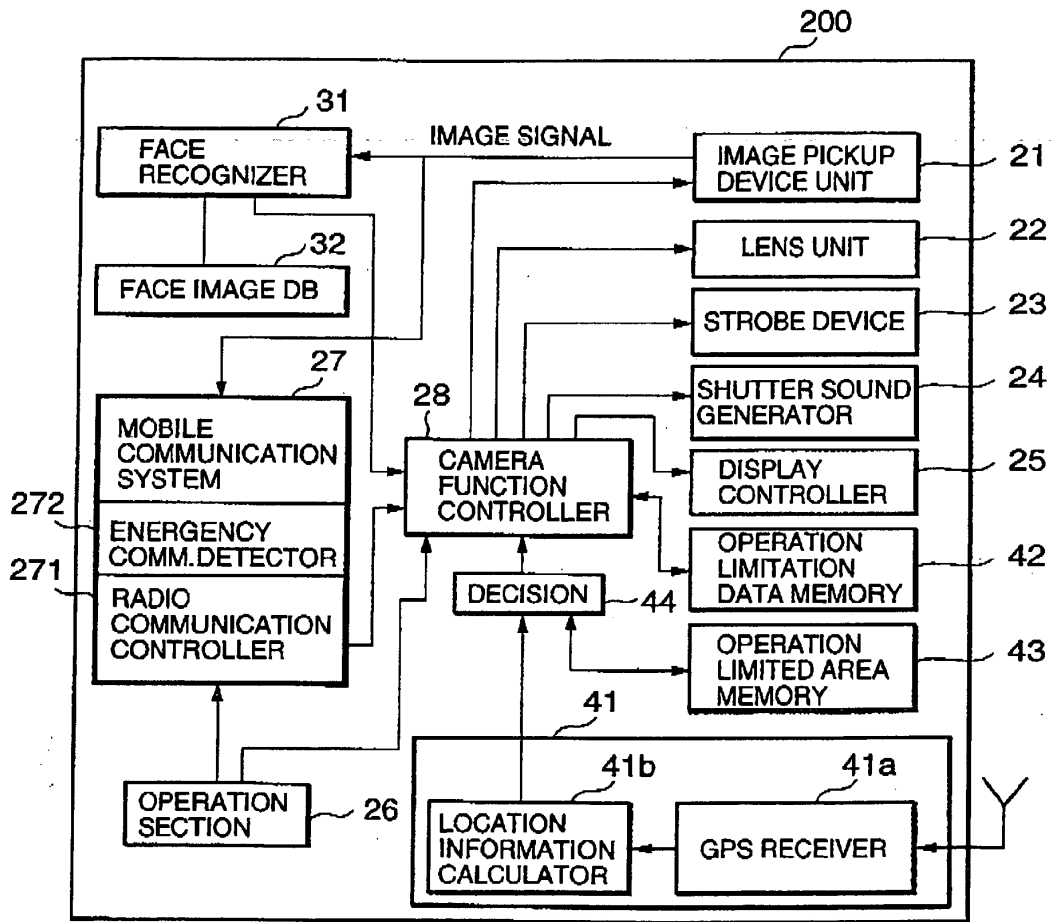
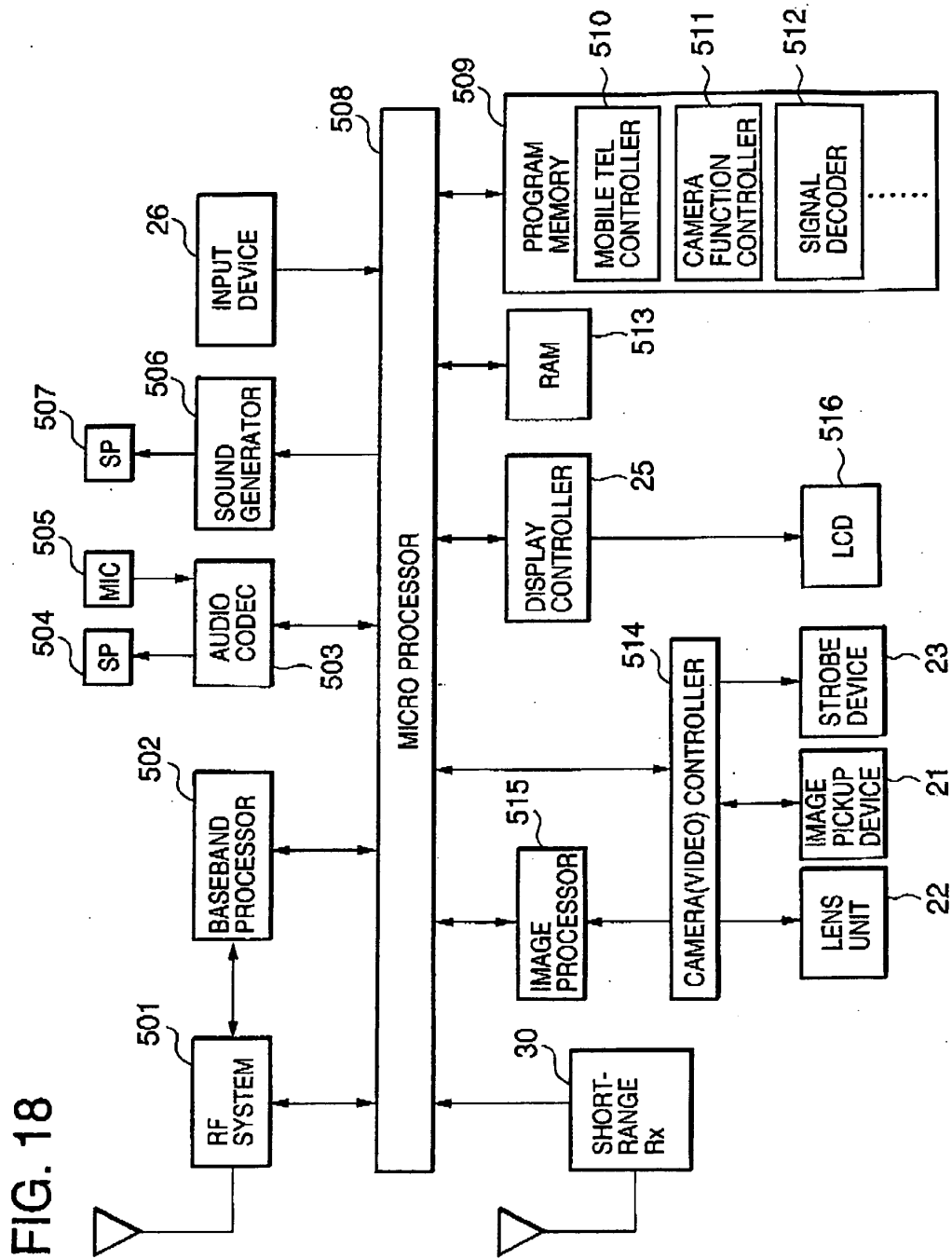


FIG. 17







European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 00 2319

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	US 2002/028674 A1 (SLETTENGREN SVEN KONRAD ET AL) 7 March 2002 (2002-03-07)	1-4, 7-10,13, 14,16, 18,19	H04M1/725
A	* figures 1-9 * * paragraphs [0003], [0006] - [0008] * * paragraphs [0025], [0027], [0028], [0030] * * paragraphs [0036], [0039], [0046], [0049] * * paragraph [0070] *	6,12,15, 17	
Y	US 2001/044321 A1 (AKVELD FELIX N ET AL) 22 November 2001 (2001-11-22)	1-4, 7-10,13, 14,16, 18,19	
A	* paragraphs [0007], [0009], [0010] * * paragraph [0044]; figure 1M *	15	
A	US 2002/055372 A1 (MOTOHASHI TERUYUKI) 9 May 2002 (2002-05-09)	1-4, 6-10, 12-16, 18,19	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04M H04N
	* paragraphs [0029], [0030] * * paragraphs [0002], [0008], [0023] * * paragraphs [0025], [0042] * * figures 1,2,8-10 *		
A	US 2002/065070 A1 (NAIKI TAKASHI) 30 May 2002 (2002-05-30)	1-4,6, 8-10,12, 16-19	
	* paragraph [0001] * * paragraphs [0004], [0006] - [0008] * * paragraphs [0013], [0014] * * paragraphs [0022] - [0037] * * paragraphs [0055], [0058], [0061] * * paragraphs [0069] - [0071], [0075] * * figures 1-4 *		
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 26 March 2004	Examiner Hagan, C
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

EPO FORM 1503 03 02 (P/01/001)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 04 00 2319

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

26-03-2004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002028674 A1	07-03-2002	AU 7982301 A	22-03-2002
		WO 0221866 A2	14-03-2002
US 2001044321 A1	22-11-2001	US 6434403 B1	13-08-2002
		AU 3238000 A	04-09-2000
		WO 0049731 A1	24-08-2000
US 2002055372 A1	09-05-2002	JP 3487280 B2	13-01-2004
		JP 2002125263 A	26-04-2002
		CN 1348259 A	08-05-2002
		GB 2370174 A	19-06-2002
US 2002065070 A1	30-05-2002	JP 2002095064 A	29-03-2002

EPO FORM P0489

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(12) **UK Patent**

(19) **GB**

(11) **2 396 779**

(13) **B**

(45) Date of publication: **25.07.2007**

(54) Title of the invention: **Mobile communications**

(51) INT CL: **H04Q 7/32** (2006.01) **H04Q 7/38** (2006.01)

(21) Application No: **0230062.2**
(22) Date of Filing: **23.12.2002**
(43) Date A Publication: **30.06.2004**

(52) UK CL (Edition X):
H4L LDDDM LEUF L201 L205 L209 L213

(56) Documents Cited:
GB 2380636 A **GB 2375690 A**
GB 2372911 A **GB 2370196 A**
GB 2363037 A **GB 2358987 A**
GB 2323245 A **EP 1098489 A2**
WO 1995/029568 A1 **US 20020142792 A1**

(58) Field of Search:
As for published application 2396779 A viz:
UK CL (Edition V) **H4L**
INT CL ⁷ **H04M, H04Q**
Other
ONLINE: WPI, JAPIO, EPODOC
updated as appropriate

(72) Inventor(s):
Craig Kelvin Bishop

(73) Proprietor(s):
Samsung Electronics Co. Ltd.
(Incorporated in the Republic of Korea)
416 Maetan-dong, Paldal-gu, Suwon-City,
Kyungki-Do, Republic of Korea

(74) Agent and/or Address for Service:
R G C Jenkins & Co
26 Caxton Street, London, SW1H 0RJ,
United Kingdom

1/6

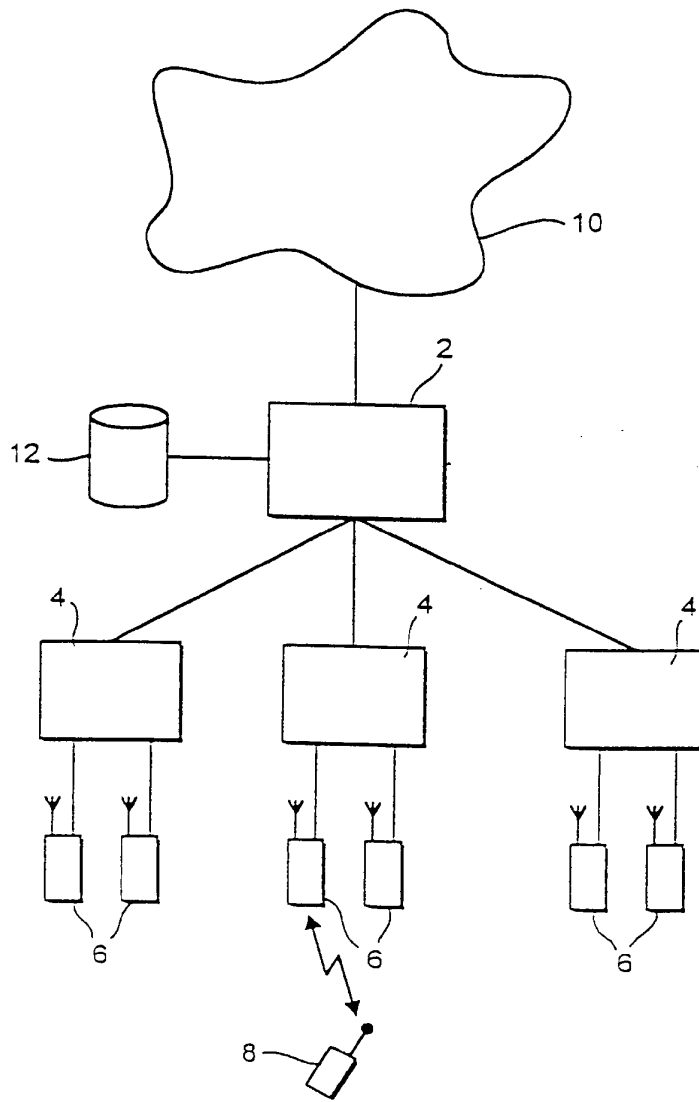


FIG. 1
PRIOR ART

Fig. 2A

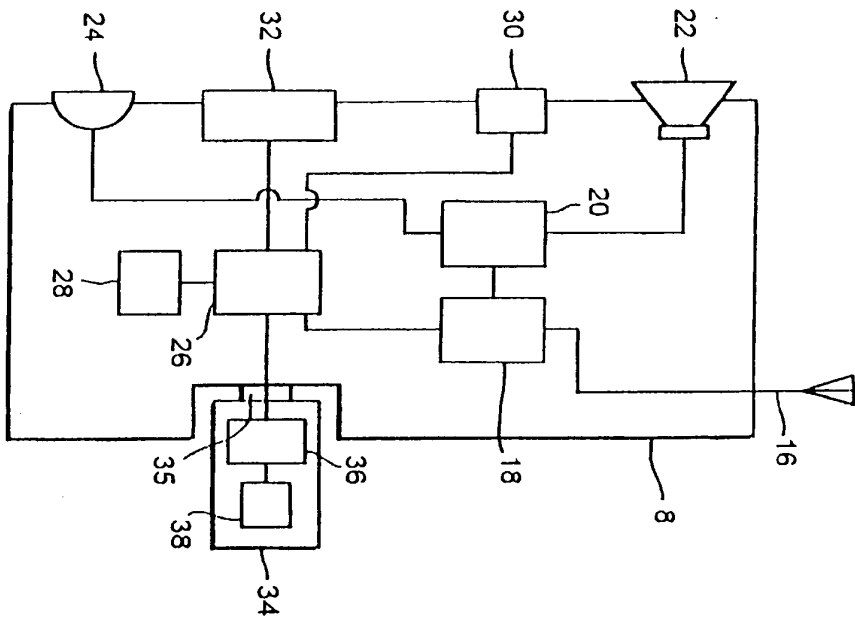
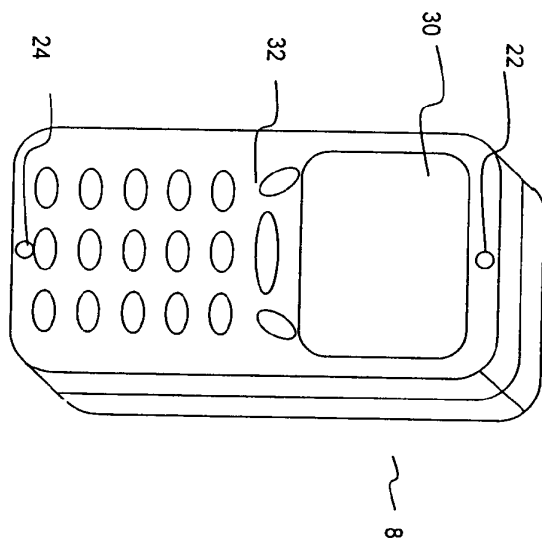


Fig. 2B



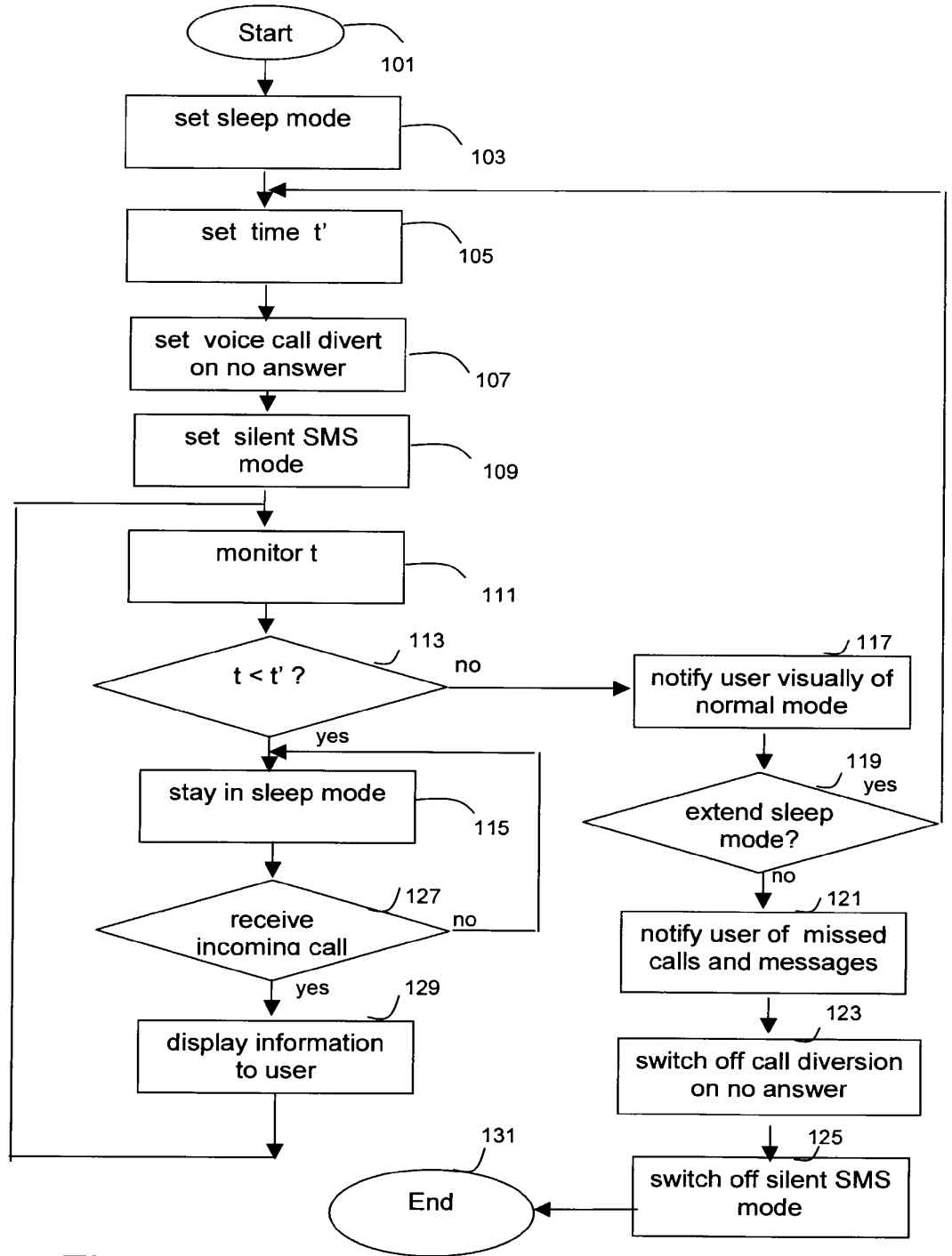


Fig. 3

4/6

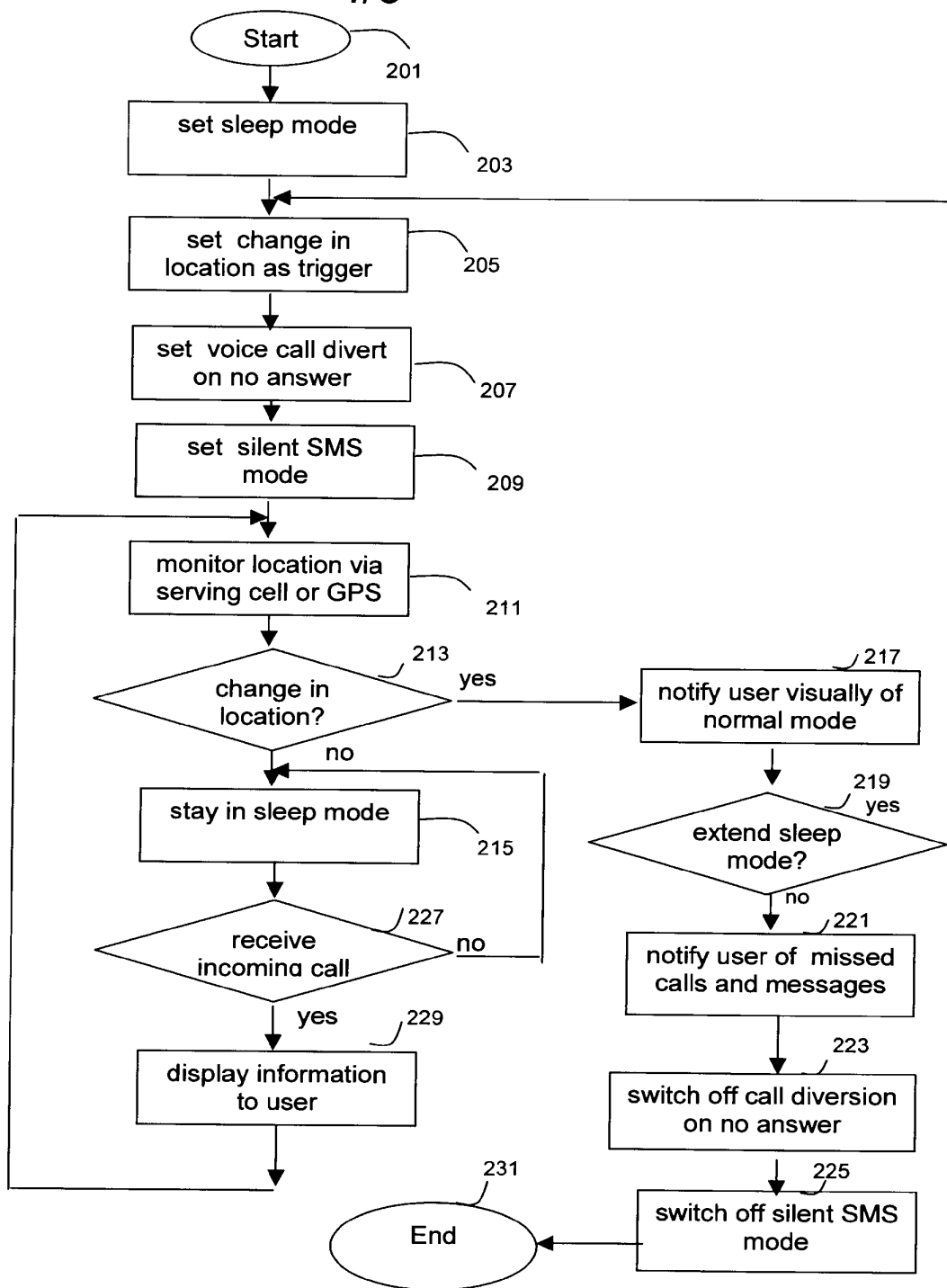


Fig. 4

please enter

time

location

other

to trigger return to
normal mode

Fig. 5A

set time trigger

time

time period

Fig. 5B

time to switch to
normal mode:

10 : 30

Fig. 5C

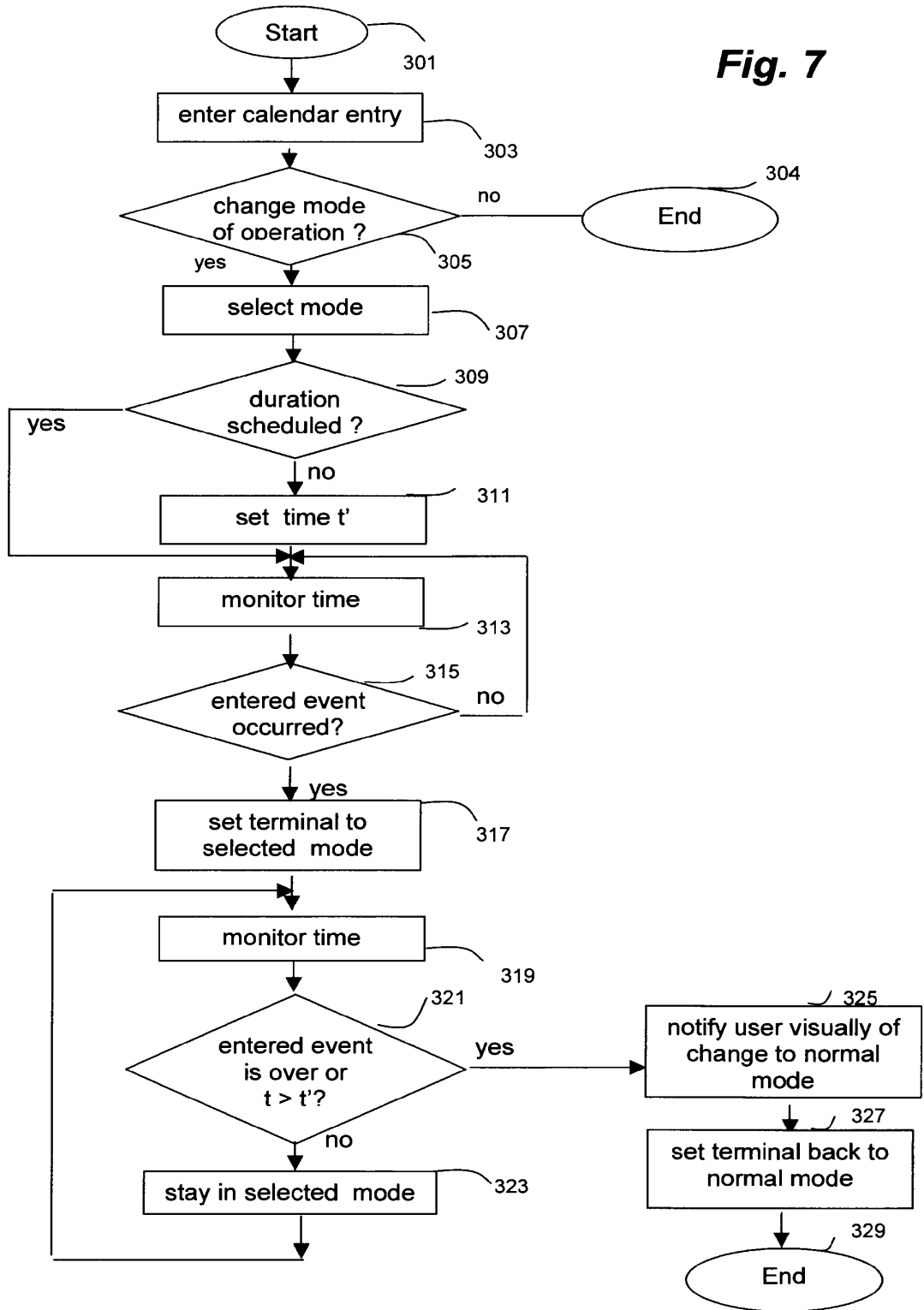
incoming call from

01234 56789

Fig. 6

6/6

Fig. 7



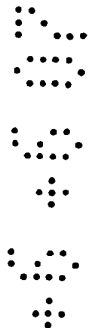
Mobile Communications

This invention relates to methods and systems of controlling a mobile terminal. More particularly, but not exclusively, the invention relates to controlling a mobile terminal by defining a profile of an operation mode and switching from a particular mode of operation to another mode of operation.

There are a number of places or occasions where a user of a mobile terminal wants to set a number of different functions or settings such that the terminal is in a particular mode of operation. For example, the user may not want the terminal to produce audible alerts, as the noise might disturb others. These places and occasions for example include theatres, cinemas, libraries, conferences or business meetings, and are referred to as Non-Mobile Friendly Events (NMFE) in the following.

For the duration of such a NMFE, the user could switch the mobile terminal to a silent mode. In this case, information about incoming calls is recorded in the usual way. However, the disadvantage is that the user has to remember to switch off silent mode of the terminal after the NMFE. In addition, the calling parties might think that the user was simply not answering the call and might try to reach the user several times which is tedious for the calling party and also leads to an unnecessary increase in signalling in the communications network.

The Nokia 8310 mobile terminal by Nokia™ is described to have various setting groups to customise the mobile's alerting tones for different



events and environments. The phone tone setting groups can be activated via the menu functions. The user may for example select a phone tone setting group called "silent". The user may also set a setting group to be active for a certain amount of time up to 24 hours. After the time period set by the user expires, the previous setting group set becomes active again.

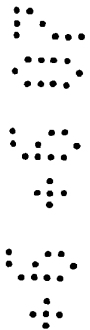
5

This option of having phone tone setting groups is very similar to switching manually to silent mode and the disadvantage remains that the calling parties are not informed that the user is currently unreachable.

The user can avoid this disadvantage by diverting all incoming calls to his voice mail box. However, in this case the user has to set the terminal manually and he has to remember to turn off call diversion after the NMFE. This would inform calling parties that the user is currently unavailable and at the same time prevent the terminal from ringing during the NMFE. However, messages received via the short message service (SMS) would still be notified audibly, unless the user switches to silent mode for SMS reception. If all calls are diverted to a voice mail box, then no signalling takes place between network and mobile, so then there is no indication of missed calls at the terminal. Information about the calls missed during the NMFE will not be recorded.

10

15



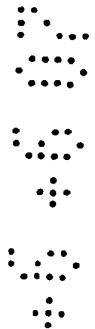
20

A further solution would be to switch off the mobile terminal for the duration of the NMFE. This would prevent the terminal from audibly alerting calls and SMS messages. The calling party would be notified that the user is currently not reachable and calls might be diverted to voice mail if the user

had set up his terminal accordingly. However, the user has no access to call information about the calls missed during the NMFE (apart from possibly the last incoming call via dialled operator services, such as the BT 1471 service). Another disadvantage is that the user will have to remember to switch on the terminal following the NMFE. Also the user usually receives an audible indication when the terminal is switched on, which might be disturbing, and the user might need to key in the personal identification number (PIN) before the terminal can be used.

In order to avoid the need to switch the terminal back on manually after the NMFE, the user may set the terminal to wake up at a particular time using the alarm function. However, the user may still need to key in the PIN before the terminal is usable. Moreover, if the NMFE takes longer than expected, the user is not able to change the specified time for wake-up without switching on the terminal and thus being disturbed by the audible indication when the terminal is switched on.

In US published patent application US 2002/0083028, a mobile terminal is described which operates automatically according to information pre-programmed by the user. The user defines certain time periods every day or week or periods dedicated to a particular event, and the terminal determines according to the information given for a particular event whether the user can be called during the scheduled time period for this event. If the terminal determines that the user cannot be alerted and a call is received, the terminal responds automatically to this call by sending a voice or SMS message to the



calling party notifying that the user is currently having a NMFE and that the user can be reached later.

A disadvantage of the described solution is that the user needs to preprogram the information about the events and in which way the user can be alerted for each of the defined events. Another disadvantage is that additional signalling is required in order to notify the calling party that the user is currently not reachable.

In US patent application US2001/0009863, a method is described for restricting incoming calls in a mobile terminal. The user can specify a particular time period in which the user does not want to receive any incoming calls. If a call is coming in, the terminal determines whether calls are restricted at that particular time by using the GSM call barring function to prevent the terminal from receiving any incoming calls. In this way call information is available and might be presented to the user after the NMFE event. However, the user is usually still audibly alerted by the reception of SMS messages and the system is not very flexible.

It is an aim of the present invention to alleviate at least some of the disadvantages described and to provide an improved method and system for controlling a mobile terminal.

According to one aspect of the invention, there is provided a method of operation of a mobile terminal for use in a mobile communication network, the method comprising the steps of: storing a plurality of predefined profiles;



5

10

15

20

and automatically switching to or from one of said profiles according to a condition selected or specified by the user of said terminal, wherein said condition is a change in location of the mobile terminal,

5 wherein the method further comprises notifying the user when the terminal is about to switch off said one profile.

According to a another aspect of the invention, there is provided a method of operation of a mobile terminal for use in a mobile communication network, the method comprising the steps of: storing a plurality of predefined profiles; and automatically switching to or from one of said profiles according
10 to a condition selected or specified by the user of said terminal, wherein said condition is the occurrence or expiry of a calendar entry,

wherein the method further comprises notifying the user when the terminal is about to switch off said one profile.

15 Preferably, said one profile comprises the settings call diversion to a voice mail box and silent mode for short message reception. In this way a convenient way is provided for setting a terminal to a silent mode without losing information about incoming call and messages.

20 The call diversion function may for example be set to divert the incoming call to a voice mail box if no answer has been received within a specified time period, such as a period of 5 seconds. As the mobile is allowed to be paged (albeit with no indication to the user) prior to the call being diverted, the information about the incoming call is accessible to the terminal.



Preferably, the user may select an event out of a number of possible events to trigger switching between two different modes of operation. Such an event may for example be location information, calendar information or a combination of those. The conditions to switch automatically between operation modes include for example a change in location or the occurrence or expiry of a selected calendar entry to initiate switching between different modes of operation. In this way there is provided a very flexible system to switch between different modes of operation.

Further aspects and advantages of the invention will be set out, by way of example only, from the following description and accompanying drawings, wherein:

Figure 1 is a general schematic outline of a GSM mobile communications network in which the present invention can be implemented;

Figure 2A is a block diagram of a mobile terminal for use in the network illustrated in Figure 1;

Figure 2B is a schematic illustration of the mobile terminal in figure 2A;

Figure 3 is a flowchart diagram illustrating the procedure of controlling a mobile terminal according to an illustrative arrangement not forming an embodiment of the present invention.

Figure 4 is a flowchart diagram illustrating the procedure of controlling a mobile terminal according to an embodiment of the present invention.

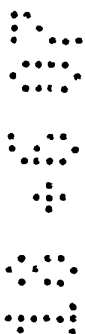
Figures 5A to C are schematic diagrams of display screens illustrating the procedure of controlling a mobile terminal according to an illustrative arrangement not forming an embodiment of the present invention.

Figure 6 is a schematic diagram of a display screen according to
5 embodiments of the present invention.

Figure 7 is a flowchart diagram illustrating the procedure of controlling a mobile terminal according to another illustrative arrangement not forming an embodiment of the present invention.

In Figure 1 a schematic outline of a mobile telecommunications
10 network according to the GSM standard is shown. A Mobile Switching Centre (MSC) is connected via communication links to a number of Base Station Controllers (BSCs) 4. The BSCs are dispersed geographically across areas served by the Mobile Switching Centre 2. Each BSC 4 controls one or more Base Transceiver Stations (BTSs) 6 located remote from, and connected
15 by further communication links to, the BSC 4. Each BTS 6 transmits radio signals to, and receives signals from, mobile stations 8 which are in an area served by that BTS 6. The area is referred to as a "cell". A GSM network is provided with a large number of such cells, which are ideally contiguous to provide continuous coverage over the whole network territory.

20 A MSC 2 is also connected via communications links to other mobile switching centres in the remainder of the mobile communications network 10, and to a public service telephone network (PSTN), which is not illustrated.



It is appreciated that the invention may alternatively be implemented in other cellular networks, such as GPRS, UMTS or CDMA2000 networks.

Referring to Figure 2A and B, a mobile station 8 comprises a transmit/receive aerial 16, a radio frequency transceiver 18, a speech
5 coder/decoder 20 connected to a loudspeaker 22 and a microphone 24, a processor circuit 26 and its associated memory 28, an LCD display 30 and a manual input port (keypad) 32. The mobile station is connected to a removable SIM 34 via electrical contacts 35.

The SIM 34 connected to the mobile station has a SIM processor 36
10 and SIM memory 38.

The SIM 34 is used for the storage and retrieval of data items by the processor 26 of the mobile station 8. The command set, data file structure and data coding format for data communicated via the interface between the mobile station processor 26 and the SIM processor 36 are all specified, in the
15 GSM system, in GSM technical specification 11.11 (3GPP TS 51.011 for release 4 onwards). In a similar manner, the Universal Subscriber Identity Module USIM is used in UMTS networks, see the Technical Specification 3GPP TS 31.102.

In the past, the SIM had a purely passive function and was used for
20 storing data, mainly relating to the identification of a particular user, to authentication and security procedures.

Today, SIM cards have extended functionality and allow applications to be stored on the SIM card and interactions between the SIM card and the



mobile equipment (ME). Such mechanisms can either be provided by the SIM application toolkit or by a SIM card, for which software can be written in a computer programming language such as Java™.

Referring now to Figure 3, the process of setting a mobile terminal to “sleep mode” is described for an illustrative arrangement not forming an embodiment of the invention. Sleep mode is a particular mode of operation, which allows a user to set the following settings on the mobile terminal: “call diversion to a voice mail box on no answer”, “silent mode for incoming calls” and “silent mode for short message reception”. The method also provides for automatic switching to sleep mode according to a condition selected or specified by the user of said terminal.

The process starts in step 101 by the user wanting to set the mobile terminal to sleep mode. In order to activate sleep mode in step 103, the user needs to press a predetermined key or a combination of keys on the terminal's keypad. The terminal then notifies the user via the display that the user needs to set a time t' at which the terminal switches off the sleep mode and re-enters the normal mode. The user enters the desired time t' in step 105 via the terminal's keypad. In steps 107 and 109 the terminal now enables the sleep mode; In step 107 the terminal sets voice call diversion to a voice mail box if no answer is received after 5 seconds. In step 109 the terminal sets silent mode for calls and SMS reception.

In step 111, the terminal continuously monitors the current time in order to determine in step 113 whether the terminal is required to stay in sleep

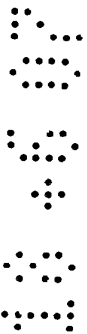
mode (step 115) or whether the time t' has arrived for switching back from sleep mode to normal mode.

In the latter case, the terminal continues by notifying the user via the terminal's display that the terminal is about to switch off sleep mode in step 117. The terminal may further notify the user (step 119) that they can extend the time period of the mobile terminal being in sleep mode by activating a predetermined key or a combination of keys. If the user decides in step 119 that the silent mode is required for an extended period, the process continues in step 105 and the user can again set a new time t' at which the terminal switches back to normal mode.

If, on the other hand, the time period does not need to be extended in step 119, in step 121 the terminal displays to the user call information of any calls which were received during the time period the terminal was set to sleep mode. The terminal also notifies the user of any received SMS messages.

In steps 123 and 125, the terminal disables the sleep mode by switching off the call diversion to the voice mail box on no answer (step 123), and by switching off the silent mode (for incoming calls and SMS) in step 125. In step 131, the terminal is now again in normal mode.

If, in step 127, a voice call is received by the mobile terminal while being set to sleep mode, the call information like the calling party's identity is stored in the terminal as a missed call prior to the call being diverted. In step 129, the terminal displays this information to the user during sleep mode, but no audible warning is given. The terminal may for example display a



15

20

screen to the user as illustrated in Figure 6. Similarly, if in step 127 a SMS message is received, the user is visually notified of the event in step 129.

In this way the user is notified by the terminal of incoming calls or messages without being disturbed by the terminal alerting the user.

5 The terminal stores the call information of all calls received during sleep mode (see step 121) and displays the information to the user when switched back to normal mode. The user may also easily access the stored information and use it for returning the missed calls after the NMFE.

10 As an alternative to switching off the call diversion in step 123, the terminal may extend the time before a call is diverted if no answer is received, such as by changing the time period from 5 to 15 seconds, thus allowing more time for the user to answer incoming calls.



15 It is appreciated that the user may at any time during sleep mode re-awake the terminal to switch it back to normal mode by activating a predetermined key or a combination of keys.



20 In this way the user may for example re-awaken the mobile terminal after the terminal informed the user of a received call by displaying the call information as described above with reference to Figure 6. The user may, for example, recognise from the information that an awaited call or a particular important call was directed to the terminal and return the call after the terminal has been re-awaken.



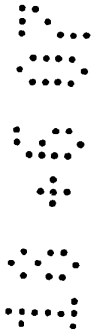
In a similar manner, the user may at any time during sleep mode re-awaken the terminal for extending the sleep period.

According to an embodiment of the present invention, the user can specify a change in location to trigger the terminal to switch off the sleep mode and to return to normal mode.

Such an embodiment might be especially useful for events where the duration of time might be difficult to predict such as certain business meetings, and where the user changes location after the event, for example leaves a conference or meeting after the event to go back to the user's office. For such an event, it is convenient to relate the automatic switching to or from sleep mode dependent on the mobile terminal's location.

Referring to Figure 4, we will now describe a process similar to that described above with reference to Figure 3 but using a location trigger rather than a time trigger to switch from sleep mode to normal mode. Steps 201 and 203 are analogous to steps 101 and 103 described above. In step 205 the user defines that the terminal is to switch off the sleep mode when it has determined a change in location. Steps 207 and 209 are again analogous to steps 107 and 109.

In step 211, the terminal monitors the location of the terminal. This can be done by using information from a global positioning system (GPS) or simply using information from which cell of the network the mobile is currently provided services. This information is for example available from the location information elementary file on the SIM. As long as no change to the mobile's location occurs, the process continues with step 215 and 211 by staying in sleep mode and further monitoring the location. If a call or



message is received while the terminal is set to sleep mode (step 227), the terminal displays the all information to the user in step 229.

If the mobile determines in step 213 that its location has changed, the process continues in step 217. Again, steps 217 to 227 are analogous to step 117 to 127 described above.

Also in this embodiment the terminal may prompt the user to “extend” the sleep mode and to enter a new event to trigger the return to the normal mode. The user may for example set the terminal to sleep mode before attending a business meeting. However, the user might change location during the meeting without wanting the terminal to switch back to normal mode. Thus, the user may after being prompted to do so in step 219, re-enter in step 205 that the terminal switches back to normal mode as soon as a further change in location is detected.



Instead of setting the trigger to a change in location, the user may also specify that the terminal switches back to normal mode if the terminal has determined that it is at a particular location, for example at the office or at home. In order to achieve this the user may define a particular cell as his “home” or “office” cell if the user is at home or in the office. The terminal then memorises and stores the according information for that particular cell and refers to this information as the “home” or “office” cell.

According to a further embodiment, the user is presented with a display as illustrated in Figure 5A after the user has activated the sleep mode.

The user is prompted to enter or select a particular “event” to be used as a trigger for switching from sleep mode to normal mode as soon as this “event” occurs.

5 The user may for example choose between the listed options “time”, “location” or others. By activating the navigation keys of the terminal, the user may select one of the options.

10 If the user selects the listed highlighted option “time” in Figure 5A, the terminal displays a screen as illustrated in Figure 5B. The user is again offered two options, i.e. either to set a time at which the terminal switches back from sleep mode or to set a time period during which the terminal stays in sleep mode.

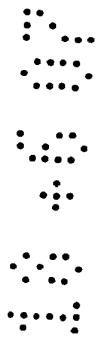


15 If the user selects to set a time in Figure 5B, a screen as illustrated in Figure 5C is subsequently presented to the user. The user may then enter the hours and minutes of the desired time into the two predefined fields by using the terminal’s keypad.

20 Although in the above described arrangements and embodiments a sleep mode has been described to include a call diversion to a voice mail box on no answer, a silent mode for incoming call and SMS reception and a visual notification of missed call information for incoming calls, it is appreciated that alternatively other predetermined modes of operation may be utilised. A similar sleep mode like the one described above may for example be achieved by replacing the call diversion function by a call barring function for all incoming calls.

More generally, the user may define “profiles” of operation modes according to the present invention. These profiles consist of several network settings or a combination of network settings and terminal settings. The user may define as many different modes of operation as he likes. Also, the user
 5 may define the modes of operation including as many settings as he likes. The user is not restricted in the choice of the settings he may want to include in the defined modes of operation.

Terminal settings are functions which are set directly on the terminal, such as the volume of a ring tone, the type of alert etc. Network settings are
 10 implemented by the service provider. These functions include for example call diversion, call barring, call holding, access to caller identity or cell identity information, etc.



By providing these predefined modes of operation, the user can switch easily between different modes of operations without requiring the user to set
 15 these commands or functions individually. Also, an application running on the terminal or the SIM can make use of the predefined profiles to switch between them. Preferably, both the network and terminal settings are standard commands and/or settings. In this way the “profiles” can be implemented easily into existing mobile terminals.

20 A further example for such a profile of an operation mode is a “noisy mode”. This mode is set up particularly for use in high noise environments, such as factory floors, airports, etc. In the noisy mode, the call and SMS indication tones are set to the maximum volume, vibration and visual alerting

modes are switched on in addition to the audible alerts, and call diversion to a voice mail box on no answer is switched off.

In this way the user is provided with a maximum of incoming call or message alerting. At the same time, the user has the maximum amount of time to answer an incoming voice call.

Other modes of operation include for example a “sales mode”, in which no information relating to outgoing calls is displayed, and call waiting and call divert on busy subscriber is disabled, a “business mode”, which includes the browser settings for connection to an office server and call forwarding to a secretary’s number on busy or no answer, or a “leisure mode”, which enables the information about the caller identity to be displayed, sets a particular “fun” ring tone, and includes browser settings for connection to a personal internet service provider and e-mail.



Preferably, the terminal provides a number of predefined modes, such as the sleep mode and the noisy mode. However, the user can also create new modes or customise existing profiles. These modes may be defined either via the menu option by listing the desired settings or by setting the terminal manually to the desired mode of operation and subsequently defining this mode of operation as a profile. By defining a name access to the operation modes is facilitated.

As an alternative to using location information to initiate switching between different modes of operation, the user can set the terminal to use

information entered to a calendar stored on the terminal to trigger the terminal to switch the terminal to a preferred mode of operation.

Many mobile terminals provide for a calendar option to store information about meetings or other events. A further embodiment of the present invention, in which the user may select a particular mode of operation for an event scheduled in the user's calendar will now be described with reference to the flowchart diagram of Figure 7.

In step 303, the user enters a new entry in his mobile terminal's calendar. In step 305, the user is presented with a screen asking whether a change in operation mode is required for the event entered into the calendar in step 303. If no change in operation mode is desired, the process ends in step 304. If the user wants to change the mode of operation for the time of the entered event, he may select a mode of operation in step 307. In order to facilitate the selection, the mobile terminal presents a screen with all the pre-defined operation modes, such that the user can select the desired mode by operating the navigation and/or confirmation keys.



The terminal then checks in step 309 whether the entered event is scheduled in the calendar for a predetermined time period. If this is not the case, the user can set a time period t' for which the terminal will stay in the selected operation mode (step 311). If, on the other hand, the duration is already scheduled in the calendar, the process continues in step 313.

In step 313, the terminal monitors the time and compares the current time with the calendar entries. If, in step 315, the time for the entered entry

arrives, the terminal is automatically set to the selected operation mode in step 317. Otherwise, the terminal keeps monitoring the time in step 313.

After the terminal is set to the selected mode in step 317, the terminal again monitors the time in step 319, in order to determine when the terminal is to be switched back to normal mode or the mode in which the terminal has been before switching to the selected mode in step 317. As long as the scheduled time for the end of the selected event has not yet arrived or the time period set in step 311 has not yet expired, the terminal stays in the selected mode (step 323) and keeps monitoring the time in step 319.

If the terminal determines in step 321 that the scheduled time period for the selected event is over or that the time period set in step 311 expired, the terminal notifies the user visually that its mode of operation is changed to normal mode (step 325). The terminal is switched back to normal mode in step 327 and the process ends in step 329.

The embodiments of the present invention are preferably implemented in the mobile terminal by means such as an application stored in the memory 28 of the mobile terminal 8, which is running on the terminal's processor 28. The application may for example be activated by the user when he selects a particular mode of operation by pressing a predetermined key or combination of keys. If more than one profile is defined for a particular terminal, the user may access a menu for these profiles and select the desired profile via that menu.



As an alternative to storing and running the application for controlling the terminal via a profile for a mode of operation on the processor of the mobile terminal, the application may be stored and run on the SIM, for example as a SIM Toolkit or a Java™ application.

5 It is to be understood that the embodiments described above are preferred embodiments only. Various features may be omitted, modified or substituted by equivalents, without departing from the scope of the present invention.




CLAIMS:

1. A method of operation of a mobile terminal for use in a mobile communication network,

5 the method comprising the steps of:
storing a plurality of predefined profiles; and
automatically switching to or from one of said profiles according to a condition selected or specified by the user of said terminal, wherein said condition is a change in location of the mobile terminal,

10 wherein the method further comprises notifying the user when the terminal is about to switch off said one profile.



2. A method according to claim 1, further comprising changing said condition while the terminal is set to said one profile in response to a user instruction.

3. A method according to claim 2, wherein the user instruction specifies a change in location for switching off said one profile.

20 4. A method of operation of a mobile terminal for use in a mobile communication network,

the method comprising the steps of:
storing a plurality of predefined profiles; and

automatically switching to or from one of said profiles according to a condition selected or specified by the user of said terminal, wherein said condition is the occurrence or expiry of a calendar entry,

5 wherein the method further comprises notifying the user when the terminal is about to switch off said one profile.

5. A method according to claim 4, further comprising changing said condition while the terminal is set to said one profile in response to a user instruction.

10

6. A method according to claim 5, wherein the user instruction specifies the occurrence or expiry of a calendar entry for switching off said one profile.



7. A method according to any of claims 1 to 6, further comprising providing a plurality of different events for selection, said events being used to set a condition relating to said events for switching to and/or from said one profile.

15

8. A method according to claim 7, wherein these events comprise time events, location events or scheduled events.

20

9. A method according to any of claims 1 to 8, wherein said one profile comprises the settings:

call diversion to a voice mail box; and
silent mode for short message reception.

5 10. A method according to any of claims 1 to 9, wherein, in said one
profile, an incoming call is diverted to a voice mail if no answer has been
received within a specified time period.

10 11. A method according to any of claims 1 to 10, wherein, in said one
profile, information regarding an incoming call is accessible to the terminal.

12. A mobile terminal adapted to perform the method of any of claims 1 to
11.

15 13. An application for installation on a subscriber identity module for use
in a mobile communications network, said application being adapted to
perform the method of any of claims 1 to 11.

20 14. An application for installation on a mobile terminal for use in a mobile
communications network, said application being adapted to perform the
method of any of claims 1 to 11.



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-168478

(43)Date of publication of application : 22.06.1999

(51)Int.Cl. H04L 12/28
G08B 25/10
H04Q 7/38

(21)Application number : 10-228083

(71)Applicant : PRONET TRACKING SYST INC

(22)Date of filing : 12.08.1998

(72)Inventor : JANDRELL LOUIS H M

(30)Priority

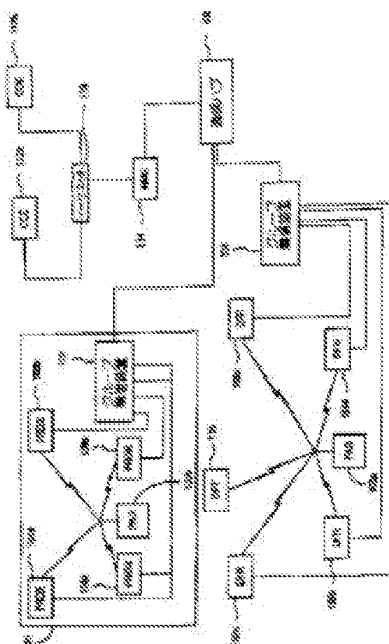
Priority number : 97 910066 Priority date : 12.08.1997 Priority country : US

(54) METHOD FOR DETERMINING RADIO POSITION AND ITS SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To realize a low interference for multiple accesses by means of a non-synchronized locator transceiver through the use of frequency hopping which is required for the use of a common band by transmitting a data packet after a prescribed time during prescribed-time waiting, when a communication channel is still idle.

SOLUTION: Personal alarm(PAD) 100b starts access of a communication channel so as to determine whether a data packet is ready to be transmitted or not and the channel is detected in order to determine whether it is busy or not in an affirmation. When the channel is in an idle state, a device waits for a specified interval (priority order-delay time) before testing the idle state again. When the channel finds the idle state, a message is transmitted. That is, the device executes transmission onto the channel only when the channel is still in the idle state after the priority order-delay interval.



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 01-194628

(43)Date of publication of application : 04.08.1989

(51)Int.Cl. H04L 9/00

(21)Application number : 63-018945

(71)Applicant : NEC CORP

(22)Date of filing : 29.01.1988

(72)Inventor : TACHIBANA NORIYUKI

(54) SECRECY PROTECTING SYSTEM

(57)Abstract:

PURPOSE: To make the wiretapping of a line difficult and to enhance confidentiality by adopting different systems for a data transmitting system used when the connection between information processor and a terminal side is confirmed and for the data transmitting system used after connection confirmation.

CONSTITUTION: When a user communicates, the transmitting system for the connection is set at a terminal side line interface part 2. The same transmitting system is set at an information processor side line interface part 5 by an information processor 4. When the user inputs a signal for a connection procedure from the terminal, input data are inserted from the interface part 2 through a communication line 3 to an interface part 5. The information processor 4 checks the data from the interface part 5, confirms the justifiability of a connection request, sends the connection confirmation completing data to the terminal side, and then, sets the transmitting system of the said user registered in the interface part 5 beforehand. On the other hand, when the terminal side receives the connection confirmation completing data, the transmitting system registered into the interface part 2 is set, and thereafter, the data are exchanged.



PATENT ABSTRACTS OF JAPAN

(11)Publication number : **03-128540**

(43)Date of publication of application : **31.05.1991**

(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12

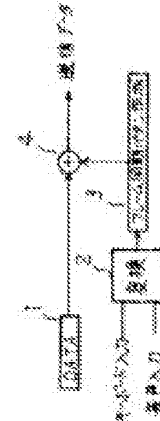
(21)Application number : 01-237070 (22)Date of filing : 14.09.1989	(71)Applicant : HITACHI LTD HITACHI COMMUN SYST INC (72)Inventor : YAMADA IZURU TAMAKOSHI MASASHI
---	--

(54) SECURITY SYSTEM

(57)Abstract:

PURPOSE: To make difficult a cipher to be deciphered by a hacker and to improve the safety of communication by changing a ciphering rule by a keyboard or voice input each time the communication is executed.

CONSTITUTION: The keyboard or voice input is coded by a converter 2 and a frame pattern is prepared by a frame synchronizing pattern preparing circuit 3 corresponding to the input. In the converter 2, a value executing the ASCII conversion of the input is defined as the frame pattern in the case of the keyboard input and a value executing the ASCII conversion of a voice recognized result is defined as the frame pattern in the case of a voice. Since the ciphering rule can arbitrarily be changed for each transmission, it is made difficult to monitor a line, to decipher the cipher by a computer and to execute wire tapping, and there is an effect to improve the safety of the communication.



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-234789

(43)Date of publication of application : 05.09.1995

(51)Int.Cl. G06F 9/44
G06F 9/44

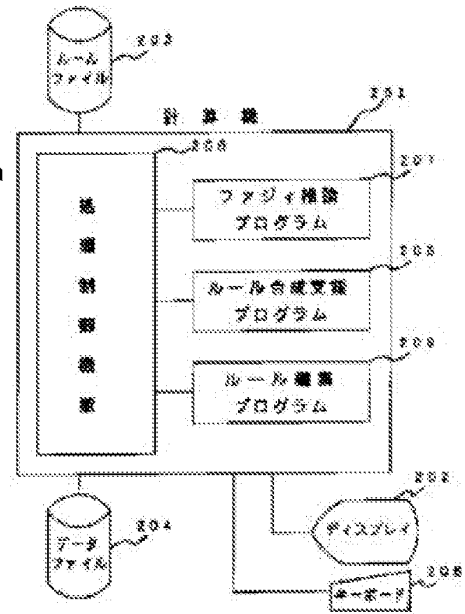
(21)Application number : 06-026474	(71)Applicant : HITACHI LTD HITACHI SEIBU SOFTWARE LTD
(22)Date of filing : 24.02.1994	(72)Inventor : SAKAMOTO MASAYUKI YASUNOBU CHIZUKO YOKOMURA KATSUYA

(54) SUPPORTING METHOD FOR RULE SYNTHESIS

(57)Abstract:

PURPOSE: To provide information necessary for the synthesis of a rule by obtaining the pattern of the if part of a new rule from the if part of an old rule so as to change the if part of the rule.

CONSTITUTION: This method consists of a computer 201, a display device 202, a rule file 203 and a data file 204. The computer 201 calculates through the use of an if-then rule stored in the rule file 203 and time series data stored in the data file 204 and outputs the result to the display device 202.



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-319706

(43)Date of publication of application : 08.12.1995

(51)Int.Cl. G06F 9/44
 G06F 9/44
 G06F 17/30

(21)Application number : 06-109305

(71)Applicant : HITACHI LTD
 HITACHI NUCLEAR ENG CO LTD

(22)Date of filing : 24.05.1994

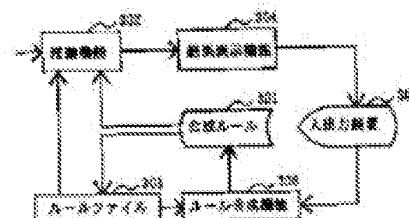
(72)Inventor : HONDA KAZUYASU
 YASUNOBU CHIZUKO
 YOKOMURA KATSUYA
 CHIN MITSUMASA

(54) RULE SYNTHESIZING METHOD

(57)Abstract:

PURPOSE: To support a method which synthesizes a rule that is suited well to a specific pattern of the time series data from existing rules by a simple operation of a user.

CONSTITUTION: The rule synthesizing method consists of a synthetic rule 301, an inference function 302, a rule file 303, a result display function 304, an input/ output device 305, and a rule synthesization function 306. An inference is carried out by the function 302 via the file 303, and the result of this inference is displayed by the function 304. The function 306 retrieves a rule that is suited to the rule synthesizing area inputted to a display out of the file 303 and generates a rule 301 based on the retrieved rule. The function 302 carries out the inference based on the rule 301, and the result of this inference is displayed by the function 304. When a new registered rule is selected out of those rules 301, the rules 301 are added to the file 303.



PATENT ABSTRACTS OF JAPAN

(11)Publication number : **08-044568**

(43)Date of publication of application : **16.02.1996**

(51)Int.Cl. G06F 9/44
G06F 9/06

(21)Application number : **06-177355** (71)Applicant : **HITACHI ZOSEN CORP**
 (22)Date of filing : **29.07.1994** (72)Inventor : **FUJIYOSHI MAKOTO**
KITAMURA AKIHARU

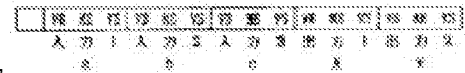
(54) ENCRYPTION METHOD FOR FUZZY RULE

(57)Abstract:

PURPOSE: To simplify encryption by expressing input data and output data of a fuzzy rule by binary data and subjecting this binary bit string to prescribed operation processing as one binary number directly or after conversion.

CONSTITUTION: Three grades (VB, ME, and VS) are provided, and the presence/ absence of each grade is expressed by binarized data (0,1) (presence/absence). For example, the fuzzy rule has three input parts (input 1, input 2, and input 3) and two output parts (output 1 and output 2), and 16-bit data is made correspond to this fuzzy rule.

Relations of input data and output data of the fuzzy rule are expressed by binary data in this manner, and this continuous binary bit string is handled as one binary number, and this binary number is ciphered by prescribed operation processing. Thus, encryption is performed by the simple method.



PATENT ABSTRACTS OF JAPAN

(11)Publication number : **08-087296**

(43)Date of publication of application : **02.04.1996**

(51)Int.Cl. G10L 5/04
G10L 3/00

(21)Application number : **06-221683**

(71)Applicant : **SECOM CO LTD**

(22)Date of filing : **16.09.1994**

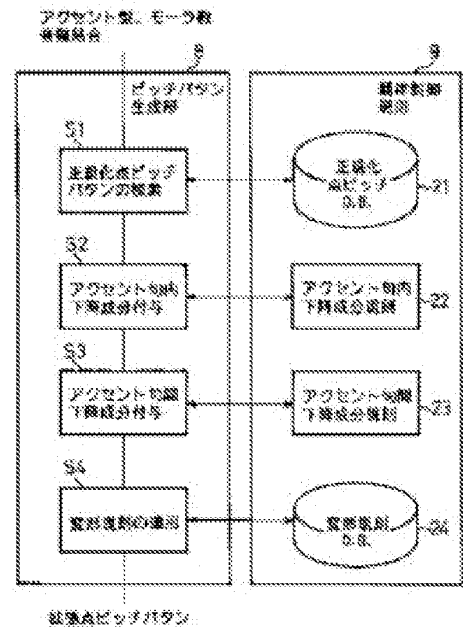
(72)Inventor : **HAMAGAMI TOMOKI**
FURUMURA MITSUO

(54) VOICE SYNTHESIZER

(57)Abstract:

PURPOSE: To correct the fault of a point pitch model, to generate a natural pitch pattern and to produce a high quality synthesized sound in a voice synthesizer.

CONSTITUTION: The voice synthesizer is provided with a first database section 21 which stores accent type point pitch patterns, a second database section 24 which stores the rule corresponding to the combination of the accent type and phoneme and a pitch pattern generating section 8 which retrieves a point pitch pattern corresponding to the paragraph, that is an object of the voice synthesis, from the section 21 and generates a new point pitch pattern based on the rule of the section 24 from the obtained point pitch pattern. Thus, pitches are given to not only the vowel centroid point but also to a phoneme boundary and the naturality in a head word in a synthesized sound and the vowel chain in an accent kernel is improved.



Electronic Acknowledgement Receipt

EFS ID:	17372883
Application Number:	14033540
International Application Number:	
Confirmation Number:	1470
Title of Invention:	System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications
First Named Inventor/Applicant Name:	William J. Johnson
Customer Number:	42640
Filer:	Craig Jeffrey Yudell/Shenise Ramdeen
Filer Authorized By:	Craig Jeffrey Yudell
Attorney Docket Number:	JOHNS-001US3
Receipt Date:	12-NOV-2013
Filing Date:	23-SEP-2013
Time Stamp:	10:53:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	JOHNS-001US3_IDS11-12-13.pdf	172652 <small>89b1d3e0b442992108216f9887af806afd4c2051</small>	no	17

Warnings:

Information:

This is not an USPTO supplied IDS fillable form					
2	Non Patent Literature	NPL1_Schilit.pdf	1206566	no	11
			27c5c826206688d395b2a8f003bce3d08610d78b		
Warnings:					
Information:					
3	Non Patent Literature	NPL2_Harter.pdf	905966	no	9
			43dd76c9011f93770639884c6e7c3b1f73df9a5a		
Warnings:					
Information:					
4	Non Patent Literature	NPL3_Egenhofer.pdf	895203	no	10
			370b26a7121a9fd30542460d15729f6d75b045bc		
Warnings:					
Information:					
5	Non Patent Literature	NPL4_Spreitzer.pdf	1068723	no	15
			70f2c6930889e6d4d75a8752fdd7d696bccce9e9		
Warnings:					
Information:					
6	Non Patent Literature	NPL5_Fitzmaurice.pdf	966621	no	11
			2be33c7fa3f4596a5e5b95af92a84d964f5b848		
Warnings:					
Information:					
7	Non Patent Literature	NPL6_Azuma.pdf	171141	no	2
			452bae768c18120b0f206366d6c30f8cf6b607d8		
Warnings:					
Information:					
8	Non Patent Literature	NPL7_Want.pdf	983700	no	12
			d57b0b2b86c7e3bfebfc0e05ea00ef4a74af52cb		
Warnings:					
Information:					
9	Non Patent Literature	NPL8_White.pdf	538955	no	7
			6b77fd67da08bfc926e28e6b720903ae8f37441d		
Warnings:					
Information:					
10	Non Patent Literature	NPL9_Phail.pdf	592687	no	8
			7f7240b83f4f0530c640c69d37a0a185fe326410		

Warnings:					
Information:					
11	Non Patent Literature	NPL10_Dingus.pdf	1114554 484064b26d75200dc32dcbaf6becde6e15ced3b6	no	7
Warnings:					
Information:					
12	Non Patent Literature	NPL11_Muffat.pdf	700311 65b9544cb798cb3a161de4f7a013d8a71e234b32	no	8
Warnings:					
Information:					
13	Non Patent Literature	NPL12_HighPerformance.pdf	1025573 a13627a0973aff8dc6ff9d5346c8956fe6a4e83	no	2
Warnings:					
Information:					
14	Non Patent Literature	NPL13_MobileStar.pdf	197438 ce55b68b08bf4e84c56f6309848e0ac3f12ec0bf	no	4
Warnings:					
Information:					
15	Non Patent Literature	NPL14_ORINCOAP1000.pdf	5698220 9d59de3c4b431602a24844dc7d65aa67dd372f30	no	38
Warnings:					
Information:					
16	Non Patent Literature	NPL15_Chen.pdf	1020321 d77ccaf9a24f81be51f09b647e4e09734fb0888d	no	11
Warnings:					
Information:					
17	Non Patent Literature	NPL16_3rdGeneration.pdf	18322767 abc26d1024fbbddf3bctcd840cfc6422c4bf496a	no	47
Warnings:					
Information:					
18	Non Patent Literature	NPL17_openwave-announces-avai.pdf	188087 bc796c733efcd99508b38ee0d70b4ba075848294	no	3
Warnings:					
Information:					
19	Non Patent Literature	NPL18_wireless-products-arm-r.pdf	107029 9c6f58284e2a3986f8f8638a9e42402997abf92b	no	5

Warnings:					
Information:					
20	Non Patent Literature	NPL19_Antonio.pdf	56745 e8c6b3606596c47f8175040092fcbca8b065eab1	no	1
Warnings:					
Information:					
21	Foreign Reference	FPD1_09006361800248ea.pdf	1043238 42ebe1e199235339379d7dffad05f3544f94c03c	no	26
Warnings:					
Information:					
22	Foreign Reference	FPD2_EP0779752A2.pdf	796027 394439401cc7e3a507db2862d4c6be59f870d595	no	14
Warnings:					
Information:					
23	Foreign Reference	FPD3_EP0838933A1.pdf	771633 fc3df6d46c271aa5d6740caa5796d468398adfa	no	18
Warnings:					
Information:					
24	Foreign Reference	FPD4_EP0915590A2.pdf	1270579 8a6d06c7507bab8f178f67819bfeb1d56c02c4c0	no	22
Warnings:					
Information:					
25	Foreign Reference	FPD5_EP0917320A2.pdf	3512735 87520cc4a26e07ce048b928bfbcafe3efaf85b6c1	no	66
Warnings:					
Information:					
26	Foreign Reference	FPD6_EP0924914A2.pdf	433356 061ab4ac5f66b40179d7e057bbd2a368f4c8851b	no	7
Warnings:					
Information:					
27	Foreign Reference	FPD7_EP0935364A2.pdf	2553718 b9f89d932c0a61e4096ac2a546294ca3e20f6b06	no	51
Warnings:					
Information:					
28	Foreign Reference	FPD8_WO9916263A3.pdf	188615 6915dd52a13a4714d3eab5c6646215f317d0ed02	no	5

Warnings:					
Information:					
29	Foreign Reference	FPD9_WO9951005.pdf	1840225	no	54
			e69205be29376041af363dcfac39439a2dfc3814		
Warnings:					
Information:					
30	Foreign Reference	FPD10_EP0712227A3.pdf	372286	no	3
			43c52cce68f81188f0a2d100c3fb201125bbc817		
Warnings:					
Information:					
31	Foreign Reference	FPD11_EP1435749.pdf	2311139	no	12
			4b05e11dabd6a39aab829b2bdcf0c88a4c3c87c		
Warnings:					
Information:					
32	Foreign Reference	FPD12_EP1445923.pdf	462296	no	35
			a69bc17e7d709330607f9fbc4d2cbb620c29cf4f		
Warnings:					
Information:					
33	Foreign Reference	FPD13_GB2396779B.pdf	838172	no	29
			02cc00684e35d14eb7a0003782a50c1c63945e0c		
Warnings:					
Information:					
34	Foreign Reference	FPD14_11168478.pdf	115472	no	1
			69dbd4b7a373e77aa12735cf00ee82485181fa1		
Warnings:					
Information:					
35	Foreign Reference	FPD15_01194628.pdf	97410	no	1
			ca92e535f51be3b2350d28494785f5c272155dea		
Warnings:					
Information:					
36	Foreign Reference	FPD16_03128540.pdf	95336	no	1
			9b743aa21aa80c709006c4a1fce462708fff378		
Warnings:					
Information:					
37	Foreign Reference	FPD17_07234789.pdf	107560	no	1
			60fedf30623a3e4af2e242eee96a8d02a2830136		

Warnings:					
Information:					
38	Foreign Reference	FPD18_07288514.pdf	102262 a3515b69509de4ef278dd4c38fe8a8564b99bcd7	no	1
Warnings:					
Information:					
39	Foreign Reference	FPD19_07319706.pdf	99134 5fcdbe8c0c628b5c5ff398a98149e4d4d37abd33	no	1
Warnings:					
Information:					
40	Foreign Reference	FPD20_0844568.pdf	94153 de640bc1c1b21284050bb274e42de44092574b2c	no	1
Warnings:					
Information:					
41	Foreign Reference	FPD21_0887296.pdf	116894 85a03e39213cd7ad64d0efdf4464b4d8037c9370	no	1
Warnings:					
Information:					
42	Non Patent Literature	FPD22_WO00002365A1.pdf	2283988 9f07f8ebb00ac87d09bf126eae6445d0c253d332	no	58
Warnings:					
Information:					
43	Non Patent Literature	FPD23_WO00211407A2.pdf	1517418 ed0c3ae235b0733d90066f216b24df2454bc3592	no	34
Warnings:					
Information:					
44	Non Patent Literature	FPD24_WO2004080092.pdf	1434647 e05c99d975ac8c556c9ffa5f13cb80bd8ec16fa5	no	35
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
45	Non Patent Literature	FPD25_WO09819484A2.pdf	959590 2360d19f977eb2add7c896c6159b18861fb5987	no	23
Warnings:					
Information:					

46	Non Patent Literature	FPD26_WO09927716A1.pdf	1197641 e541634f506f961a368625c7b03a3768606a5ddb	no	31
Warnings:					
Information:					
47	Non Patent Literature	FPD27_WO09955012A2.pdf	820743 9fc3dc65e3cce8de2025ec9e08dce83e45b06db	no	22
Warnings:					
Information:					
Total Files Size (in bytes):				61369526	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

42640 7590 01/06/2014
Yudell Isidore Ng Russell PLLC
8911 N. Capital of Texas Hwy.,
Suite 2110
Austin, TX 78759

EXAMINER

BATISTA, MARCOS

ART UNIT PAPER NUMBER

2642

DATE MAILED: 01/06/2014

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.

14/033,540 09/23/2013 William J. Johnson JOHNS-001US3 1470

TITLE OF INVENTION: System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications

Table with 7 columns: APPLN. TYPE, ENTITY STATUS, ISSUE FEE DUE, PUBLICATION FEE DUE, PREV. PAID ISSUE FEE, TOTAL FEE(S) DUE, DATE DUE

nonprovisional SMALL \$480 \$0 \$0 \$480 04/07/2014

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
 Commissioner for Patents
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 or Fax (571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

42640 7590 01/06/2014
 Yudell Isidore Ng Russell PLLC
 8911 N. Capital of Texas Hwy.,
 Suite 2110
 Austin, TX 78759

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

_____ (Depositor's name)
_____ (Signature)
_____ (Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/033,540	09/23/2013	William J. Johnson	JOHNS-001US3	1470

TITLE OF INVENTION: System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	04/07/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
BATISTA, MARCOS	2642	455-456300

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
 Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
 "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
 (1) The names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____
 (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____
 3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)
 PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.
 (A) NAME OF ASSIGNEE _____ (B) RESIDENCE: (CITY and STATE OR COUNTRY) _____

Please check the appropriate assignee category or categories (will not be printed on the patent): Individual Corporation or other private group entity Government

4a. The following fee(s) are submitted:
 Issue Fee
 Publication Fee (No small entity discount permitted)
 Advance Order - # of Copies _____

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)
 A check is enclosed.
 Payment by credit card. Form PTO-2038 is attached.
 The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
 Applicant certifying micro entity status. See 37 CFR 1.29
 Applicant asserting small entity status. See 37 CFR 1.27
 Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____
 Typed or printed name _____ Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P. O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
14/033,540 09/23/2013 William J. Johnson JOHNS-001US3 1470

42640 7590 01/06/2014
Yudell Isidore Ng Russell PLLC
8911 N. Capital of Texas Hwy.,
Suite 2110
Austin, TX 78759

EXAMINER

BATISTA, MARCOS

ART UNIT PAPER NUMBER

2642

DATE MAILED: 01/06/2014

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

**Notices of Allowance and Fee(s) Due mailed between October 1, 2013 and
December 31, 2013**

(Addendum to PTOL-85)

If the “Notice of Allowance and Fee(s) Due” has a mailing date on or after October 1, 2013 and before January 1, 2014, the following information is applicable to this application.

If the issue fee is being timely paid on or after January 1, 2014, the amount due is the issue fee and publication fee in effect January 1, 2014. On January 1, 2014, the issue fees set forth in 37 CFR 1.18 decrease significantly and the publication fee set forth in 37 CFR 1.18(d)(1) decreases to \$0.

If an issue fee or publication fee has been previously paid in this application, applicant is not entitled to a refund of the difference between the amount paid and the amount in effect on January 1, 2014.

Notice of Allowability	Application No. 14/033,540	Applicant(s) JOHNSON, WILLIAM J.	
	Examiner MARCOS BATISTA	Art Unit 2642	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. This communication is responsive to Applicant's Patent Application filed on September 23, 2013.
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
2. An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. The allowed claim(s) is/are 1-21. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

- a) All b) Some *c) None of the:
1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has **THREE MONTHS FROM THE "MAILING DATE"** of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in **ABANDONMENT** of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. **CORRECTED DRAWINGS** (as "replacement sheets") must be submitted.
 including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. **DEPOSIT OF and/or INFORMATION** about the deposit of **BIOLOGICAL MATERIAL** must be submitted. Note the attached Examiner's comment regarding **REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL**.

Attachment(s)

- | | |
|---|---|
| <ol style="list-style-type: none"> 1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) 2. <input checked="" type="checkbox"/> Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____ 3. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material 4. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____ | <ol style="list-style-type: none"> 5. <input type="checkbox"/> Examiner's Amendment/Comment 6. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance 7. <input type="checkbox"/> Other _____ |
|---|---|

--	--

DETAILED ACTION

1. This Action is in response to Applicant's Patent Application filed on September 23, 2013. **Claims 1-21** are still pending in the present application.

2. The present application is being examined under the pre-AIA first to invent provisions.

Information Disclosure Statement

3. The information disclosure statement submitted on 11/12/2013 has been considered by the Examiner and made of record in the application file. However, IDS entry 14 under the Non-Patent Literature was not considered due missing the date.

Allowable Subject Matter

4. **Claims 1-21** are allowed.

5. The following is an Examiner's statement of reasons for allowance:

Consider claims 1 and 21, the prior art of Bienas et al. (US 20070275730 A1) in view of Blackstock et al. (US 20060010202 A1), discloses a system for determining the location and identity of at least one mobile device and exchanging the location information and identity with nearby mobile devices.

However, the combination of Bienas in view of Blackstock failed to disclose or suggest each and every limitation recited in claims 1-21 of the claimed invention when considered as a whole.

Any comments considered necessary by Applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Marcos Batista, whose telephone number is (571) 270-5209. The Examiner can normally be reached on Monday-Thursday from 8:00am to 5:00pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Rafael Pérez-Gutiérrez can be reached at (571) 272-7915. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 703-305-3028.

Application/Control Number: 14/033,540

Page 4

Art Unit: 2642

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-2600.

*/Marcos Batista/
Primary Examiner, Art Unit 2642
December 19, 2013*

Notice of References Cited	Application/Control No. 14/033,540	Applicant(s)/Patent Under Reexamination JOHNSON, WILLIAM J.	
	Examiner MARCOS BATISTA	Art Unit 2642	Page 1 of 1

U.S. PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-2006/0010202 A1	01-2006	Blackstock et al.	709/204
*	B US-2007/0275730 A1	11-2007	Bienas et al.	455/456.1
	C US-			
	D US-			
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			


FOREIGN PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

NON-PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes 	Application/Control No. 14033540	Applicant(s)/Patent Under Reexamination JOHNSON, WILLIAM J.
	Examiner MARCOS BATISTA	Art Unit 2642

CPC- SEARCHED		
Symbol	Date	Examiner
h04w4/04, h04w4/06, h04w40/20, h04w4/02	12/19/2013	mb


CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
455	04.2, 456.34	12/19/2013	mb
370	338	12/19/2013	mb

SEARCH NOTES		
Search Notes	Date	Examiner
Intentor's Name Search	12/19/2013	mb
East Search	12/19/2013	mb
IDS Search	12/19/2013	mb

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
455	404.2, 456.3	12/19/2013	mb
370	338	12/19/2013	mb

	/MARCOS BATISTA/ Primary Examiner. Art Unit 2642
--	---

<i>Index of Claims</i> 	Application/Control No. 14033540	Applicant(s)/Patent Under Reexamination JOHNSON, WILLIAM J.
	Examiner MARCOS BATISTA	Art Unit 2642

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claims renumbered in the same order as presented by applicant
 CPA
 T.D.
 R.1.47

CLAIM		DATE							
Final	Original	12/19/2013							
	1	=							
	2	=							
	3	=							
	4	=							
	5	=							
	6	=							
	7	=							
	8	=							
	9	=							
	10	=							
	11	=							
	12	=							
	13	=							
	14	=							
	15	=							
	16	=							
	17	=							
	18	=							
	19	=							
	20	=							
	21	=							



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 1470

SERIAL NUMBER 14/033,540	FILING or 371(c) DATE 09/23/2013 RULE	CLASS 455	GROUP ART UNIT 2642	ATTORNEY DOCKET NO. JOHNS-001US3		
APPLICANTS						
INVENTORS William J. Johnson, Flower Mound, TX;						
** CONTINUING DATA ***** This application is a CON of 12/077,041 03/14/2008 PAT 8600341						
** FOREIGN APPLICATIONS *****						
** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY ** 10/08/2013						
Foreign Priority claimed <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No		<input type="checkbox"/> Met after Allowance		STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS
35 USC 119(a-d) conditions met <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No		Initials		TX	70	21
Verified and Acknowledged <u>/MARCOS BATISTA/</u> Examiner's Signature						INDEPENDENT CLAIMS 2
ADDRESS Yudell Isidore Ng Russell PLLC 8911 N. Capital of Texas Hwy., Suite 2110 Austin, TX 78759 UNITED STATES						
TITLE System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications						
FILING FEE RECEIVED 1170	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:				<input type="checkbox"/> All Fees	
					<input type="checkbox"/> 1.16 Fees (Filing)	
					<input type="checkbox"/> 1.17 Fees (Processing Ext. of time)	
					<input type="checkbox"/> 1.18 Fees (Issue)	
					<input type="checkbox"/> Other _____	
					<input type="checkbox"/> Credit	

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	41800	h04w4/04.cpc. or h04w4/06.cpc. or h04w40/20.cpc.or h04w4/02.cpc.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2013/12/19 16:59
L2	703	1 and ((exchang\$3 or send\$3 or transmit\$4) with (location or position) with (proxim\$\$ or nearby))	US-PGPUB; USPAT	ADJ	ON	2013/12/19 16:59
L3	8	1 and ((exchang\$3 or send\$3 or transmit\$4) with (location or position) with (proxim\$\$ or nearby) with (reference))	US-PGPUB; USPAT	ADJ	ON	2013/12/19 17:00
L4	18668	((455/404.2,456.3) or (370/338)).CCLS.	US-PGPUB; USPAT	OR	OFF	2013/12/19 17:00
L5	459	L4 and ((exchang\$3 or send\$3 or transmit\$4) with (location or position) with (proxim\$\$ or nearby))	US-PGPUB; USPAT	ADJ	ON	2013/12/19 17:00
L6	10	L5 and ((exchang\$3 or send\$3 or transmit\$4) with (location or position) with (proxim\$\$ or nearby) with (reference))	US-PGPUB; USPAT	ADJ	ON	2013/12/19 17:00
L8	5	6 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2013/12/19 17:00
L9	6	3 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2013/12/19 17:01
L10	8	"12077041"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2013/12/19 17:12
S3	6	"12077041"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/07 19:51
S4	1580	((WILLIAM) near2 (JOHNSON)).INV.	US-PGPUB; USPAT	ADJ	ON	2011/03/07 19:53

S7	88	"20020035493" "20020046069" "20020046077" "20020091991" "20040151151" "20040228330" "20040246940" "20040252051" "20040264442" "20050002419" "20050004838" "20060022048" "20070005188" "20070232326" "20070233387" "20070276587" "20080030308" "4644351" "5195031" "5337044" "5469362" "5758049" "5835061" "5969678" "6073062" "6236365" "6246948" "6252544" "6259405" "6266615" "6326918" "6345288" "6405123" "6414635" "6452498" "6456234" "6571279" "6615131" "6697018" "6731238" "6759960" "7009556" "7386396").PN.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/07 20:09
S8	1581	((WILLIAM) near2 (JOHNSON)).INV.	US-PGPUB; USPAT	ADJ	ON	2011/03/08 11:00
S9	7	S8 and (whereabouts same mobile data same determin\$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 11:00
S10	271	("20010018349" "20010022558" "20020035493" "20020046069" "20020046077" "20020046084" "20020091991" "20020164999" "20020167442" "20030014181" "20030069683" "20030222819" "20040010358" "20040151151" "20040228330" "20040246940" "20040252051" "20040264442" "20050002419" "20050004838" "20050046584" "20050153681" "20060022048" "20060025158" "20060284767" "20070001875" "20070005118" "20070005188" "20070232326" "20070233387" "20070233388" "20070276587" "20080024360" "20080024364" "20080030308" "20080113672" "20080310850" "20090031006" "20090033540" "20090228961" "20090234743" "20090259573" "20090271271" "20090281724" "20090286549" "4644351" "5182555" "5187810" "5195031" "5295064" "5337044" "5371678" "5379057" "5406490" "5469362" "5523950" "5675362" "5689252" "5689431" "5745865" "5758049" "5835061" "5845227" "5905451" "5908465" "5933100" "5969678" "6073062" "6101443" "6119014" "6122520" "6166627" "6185427" "6195609" "6236365" "6236933" "6246948" "6252544" "6259405" "6261086" "6266615" "6278884" "6298306" "6314369" "6314406" "6321158" "6323846" "6324692" "6326918"	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 12:25

		"6345288" "6353398" "6370629" "6381603" "6405123" "6414635" "6415227" "6434530" "6452498" "6456234" "6456234" "6490519" "6564143" "6571279" "6574484" "6611687" "6615131" "6615213" "6677894" "6681120" "6697018" "6711474" "6718344" "6731238" "6731238" "6741926" "6748318" "6759960" "6762772" "6847969" "6853911" "6868074" "6882313" "6888536" "6912398" "6915208" "6948656" "6954735" "7009556" "7058594" "7103470" "7236883" "7257392" "7298327" "7313467" "7386396" "7500607" "7525484" "7577448" "7663502" "7792273").PN.				
S11	263	S10 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 12:26
S12	1322	(455/404.2).OCLS.	US-PGPUB; USPAT	OR	OFF	2011/03/08 12:35
S13	131	S12 and (Indirect\$3 or(ILM))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 12:35
S14	121	S13 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 12:36
S15	25	S12 and (Indirect\$3 near5 (locat\$3 or position or whereabouts))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 12:46
S16	25	S15 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 12:46
S17	7	09/797517	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 13:14
S18	3	US-20050079876-A1	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT;	ADJ	ON	2011/03/08 13:22

			IBM_TDB			
S19	1	("7653388").FN.	US-PGPUB; USPAT	OR	OFF	2011/03/08 15:11
S20	1389	(determin\$3 near5 (locat\$3 or position or whereabouts)) with (UE or WTRU or subscriber or ((radio or mobile or wireless or cell or cellular or portable or hand\$held or remote) adj2 (apparatus or phone or telephone or device or unit or terminal or station or hand\$set))) with (nearby or approximat\$3 or (reference (location or position)))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 15:47
S21	1293	(determin\$3 near5 (locat\$3 or position or whereabouts)) with (UE or WTRU or subscriber or ((radio or mobile or wireless or cell or cellular or portable or hand\$held or remote) adj2 (apparatus or phone or telephone or device or unit or terminal or station or hand\$set))) with (indirect\$3 or ((reference or known) adj2 (location or position)))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 15:49
S22	35	(determin\$3 near5 (locat\$3 or position or whereabouts)) with (UE or WTRU or subscriber or ((radio or mobile or wireless or cell or cellular or portable or hand\$held or remote) adj2 (apparatus or phone or telephone or device or unit or terminal or station or hand\$set))) with (indirect\$3)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 15:50
S23	27	S22 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 15:50
S24	2	WO-2005034557-a\$	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 16:31
S25	2	US-20070275730-A\$	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 16:32
S26	2	WO-2005034557-A1	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 17:53
S27	19	S12 and (heterogeneous)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 18:01
S28	17	S27 and (@rlad<"20080314" or	US-PGPUB;	ADJ	ON	2011/03/08

		@ad<"20080314")	USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB			18:01
S29	232	(determin\$3 near3 (locat\$3 or position or whereabouts)) same (heterogeneous)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 18:09
S30	207	S29 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 18:09
S31	53	(determin\$3 near3 (locat\$3 or position or whereabouts)) same (heterogeneous) same (UE or WTRU or subscriber or ((radio or mobile or wireless or cell or cellular or portable or hand\$held or remote) adj2 (apparatus or phone or telephone or device or unit or terminal or station or hand\$set)))	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 18:10
S32	49	S31 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 18:10
S33	146	(UE or WTRU or subscriber or ((radio or mobile or wireless or cell or cellular or portable or hand\$held or remote) adj2 (apparatus or phone or telephone or device or unit or terminal or station or hand\$set))) with (NTP or network time protocol)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 18:52
S34	119	S33 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 18:52
S35	3	11/155796	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 18:54
S36	7	S10 and S20	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 20:23
S37	7	S36 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT;	ADJ	ON	2011/03/08 20:23

			IBM_TDB			
S38	4584	(370/331).CCLS.	US-PGPUB; USPAT	OR	OFF	2011/03/08 20:27
S39	13	S38 and S20	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 20:28
S40	13	S39 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/03/08 20:28
S41	38	determin\$3 with (location or position) with (nearby or neighbor\$3 or proxim\$4) with (peer)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/08/30 14:03
S42	25	S41 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/08/30 14:03
S43	1678	(wifi or ad\$hoc or bluetooth or short rage or p2p or peer\$2peer or peer\$to\$peer) with (transmit\$3 or echang\$3 or send\$3) with (location or position)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/08/30 15:31
S44	127	(wifi or ad\$hoc or bluetooth or short rage or p2p or peer\$2peer or peer\$to\$peer) with (transmit\$3 or exchang\$3 or send\$3) with (location or position) with (identi\$4)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/08/30 15:32
S45	106	S44 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/08/30 15:32
S46	2	US-20080133336-A1	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/08/30 15:53
S47	2	US-20080132251-A1	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/08/30 15:53
S48	7271	determin\$3 with (location or position) with (sound)	US-PGPUB; USPAT; FPRS;	ADJ	ON	2011/09/01 18:02

			EPO; JPO; DERWENT; IBM_TDB			
S49	562	determin\$3 with (location or position) with (sound wave)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/09/01 18:02
S54	283845	((("370") or ("455")).CLAS.	US-PGPUB; USPAT	OR	OFF	2011/09/01 18:04
S56	5	S54 and S49	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/09/01 18:04
S57	5	S56 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/09/01 18:05
S58	1364	determin\$3 with (location or position) with ((sound or acoustic) adj2 wave)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/09/01 18:08
S59	8	S54 and S58	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/09/01 18:08
S60	25	((repel\$3 or scar\$3)near2 (pest or animal)) with ((sound or acoustic) adj2 wave)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/09/01 21:01
S61	19	S60 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/09/01 21:02
S62	6	11/445727	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/09/01 21:07
S63	3	US-20050243820-A1	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/09/02 10:36
S64	3	US-20030060210-A1	US-PGPUB;	ADJ	ON	2011/09/02

			USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB			10:45
S65	3	US-20070257833-A1	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/09/02 11:55
S66	583	determin\$3 near5 (location or position) near5((sound or acoustic) adj2 wave)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/09/02 11:59
S67	549	S66 and (@rlad< "20080314" or @ad< "20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/09/02 11:59
S68	8	09/806618	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2011/09/02 12:01
S69	99	("6252544" "6259405" "6326918" "6615131" "20020091991" "4644351" "5758049" "6246948" "6345288" "6571279" "7009556" "20070276587" "20070275730" "5337044" "5835061" "5969678" "6236365" "6731238" "20070005188" "20020035493" "20020046069" "20020046077" "20040228330" "6759960" "20060136544" "20040264442" "20050004838" "20070232326" "20040246940" "6073062" "6405123" "6414635" "20040252051" "20040201459" "20070281716" "20040151151" "20050002419" "6266615" "20080030308" "7386396" "20060240828" "5195031" "5469362" "6452498" "6456234" "6697018" "20060022048" "20070233387").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2013/03/14 12:32
S70	5	(UE or WTRU or subscriber or ((radio or mobile or wireless or cell or cellular or portable or hand\$held or remote or user) adj2 (apparatus or phone or telephone or device or unit or terminal or station or hand\$set or equipment))) with (send\$3 or provid\$3 or transmit\$4 or exchang\$3) with ((subscriber or user)near2 (id or identity or identification)) with (ad\$hoc)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2013/03/14 16:40
S71	3	S70 and (@rlad< "20080314" or @ad< "20080314")	US-PGPUB; USPAT; FPRS;	ADJ	ON	2013/03/14 16:40

			EPO; JPO; DERWENT; IBM_TDB			
S72	25	(send\$3 or provid\$3 or transmit\$4 or exchang\$3) with ((subscriber or user)near2 (id or identity or identification)) with (ad\$hoc)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2013/03/14 16:47
S73	22	S72 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2013/03/14 16:47
S75	295	(send\$3 or provid\$3 or transmit\$4 or exchang\$3) with ((subscriber or user)near2 (id or identity or identification)) with (ad\$hoc or bluetooth or serverless)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2013/03/14 16:54
S76	238	S75 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2013/03/14 16:55
S77	101	(send\$3 or provid\$3 or transmit\$4 or exchang\$3) with ((subscriber or user)near2 (id or identity or identification)) with (ad\$hoc or serverless or peer\$peer or peer\$to\$peer)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2013/03/14 16:56
S78	81	S77 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2013/03/14 16:56
S79	2	11/211112	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2013/03/14 17:17
S80	3	US-20060194589-a\$	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2013/07/02 12:45
S81	77	((determin\$3 or calculat\$3) near5 (locat\$3 or position or whereabouts)) with (UE or WTRU or subscriber or ((radio or mobile or wireless or cell or cellular or portable or hand\$held or remote) adj2 (apparatus or phone or telephone or device or unit or terminal or station or hand\$set))) with (ad\$hoc or peer\$peer or serverless or localized)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2013/07/02 12:52

EAST Search History

S82	46	S81 and (@rlad<"20080314" or @ad<"20080314")	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2013/07/02: 12:53
S83	1787	((WILLIAM) near2 (JOHNSON)).INV.	US-PGPUB; USPAT	ADJ	ON	2013/12/19: 16:28
S87	18668	((455/404.2,456.3) or (370/338)).CCLS.	US-PGPUB; USPAT	OR	OFF	2013/12/19: 16:55
S89	459	S87 and ((exchang\$3 or send\$3 or transmit\$4) with (location or position) with (proxim\$\$ or nearby))	US-PGPUB; USPAT	ADJ	ON	2013/12/19: 16:56

12/ 19/ 2013 5:46:11 PM

C:\Users\mbatista\Documents\EAST\Workspaces\14033540 SYSTEM AND METHOD FOR LOCATION BASED EXCHANGES OF DATA FACILITATING DISTRIBUTED LOCAL APPLICATIONS.wsp

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	3636421		1972-03-26	Barker et al.	
	2	4021780		1977-05-01	Narey et al.	
	3	4445118		1984-04-01	Taylor et al.	
	4	4757267		1988-07-01	Riskin	
	5	4841560		1989-06-01	Chan et al.	
	6	4922516		1990-05-01	Butler et al.	
	7	4977399		1990-12-01	Price et al.	
	8	5095532		1992-03-10	Mardus	
	9	5122795		1992-06-01	Cublely et al.	
	10	5185857		1993-02-09	Rozmanith et al	
	11	5223844		1993-06-29	Mansell et al.	
	12	5243652		1993-09-07	Teare et al.	
	13	5303393		1994-04-12	Noreen et al.	
	14	5321242		1994-06-14	Heath, Jr.	
	15	5365516		1994-11-15	Jandrell	
	16	5371794		1994-12-06	Diffie et al.	
	17	5390237		1995-02-12	Hoffman et al.	
	18	5404505		1995-04-04	Levinson	
	19	5432841		1995-07-11	Rimer	
	20	5444444		1995-08-22	Ross	
	21	5451757		1995-09-19	Heath, Jr.	
	22	5461627		1995-10-24	Rypinski	
	23	5264822		1993-11-23	Vogelman et al.	
	24	5475735		1995-12-10	Williams et al.	
	25	5485163		1996-01-16	Singer et al.	
	26	5487103		1996-01-23	Richardson	
	27	5493309		1996-02-20	Bjornholt et al.	
	28	5497414		1996-03-01	Bartholomew	
	29	5504482		1996-04-02	Schreder	
	30	5511111		1996-04-01	Serbetcioğlu et al.	
	31	5511233		1996-04-23	Otten	
	32	5512908		1996-04-01	Herrick	
	33	5513263		1996-04-30	White et al.	
	34	5528248		1996-06-18	Steiner et al.	
	35	5544354		1996-08-06	May et al.	
	36	5559520		1996-09-24	Barzegar et al.	
	37	5566235		1996-10-15	Hetz	
	38	5870555		1999-02-09	Pruett et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	39	5581479		1996-12-03	McLaughlin	
	40	5588042		1996-12-24	Comer	
	41	5590398		1996-12-31	Matthews	
	42	5596625		1997-01-21	LeBlanc	
	43	5602843		1997-02-11	Gray	
	44	5610973		1997-03-11	Comer	
	45	5625364		1997-04-29	Herrick et al.	
	46	5627549		1997-05-06	Park	
	47	5636245		1997-06-03	Ernst et al.	
	48	5646632		1997-07-08	Khan et al.	
	49	5654959		1997-08-05	Baker et al.	
	50	5657375		1997-08-22	Connolly et al.	
	51	5661492		1997-08-26	Shoap et al.	
	52	5663734		1997-09-02	Krasner	
	53	5664948		1997-09-09	Dimitriadis et al.	
	54	5666481		1997-09-09	Lewis	
	55	5687212		1997-11-11	Kinser, Jr. et al	
	56	5689431		1997-11-18	Rudow et al.	
	57	5694453		1997-12-02	Fuller et al.	
	58	5701301		1997-12-23	Weisser, Jr.	
	59	5712899		1998-01-27	Pace, II, Harold	
	60	5713075		1998-01-27	Threadgill et al.	
	61	5714948		1998-02-03	Farmakis et al.	
	62	5717688		1998-02-10	Belanger et al.	
	63	5720033		1998-02-17	Deo	
	64	5724521		1998-03-03	Dedrick	
	65	5727057		1998-03-10	Emery et al.	
	66	5729680		1998-03-17	Belanger et al.	
	67	5771283		1998-06-23	Chang et al.	
	68	5774534		1998-06-30	Mayer	
	69	5778304		1998-07-07	Grube et al.	
	70	5790974		1998-08-04	Tognazzini, Bruce	
	71	5794210		1998-08-11	Goldhaber et al.	
	72	5796727		1998-08-18	Harrison et al.	
	73	5798733		1998-08-25	Ethridge	
	74	5806018		1998-09-08	Smith et al.	
	75	5812763		1998-09-22	Teng	
	76	5819155		1998-10-06	Worthey et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	77	5835061		1998-11-10	Stewart	
	78	5838774		1998-11-17	Weisser, Jr.	
	79	5842010		1998-11-24	Jain et al.	
	80	5845211		1998-12-01	Roach	
	81	5852775		1998-12-22	Hidary, Murray	
	82	5855007		1998-12-29	Jovicic et al.	
	83	5870724		1999-02-09	Lawlor et al.	
	84	5875186		1999-02-23	Belanger et al.	
	85	5875401		1999-02-23	Rochkind	
	86	5878126		1999-03-02	Velamuri et al.	
	87	5880958		1999-03-09	Helms et al.	
	88	5881131		1999-03-09	Farris et al.	
	89	5884284		1999-03-16	Peters et al.	
	90	5889953		1999-03-30	Thebaut et al.	
	91	5896440		1999-04-20	Reed et al.	
	92	5897640		1999-04-27	Veghte et al.	
	93	5903636		1999-05-11	Malik	
	94	5907544		1999-05-25	Rypinski	
	95	5920846		1999-07-06	Storch et al.	
	96	5922040		1999-07-13	Prabhakaran	
	97	5923702		1999-07-13	Brenner et al.	
	98	5933420		1999-08-03	Jaszewski et al.	
	99	5938721		1999-08-17	Dussell et al.	
	100	5949867		1999-09-07	Sonnenberg	
	101	5950130		1999-09-07	Coursey	
	102	5961593		1999-10-05	Gabber et al.	
	103	5963866		1999-10-05	Palamara et al.	
	104	5963913		1999-10-05	Henneuse et al.	
	105	5968176		1999-10-19	Nessett et al.	
	106	5969678		1999-10-19	Stewart	
	107	5982867		1999-11-09	Urban et al.	
	108	5983091		1999-11-09	Rodriguez	
	109	5987381		1999-11-16	Oshizawa	
	110	5991287		1999-11-23	Diepstraten et al.	
	111	5995015		1999-11-30	De Temple et al.	
	112	6006090		1999-12-21	Coleman et al.	
	113	6009398		1999-12-28	Mueller et al.	
	114	6011975		2000-01-04	Emery et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	115	6026151		2000-02-15	Bauer et al.	
	116	6028921		2000-02-22	Malik et al.	
	117	6047327		2000-04-04	Tso et al.	
	118	6055637		2000-04-25	Hudson et al.	
	119	6058106		2000-05-02	Cudak et al.	
	120	6067297		2000-05-23	Beach	
	121	6076080		2000-06-13	Morscheck et al.	
	122	6085086		2000-07-04	La Porta et al.	
	123	6091956		2000-07-18	Hollenberg	
	124	6101381		2000-08-08	Tajima et al.	
	125	6101443		2000-08-08	Kato et al.	
	126	6112186		2000-08-29	Bergh et al.	
	127	6115669		2000-09-05	Watanabe et al.	
	128	6122520		2000-09-19	Want et al.	
	129	6133853		2000-10-17	Obradovich et al.	
	130	6138003		2000-10-24	Kingdon et al.	
	131	6138119		2000-10-24	Hall et al.	
	132	6141609		2000-10-31	Herdeg et al.	
	133	6144645		2000-11-07	Struhsaker et al.	
	134	6154152		2000-11-28	Ito	
	135	6154637		2000-11-28	Wright et al.	
	136	6157829		2000-12-05	Grube et al.	
	137	6163274		2000-12-19	Lindgren, Gary L.	
	138	6167255		2000-12-26	Kennedy, III et al.	
	139	6182226		2001-01-30	Reid et al.	
	140	6184829		2001-02-06	Stilp	
	141	6185426		2001-02-06	Alperovich et al.	
	142	6185484		2001-02-06	Rhinehart	
	143	6192314		2001-02-20	Khavakh et al.	
	144	6202054		2001-03-13	Lawlor et al.	
	145	6205478		2001-03-20	Sugano et al.	
	146	6208854		2001-03-27	Roberts et al.	
	147	6208866		2001-03-27	Rouhollahzadeh et al.	
	148	6226277		2001-05-01	Chuah	
	149	6229477		2001-05-08	Chang et al.	
	150	6229810		2001-05-08	Gerszberg et al.	
	151	6233329		2001-05-15	Urban et al.	
	152	6233452		2001-05-15	Nishino	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	153	6236360		2001-05-22	Rudow et al.	
	154	6236940		2001-05-22	Rudow et al.	
	155	6246361		2001-06-12	Weill et al.	
	156	6259405		2001-07-10	Stewart et al.	
	157	6263209		2001-07-17	Reed et al.	
	158	6278938		2001-08-21	Alumbaugh	
	159	6285665		2001-09-04	Chuah et al.	
	180	6285931		2001-09-04	Hattori et al.	
	181	6298234		2001-10-02	Brunner	
	182	6308273		2001-10-23	Goertzel et al.	
	183	6311069		2001-10-30	Havinis et al.	
	184	6317718		2001-11-13	Fano	
	185	6321092		2001-11-20	Fitch et al.	
	186	6324396		2001-11-27	Vasa et al.	
	187	6326918		2001-12-04	Stewart	
	188	6327254		2001-12-04	Chuah	
	189	6327357		2001-12-04	Meek et al.	
	190	6332127		2001-12-18	Bandera et al.	
	191	6332163		2001-12-21	Bowman-Amuah	
	192	6343290		2002-01-29	Cossins et al.	
	193	6353664		2002-03-05	Cannon et al.	
	194	6359880		2002-03-19	Curry et al.	
	195	6360101		2002-03-19	Irvin	
	196	6366561		2002-04-02	Bender	
	197	6377548		2002-04-23	Chuah et al.	
	198	6377810		2002-04-23	Geiger et al.	
	199	6377982		2002-04-23	Rai et al.	
	200	6385531		2002-05-07	Bates et al.	
	201	6385591		2002-05-07	Mankoff	
	202	6389426		2002-05-14	Turnbull et al.	
	203	6393482		2002-05-21	Rai et al.	
	204	6400722		2002-06-04	Chuah et al.	
	205	6414950		2002-07-02	Rai et al.	
	206	6415019		2002-07-02	Savaglio et al.	
	207	6418308		2002-07-09	Heinonen et al.	
	208	6421441		2002-07-16	Dzuban	
	209	6421714		2002-07-16	Rai et al.	
	210	6427073		2002-07-30	Kortelsalmi et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	211	6427119		2002-07-30	Stefan et al.	
	212	6430276		2002-08-06	Bouvier et al.	
	213	6430562		2002-08-06	Kardos et al.	
	214	6442391		2002-08-27	Johansson et al.	
	215	6442687		2002-08-27	Savage, Colin	
	216	6449272		2002-09-10	Chuah et al.	
	217	6449497		2002-09-10	Kirbas et al.	
	218	6463533		2002-10-08	Calamera et al.	
	219	6470378		2002-10-22	Tracton et al.	
	220	6470447		2002-10-22	Lambert et al.	
	221	6473626		2002-10-29	Nevoux et al.	
	222	6477382		2002-11-05	Mansfield et al.	
	223	6477526		2002-11-05	Hayashi et al.	
	224	6484029		2002-11-19	Hughes et al.	
	225	6484092		2002-11-19	Seibel	
	226	6484148		2002-11-19	Boyd	
	227	6490291		2002-12-03	Lee et al.	
	228	6496491		2002-12-17	Chuah et al.	
	229	6496931		2002-12-17	Rajchel et al.	
	230	6505046		2003-01-07	Baker	
	231	6505048		2003-01-07	Moles et al.	
	232	6505049		2003-01-07	Dorenbosch	
	233	6505120		2003-01-07	Yamashita et al.	
	234	6505163		2003-01-07	Zhang et al.	
	235	6512754		2003-01-28	Feder et al.	
	236	6516055		2003-02-04	Bedeski et al.	
	237	6516416		2003-02-04	Gregg et al.	
	238	6519252		2003-02-11	Sallberg	
	239	6519458		2003-02-11	Oh et al.	
	240	6522876		2003-02-18	Weiland et al.	
	241	6526275		2003-02-25	Calvert	
	242	6526349		2003-02-25	Bullock et al.	
	243	6532418		2003-03-11	Chun et al.	
	244	6545596		2003-04-08	Moon	
	245	6546257		2003-04-08	Stewart	
	246	6560442		2003-05-06	Yost et al.	
	247	6560461		2003-05-06	Fomukong et al.	
	248	6577643		2003-06-10	Rai et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	249	6577644		2003-06-10	Chuah et al.	
	250	6594482		2003-07-15	Findikli et al.	
	251	6618474		2003-09-09	Reese, Morris	
	252	6618593		2003-09-09	Drutman et al.	
	253	6622016		2003-09-16	Sladek et al.	
	254	6628627		2003-09-30	Zendle et al.	
	255	6628928		2003-09-30	Crosby et al.	
	256	6628938		2003-09-30	Rachabathuni et al.	
	257	6633633		2003-10-14	Bedingfield	
	258	6640184		2003-10-28	Rabe, Duane Carl	
	259	6647257		2003-11-11	Owensby, Craig A.	
	260	6647269		2003-11-11	Hendrey et al.	
	261	6650901		2003-11-18	Schuster et al.	
	262	6654610		2003-11-25	Chen et al.	
	263	6662014		2003-12-09	Walsh	
	264	6665536		2003-12-16	Mahany	
	265	6665718		2003-12-16	Chuah et al.	
	266	6671272		2003-12-30	Vaziri et al.	
	267	6675017		2004-01-06	Zellner et al.	
	268	6675208		2004-01-06	Rai et al.	
	269	6677894		2004-01-13	Sheynblat et al.	
	270	6697783		2004-02-24	Brinkman et al.	
	271	6701160		2004-03-02	Pinder et al.	
	272	6701251		2004-03-02	Stefan et al.	
	273	6704311		2004-03-09	Chuah et al.	
	274	6716101		2004-04-06	Meadows et al.	
	275	6721406		2004-04-13	Contractor	
	276	6725048		2004-04-20	Mao et al.	
	277	6732080		2004-05-04	Blants	
	278	6732101		2004-05-04	Cook	
	279	6732176		2004-05-04	Stewart et al.	
	280	6738808		2004-05-18	Zellner et al.	
	281	6754504		2004-06-22	Reed	
	282	6754582		2004-06-22	Smith et al.	
	283	6772064		2004-08-03	Smith et al.	
	284	6799049		2004-09-28	Zellner et al.	
	285	6801509		2004-10-05	Chuah et al.	
	286	6816720		2004-11-09	Hussain et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	287	6819929		2004-11-16	Antonucci et al.	
	288	6829475		2004-12-07	Lee et al.	
	289	6850758		2005-02-01	Paul et al.	
	290	6867733		2005-03-15	Sandhu et al.	
	291	6868074		2005-03-15	Hanson, Joel	
	292	6874011		2005-03-29	Spielman	
	293	6876858		2005-04-15	Duvall et al.	
	294	6898569		2005-05-24	Bansal et al.	
	295	6937869		2005-08-30	Rayburn	
	296	6954147		2005-10-11	Cromer et al.	
	297	6985747		2006-01-10	Chithambaram	
	298	6999572		2006-02-04	Shaffer et al.	
	299	7005985		2006-02-28	Steeves	
	300	7023995		2006-04-04	Olsson	
	301	7043231		2006-05-09	Bhatia et al.	
	302	7069319		2006-06-27	Zellner et al.	
	303	7085555		2006-08-01	Zellner et al.	
	304	7103368		2006-09-05	Teshima	
	305	7103476		2006-09-05	Smith et al.	
	306	7106843		2006-09-12	Gainsboro et al.	
	307	7110749		2006-09-19	Zellner et al.	
	308	7116977		2006-10-03	Moton et al.	
	309	7124101		2006-10-17	Mikurak	
	310	7130631		2006-10-31	Enzmann et al.	
	311	7139722		2006-11-21	Perrella et al.	
	312	7181225		2007-02-20	Moton et al.	
	313	7181529		2007-02-20	Bhatia et al.	
	314	7188027		2007-03-06	Smith et al.	
	315	7190960		2007-03-13	Wilson et al.	
	316	7203502		2007-04-10	Wilson et al.	
	317	7212829		2007-05-01	Lau et al.	
	318	7224978		2007-05-29	Zellner et al.	
	319	7236799		2007-06-26	Wilson et al.	
	320	7245925		2007-07-17	Zellner	
	321	7260378		2007-08-21	Holland et al.	
	322	7272493		2007-09-18	Hamrick et al.	
	323	7292939		2007-11-06	Smith et al.	
	324	7295924		2007-11-13	Smith et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	325	7362851		2008-04-22	Contractor	
	326	7383052		2008-06-03	Moton et al.	
	327	RE39717		2007-07-03	Yates et al.	
	328	5363377		1994-11-08	Sharpe	
	329	5625668		1997-04-29	Loomis	
	330	5455807		1995-10-03	Nepple	
	331	5586254		1996-12-07	Kondo et al.	
	332	5089814		1992-02-18	DeLuca et al.	
	333	5265070		1993-11-23	Minowa	
	334	5131020		1992-07-14	Liebesny et al.	
	335	5245608		1993-09-14	Deaton et al.	
	336	5583864		1996-12-10	Lightfoot et al.	
	337	5590196		1996-12-13	Moreau	
	338	5594779		1997-01-14	Goodman	
	339	5592470		1997-01-07	Rudrapatna et al.	
	340	5664948		1997-09-09	Dimitriadis et al.	
	341	5677905		1997-10-14	Bigham	
	342	5704049		1997-12-30	Briechle	
	342	5887259		1999-03-23	Zicker et al.	
	343	6067082		2000-05-23	Enmei	
	344	6157946		2000-12-05	Itakura et al.	
	345	7155199		2006-12-26	Zalewski et al.	
	346	5121126		1992-06-09	Clagett	
	347	5608854		1997-03-04	Labeledz et al.	
	348	5561704		1996-10-01	Samilando	
	349	5892454		1999-04-06	Schipper et al.	
	350	6340958		2002-01-22	Cantu et al.	
	351	5347632		1994-09-13	Filepp et al.	
	352	6018293		2000-01-25	Smith et al.	
	353	5539395		1996-07-23	Buss et al.	
	354	5214793		1993-05-25	Conway et al.	
	355	5826195		1998-10-20	Westerlage et al.	
	356	6820062		2004-11-05	Gupta et al.	
	357	6937998		2005-08-30	Swartz et al.	
	358	6759960		2004-07-06	Stewart et al.	
	359	6697018		2004-02-24	Stewart et al.	
	360	7058594		2006-06-06	Stewart et al.	
	361	7009556		2006-03-07	Stewart et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	362	4255619		1981-03-10	Saito	
	363	4536647		1985-08-20	Atalla et al.	
	364	4845504		1989-07-04	Roberts, et al.	
	365	4973952		1990-11-27	Malec et al.	
	366	4974170		1990-11-27	Bouve et al.	
	367	5363245		1997-06-03	Ernst et al.	
	368	5870724		1999-02-09	Lawlor et al.	
	369	6407673		2002-06-18	Lane	
	370	6408307		2002-06-18	Semple et al.	
	371	6414635		2002-07-02	Stewart et al.	
	372	6442479		2002-08-27	Barton	
	373	6452498		2002-09-17	Stewart	
	374	6615131		2003-09-02	Rennard et al.	
	375	6405123		2002-06-11	Rennard et al.	
	376	626615		2001-07-24	Jin	
	377	4644351		1987-02-17	Zabarsky et al.	
	378	5337044		1944-08-09	Folger et al.	
	379	5469362		1995-11-23	Hunt et al.	
	380	5758049		1998-11-10	Johnson et al.	
	381	5835061		1998-11-10	Stewart	
	382	5969678		1998-10-19	Stewart	
	383	6073062		2000-06-06	Hoshino et al.	
	384	6236362		2001-05-22	Leblanc et al.	
	385	6326918		2001-12-04	Stewart	
	386	6259405		2001-07-10	Stewart et al.	
	387	6252544		2001-06-26	Hoffberg	
	388	6414635		2002-07-02	Stewart et al.	
	389	6452498		2002-09-17	Stewart	
	390	6697018		2004-02-24	Stewart	
	391	6731238		2004-05-04	Johnson	
	392	6759960		2004-07-06	Stewart	
	393	7009556		2006-03-07	Stewart	
	394	5196031		1993-03-16	Ordish	
	395	6345288		2002-02-05	Reed et al.	
	396	6571279		2003-05-27	Herz et al.	
	397	6456234		2002-09-24	Johnson	
	398	6246948		2001-06-12	Thakker	
	399	7386396		2008-06-10	Johnson	

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Complete if Known		
				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	400	7177651		2007-02-13	Almassy	
	401	7787887		2010-08-31	Gupta et al.	
	402	6427115		2002-07-30	Sekiyama	
	403	6370389		2002-04-09	Isomursu et al.	
	404	6381311		2002-04-30	Joyce et al.	
	405	6389055		2002-05-14	August et al.	

Substitute for form 1449/PTO				Complete if Known		
				Application Number	14/033,540	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENT APPLICATION PUBLICATIONS						
Examiner Initials	Cite No.	Publication Number	Kind Code	Publication Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	2001/0021646		2001-09-13	Antonucci et al.	
	2	2001/0034709		2001-10-25	Stoifo et al.	
	3	2001/0049275		2001-12-06	Pierry et al.	
	4	2001/0051911		2001-12-13	Marks et al.	
	5	2002/0037709		2002-03-28	Bhatia et al.	
	6	2002/0037722		2002-03-28	Hussain et al.	
	7	2002/0037731		2002-03-28	Mao et al.	
	8	2002/0037744		2002-03-28	Bhatia et al.	
	9	2002/0037750		2002-03-28	Hussain et al.	
	10	2002/0038362		2002-03-28	Bhatia et al.	
	11	2002/0038384		2002-03-28	Khan et al.	
	12	2002/0038386		2002-03-28	Bhatia et al.	
	13	2002/0052781		2002-05-02	Aufricht et al.	
	14	2002/0077083		2002-06-20	Zellner et al.	
	15	2002/0077084		2002-06-20	Zellner et al.	
	16	2002/0077118		2002-06-20	Zellner et al.	
	17	2002/0077130		2002-06-20	Owensby	
	18	2002/0077897		2002-06-20	Zellner et al.	
	19	2002/0087335		2002-07-01	Meyers et al.	
	20	2002/0090932		2002-07-04	Bhatia et al.	
	21	2002/0095312		2002-07-18	Wheat	
	22	2002/0102993		2002-08-01	Hendrey et al.	
	23	2002/0107027		2002-08-08	O'Neil	
	24	2002/0120713		2002-08-29	Gupta et al.	
	25	2002/0161637		2002-10-31	Sugaya	
	26	2002/0174147		2002-11-21	Wang et al.	
	27	2003/0016233		2003-01-23	Charpentier	
	28	2003/0140088		2003-07-24	Robinson et al.	
	29	2003/0169151		2003-09-11	Ebling et al.	
	30	2004/0002329		2004-01-01	Bhatia et al.	
	31	2004/0097243		2004-05-20	Zellner et al.	
	32	2004/0111269		2004-06-10	Koch	
	33	2004/0164898		2004-08-26	Stewart	
	34	2004/0203903		2004-10-14	Wilson et al.	
	35	2004/0205198		2004-10-14	Zellner et al.	
	36	2004/0266453		2004-12-30	Maanoja et al.	
	37	2005/0043036		2005-02-24	loppe et al.	
	38	2005/0060365		2005-03-17	Robinson et al.	
	39	2005/0096067		2005-05-05	Martin, Dannie E.	
	40	2005/0114777		2005-05-26	Szeto	
	41	2005/0151655		2005-07-14	Hamrick et al.	
	42	2005/0246097		2005-11-03	Hamrick et al.	
	43	2005/0272445		2005-12-08	Zellner, Samuel	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENT APPLICATION PUBLICATIONS						
Examiner Initials	Cite No.	Publication Number	Kind Code	Publication Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	44	2006/0030335		2006-02-09	Zellner et al.	
	45	2006/0030339		2006-02-09	Zhovnirovsky et al.	
	46	2006/0059043		2006-03-16	Chan et al.	
	47	2006/0089134		2006-04-27	Moton et al.	
	48	2006/0094447		2006-05-04	Zellner, Samuel	
	49	2006/0099966		2006-05-11	Moton et al.	
	50	2006/0105784		2006-05-18	Zellner et al.	
	51	2006/0106537		2006-05-18	Hamrick et al.	
	52	2006/0167986		2006-07-27	Trzyna et al.	
	53	2006/0189327		2006-08-24	Zellner et al.	
	54	2006/0189332		2006-08-24	Benco et al.	
	55	2006/0195570		2006-08-31	Zellner et al.	
	56	2006/0253252		2006-11-09	Hamrick et al.	
	57	2007/0010260		2007-01-11	Zellner et al.	
	58	2007/0042789		2007-02-22	Moton et al.	
	59	2007/0105565		2007-05-10	Enzmann et al.	
	60	2007/0124721		2007-05-31	Cowing et al.	
	61	2007/0136603		2007-06-14	Kuecuekyan	
	62	2007/0250920		2007-10-25	Lindsay	
	63	2008/0096529		2008-04-24	Zellner	
	64	2005/0017068		2005-01-27	Zalewski et al.	
	65	2001/0028301		2001-10-11	Geiger et al.	
	66	2001/0007450		2001-07-12	Begum	
	67	2004/0186902		2004-09-23	Stewart et al.	
	68	2006/0164302		2006-07-27	Stewart et al.	
	69	2006/0183467		2006-08-17	Stewart et al.	
	70	2006/0059043		2006-03-16	Stewart et al.	
	71	2002/0035474		2002-03-31	Alpdemir	
	72	2001/0001239		2001-05-17	Stewart	
	73	2002/0046090		2002-04-18	Stewart	
	74	2003/0003990		2003-01-02	Von Kohorn	
	75	2003/0018527		2003-01-23	Filepp et al.	
	76	2002/0035493		2002-03-21	Mozayeny et al.	
	77	2002/0046069		2002-04-18	Mozayeny et al.	
	78	2002/0046077		2002-04-18	Mozayeny et al.	
	79	2002/0091991		2002-07-11	Castro	
	80	2005/0004838		2005-01-06	Perkowski et al.	
	81	2005/0002419		2005-01-06	Doviak et al.	
	82	2004/0264442		2004-12-30	Kubler et al.	
	83	2004/0246940		2004-12-09	Kubler et al.	
	84	2004/0228330		2004-11-18	Kubler et al.	
	85	2004/0151151		2004-08-05	Kubler et al.	
	86	2004/0252051		2004-12-16	Johnson	
	87	2007/0005188		2007-01-04	Johnson	
	88	2007/0233387		2007-10-04	Johnson	

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Complete if Known		
				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENT APPLICATION PUBLICATIONS						
Examiner Initials	Cite No.	Publication Number	Kind Code	Publication Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	89	2007/0276587		2007-11-29	Johnson	
	90	2007/0232326		2007-10-04	Johnson	
	91	2008/0030308		2008-02-07	Johnson	
	92	2006/0022048		2006-02-02	Johnson	
	93	2009/0233622		2009-09-17	Johnson	
	94	2009/0233633		2009-09-17	Johnson	
	95	2010/0069035		2010-03-18	Johnson	
	96	2010/0227595		2010-09-09	Johnson	
	97	2006/0010202		2006-01-12	Blackstock et al.	
	98	2004/0201459		2004-10-14	Rich et al.	
	99	2006/0136544		2006-06-22	Atsmon et al.	
	100	2007/0281716		2007-12-06	Altman et al.	
	101	2006/0240828		2006-10-26	Jain et al.	
	102	2007/0275730		2007-11-29	Bienas et al.	
	103	2006/0194589		2006-08-31	Sankisa	
	104	2007/0287473		2007-12-13	Dupray	
	105	2008/0071761		2008-03-20	Singh et al.	
	106	2004/0116131		2004-06-17	Hochrainer et al.	
	107	2007/0275730		2007-11-29	Bienas et al.	
	108	2007/0244633		2007-10-18	Phillips et al.	
	109	2008/0170679		2008-07-17	Sheha et al.	
	110	2005/0050227		2005-03-03	Michelman	
	111	2003/0030731		2003-02-13	Colby	
	112	2006/0009190		2006-01-12	Laliberte	
	113	2006/0198359		2006-09-07	Fok et al.	
	114	2001/0005864		2001-06-28	Mousseau et al.	
	115	2010/0146160		2010-06-10	Piekarski	
	116	2005/0283833		2005-12-22	Lalonde et al.	
	117	2010/0159946		2010-06-24	Cheung et al.	
	118	2002/0095454		2002-07-18	Reed et al.	
	119	2006/0252465		2006-11-09	Karstens et al.	
	120	2008/0301561		2008-12-04	Bain	
	121	2009/0067593		2009-03-12	Ahlin	
	122	2009/0167524		2009-07-02	Chesnutt et al.	
	123	2009/0190734		2009-07-16	White et al.	
	124	2009/0054077		2009-02-26	Gauthier et al.	
	125	2006/0194589		2006-08-31	Sankisa	
	126	2011/0021145		2011-01-27	Johnson et al.	
	127	2010/0235748		2010-09-16	Johnson et al.	
	128	2009/0233623		2009-09-17	Johnson et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
FOREIGN PATENT DOCUMENTS						
Examiner Initial	Cite No.	Foreign Patent Document Number	Kind Code	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	WO 00/076249		2000-12-14	Telefonaktiebolaget LM Ericsson	
	2	EP 779752		2004-06-16	AT&T Corp.	
	3	EP 838933		2008-04-29	IBM Corporation	
	4	EP 915590		1999-05-12	Unwired Planet, Inc.	
	5	EP 917320		1999-05-19	Lucent Technologies, Inc.	
	6	EP 924914		2003-04-23	Nokia Corporation	
	7	EP 935364		1999-08-11	AT&T Corp.	
	8	WO 99/16263		1999-04-01	Nokia Telecommunications	
	9	WO 99/51005		1999-10-07	Transaccess Corp.	
	10	EP 0712227		1996-05-01	Harris Corporation	
	11	EP 1435749		2004-07-01	Evolium S.A.S.	
	12	EP 1445923		2004-08-01	NEC Corporation	
	13	GB 2396779		2004-06-01	Samsung Electronics Co., Ltd	
	14	JP 11-168478		1999-06-01	Pronet Tracking System, Inc.	
	15	JP 01-194628		1989-08-01	NEC Corporation	
	16	JP 03-128540		1991-05-01	Hitachi Comm. Syst., Inc.	
	17	JP 07-234789		1995-09-01	Hitachi Ltd	
	18	JP 07-288514		1995-10-01	Mita Ind. Co., Ltd	
	19	JP 07-319706		1995-12-01	Hitachi Ltd	
	20	JP 08-44568		1996-02-01	Hitachi Zosen Group	
	21	JP 08-87296		1996-04-01	Hamagami et al.	
	22	WO 00/02365		2000-01-01	Bell South Int. Prop. Corp.	
	23	WO 02/11407		2002-02-01	Bell South Int. Prop. Corp.	
	24	WO 04/80092		2004-09-01	Siemens Aktiengesellschaft	
	25	WO 98/19484		1998-05-01	Siemens Aktiengesellschaft	
	26	WO 99/27716		1999-06-01	Ericsson, Inc.	
	27	WO 99/55012		1999-10-01	Netline Communications Technologies LTD	


Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Complete if Known	
		Application Number	14/033,540
		Filing Date	2013-09-23
		First Named Inventor	William J. Johnson
		Examiner Name	Not yet assigned
		Art Unit	2668
		Attorney Docket No.	JOHNS-001US3
NON PATENT LITERATURE			
Examiner Initial	Cite No.	Include name of author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	
	1	Bill N. Schilit and Marvin M. Theimer, Disseminating Active Map Information Mobile Hosts, IEEE Network, September/October 1994.	
	2	Andy Harter and Andy Hooper, A Distributed Location system for the Active Office, IEEE Network, January/February 1994.	
	3	Max J. Egenhofer, Spatial SQL: A Query and Presentation Language, IEEE Network, February 1994.	
	4	Mike Spreitzer and Marvin Theimer, Providing Location Information in a Ubiquitous Computing Environment, Proceedings of the Fourteenth ACM Symposium on Operating Systems Principles, December 1993.	
	5	George W. Fitzmaurice, Situated Information Spaces and Spatially Aware Palmtop Computers, Communication of the ACM, July 1993.	
	6	Ronald Azuma, Tracking Requirements for Augmented Reality, Communications of the ACM, Vol. 36 No. 1, January 1992.	
	7	Roy Want, et al., The Active Badge Location System, ACM Transactions on Information Systems, Vol. 10, No. 1, January 1992.	
	8	Marvin White, Emerging Requirements for Digital Maps for In-Vehicle Pathfinding and Other Traveller Assistance, Vehicular Navigation and Information Systems Conference Proceedings, Part 1, October 1991.	
	9	Fred Phail, The Power of a Personal Computer for Car Information and Communications Systems, Vehicular Navigation and Information Systems Conference Proceedings, Part 1, October 1991.	
	10	Thomas A. Dingus, et al., Human Factors Engineering the TravTek Driver Interface, Vehicular Navigation and Information Systems Conference Proceedings, Part II, October 1991.	
	11	Michael Muffat et al., European Cooperation on Dual Mode Route Guidance Perspectives for Advanced Research Partners, Vehicular Navigation and Information Systems Conference Proceedings, Part II, October 1991.	
	12	High-Performance Wireless Access Point for the Enterprise, ORINOCO™ AP-100 Access Point for the Enterprise, Lucent Technologies, 2000	
	13	MobileStar Network, MobileStar Network First to Provide Business Travelers with High-Speed Data Access via the Internet-Wirelessly, New York, NY, June 24, 1998	
	14	ORINOCO AP-1000 - Getting Started, Lucent Technologies	
	15	Harry Chen, et al., "Dynamic Service Discovery for Mobile Computing: Intelligent Agents Meet Jini in the Aether," Cluster Computing, Special Issue on Internet Scalability, vol. 4, no. 4, February 2001	
	16	3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; Functional Stage 2 Description of Location Services in UMTS (1999)	
	17	http://www.openwave.com/us/news_room/press_releases/2001/20020320 , "Open Wave Announces Availability to End-to-End Set of Location Services for Wireless Internet".	
	18	Trembly, A., "Wireless products arm road warriors," National Underwriter, Vol. 105, No. 3, pp 23-25, Dialog 02113577 67213220 (January 2001)	
	19	Antonio, Interfaces and Algorithms for a Wide -Area Event Notification Service, October 1999.	

Examiner: /Marcos Batista/

Date Considered: 12/19/2013

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Complete if Known		
	Application Number	14/033,540	
	Filing Date	2013-09-23	
	First Named Inventor	William J. Johnson	
	Examiner Name	Not yet assigned	
	Art Unit	2668	
Attorney Docket No.	JOHNS-001US3		
CERTIFICATION STATEMENT			
Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):			
<input type="checkbox"/> That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).			
OR			
<input type="checkbox"/> That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).			
<input type="checkbox"/> See attached certification statement.			
<input type="checkbox"/> Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.			
<input checked="" type="checkbox"/> None			
SIGNATURE			
A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.			
Signature	/Craig J. Yudell/	Date (YYYY-MM-DD)	2013-11-12
Name/Print	Craig J. Yudell	Registration No.	39,083
This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.			

Issue Classification 	Application/Control No. 14033540	Applicant(s)/Patent Under Reexamination JOHNSON, WILLIAM J.
	Examiner MARCOS BATISTA	Art Unit 2642

<input checked="" type="checkbox"/> Claims renumbered in the same order as presented by applicant <input type="checkbox"/> CPA <input type="checkbox"/> T.D. <input type="checkbox"/> R.1.47															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		17												
	2		18												
	3		19												
	4		20												
	5		21												
	6														
	7														
	8														
	9														
	10														
	11														
	12														
	13														
	14														
	15														
	16														

NONE		Total Claims Allowed:	
		21	
(Assistant Examiner)	(Date)		
/MARCOS BATISTA/ Primary Examiner. Art Unit 2642	12/19/2013	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	19



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 4 columns: APPLICATION NUMBER (14/033,540), FILING OR 371(C) DATE (09/23/2013), FIRST NAMED APPLICANT (William J. Johnson), ATTY. DOCKET NO./TITLE (JOHNS-001US3)

CONFIRMATION NO. 1470

PUBLICATION NOTICE

42640
Yudell Isidore Ng Russell PLLC
8911 N. Capital of Texas Hwy.,
Suite 2110
Austin, TX 78759



Title: System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications

Publication No. US-2014-0024396-A1

Publication Date: 01/23/2014

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application Of:	§	ATTY. DOCKET NO.:	JOHNS-001US3
	§		
JOHNSON	§	Examiner:	BATISTA, MARCOS
	§		
Serial No.: 14/033,540	§	Art Unit:	2642
	§		
Filed: SEPTEMBER 23, 2013	§	Confirmation No.	1470
	§		
For: SYSTEM AND METHOD FOR	§		
LOCATION BASED	§		
EXCHANGES OF DATA	§		
FACILITATING DISTRIBUTED	§		
LOCATIONAL APPLICATIONS	§		

AMENDMENT A UNDER 37 C.F.R. § 1.312

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Arlington, Virginia 22313-1450

Sir:

A Notice of Allowance was issued in the subject application on January 6, 2014. Please amend the above-identified application as indicated below. No new matter has been entered by these amendments. Please charge additional claim fees to **Deposit Account Number 50-3083**.

CLAIMS

1. (Previously Presented) A method by a sending data processing system, the method comprising:

accessing, by the sending data processing system, identity information for describing an originator identity associated with the sending data processing system;

accessing, by the sending data processing system, application information for an application in use at the sending data processing system;

accessing, by the sending data processing system, location information associated with the sending data processing system;

accessing, by the sending data processing system, reference information for further describing the location information associated with the sending data processing system;

preparing, by the sending data processing system, a broadcast unidirectional wireless data record including:

the identity information for describing the originator identity associated with the sending data processing system,

the application information for the application in use at the sending data processing system,

the location information associated with the sending data processing system, and

the reference information for further describing the location information associated with the sending data processing system;

maintaining, by the sending data processing system, a configuration for when to perform beaconing of the broadcast unidirectional wireless data record; and

transmitting, by the sending data processing system, the broadcast unidirectional wireless data record for receipt by a plurality of receiving mobile data processing systems in a wireless vicinity of the sending data processing system wherein the broadcast unidirectional wireless data record is beamed by the sending data processing system in accordance with the configuration for when to perform beaconing, and wherein the broadcast unidirectional wireless data record includes at least:

the identity information for describing the originator identity associated with the sending data processing system wherein the identity information is for an alert determined by each receiving mobile data processing system of the plurality of receiving mobile data processing systems that the each receiving mobile data processing system is in the wireless vicinity of the sending data processing system,

the application information for the application in use at the sending data processing system,

the location information associated with the sending data processing system to be used by the each receiving mobile data processing system for determining their own location relative to the location information, and

the reference information for further describing the location information associated with the sending data processing system for describing to the each receiving mobile data processing system useful information associated with the sending data processing system.

2. (Previously Presented) The method of claim 1 wherein the broadcast unidirectional wireless data record includes web site information associated with the sending data processing system.
3. (Previously Presented) The method of claim 1 wherein the broadcast unidirectional wireless data record includes environmental condition information associated with the sending data processing system.
4. (Previously Presented) The method of claim 1 wherein the broadcast unidirectional wireless data record includes information for at least one service associated with the sending data processing system.
5. (Previously Presented) The method of claim 1 wherein the broadcast unidirectional wireless data record includes information for at least one transaction associated with the sending data processing system.

6. (Previously Presented) The method of claim 1 wherein the broadcast unidirectional wireless data record includes information for one or more data processing systems remote to the sending data processing system.

7. (Previously Presented) The method of claim 1 wherein the broadcast unidirectional wireless data record includes information for distinguishing an elevation or altitude.

8. (Previously Presented) The method of claim 1 wherein the broadcast unidirectional wireless data record includes confidence information for describing a reliability of data in the broadcast unidirectional wireless data record.

9. (Previously Presented) The method of claim 1 wherein the broadcast unidirectional wireless data record includes information that is presented to a user interface of the each receiving mobile data processing system.

10. (Previously Presented) The method of claim 1 wherein the broadcast unidirectional wireless data record includes information that is processed by the each receiving mobile data processing system for determining by the each receiving mobile data processing system what to present to a user interface.

11. (Previously Presented) The method of claim 1 wherein the broadcast unidirectional wireless data record includes at least one of:

information for a location technology used to locate the sending data processing system,

information for a triangulation measurement associated with the sending data processing system,

information for a time difference of arrival measurement associated with the sending data processing system,

information for a time of arrival measurement associated with the sending data processing system,

information for an angle of arrival measurement associated with the sending data processing system,

information for a yaw measurement associated with the sending data processing system,

information for a pitch measurement associated with the sending data processing system,

information for a roll measurement associated with the sending data processing system,

information for an accelerometer measurement associated with the sending data processing system,

information for a communications signal strength of a transmission associated with the sending data processing system,

information for a communications wave spectrum characteristic of a transmission associated with the sending data processing system,

information for a communications wave spectrum class of a transmission associated with the sending data processing system,

information for a communications wave spectrum frequency of a transmission associated with the sending data processing system,

information associated with a wireless data record received by the sending data processing system from a particular data processing system,

information maintained by an application associated with the sending data processing system,

information for an application in use at the sending data processing system,

information for an application context of an application associated with the sending data processing system,

information for a navigation Application Programming Interface associated with the sending data processing system,

information for a situational location associated with the sending data processing system,

information for a speed associated with the sending data processing system,

information for a heading associated with the sending data processing system,

time information associated with the sending data processing system,

information for a service condition associated with the sending data processing system,

information for a physical address associated with the sending data processing system,

information for a logical address associated with the sending data processing system,

information for a user configuration associated with the sending data processing system,
information for monitoring movement of the sending data processing system,
information for an identifier associated with the sending data processing system, or
information in accordance with one or more permissions configured by a user associated
with the sending data processing system.

12. (Previously Presented) The method of claim 1 wherein the broadcast unidirectional wireless data record includes information that can be processed according to a user configured permission maintained at the each receiving mobile data processing system.

13. (Previously Presented) The method of claim 12 wherein the user configured permission is configured by a user of the sending data processing system for providing permission to an identity of at least one of the plurality of receiving mobile data processing systems.

14. (Previously Presented) The method of claim 12 wherein the user configured permission is configured by a user of at least one of the plurality of receiving mobile data processing systems for providing permission to an identity associated with the sending data processing system.

15. (Previously Presented) The method of claim 12 wherein the user configured permission enables providing an alert for who is nearby.

16. (Previously Presented) The method of claim 1 wherein the identity information is a dependable and recognizable derivative of the originator identity associated with the sending data processing system.

17. (Previously Presented) The method of claim 1 wherein the location information associated with the sending data processing system is determined by the sending data processing system with a direct location method, or an indirect location method, or with information communicated to the sending data processing system by a remote data processing system.

18. (Previously Presented) The method of claim 1 wherein the transmitting, by the sending data processing system, the broadcast unidirectional wireless data record for receipt by the plurality of receiving mobile data processing systems in the wireless vicinity of the sending data processing system includes transmitting the broadcast unidirectional wireless data record by a plurality of distinctly different radio communication interfaces of the sending data processing system.

19. (Previously Presented) The method of claim 1 including:

searching, by the sending data processing system, a plurality of data records in a historical collection; and

retrieving, by the sending data processing system, one of the plurality of data records for the preparing, by the sending data processing system, the broadcast unidirectional wireless data record.

20. (Previously Presented) The method of claim 1 including presenting information for the broadcast unidirectional wireless data record to a user interface for a user to manage the information for the broadcast unidirectional wireless data record by at least one of: view the information for the broadcast unidirectional wireless data record, delete the information for the broadcast unidirectional wireless data record, modify the information for the broadcast unidirectional wireless data record, or add to the information for the broadcast unidirectional wireless data record.

21. (Previously Presented) A sending data processing system, comprising:

one or more processors; and

at least one memory coupled to the one or more processors, wherein the at least one memory includes executable instructions, which when executed by the one or more processors, results in the system:

accessing, by the sending data processing system, identity information for describing an originator identity associated with the sending data processing system;

accessing, by the sending data processing system, application information for an application in use at the sending data processing system;

accessing, by the sending data processing system, location information associated with the sending data processing system;

accessing, by the sending data processing system, reference information for further describing the location information associated with the sending data processing system;

preparing, by the sending data processing system, a broadcast unidirectional wireless data record including:

the identity information for describing the originator identity associated with the sending data processing system,

the application information for the application in use at the sending data processing system,

the location information associated with the sending data processing system, and

the reference information for further describing the location information associated with the sending data processing system;

maintaining, by the sending data processing system, a configuration for when to perform beaconing of the broadcast unidirectional wireless data record; and

transmitting, by the sending data processing system, the broadcast unidirectional wireless data record for receipt by a plurality of receiving mobile data processing systems in a wireless vicinity of the sending data processing system wherein the broadcast unidirectional wireless data record is beamed by the sending data processing system in accordance with the configuration for when to perform beaconing, and wherein the broadcast unidirectional wireless data record includes at least:

the identity information for describing the originator identity associated with the sending data processing system wherein the identity information is for an alert determined by each receiving mobile data processing system of the plurality of receiving mobile data processing systems that the each receiving mobile data processing system is in the wireless vicinity of the sending data processing system,

the application information for the application in use at the sending data processing system,

the location information associated with the sending data processing system to be used by the each receiving mobile data processing system for determining their own location relative to the location information, and

the reference information for further describing the location information associated with the sending data processing system for describing to the each receiving mobile data processing system useful information associated with the sending data processing system.

22. (New) The sending data processing system of claim 21 wherein the broadcast unidirectional wireless data record includes web site information associated with the sending data processing system.

23. (New) The sending data processing system of claim 21 wherein the broadcast unidirectional wireless data record includes environmental condition information associated with the sending data processing system.

24. (New) The sending data processing system of claim 21 wherein the broadcast unidirectional wireless data record includes information for at least one service associated with the sending data processing system.

25. (New) The sending data processing system of claim 21 wherein the broadcast unidirectional wireless data record includes information for at least one transaction associated with the sending data processing system.

26. (New) The sending data processing system of claim 21 wherein the broadcast unidirectional wireless data record includes information for one or more data processing systems remote to the sending data processing system.

27. (New) The sending data processing system of claim 21 wherein the broadcast unidirectional wireless data record includes information for distinguishing an elevation or altitude.

28. (New) The sending data processing system of claim 21 wherein the broadcast unidirectional wireless data record includes confidence information for describing a reliability of data in the broadcast unidirectional wireless data record.

29. (New) The sending data processing system of claim 21 wherein the broadcast unidirectional wireless data record includes information that is presented to a user interface of the each receiving mobile data processing system.

30. (New) The sending data processing system of claim 21 wherein the broadcast unidirectional wireless data record includes information that is processed by the each receiving mobile data processing system for determining by the each receiving mobile data processing system what to present to a user interface.

31. (New) The sending data processing system of claim 21 wherein the broadcast unidirectional wireless data record includes at least one of:

- information for a location technology used to locate the sending data processing system,
- information for a triangulation measurement associated with the sending data processing system,

- information for a time difference of arrival measurement associated with the sending data processing system,

- information for a time of arrival measurement associated with the sending data processing system,

- information for an angle of arrival measurement associated with the sending data processing system,

- information for a yaw measurement associated with the sending data processing system,

- information for a pitch measurement associated with the sending data processing system,

- information for a roll measurement associated with the sending data processing system,

information for an accelerometer measurement associated with the sending data processing system,

information for a communications signal strength of a transmission associated with the sending data processing system,

information for a communications wave spectrum characteristic of a transmission associated with the sending data processing system,

information for a communications wave spectrum class of a transmission associated with the sending data processing system,

information for a communications wave spectrum frequency of a transmission associated with the sending data processing system,

information associated with a wireless data record received by the sending data processing system from a particular data processing system,

information maintained by an application associated with the sending data processing system,

information for an application in use at the sending data processing system,

information for an application context of an application associated with the sending data processing system,

information for a navigation Application Programming Interface associated with the sending data processing system,

information for a situational location associated with the sending data processing system,

information for a speed associated with the sending data processing system,

information for a heading associated with the sending data processing system,

time information associated with the sending data processing system,

information for a service condition associated with the sending data processing system,

information for a physical address associated with the sending data processing system,

information for a logical address associated with the sending data processing system,

information for a user configuration associated with the sending data processing system,

information for monitoring movement of the sending data processing system,

information for an identifier associated with the sending data processing system, or

information in accordance with one or more permissions configured by a user associated with the sending data processing system.

32. (New) The sending data processing system of claim 21 wherein the broadcast unidirectional wireless data record includes information that can be processed according to a user configured permission maintained at the each receiving mobile data processing system.

33. (New) The sending data processing system of claim 32 wherein the user configured permission is configured by a user of the sending data processing system for providing permission to an identity of at least one of the plurality of receiving mobile data processing systems.

34. (New) The sending data processing system of claim 32 wherein the user configured permission is configured by a user of at least one of the plurality of receiving mobile data processing systems for providing permission to an identity associated with the sending data processing system.

35. (New) The sending data processing system of claim 32 wherein the user configured permission enables providing an alert for who is nearby.

36. (New) The sending data processing system of claim 21 wherein the identity information is a dependable and recognizable derivative of the originator identity associated with the sending data processing system.

37. (New) The sending data processing system of claim 21 wherein the location information associated with the sending data processing system is determined by the sending data processing system with a direct location method, or an indirect location method, or with information communicated to the sending data processing system by a remote data processing system.

38. (New) The sending data processing system of claim 21 wherein the transmitting, by the sending data processing system, the broadcast unidirectional wireless data record for receipt by the plurality of receiving mobile data processing systems in the wireless vicinity of the sending data processing system includes transmitting the broadcast unidirectional wireless data record by

a plurality of distinctly different radio communication interfaces of the sending data processing system.

39. (New) The sending data processing system of claim 21 including:

searching, by the sending data processing system, a plurality of data records in a historical collection; and

retrieving, by the sending data processing system, one of the plurality of data records for the preparing, by the sending data processing system, the broadcast unidirectional wireless data record.

40. (New) The sending data processing system of claim 21 including presenting information for the broadcast unidirectional wireless data record to a user interface for a user to manage the information for the broadcast unidirectional wireless data record by at least one of: view the information for the broadcast unidirectional wireless data record, delete the information for the broadcast unidirectional wireless data record, modify the information for the broadcast unidirectional wireless data record, or add to the information for the broadcast unidirectional wireless data record.

REMARKS

Applicant has added new dependent claims 22-40. No new matter has been entered by these amendments.

Specifically, new claims 22-40 are clones of allowed claims 2-20, respectively, followed by minimal editing to depend from allowed independent claim 21. Allowed independent claim 21 is a system version of allowed independent claim 1. Allowed claims 2-20 depend from allowed claim 1. New claims are dependent on allowed claims and should therefore be in condition for allowance.

Applicant invites the Examiner to contact the undersigned at the below listed telephone number if a telephone conference would expedite prosecution of this application.

Respectfully submitted,

/Craig J. Yudell/

Craig J. Yudell
Reg. No. 39,083
YUDELL ISIDORE NG RUSSELL PLLC
8911 N. Capital of Texas Highway, Suite 2110
Austin, Texas 78759
512.343.6116
ATTORNEY FOR APPLICANT

Electronic Patent Application Fee Transmittal

Application Number:	14033540			
Filing Date:	23-Sep-2013			
Title of Invention:	System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications			
First Named Inventor/Applicant Name:	William J. Johnson			
Filer:	Craig Jeffrey Yudell/Shenise Ramdeen			
Attorney Docket Number:	JOHNS-001US3			
Filed as Small Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	2202	19	40	760
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				760

Electronic Acknowledgement Receipt

EFS ID:	18049140
Application Number:	14033540
International Application Number:	
Confirmation Number:	1470
Title of Invention:	System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications
First Named Inventor/Applicant Name:	William J. Johnson
Customer Number:	42640
Filer:	Craig Jeffrey Yudell/Shenise Ramdeen
Filer Authorized By:	Craig Jeffrey Yudell
Attorney Docket Number:	JOHNS-001US3
Receipt Date:	28-JAN-2014
Filing Date:	23-SEP-2013
Time Stamp:	16:27:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$760
RAM confirmation Number	2955
Deposit Account	503083
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)
 Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)
 Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment after Notice of Allowance (Rule 312)	JOHNS-001US3_Rule312Amendment01-28-14.pdf	112234 c289a1da60887c347cf9e2abf03aa5c473c8447d	no	14

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	30474 c7e70d1e74b42f9ef36e7b804f558c934d5f1caf	no	2
---	----------------------	--------------	---	----	---

Warnings:

Information:

Total Files Size (in bytes): 142708

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes details for application 14/033,540 filed 09/23/2013 by William J. Johnson, attorney JOHNS-001US3, confirmation 1470. Also includes examiner BATISTA, MARCOS, art unit 2642, and notification date 03/26/2014 via electronic mode.

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Patents@yudellisidore.com

Response to Rule 312 Communication	Application No. 14/033,540	Applicant(s) JOHNSON, WILLIAM J.
	Examiner Marcos Batista	Art Unit 2642
-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --		
<p>1. <input checked="" type="checkbox"/> The amendment filed on <u>28 January 2014</u> under 37 CFR 1.312 has been considered, and has been:</p> <p>a) <input checked="" type="checkbox"/> entered.</p> <p>b) <input type="checkbox"/> entered as directed to matters of form not affecting the scope of the invention.</p> <p>c) <input type="checkbox"/> disapproved because the amendment was filed after the payment of the issue fee. Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.</p> <p>d) <input type="checkbox"/> disapproved. See explanation below.</p> <p>e) <input type="checkbox"/> entered in part. See explanation below.</p>		
		/Marcos Batista/ Primary Examiner, Art Unit 2642

03/21/2014

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application Of:	ATTY. DOCKET NO.:	JOHNS-001US3
	§	
JOHNSON	§	
	§	Examiner: BATISTA, MARCOS
	§	
Serial No.: 14/033,540	§	Art Unit: 2642
	§	
Filed: SEPTEMBER 23, 2013	§	Confirmation No. 1470
	§	
For: SYSTEM AND METHOD FOR	§	
LOCATION BASED	§	
EXCHANGES OF DATA	§	
FACILITATING DISTRIBUTED	§	
LOCATIONAL APPLICATIONS	§	

AMENDMENT A UNDER 37 C.F.R. § 1.312

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Arlington, Virginia 22313-1450

Sir:

A Notice of Allowance was issued in the subject application on January 6, 2014. Please amend the above-identified application as indicated below. No new matter has been entered by these amendments. Please charge additional claim fees to **Deposit Account Number 50-3083**.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
 or **Fax (571) 273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CORRENT CORRESPONDENCE ADDRESS (Use this Block 1 for any change of address)

42540 7591 01/05/2014
Yudell Isidore Ng Russell PLLC
 8911 N. Capital of Texas Hwy.,
 Suite 2110
 Austin, TX 78750

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Date of Mailing/Transmission
Signature
Title

APPLICATION NO.	FILED DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
146011540	09/23/2013	William J. Johnson	JOHNS-001US3	1470

TITLE OF INVENTION: System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications

APP. TYPE	ENTITY #/CLASS	ISSUE FEE DUE	PUBLICATION FEE DUE	FEE PAID ISSUE FEE	ISSUE FEE DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	04/07/2014

EXAMINER	ART UNIT	CLASSIFICATION
BATISTA, MARCOS	2642	435-496300

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.333).

Change of correspondence address for (Change of Correspondence Address form PTO/SB/122) attached.

"Fee Address" indication for "Flat Address" indication form PTO/SB/47, Rev. 03-02 or more recent) attached. Use of a Customer Number is required.

2. Fee printing on the patent form page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively, **Yudell Isidore Ng Russell PLLC**

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recording as set forth in 37 CFR 1.15. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE _____ (B) RESIDENCE: (CITY and STATE OR COUNTRY) _____

Please check the appropriate assignee category or categories (will not be printed on the patent): Individual Corporation or other private group entity Government

4a. The following fee(s) are submitted:

Issue Fee

Publication Fee (No small entity discount permitted)

Advance Order - # of Copies _____

4b. Payment of Fee(s) (Please first reapply any previously paid issue fee shown above)

A check is enclosed.

Payment by credit card, Form PTO-2038 is attached.

The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number **503083** (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

Applicant certifying micro entity status. See 37 CFR 1.29

Applicant asserting small entity status. See 37 CFR 1.27

Applicant changing to regular undiscouted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.33 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signatures: /Craig J. Yudell/ Date: 2014-03-28

Typed or printed name: Craig J. Yudell Registration No.: 39083

Electronic Patent Application Fee Transmittal

Application Number:	14033540
Filing Date:	23-Sep-2013
Title of Invention:	System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications
First Named Inventor/Applicant Name:	William J. Johnson
Filer:	Craig Jeffrey Yudell/Shenise Ramdeen
Attorney Docket Number:	JOHNS-001US3

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	2501	1	480	480
Publ. Fee- Early, Voluntary, or Normal	1504	1	0	0

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				480

Electronic Acknowledgement Receipt

EFS ID:	18612125
Application Number:	14033540
International Application Number:	
Confirmation Number:	1470
Title of Invention:	System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications
First Named Inventor/Applicant Name:	William J. Johnson
Customer Number:	42640
Filer:	Craig Jeffrey Yudell/Shenise Ramdeen
Filer Authorized By:	Craig Jeffrey Yudell
Attorney Docket Number:	JOHNS-001US3
Receipt Date:	28-MAR-2014
Filing Date:	23-SEP-2013
Time Stamp:	13:32:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$480
RAM confirmation Number	12457
Deposit Account	503083
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)
 Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)
 Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	JOHNS-001US3_IssueFeeTransmittal03-28-14.pdf	91214 980327dd7c3454f29da97dfa490b075cfe0aa374	no	1

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	32045 7bfa9d4983030d6682e5535232d7bdf7c1dd488	no	2
---	----------------------	--------------	--	----	---

Warnings:

Information:

Total Files Size (in bytes): 123259

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.


Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENT APPLICATION PUBLICATIONS						
Examiner Initials	Cite No.	Publication Number	Kind Code	Publication Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	89	2007/0276587		2007-11-29	Johnson	
	90	2007/0232326		2007-10-04	Johnson	
	91	2008/0030308		2008-02-07	Johnson	
	92	2006/0022048		2006-02-02	Johnson	
	93	2009/0233622		2009-09-17	Johnson	
Change(s) applied to document, /G.R.P./ 2/18/2014	94	2009/0233638 23		2009-09-17	Johnson	
	95	2010/0069035		2010-03-18	Johnson	
	96	2010/0227595		2010-09-09	Johnson	
	97	2006/0010202		2006-01-12	Blackstock et al.	
	98	2004/0201459		2004-10-14	Rich et al.	
	99	2006/0136544		2006-06-22	Atsmon et al.	
	100	2007/0281716		2007-12-06	Altman et al.	
	101	2006/0240828		2006-10-26	Jain et al.	
	102	2007/0275730		2007-11-29	Bienas et al.	
	103	2006/0194589		2006-08-31	Sankisa	
	104	2007/0287473		2007-12-13	Dupray	
	105	2008/0071761		2008-03-20	Singh et al.	
	106	2004/0116131		2004-06-17	Hochrainer et al.	
	107	2007/0275730		2007-11-29	Bienas et al.	
	108	2007/0244633		2007-10-18	Phillips et al.	
	109	2008/0170679		2008-07-17	Sheha et al.	
	110	2005/0050227		2005-03-03	Michelman	
	111	2003/0030731		2003-02-13	Colby	
	112	2006/0009190		2006-01-12	Laliberte	
	113	2006/0198359		2006-09-07	Fok et al.	
	114	2001/0005864		2001-06-28	Mousseau et al.	
	115	2010/0146160		2010-06-10	Piekarski	
	116	2005/0283833		2005-12-22	Lalonde et al.	
	117	2010/0159946		2010-06-24	Cheung et al.	
	118	2002/0095454		2002-07-18	Reed et al.	
	119	2006/0252465		2006-11-09	Karstens et al.	
	120	2008/0301561		2008-12-04	Bain	
	121	2009/0067593		2009-03-12	Ahlin	
	122	2009/0167524		2009-07-02	Chesnutt et al.	
	123	2009/0190734		2009-07-16	White et al.	
	124	2009/0054077		2009-02-26	Gauthier et al.	
	125	2006/0194589		2006-08-31	Sankisa	
	126	2011/0021145		2011-01-27	Johnson et al.	
	127	2010/0235748		2010-09-16	Johnson et al.	
	128	2009/0233623		2009-09-17	Johnson et al.	

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	362	4255619		1981-03-10	Saito	
	363	4536647		1985-08-20	Atalla et al.	
	364	4845504		1989-07-04	Roberts, et al.	
	365	4973952		1990-11-27	Malec et al.	
	366	4974170		1990-11-27	Bouve et al.	
Change(s) applied to document, /G.R.P./ 2/18/2014	367	5303245 5636245		1997-06-03	Ernst et al.	
	368	5870724		1999-02-09	Lawlor et al.	
	369	6407673		2002-06-18	Lane	
	370	6408307		2002-06-18	Semple et al.	
	371	6414635		2002-07-02	Stewart et al.	
	372	6442479		2002-08-27	Barton	
	373	6452498		2002-09-17	Stewart	
	374	6615131		2003-09-02	Rennard et al.	
	375	6405123		2002-06-11	Rennard et al.	
	Change(s) applied to document, /G.R.P./ 2/12/2014	376	626615 6266615		2001-07-24	Jin
377		4644351		1987-02-17	Zabarsky et al.	
378		5337044		1944-08-09	Folger et al.	
379		5469362		1995-11-23	Hunt et al.	
380		5758049		1998-11-10 05/1998	Johnson et al.	
381		5835061		1998-11-10	Stewart	
382		5969678		1998-10-19 10/1999	Stewart	
383		6073062		2000-06-06	Hoshino et al.	
384		6236362 6236365		2001-05-22	Leblanc et al.	
385		6326918		2001-12-04	Stewart	
386	6259405		2001-07-10	Stewart et al.		
387	6252544		2001-06-26	Hoffberg		
388	6414635		2002-07-02	Stewart et al.		
389	6452498		2002-09-17	Stewart		
390	6697018		2004-02-24	Stewart		
391	6731238		2004-05-04	Johnson		
392	6759960		2004-07-06	Stewart		
393	7009556		2006-03-07	Stewart		
394	5496001 5195031		1993-03-16	Ordish		
395	6345288		2002-02-05	Reed et al.		
396	6571279		2003-05-27	Herz et al.		
397	6456234		2002-09-24	Johnson		
398	6246948		2001-06-12	Thakker		
399	7386396		2008-06-10	Johnson		

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	287	6819929		2004-11-16	Antonucci et al.	
	288	6829475		2004-12-07	Lee et al.	
	289	6850758		2005-02-01	Paul et al.	
	290	6867733		2005-03-15	Sandhu et al.	
	291	6868074		2005-03-15	Hanson, Joel	
	292	6874011		2005-03-29	Spielman	
	293	6876858		2005-04-15	Duvall et al.	
	294	6898569		2005-05-24	Bansal et al.	
	295	6937869		2005-08-30	Rayburn	
	296	6954147		2005-10-11	Cromer et al.	
	297	6985747		2006-01-10	Chithambaram	
	298	6999572		2006-02-04	Shaffer et al.	
	299	7005985		2006-02-28	Steeves	
	300	7023995		2006-04-04	Olsson	
	301	7043231		2006-05-09	Bhatia et al.	
	302	7069319		2006-06-27	Zellner et al.	
	303	7085555		2006-08-01	Zellner et al.	
	304	7103368		2006-09-05	Teshima	
	305	7103476		2006-09-05	Smith et al.	
	306	7106843		2006-09-12	Gainsboro et al.	
	307	7110749		2006-09-19	Zellner et al.	
	308	7116977		2006-10-03	Moton et al.	
	309	7124101		2006-10-17	Mikurak	
	310	7130631 ^o		2006-10-31	Enzmann et al.	
	311	7139722		2006-11-21	Perrella et al.	
	312	7181225		2007-02-20	Moton et al.	
	313	7181529		2007-02-20	Bhatia et al.	
	314	7188027		2007-03-06	Smith et al.	
	315	7190960		2007-03-13	Wilson et al.	
	316	7203502		2007-04-10	Wilson et al.	
	317	7212829		2007-05-01	Lau et al.	
	318	7224978		2007-05-29	Zellner et al.	
	319	7236799		2007-06-26	Wilson et al.	
	320	7245925		2007-07-17	Zellner	
	321	7260378		2007-08-21	Holland et al.	
	322	7272493		2007-09-18	Hamrick et al.	
	323	7292939		2007-11-06	Smith et al.	
	324	7295924		2007-11-13	Smith et al.	

Change(s) applied
to document,
/G.R.P./
2/18/2014

Substitute for form 1449/PTO				Complete if Known		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	14/033,540	
				Filing Date	2013-09-23	
				First Named Inventor	William J. Johnson	
				Examiner Name	Not yet assigned	
				Art Unit	2668	
				Attorney Docket No.	JOHNS-001US3	
U.S. PATENTS						
Examiner Initials	Cite No.	Patent Number	Kind Code	Issue Date YYYY-MM-DD	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	3636421		1972-03-26 01/1972	Barker et al.	
	2	4021780		1977-05-01	Narey et al.	
	3	4445118		1984-04-01	Taylor et al.	
	4	4757267		1988-07-01	Riskin	
	5	4841560		1989-06-01	Chan et al.	
	6	4922516		1990-05-01	Butler et al.	
Change(s) applied to document, /G.R.P./ 2/18/2014	7	4977399		1990-12-01	Price et al.	
	8	5095532		1992-03-10	Mardus	
	9	5122795		1992-06-01	Cublely et al.	
	10	5185857		1993-02-09	Rozmanith et al	
	11	5223844		1993-06-29	Mansell et al.	
	12	5243652		1993-09-07	Teare et al.	
	13	5303393		1994-04-12	Noreen et al.	
	14	5321242		1994-06-14	Heath, Jr.	
	15	5365516		1994-11-15	Jandrell	
	16	5371794		1994-12-06	Diffie et al.	
	17	5390237		1995-02-12	Hoffman et al.	
	18	5404505		1995-04-04	Levinson	
	19	5432841		1995-07-11	Rimer	
	20	5444444		1995-08-22	Ross	
	21	5451757		1995-09-19	Heath, Jr.	
	22	5461627		1995-10-24	Rypinski	
	23	5264822		1993-11-23	Vogelman et al.	
	24	5475735		1995-12-10	Williams et al.	
	25	5485163		1996-01-16	Singer et al.	
	26	5487103		1996-01-23	Richardson	
	27	5493309		1996-02-20	Bjornholt et al.	
	28	5497414		1996-03-01	Bartholomew	
	29	5504482		1996-04-02	Schreder	
	30	5511111		1996-04-01	Serbetcioğlu et al.	
	31	5511233		1996-04-23	Otten	
	32	5512908		1996-04-01	Herrick	
	33	5513263		1996-04-30	White et al.	
	34	5528248		1996-06-18	Steiner et al.	
	35	5544354		1996-08-06	May et al.	
	36	5559520		1996-09-24	Barzegar et al.	
	37	5566235		1996-10-15	Hetz	
	38	5870555		1999-02-09	Pruett et al.	

Search Notes 	Application/Control No. 14033540	Applicant(s)/Patent Under Reexamination JOHNSON, WILLIAM J.
	Examiner MARCOS BATISTA	Art Unit 2642

CPC- SEARCHED		
Symbol	Date	Examiner
h04w4/04, h04w4/06, h04w40/20, h04w4/02	12/19/2013	mb


CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
455370	04.2, 456.34338	12/19/201312/19/2013	mbmb

SEARCH NOTES		
Search Notes	Date	Examiner
Intentor's Name SearchEast SearchIDS Search	12/19/201312/19/201312/19/2013	mbmbmb


INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
455	404.2, 456.3	12/19/2013	mb
370	338	12/19/2013	mb

--	--

Issue Classification 	Application/Control No. 14033540	Applicant(s)/Patent Under Reexamination JOHNSON, WILLIAM J.	
	Examiner MARCOS BATISTA	Art Unit 2642	


US ORIGINAL CLASSIFICATION					INTERNATIONAL CLASSIFICATION															
CLASS		SUBCLASS			CLAIMED					NON-CLAIMED										
455		456.3			H	0	4	W	24 / 00 (2009.0)											
CROSS REFERENCE(S)																				
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)																			
370	338																			

NONE		Total Claims Allowed:	
		40	
(Assistant Examiner)	(Date)		
/MARCOS BATISTA/ Primary Examiner. Art Unit 2642	05/12/2014	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	19

Issue Classification 	Application/Control No. 14033540	Applicant(s)/Patent Under Reexamination JOHNSON, WILLIAM J.
	Examiner MARCOS BATISTA	Art Unit 2642

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant <input type="checkbox"/> CPA <input type="checkbox"/> T.D. <input type="checkbox"/> R.1.47															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	17	17	33	33										
2	2	18	18	34	34										
3	3	19	19	35	35										
4	4	20	20	36	36										
5	5	21	21	37	37										
6	6	22	22	38	38										
7	7	23	23	39	39										
8	8	24	24	40	40										
9	9	25	25												
10	10	26	26												
11	11	27	27												
12	12	28	28												
13	13	29	29												
14	14	30	30												
15	15	31	31												
16	16	32	32												

NONE			Total Claims Allowed:	
(Assistant Examiner)	(Date)	40		
/MARCOS BATISTA/ Primary Examiner. Art Unit 2642	05/12/2014	O.G. Print Claim(s)	O.G. Print Figure	
(Primary Examiner)	(Date)	1	19	

<i>Index of Claims</i> 	Application/Control No. 14033540	Applicant(s)/Patent Under Reexamination JOHNSON, WILLIAM J.
	Examiner MARCOS BATISTA	Art Unit 2642

✓	Rejected
=	Allowed


-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claims renumbered in the same order as presented by applicant
 CPA
 T.D.
 R.1.47

CLAIM		DATE									
Final	Original	12/19/2013									
1	1	=									
2	2	=									
3	3	=									
4	4	=									
5	5	=									
6	6	=									
7	7	=									
8	8	=									
9	9	=									
10	10	=									
11	11	=									
12	12	=									
13	13	=									
14	14	=									
15	15	=									
16	16	=									
17	17	=									
18	18	=									
19	19	=									
20	20	=									
21	21	=									
22	22	=									
23	23	=									
24	24	=									
25	25	=									
26	26	=									
27	27	=									
28	28	=									
29	29	=									
30	30	=									
31	31	=									
32	32	=									
33	33	=									
34	34	=									
35	35	=									
36	36	=									

<i>Index of Claims</i> 	Application/Control No. 14033540	Applicant(s)/Patent Under Reexamination JOHNSON, WILLIAM J.
	Examiner MARCOS BATISTA	Art Unit 2642

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant			<input type="checkbox"/> CPA			<input type="checkbox"/> T.D.			<input type="checkbox"/> R.1.47		
CLAIM			DATE								
Final	Original	12/19/2013									
37	37	=									
38	38	=									
39	39	=									
40	40	=									



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/033,540	09/23/2013	William J. Johnson	JOHNS-001US3	1470
42640	7590	05/15/2014	EXAMINER	
Yudell Isidore Ng Russell PLLC 8911 N. Capital of Texas Hwy., Suite 2110 Austin, TX 78759			BATISTA, MARCOS	
			ART UNIT	PAPER NUMBER
			2642	
			NOTIFICATION DATE	DELIVERY MODE
			05/15/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Patents@yudellisidore.com

Notice of Allowability	Application No. 14/033,540	Applicant(s) JOHNSON, WILLIAM J.	
	Examiner Marcos Batista	Art Unit 2642	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. This communication is responsive to Amendment after Notice of Allowance (Rule 312) filed on 1/28/2014.
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
2. An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. The allowed claim(s) is/are 1-40. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to FPHfeedback@uspto.gov.
4. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

- a) All b) Some *c) None of the:
1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has **THREE MONTHS FROM THE "MAILING DATE"** of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in **ABANDONMENT** of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|--|--|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Examiner's Amendment/Comment |
| 2. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____ | 6. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| 3. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 7. <input type="checkbox"/> Other _____. |
| 4. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____. | |

--	--

Detailed Action

1. This Action is in response to Applicant's Amendment after Notice of Allowance (Rule 312) filed on January 28, 2014. **Claims 22-40 have been added, therefore, claims 1-40** are now pending in the present application.

2. The present application is being examined under the pre-AIA first to invent provisions.

Information Disclosure Statement

3. The information disclosure statement submitted on 11/12/2013 has been considered by the Examiner and made of record in the application file. However, IDS entry 14 under the Non-Patent Literature was not considered due missing the date.

Allowable Subject Matter

4. **Claims 1-40** are allowed.

5. The following is an Examiner's statement of reasons for allowance:

Consider claims 1 and 21, the prior art of Bienas et al. (US 20070275730 A1) in view of Blackstock et al. (US 20060010202 A1), discloses a system for determining the location and identity of at least one mobile device and exchanging the location information and identity with nearby mobile devices.

However, the combination of Bienas in view of Blackstock failed to disclose or suggest each and every limitation recited in claims 1-40 of the claimed invention when considered as a whole.

Any comments considered necessary by Applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Marcos Batista, whose telephone number is (571) 270-5209. The Examiner can normally be reached on Monday-Thursday from 8:00am to 5:00pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Rafael Pérez-Gutiérrez can be reached at (571) 272-7915. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you

Application/Control Number: 14/033,540

Page 4

Art Unit: 2642

have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 703-305-3028.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-2600.

*/Marcos Batista/
Primary Examiner, Art Unit 2642
May 12, 2014*



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P. O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	------------	------------	---------------------	------------------

14/033,540

06/24/2014

8761804

JOHNS-001US3

1470

42640

7590

06/04/2014

Yudell Isidore Ng Russell PLLC
8911 N. Capital of Texas Hwy.,
Suite 2110
Austin, TX 78759

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

William J. Johnson, Flower Mound, TX;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): William J. Johnson

Confirmation No.: 1470

Serial No.: 14/033,540, Filed September 23, 2013

Art Unit: 2642

Patent No.: 8,761,804, Issued June 24, 2014

Examiner: M. Batista

Title: SYSTEM AND METHOD FOR LOCATION BASED EXCHANGES

OF DATA FACILITATING DISTRIBUTED LOCATIONAL APPLICATIONS

Filed via EFS Web

TO: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**SUBMISSION UNDER 37 C.F.R. § 1.28(c) TO PAY FEE(S) AT
LARGE ENTITY RATE DUE TO CORRECTION OF ENTITY STATUS**

This paper is being filed in order to correct fee amounts paid due to an incorrect designation of small entity in this application made upon payment of the second maintenance fee. This error was made inadvertently, in good faith, and with no intent to deceive. The error was not caught until recently. Consistent with 37 C.F.R. § 1.28(c), a calculation of the deficiency owed, and an itemization of the same, is set forth in the table below. The itemization of the deficiency owed is as follows:

Fee/Code	Current Fee Amount	Fee Paid/Date	Deficiency Owed
Maintenance fee due at 3.5 years (Fee code 1551)	\$2,000	\$800 November 2, 2017	\$1,200

Per the undersigned's calculations, a total deficiency of **\$1,200** is owed. The undersigned authorizes the Office to charge this amount, and to charge any additional fees that may be due, or credit any overpayment, to Deposit Account 50-4364 (382740.00001).

Respectfully submitted,

May 19, 2021
Date

/Mark D. Simpson/
Mark D. Simpson, Esquire
Registration No. 32,942

SAUL EWING ARNSTEIN & LEHR LLP
Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102-2189
Telephone: 215 972 7880
Facsimile: 215 972 4169
Email: Mark.Simpson@saul.com

Electronic Acknowledgement Receipt

EFS ID:	42766267
Application Number:	14033540
International Application Number:	
Confirmation Number:	1470
Title of Invention:	System and Method for Location Based Exchanges of Data Facilitating Distributed Locational Applications
First Named Inventor/Applicant Name:	William J. Johnson
Customer Number:	42640
Filer:	Mark D. Simpson/Lynn White
Filer Authorized By:	Mark D. Simpson
Attorney Docket Number:	JOHNS-001US3
Receipt Date:	19-MAY-2021
Filing Date:	23-SEP-2013
Time Stamp:	15:33:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	38528050_1.PDF	1115305 b60df2ddd7c55597bed66f4b45a939d9970153cf	no	1

Warnings:

Information:					
2	Assignee showing of ownership per 37 CFR 3.73	38522305_1.PDF	290445 5f2e4d1135d63d650b24d2df30b1dad346327859	no	3
Warnings:					
Information:					
3	Notification of loss of entitlement to small entity status	38528051_1.PDF	97535 8083c425296e73da08dc04db5875291781633746	no	1
Warnings:					
Information:					
Total Files Size (in bytes):			1503285		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

PATENT - POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS	Patent Number	8,761,804
	Issue Date	24 June 2014
	First Named Inventor	William J. Johnson
	Title	SYSTEM AND METHOD FOR LOCATION BASED...APPLICATIONS
	Attorney Docket No.	382740.00001

I hereby revoke all previous powers of attorney given in the above-identified patent.

A Power of Attorney is submitted herewith.

OR

I hereby appoint Practitioner(s) associated with the Customer Number identified in the box at right as my/our attorney(s) or agent(s) with respect to the patent identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: 78905

OR

I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) with respect to the patent identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified patent to:

The address associated with the above-identified Customer Number.

OR

The address associated with the Customer Number identified in the box at right:

OR

Firm or individual Name

Address

City

State

Zip

Country

Telephone

Email

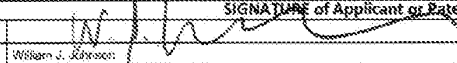
I am the:

Applicant.

OR

Patent owner.
 Statement under 37 CFR 3.73(c) (Form PTO/AIA/86) submitted herewith or filed on _____

SIGNATURE of Applicant or Patent Owner

Signature		Date	5/19/21
Name	William J. Johnson	Telephone	
Title and Company	Director, BRACIS LLC		

NOTE: Signatures of all the applicants or patent owners of the entire interest or their representative(s) are required. If more than one signature is required, submit multiple forms, check the box below, and identify the total number of forms submitted in the blank below.

A total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.51, 1.52, and 1.53. The information is required to obtain or retain a benefit by the public, which is to update (and by the USPTO to process) the file of a patent or reexamination proceeding. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: BILLJCO LLC
Application No./Patent No.: 8761804 Filed/Issue Date: 2014-06-24
Titled: LOCATION BASED EXCHANGE PERMISSIONS
BILLJCO LLC, a LLC
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. The assignee of the entire right, title, and interest.
2. An assignee of less than the entire right, title, and interest (check applicable box):
 - The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
 - There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

- A. An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 043147, Frame 0643, or for which a copy thereof is attached.

- B. A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

[Page 1 of 2]

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

Additional documents in the chain of title are listed on a supplemental sheet(s).

As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Mark D. Simpson/

19 May 2021

Signature

Date

Mark D. Simpson

32942

Printed or Typed Name

Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): William J. Johnson

Confirmation No.: 1470

Serial No.: 14/033,540, Filed September 23, 2013

Art Unit: 2642

Patent No.: 8,761,804, Issued June 24, 2014

Examiner: M. Batista

Title: SYSTEM AND METHOD FOR LOCATION BASED EXCHANGES
OF DATA FACILITATING DISTRIBUTED LOCATIONAL APPLICATIONS

Filed via EFS Web

TO: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**SUBMISSION UNDER 37 C.F.R. § 1.28(c) TO PAY FEE(S) AT
LARGE ENTITY RATE DUE TO CORRECTION OF ENTITY STATUS**

This paper is being filed in order to correct fee amounts paid due to an incorrect designation of small entity in this application made upon payment of the second maintenance fee. This error was made inadvertently, in good faith, and with no intent to deceive. The error was not caught until recently. Consistent with 37 C.F.R. § 1.28(c), a calculation of the deficiency owed, and an itemization of the same, is set forth in the table below. The itemization of the deficiency owed is as follows:

Fee/Code	Current Fee Amount	Fee Paid/Date	Deficiency Owed
Maintenance fee due at 3.5 years (Fee code 1551)	\$2,000	\$800 November 2, 2017	\$1,200

Per the undersigned's calculations, a total deficiency of **\$1,200** is owed. The undersigned authorizes the Office to charge this amount, and to charge any additional fees that may be due, or credit any overpayment, to Deposit Account 50-4364 (382740.00001).

Respectfully submitted,

May 19, 2021
Date

/Mark D. Simpson/
Mark D. Simpson, Esquire
Registration No. 32,942

SAUL EWING ARNSTEIN & LEHR LLP
Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102-2189
Telephone: 215 972 7880
Facsimile: 215 972 4169
Email: Mark.Simpson@saul.com



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/033,540	09/23/2013	William J. Johnson	JOHNS-001US3

CONFIRMATION NO. 1470

POA ACCEPTANCE LETTER



78905
Saul Ewing Arnstein & Lehr LLP (Philadelphia)
Attn: Patent Docket Clerk
Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102-2186

Date Mailed: 05/24/2021

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 05/19/2021.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/thaile/

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following
 Trademarks or Patents. (the patent action involves 35 U.S.C. § 292.);

DOCKET NO. 2:21-cv-181	DATE FILED 5/25/2021	U.S. DISTRICT COURT Eastern District of Texas
PLAINTIFF BILLJCO, LLC		DEFENDANT CISCO SYSTEMS, INC.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8,761,804	6/24/2014	BILLJCO, LLC
2 10,292,011	5/14/2019	BILLJCO, LLC
3 10,477,994	11/19/2019	BILLJCO, LLC
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY <input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input type="checkbox"/> Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	--

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following
 Trademarks or Patents. (the patent action involves 35 U.S.C. § 292.);

DOCKET NO. 2:21-cv-183	DATE FILED 5/25/2021	U.S. DISTRICT COURT Eastern District of Texas
PLAINTIFF BILLJCO, LLC		DEFENDANT HEWLETT PACKARD ENTERPRISE COMPANY, ARUBA NETWORKS, INC.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8,761,804	6/24/2014	BILLJCO, LLC
2 10,292,011	5/14/2019	BILLJCO, LLC
3 10,477,994	11/19/2019	BILLJCO, LLC
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY <input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input type="checkbox"/> Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	--

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas on the following
 Trademarks or Patents. (the patent action involves 35 U.S.C. § 292.);

DOCKET NO. 6:21-cv-528	DATE FILED 5/25/2021	U.S. DISTRICT COURT Western District of Texas
PLAINTIFF BILLJCO, LLC		DEPENDANT APPLE INC.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8,566,839	10/22/2013	BILLJCO, LLC
2 8,639,267	1/28/2014	BILLJCO, LLC
3 8,761,804	6/24/2014	BILLJCO, LLC
4 9,088,868	7/21/2015	BILLJCO, LLC
5 10,292,011	5/14/2019	BILLJCO, LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED 5/25/2021	INCLUDED BY <input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input checked="" type="checkbox"/> Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 10,477,994	11/19/2019	BILLJCO, LLC
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NUMBER, FILING OR 371(C) DATE, FIRST NAMED APPLICANT, ATTY.DOCKET NO./TITLE, REQUEST ID. Values: 14/033,540, 09/23/2013, William J. Johnson, JOHNS-001US3, 154384

Acknowledgement of Loss of Entitlement to Entity Status Discount

The entity status change request below filed through Private PAIR on 12/14/2021 has been accepted.

CERTIFICATIONS:

Change of Entity Status:
X Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be notification of loss of entitlement to small or micro entity status, as applicable.

This portion must be completed by the signatory or signatories making the entity status change in accordance with 37 CFR 1.4(d)(4).

Table with 2 columns: Label, Value. Rows: Signature: /Mark D. Simpson/, Name: Mark D. Simpson, Registration Number: 32942