FIG. 10A

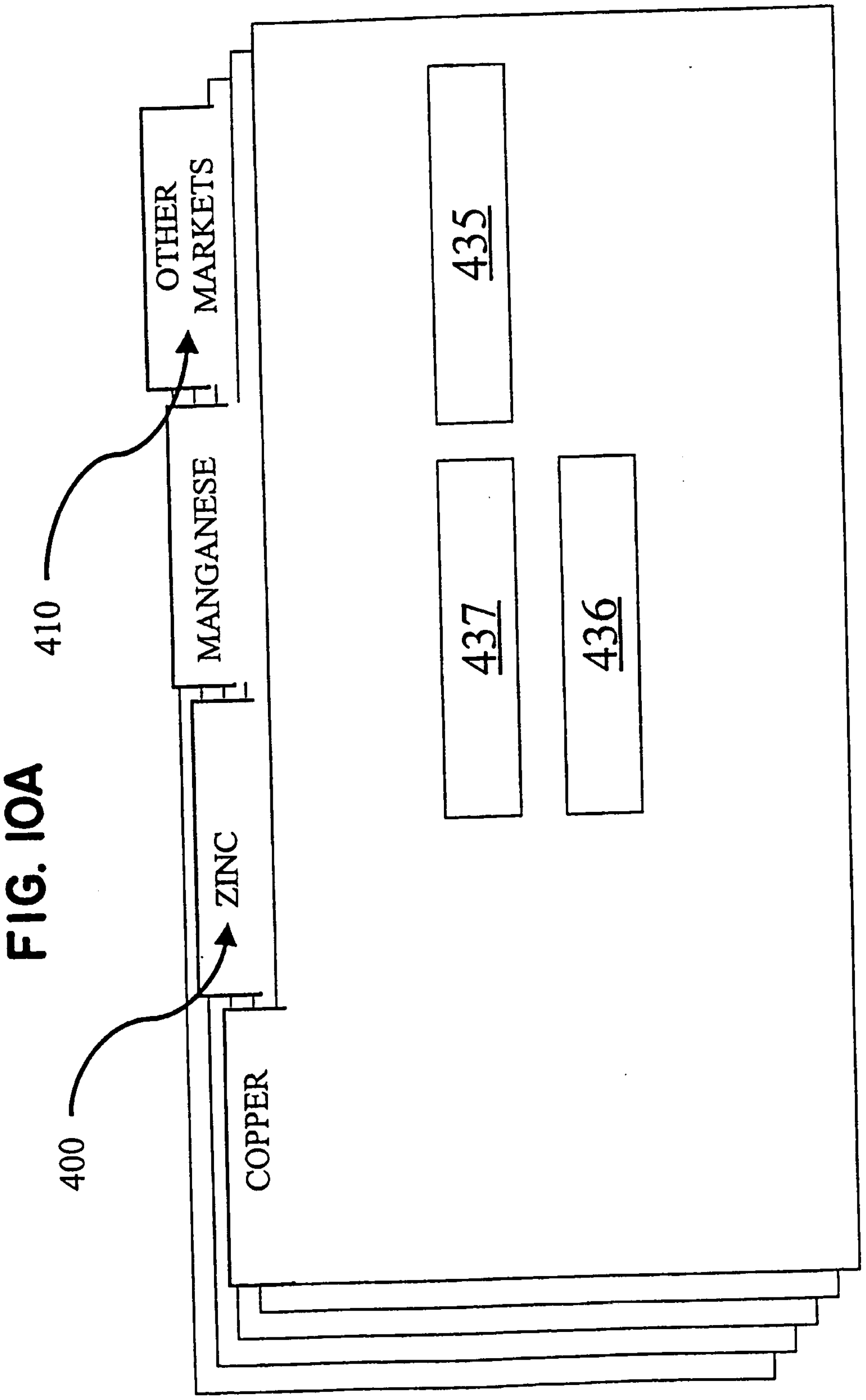
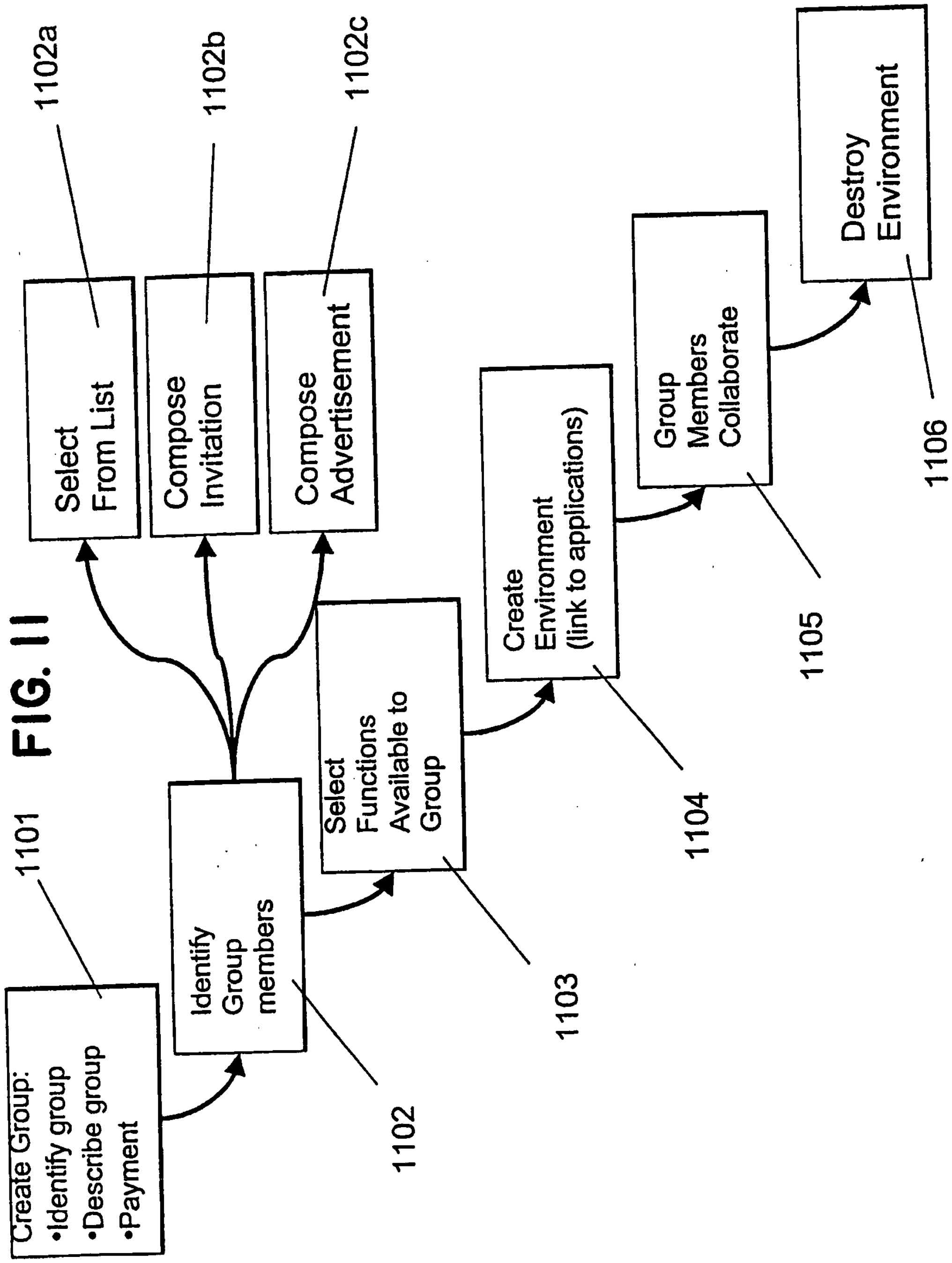


FIG. 11


Create Group:
•Identify group
•Describe group
•Payment
1101
Identify Group members
1102
Select From List
1102a
Compose Invitation
1102b
Compose Advertisement
1102c
Select Functions Available to Group
1103
Create Environment (link to applications)
1104
Group Members Collaborate
1105
Destroy Environment
1106

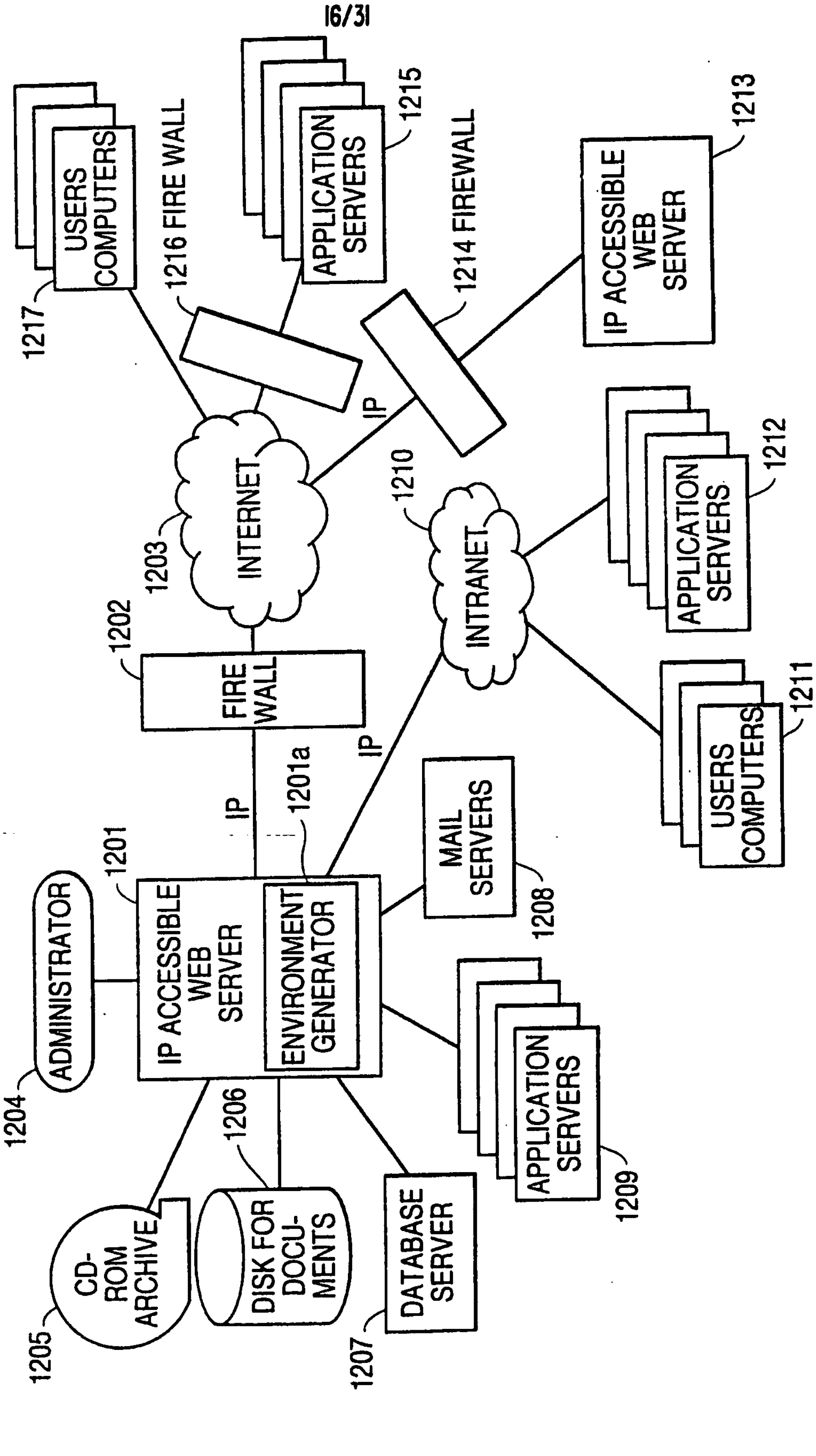
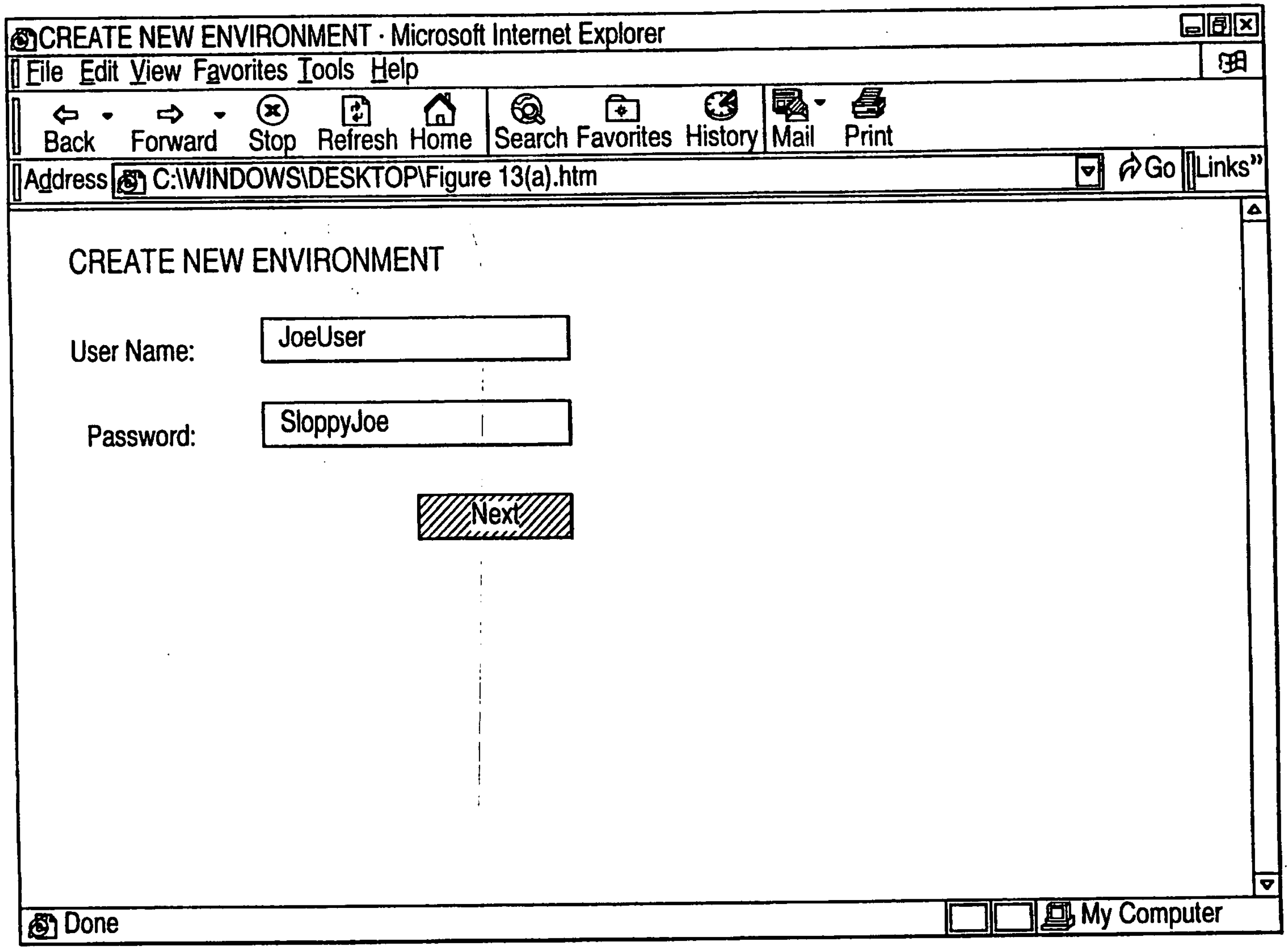

1201
IP ACCESSIBLE WEB SERVER
ENVIRONMENT GENERATOR
1201a
1204
ADMINISTRATOR
1205
CD-ROM ARCHIVE
1206
DISK FOR DOCU-MENTS
1207
DATABASE SERVER
1208
MAIL SERVERS
1209
APPLICATION SERVERS
IP
1202
FIRE WALL
1203
INTERNET
IP
1210
INTRANET
1211
USERS COMPUTERS
1212
APPLICATION SERVERS
1213
IP ACCESSIBLE WEB SERVER
1214 FIREWALL
IP
1215
APPLICATION SERVERS
1216 FIRE WALL
1217
USERS COMPUTERS

FIG. 12

FIG. 13A



CREATE NEW ENVIRONMENT · Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address
Go
Links"
Done
My Computer
Next

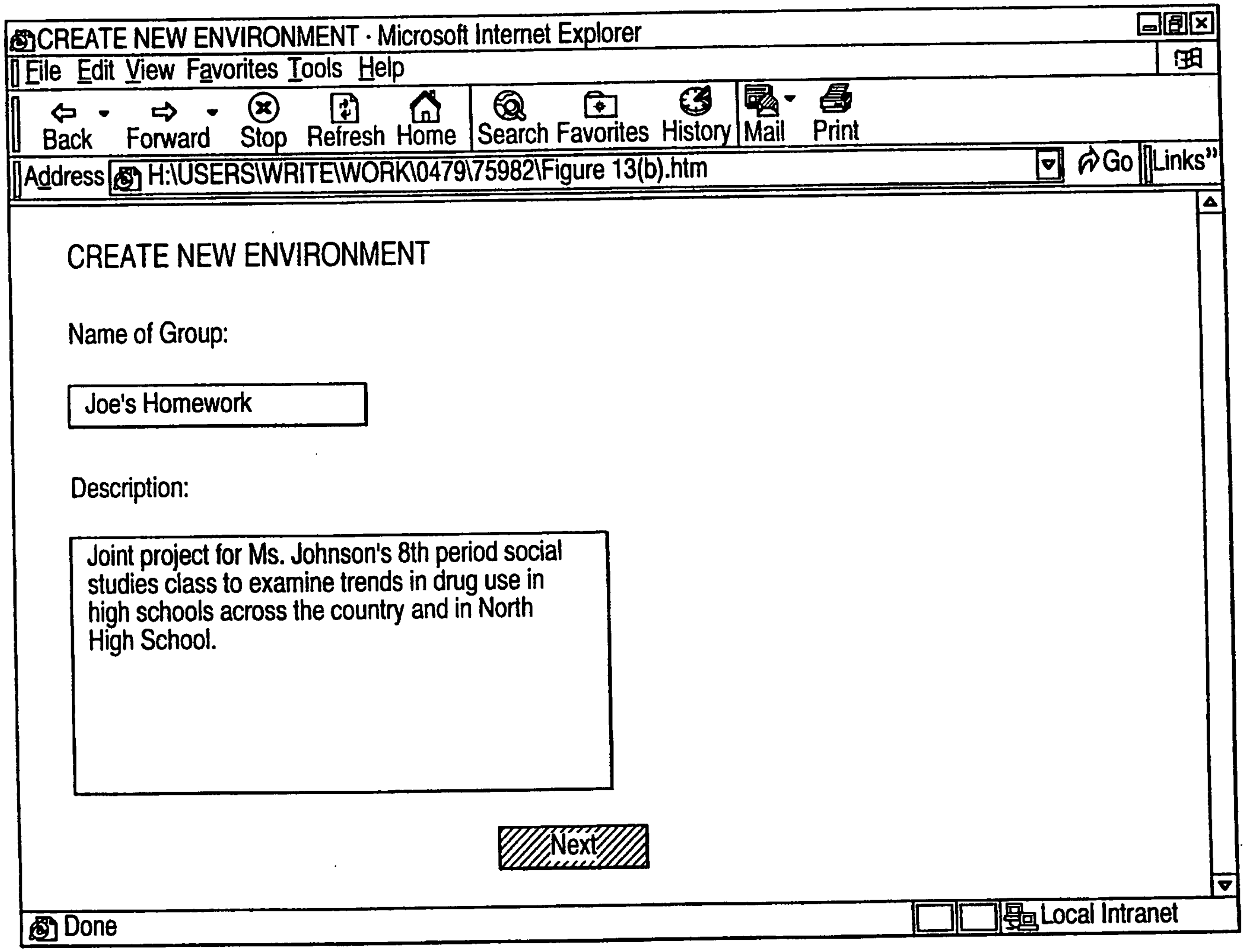
Address C:\WINDOWS\DESKTOP\Figure 13(a).htm

CREATE NEW ENVIRONMENT

User Name: JoeUser

Password: SloppyJoe

FIG. 13B



H:\USERS\WRITE\WORK\0479\75982\Figure 13(b).htm

CREATE NEW ENVIRONMENT

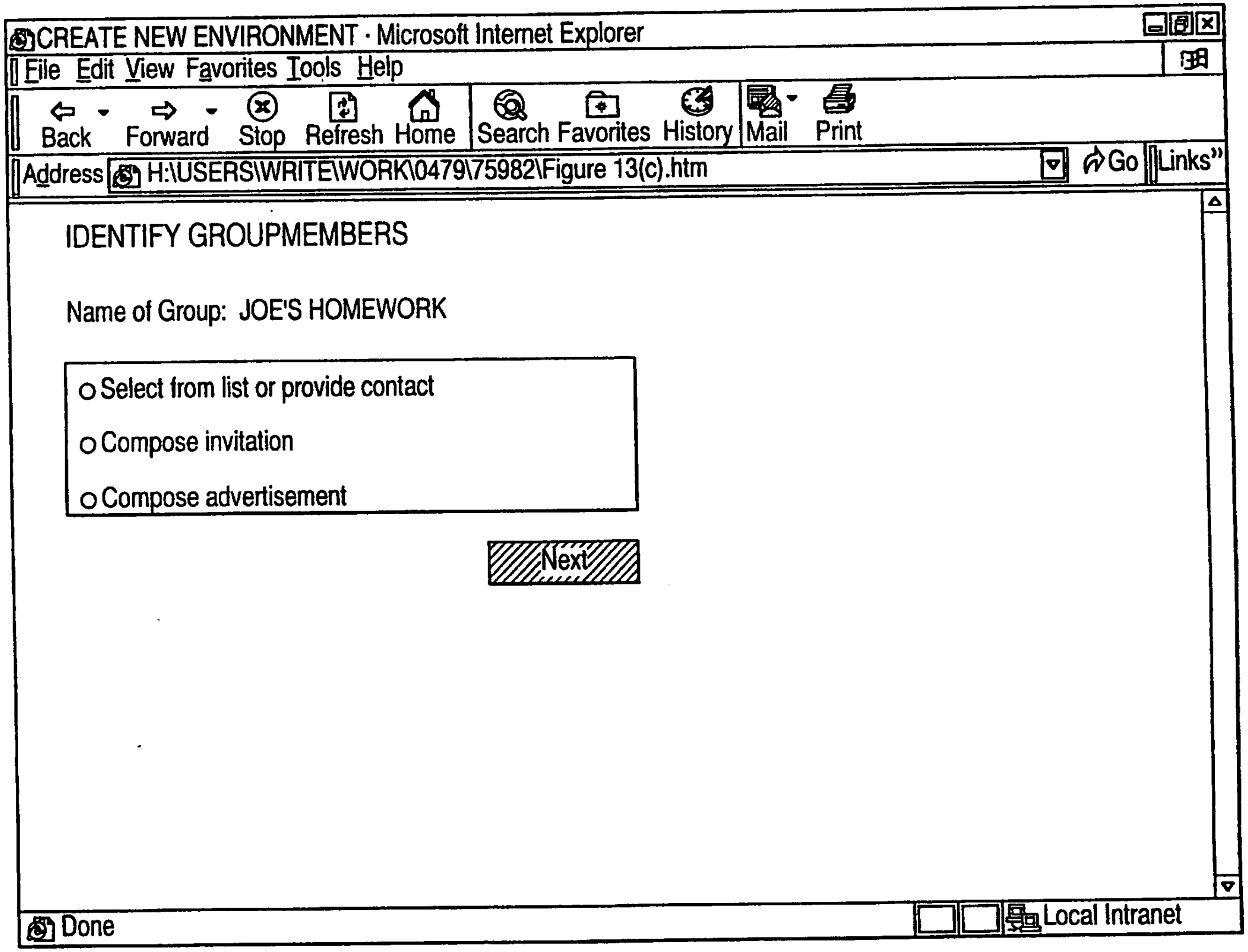
Name of Group:

Joe's Homework

Description:

Joint project for Ms. Johnson's 8th period social studies class to examine trends in drug use in high schools across the country and in North High School.

FIG. 13C



H:\USERS\WRITE\WORK\0479\75982\Figure 13(c).htm

IDENTIFY GROUPMEMBERS

Name of Group: JOE'S HOMEWORK

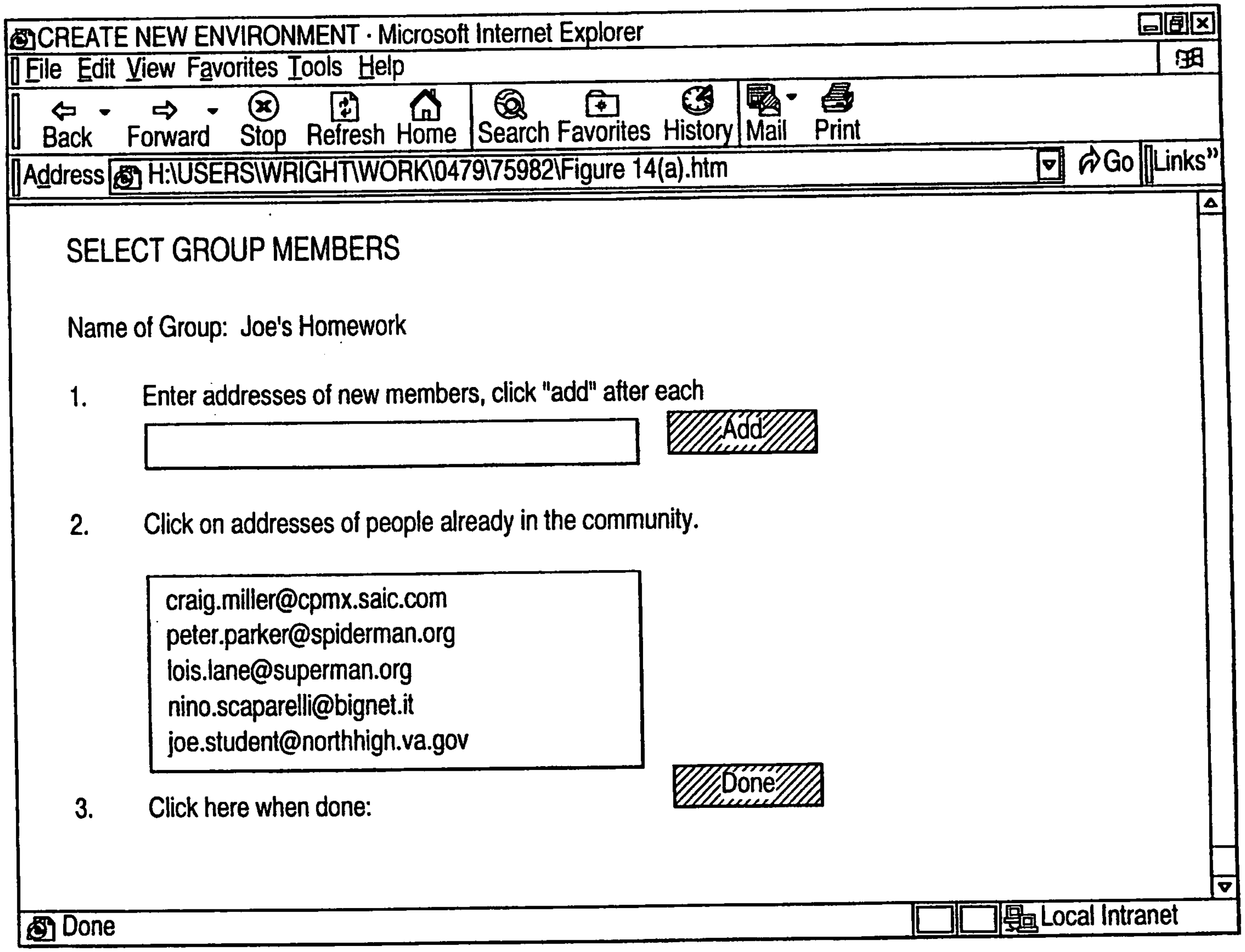
○ Select from list or provide contact

○ Compose invitation

○ Compose advertisement

Next

FIG. 14A



Address: H:\USERS\WRIGHT\WORK\0479\75982\Figure 14(a).htm

SELECT GROUP MEMBERS

Name of Group: Joe's Homework

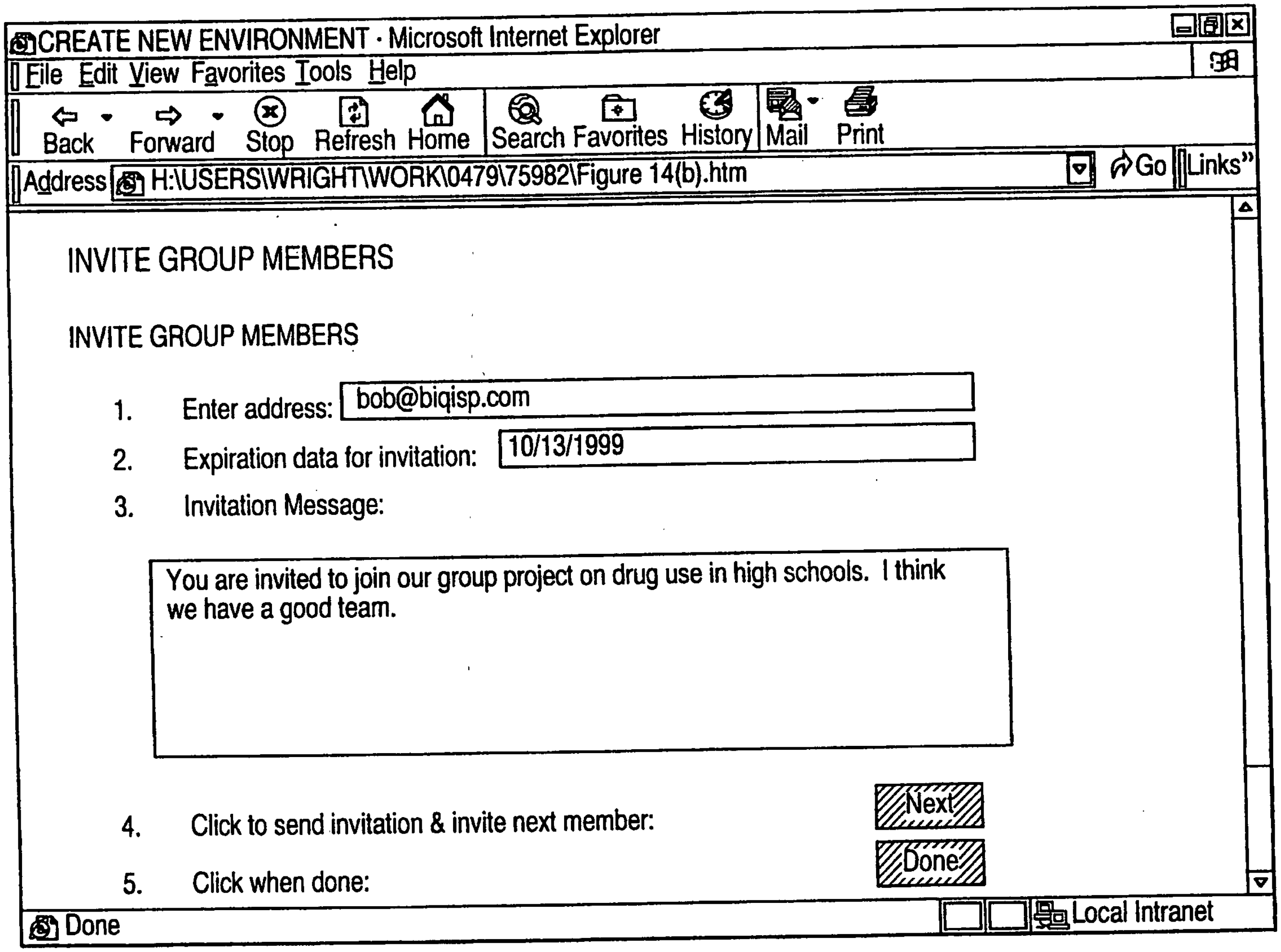
1. Enter addresses of new members, click "add" after each

2. Click on addresses of people already in the community.

craig.miller@cpmx.saic.com
peter.parker@spiderman.org
lois.lane@superman.org
nino.scaparelli@bignet.it
joe.student@northhigh.va.gov

3. Click here when done:

FIG. 14B


CREATE NEW ENVIRONMENT · Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Address
H:\USERS\WRIGHT\WORK\0479\75982\Figure 14(b).htm
Go
Links”

INVITE GROUP MEMBERS

INVITE GROUP MEMBERS

1. Enter address: bob@biqisp.com

2. Expiration data for invitation: 10/13/1999

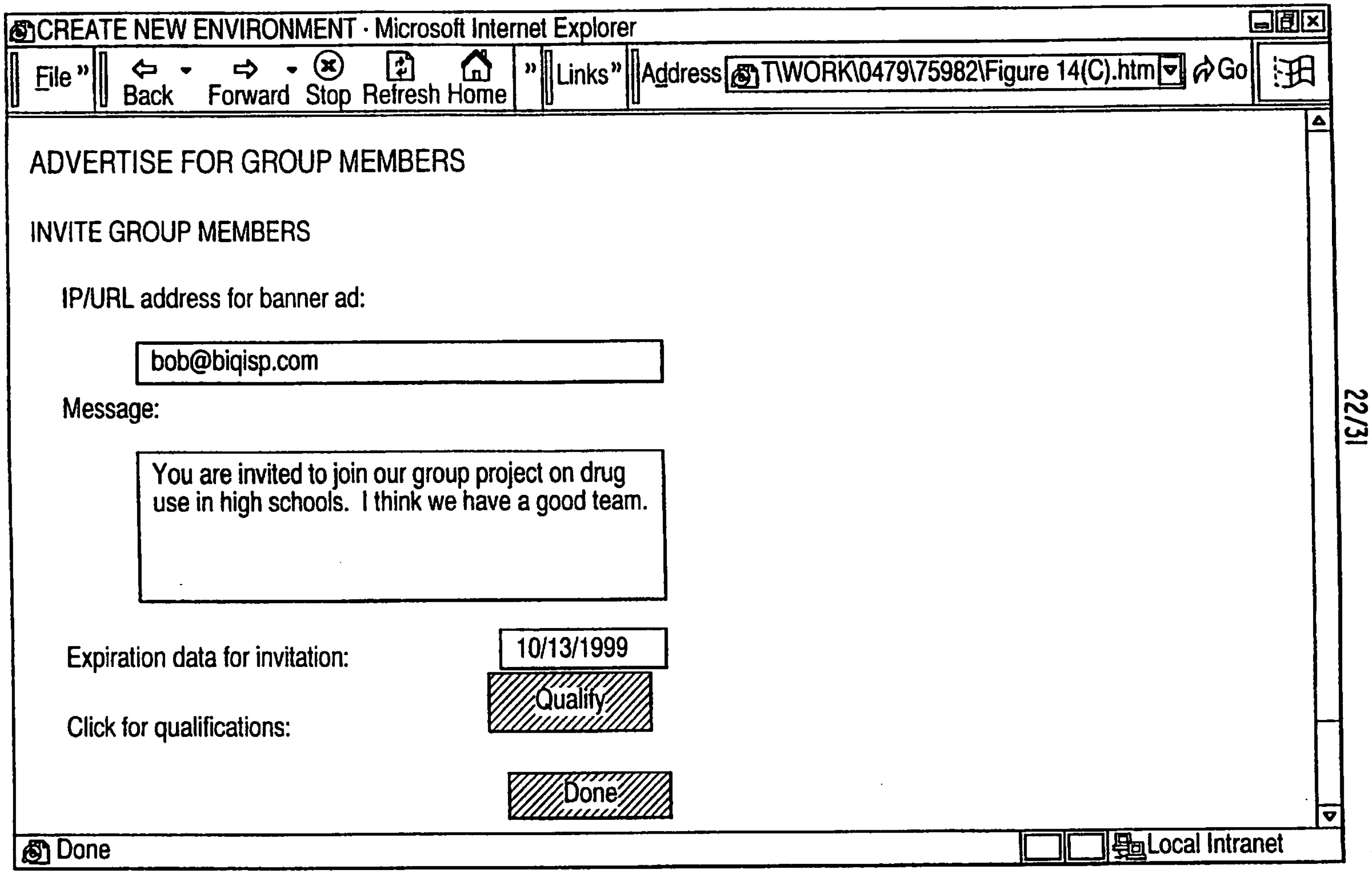
3. Invitation Message:

You are invited to join our group project on drug use in high schools. I think we have a good team.

4. Click to send invitation & invite next member: Next

5. Click when done: Done

FIG. 14C


CREATE NEW ENVIRONMENT · Microsoft Internet Explorer
File »
Back
Forward
Stop
Refresh
Home
Links »
Address
T\WORK\0479\75982\Figure 14(C).htm
Go
Qualify
Done
Done
Local Intranet

ADVERTISE FOR GROUP MEMBERS

INVITE GROUP MEMBERS

IP/URL address for banner ad:

bob@biqisp.com

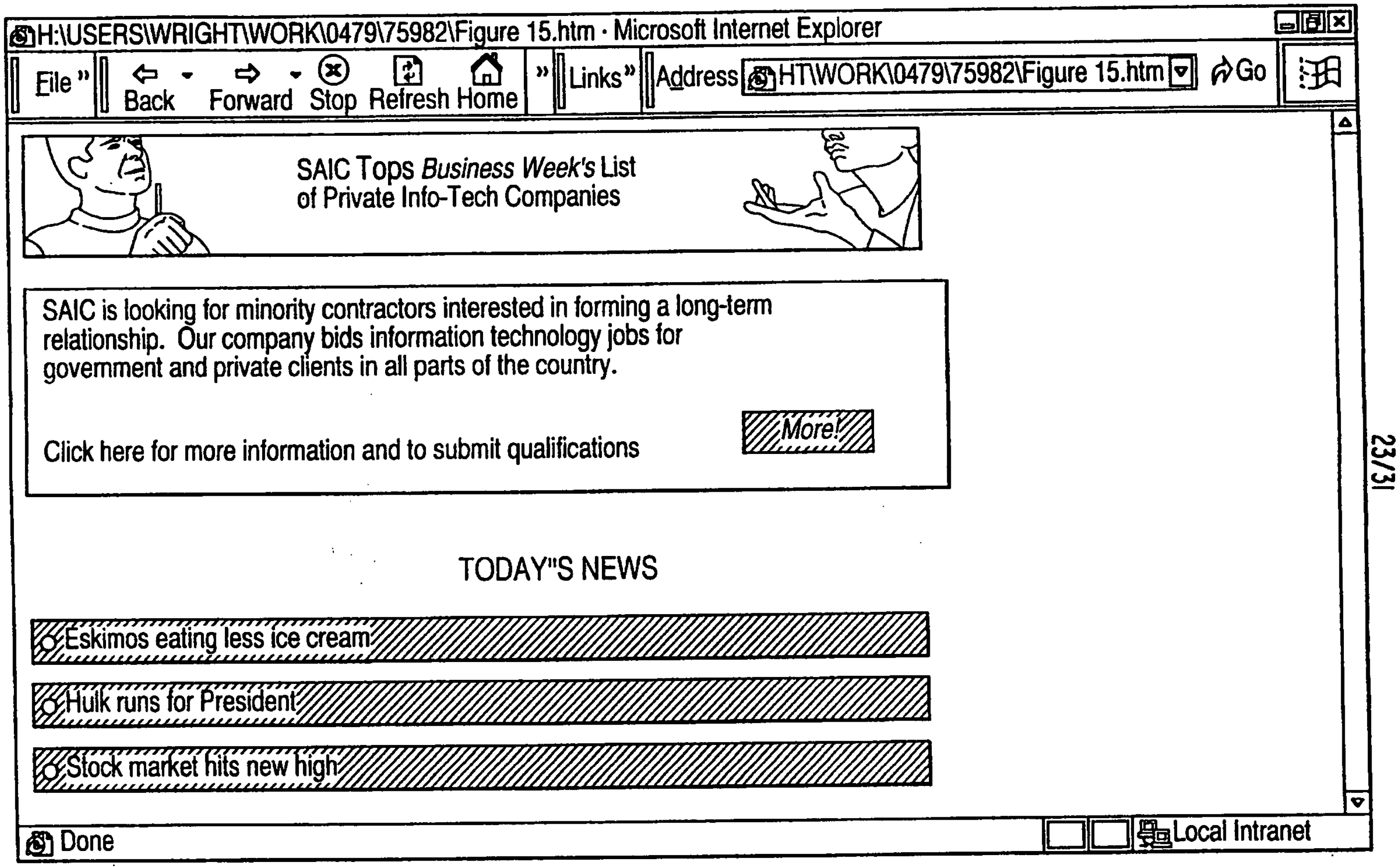
Message:

You are invited to join our group project on drug use in high schools. I think we have a good team.

Expiration data for invitation: 10/13/1999

Click for qualifications:

FIG. 15


H:\USERS\WRIGHT\WORK\0479\75982\Figure 15.htm · Microsoft Internet Explorer
File »
Back
Forward
Stop
Refresh
Home
»
Links »
Address
HT\WORK\0479\75982\Figure 15.htm
Go
Done
Local Intranet

SAIC Tops *Business Week's* List of Private Info-Tech Companies

SAIC is looking for minority contractors interested in forming a long-term relationship. Our company bids information technology jobs for government and private clients in all parts of the country.

Click here for more information and to submit qualifications

More!

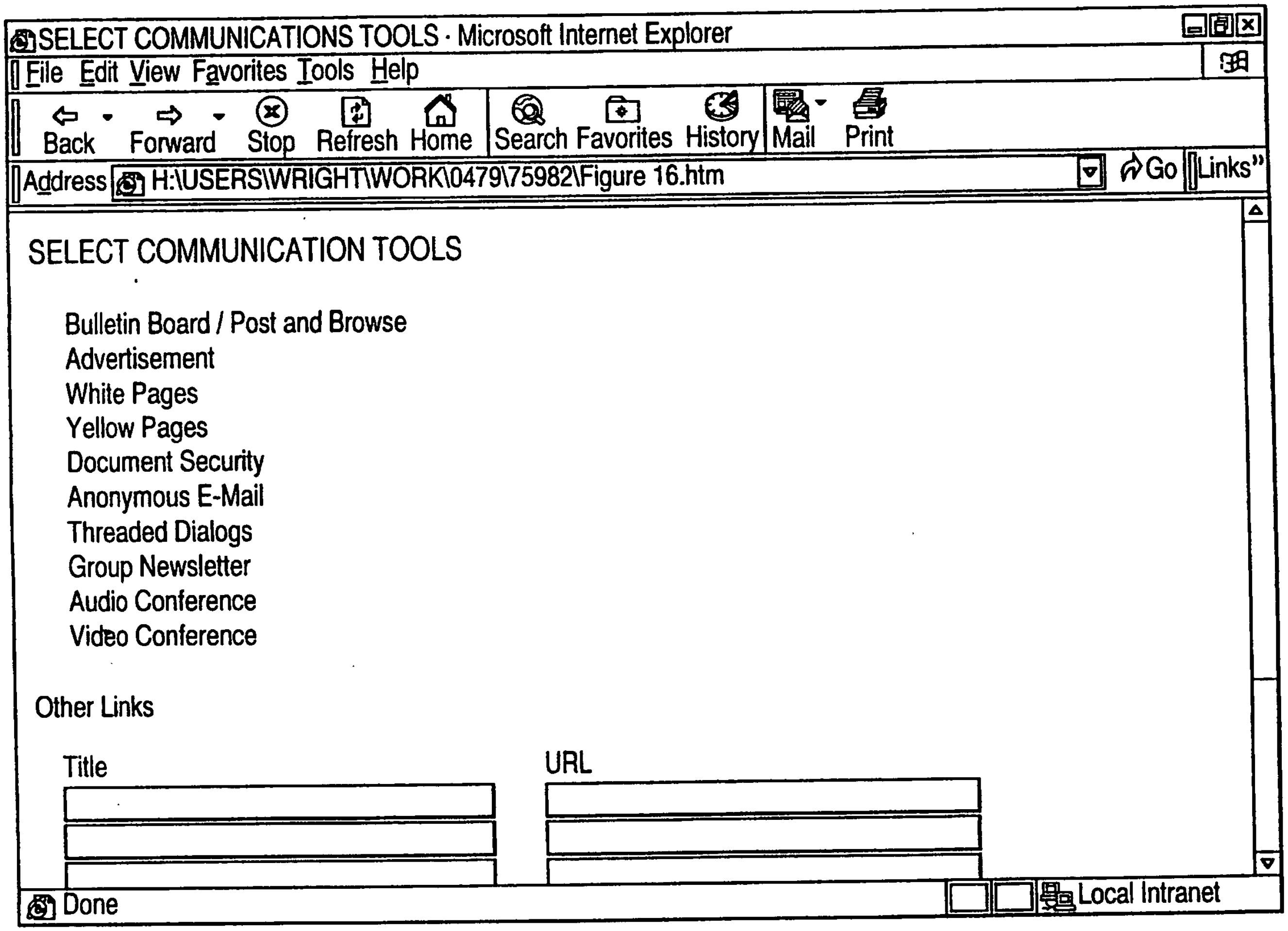
TODAY"S NEWS

○ Eskimos eating less ice cream

○ Hulk runs for President

○ Stock market hits new high

FIG. 16


SELECT COMMUNICATIONS TOOLS · Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Address
Go
Links"
Done
Local Intranet

H:\USERS\WRIGHT\WORK\0479\75982\Figure 16.htm

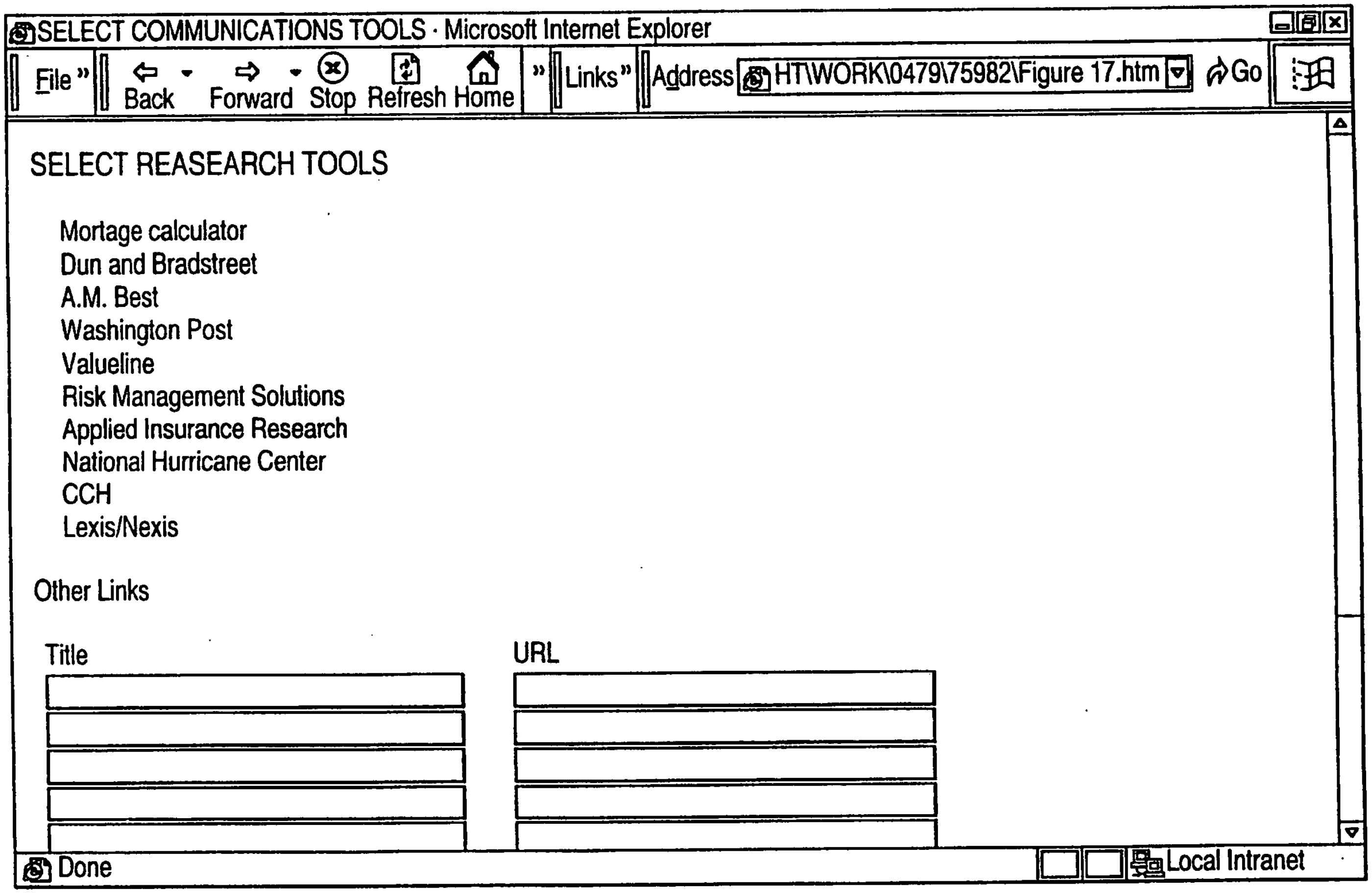
SELECT COMMUNICATION TOOLS

Bulletin Board / Post and Browse
Advertisement
White Pages
Yellow Pages
Document Security
Anonymous E-Mail
Threaded Dialogs
Group Newsletter
Audio Conference
Video Conference

Other Links

Title	URL

FIG. 17


SELECT COMMUNICATIONS TOOLS · Microsoft Internet Explorer
File »
Back
Forward
Stop
Refresh
Home
»
Links »
Address
HT\WORK\0479\75982\Figure 17.htm
Go
Done
Local Intranet

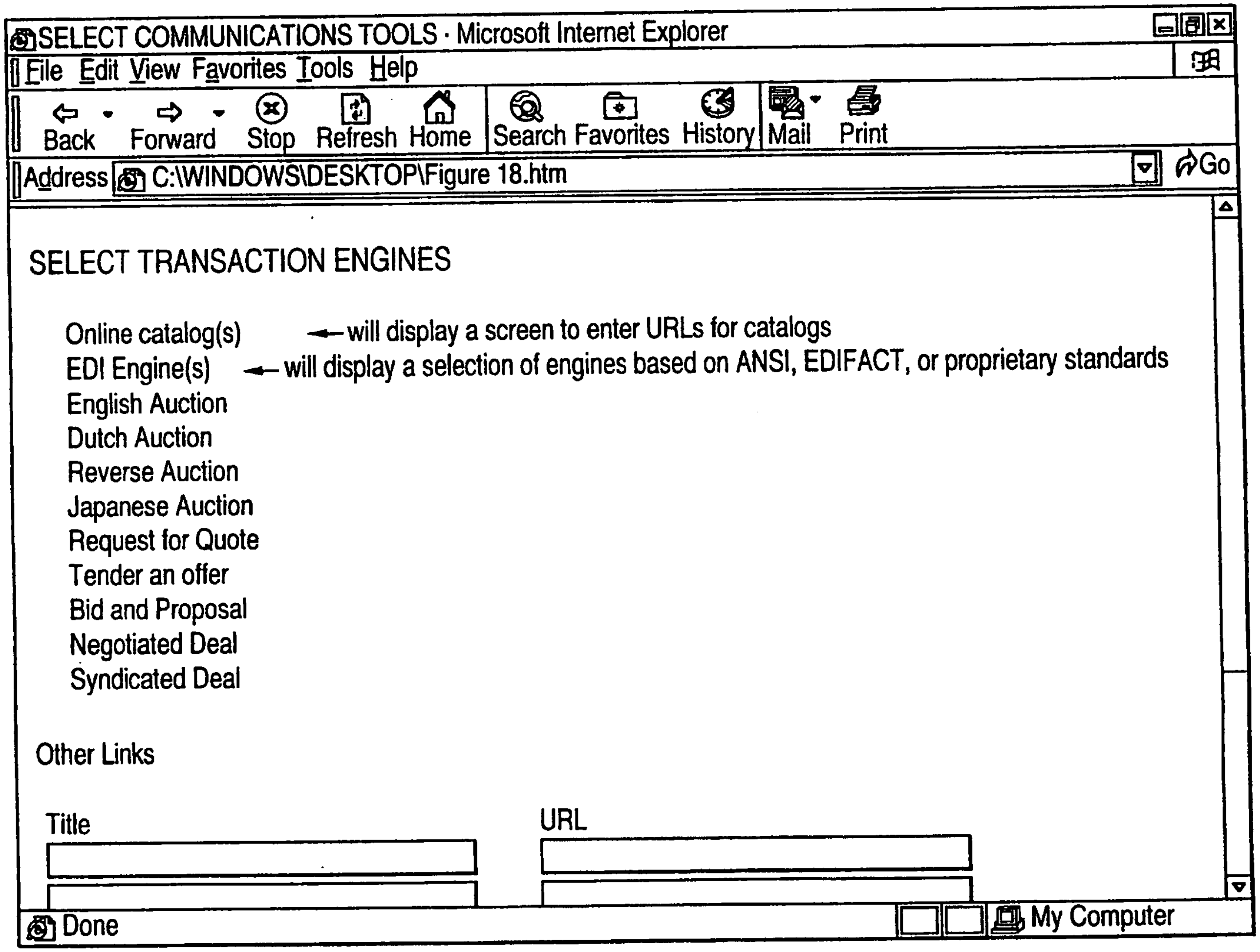
SELECT REASEARCH TOOLS

Mortage calculator
Dun and Bradstreet
A.M. Best
Washington Post
Valueline
Risk Management Solutions
Applied Insurance Research
National Hurricane Center
CCH
Lexis/Nexis

Other Links

Title	URL

FIG. 18


SELECT COMMUNICATIONS TOOLS · Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Address
Go
Done
My Computer

C:\WINDOWS\DESKTOP\Figure 18.htm

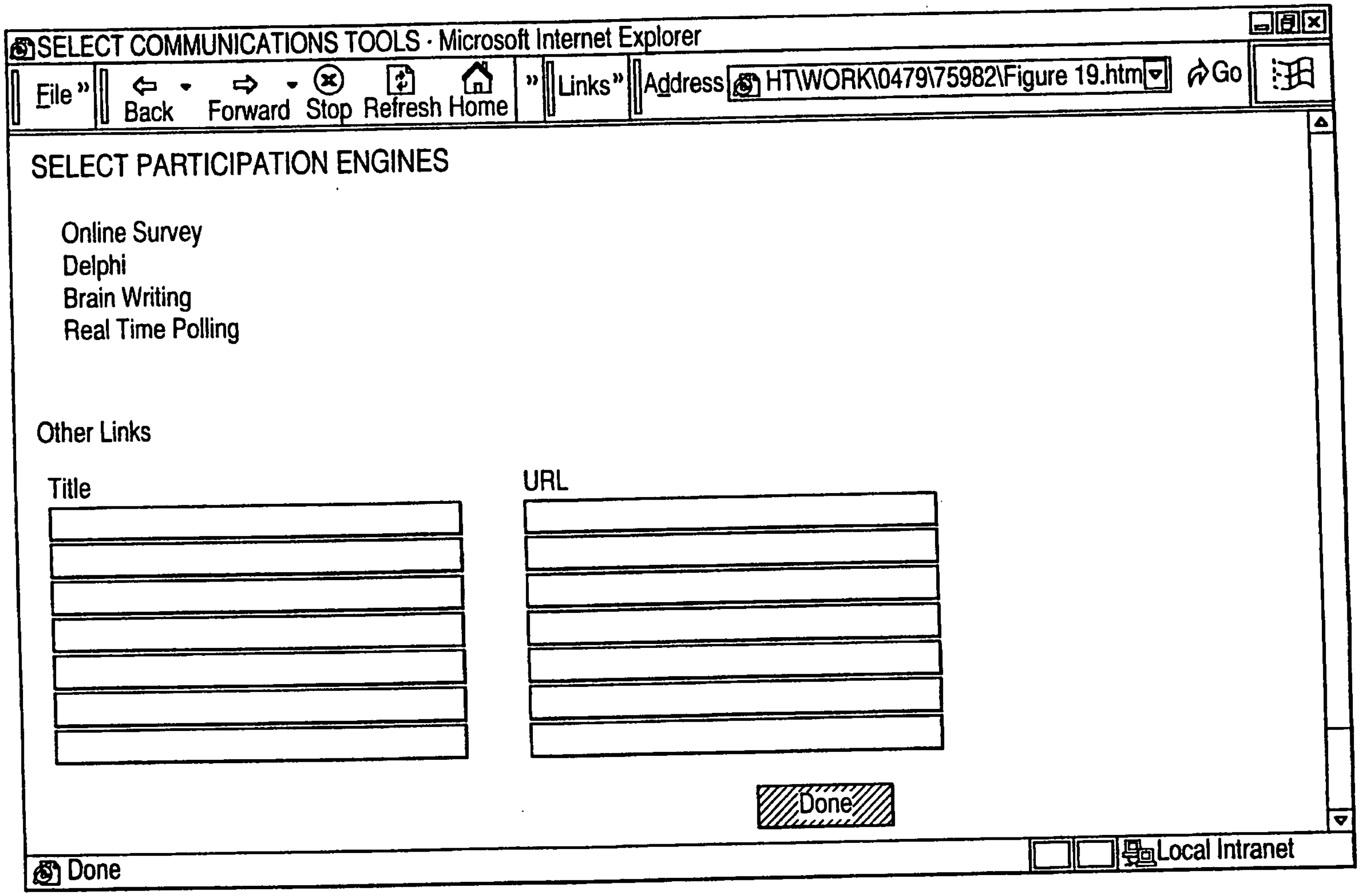
SELECT TRANSACTION ENGINES

Online catalog(s) ← will display a screen to enter URLs for catalogs
EDI Engine(s) ← will display a selection of engines based on ANSI, EDIFACT, or proprietary standards
English Auction
Dutch Auction
Reverse Auction
Japanese Auction
Request for Quote
Tender an offer
Bid and Proposal
Negotiated Deal
Syndicated Deal

Other Links

Title	URL

FIG. 19


SELECT COMMUNICATIONS TOOLS - Microsoft Internet Explorer
File »
Back
Forward
Stop
Refresh
Home
»
Links»
Address
HT\WORK\0479\75982\Figure 19.htm
Go
Done
Done
Local Intranet

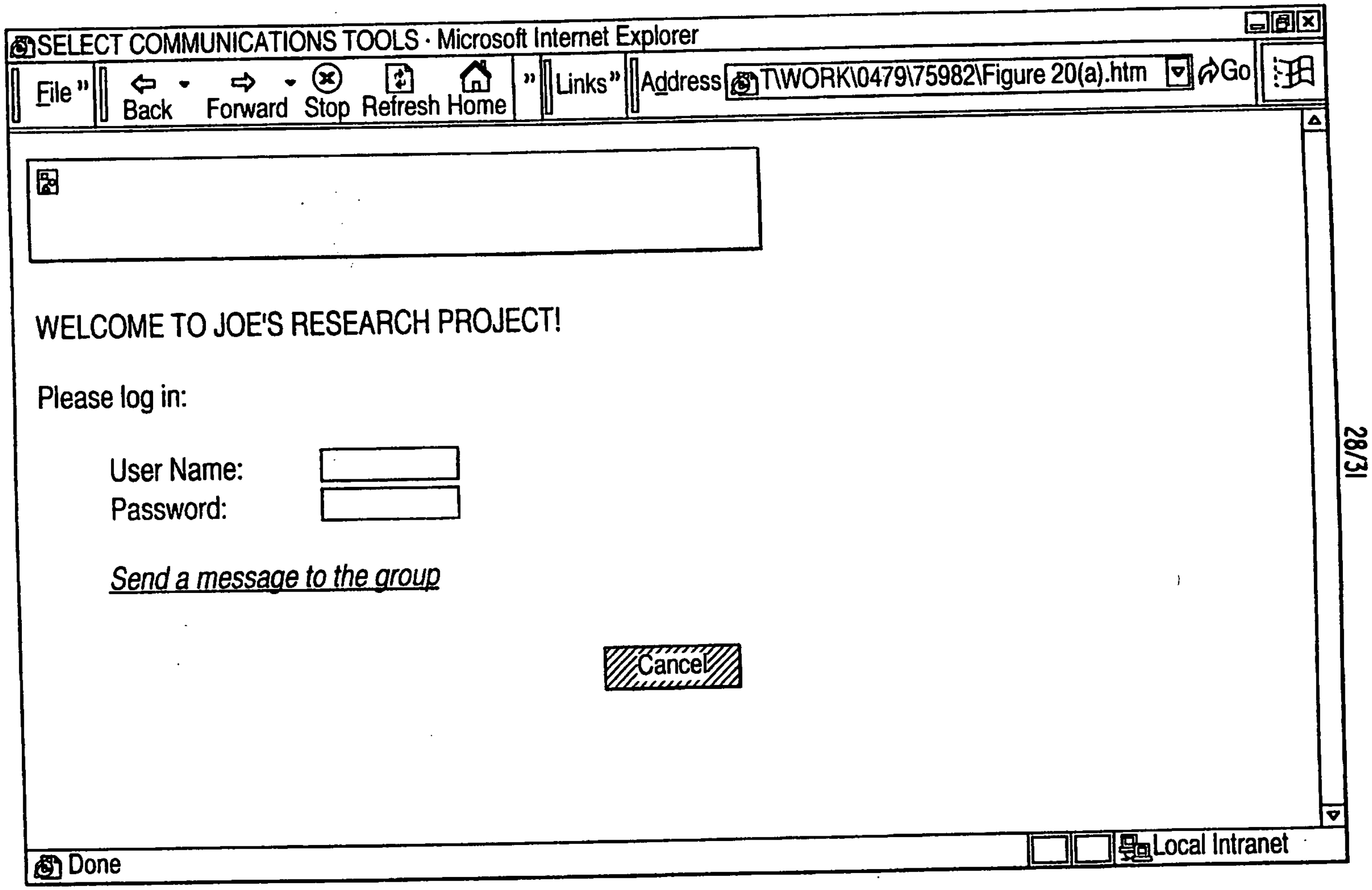
SELECT PARTICIPATION ENGINES

Online Survey
Delphi
Brain Writing
Real Time Polling

Other Links

Title	URL

FIG. 20A


SELECT COMMUNICATIONS TOOLS - Microsoft Internet Explorer
File
Back
Forward
Stop
Refresh
Home
Links
Address
T\WORK\0479\75982\Figure 20(a).htm
Go
Cancel
Done
Local Intranet

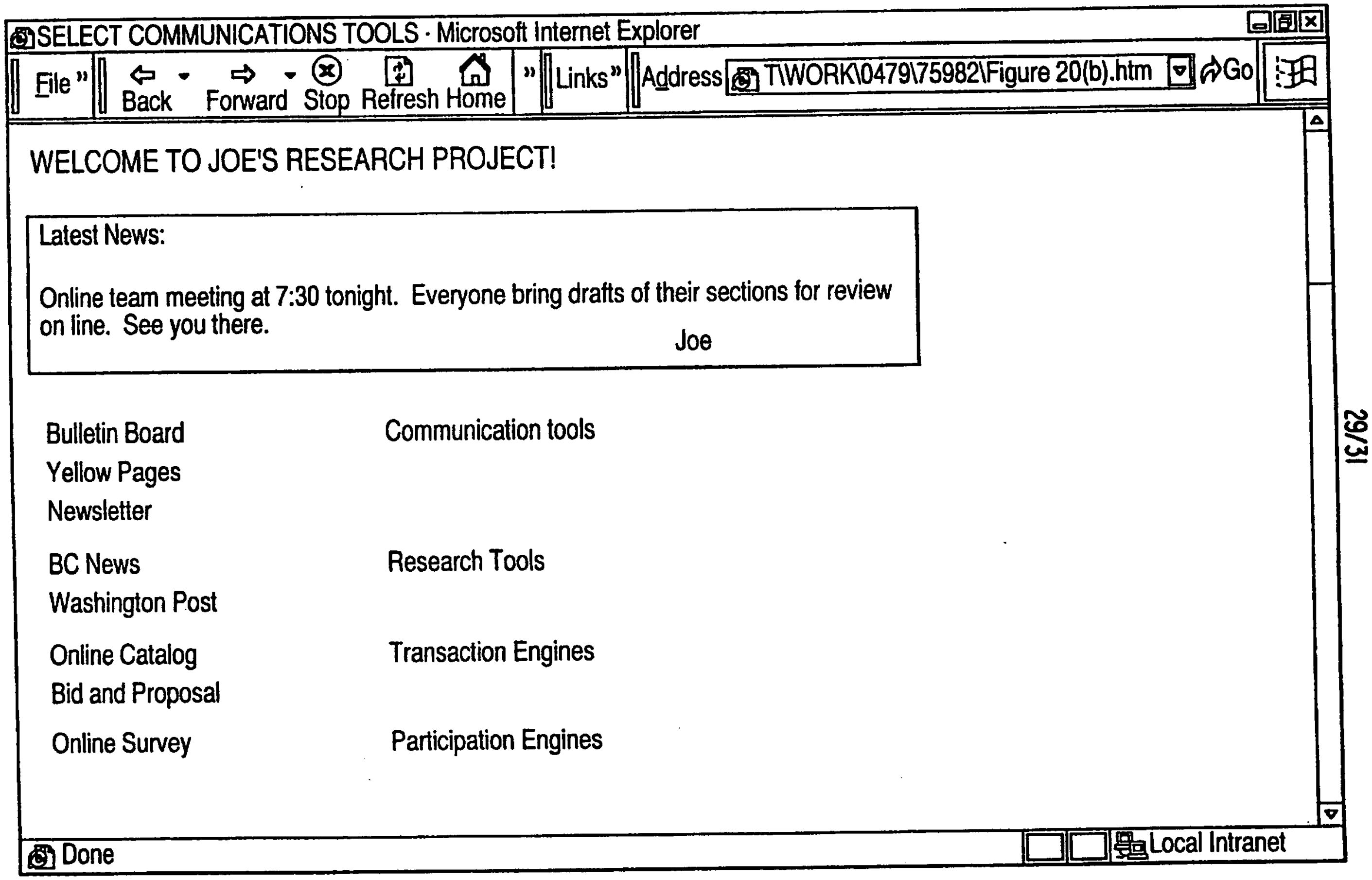
WELCOME TO JOE'S RESEARCH PROJECT!

Please log in:

User Name:
Password:

Send a message to the group

FIG. 20B


SELECT COMMUNICATIONS TOOLS - Microsoft Internet Explorer
File »
Back
Forward
Stop
Refresh
Home
»
Links »
Address
T\WORK\0479\75982\Figure 20(b).htm
Go
Done
Local Intranet

WELCOME TO JOE'S RESEARCH PROJECT!

Latest News:

Online team meeting at 7:30 tonight. Everyone bring drafts of their sections for review on line. See you there.

Joe

Bulletin Board
Yellow Pages
Newsletter

Communication tools

BC News
Washington Post

Research Tools

Online Catalog
Bid and Proposal

Transaction Engines

Online Survey

Participation Engines

FIG. 21

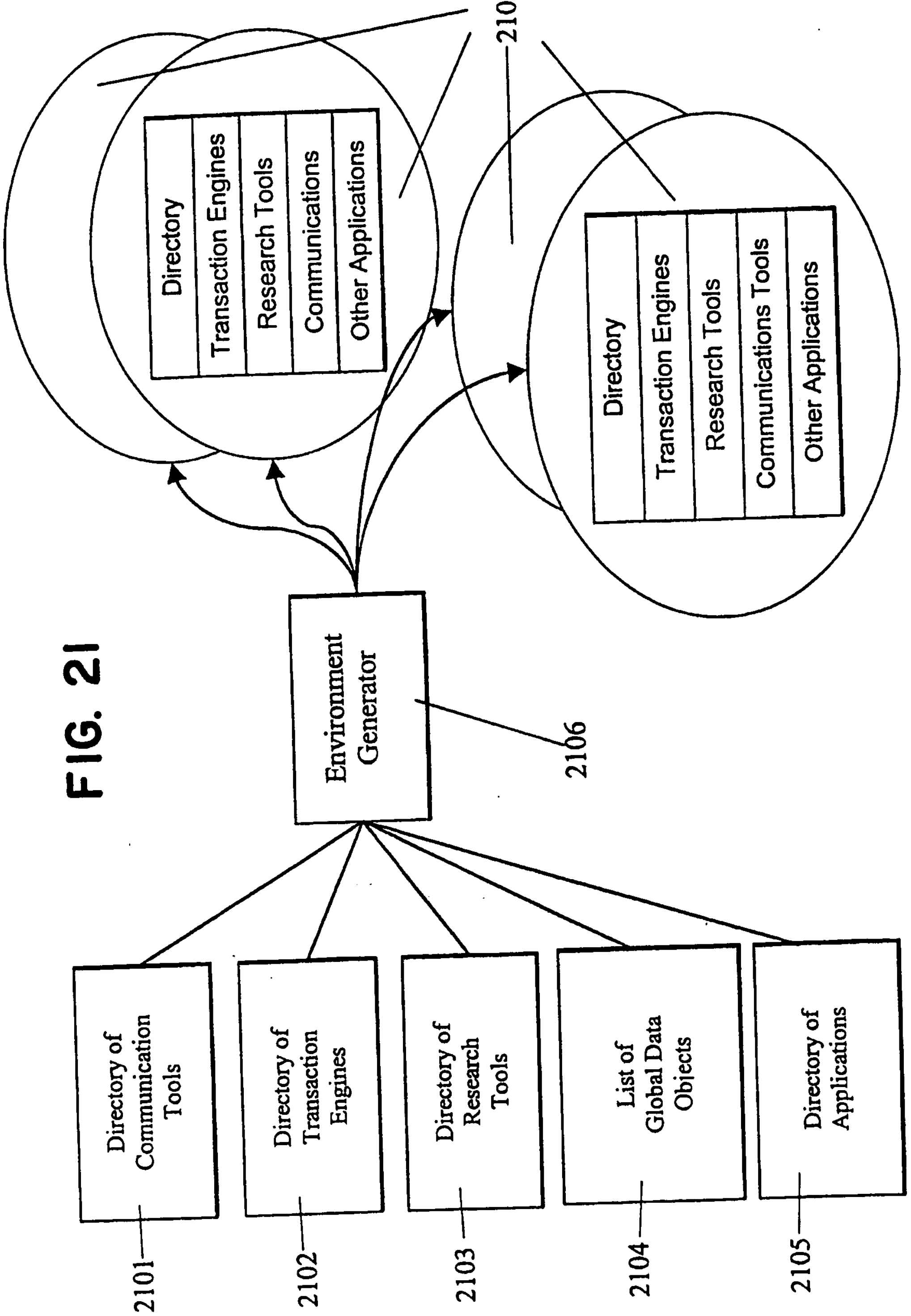
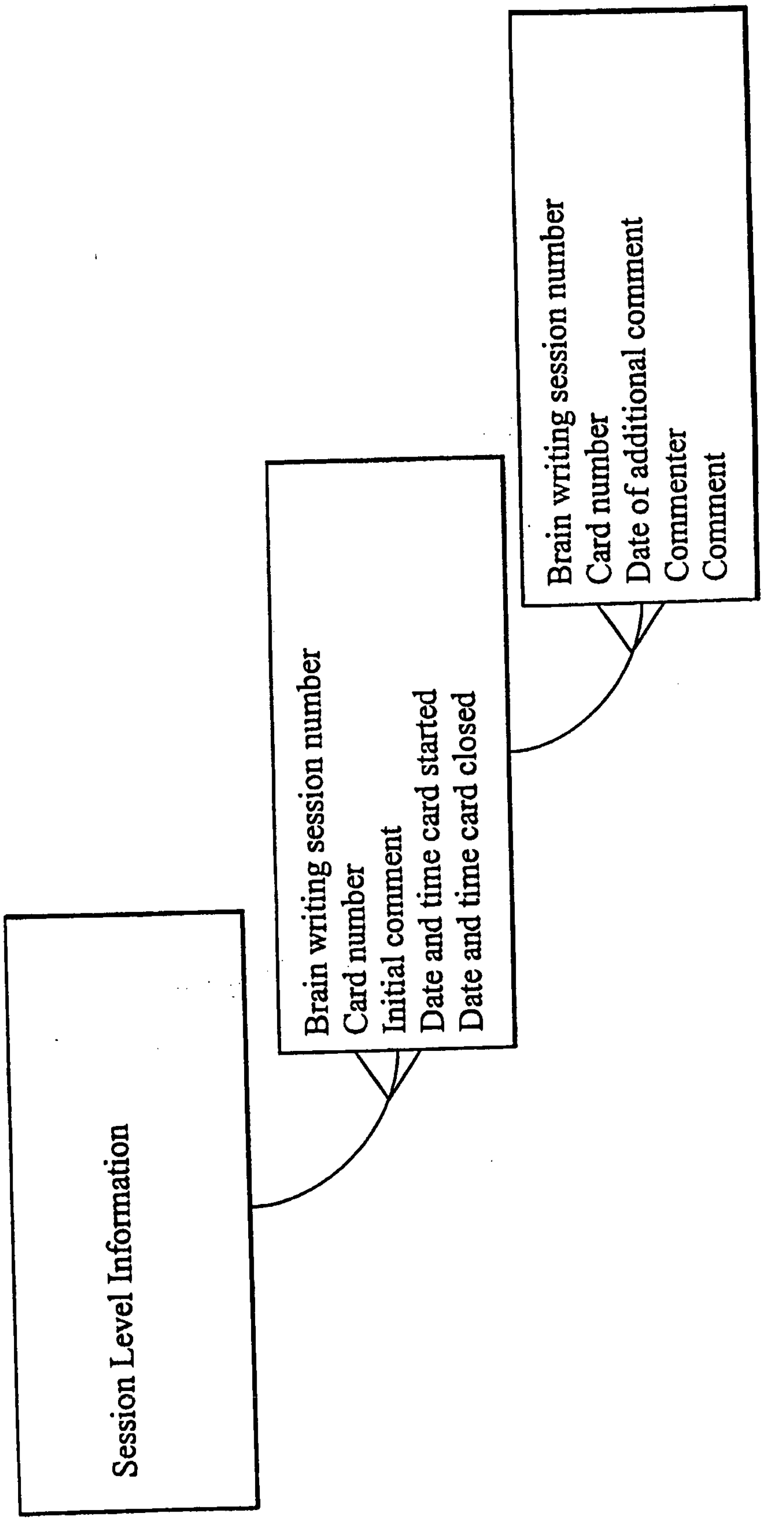

2107
Directory
Transaction Engines
Research Tools
Communications
Other Applications
Directory
Transaction Engines
Research Tools
Communications Tools
Other Applications
Environment Generator
2106
Directory of Communication Tools
Directory of Transaction Engines
Directory of Research Tools
List of Global Data Objects
Directory of Applications
2101
2102
2103
2104
2105

FIG. 22


Session Level Information
Brain writing session number
Card number
Initial comment
Date and time card started
Date and time card closed
Brain writing session number
Card number
Date of additional comment
Commenter
Comment

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
G06F 11/00

A1

(11) International Publication Number: WO 00/70458

(43) International Publication Date: 23 November 2000 (23.11.00)

(21) International Application Number: PCT/US00/08219

(22) International Filing Date: 15 May 2000 (15.05.00)

(30) Priority Data:
60/134,547 17 May 1999 (17.05.99) US

(71) Applicant: COMSEC CORPORATION [US/US]; 10217 Cedar Pond Drive, Vienna, VA 22182 (US).

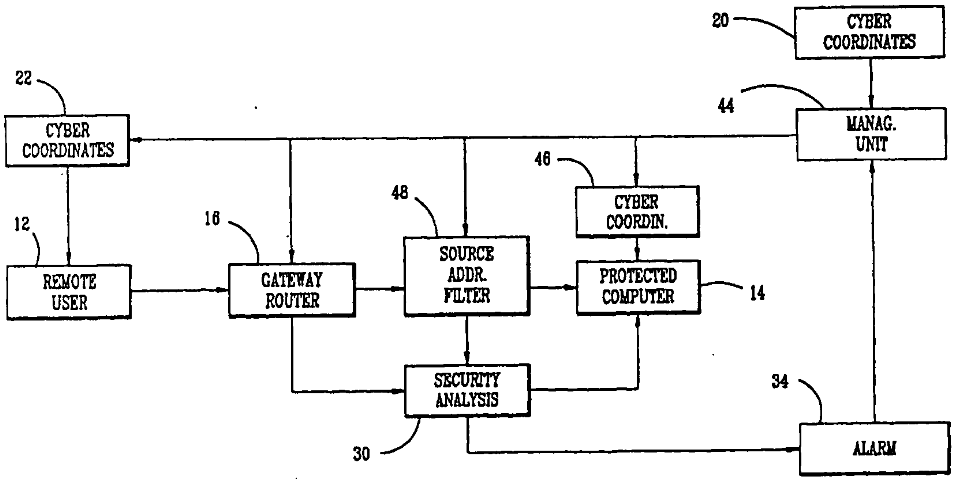
(72) Inventor: SHEYMOV, Victor, I.; 10217 Cedar Pond Drive, Vienna, VA 22182 (US).

(74) Agent: SIXBEY, Daniel, W.; Nixon Peabody LLP, Suite 800, 8180 Greensboro Drive, McLean, VA 22102 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, 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, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, 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.

(54) Title: METHOD OF COMMUNICATIONS AND COMMUNICATION NETWORK INTRUSION PROTECTION METHODS AND INTRUSION ATTEMPT DETECTION SYSTEM



(57) Abstract

The intrusion protection method and system for a communication network provides address agility wherein the cyber coordinates of a target host (14) are changed both on a determined time schedule and when an intrusion attempt is detected. The system includes a managment unit (18) which generates a random sequence of cyber coordinates and maintains a series of tables containing the current and next set of cyber coordinates. These cyber coordinates are distributed to authorized users (12) under an encryption process to prevent unauthorized access.

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	TM	Turkmenistan
BF	Burkina Faso	GR	Greece		Republic of Macedonia	TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's	NZ	New Zealand		
CM	Cameroon		Republic of Korea	PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD OF COMMUNICATIONS AND COMMUNICATION NETWORK INTRUSION PROTECTION METHODS AND INTRUSION ATTEMPT DETECTION SYSTEM

This application is a continuation-in-part application of U.S. Serial No. 60/134,547 filed May 17, 1999.

Background Art

Historically, every technology begins its evolution focusing mainly on performance parameters, and only at a certain developmental stage does it address the security aspects of its applications. Computer and communications networks follow this pattern in a classic way. For instance, first priorities in development of the Internet were reliability, survivability, optimization of the use of communications channels, and maximization of their speed and capacity. With a notable exception of some government systems, communications security was not an early high priority, if at all. Indeed, with a relatively low number of users at initial stages of Internet development, as well as with their exclusive nature, problems of potential cyber attacks would have been almost unnatural to address, considering the magnitude of other technical and organizational problems to overcome at that time. Furthermore, one of the ideas of the Internet was "democratization" of communications channels and of access to information, which is almost contradictory to the concept of security. Now we are faced with a situation, which requires adequate levels of security in communications while preserving already achieved "democratization" of communications channels and access to information.

All the initial objectives of the original developers of the Internet were achieved with results spectacular enough to almost certainly surpass their expectations. One of the most remarkable results of the Internet development to date is the mentioned "democratization". However in its unguarded way "democratization" apparently is either premature to a certain percentage of the Internet users, or contrary to human nature, or both. The fact remains that this very percentage of users presents a serious threat to the integrity of national critical infrastructure, to privacy of information, and to further advance of commerce by utilization of the Internet capabilities. At this stage it seems crucial to address security issues but, as usual, it is desirable to be done within already existing structures and technological conventions.

Existing communications protocols, while streamlining communications, still lack underlying entropy sufficient for security purposes. One way to increase entropy, of course, is encryption as illustrated by U.S. Patent No. 5,742,666 to Finley. Here each node in the Internet encrypts the destination address with a code which only the next node can unscramble.

Encryption alone has not proven to be a viable security solution for many communications applications. Even within its core purpose, encryption still retains certain security problems, including distribution and safeguarding of the keys. Besides, encryption represents a "ballast", substantially reducing information processing speed and transfer time. These factors discourage its use in many borderline cases.

Another way is the use of the passwords. This method has been sufficient against humans, but it is clearly not working against computers. Any security success of the password-based security is temporary at best. Rapid advances in computing power make even the most sophisticated password arrangement a short-term solution.

Recent studies clearly indicate that the firewall technology, as illustrated by U.S. Patent No. 5,898,830 to Wesinger et al., also does not provide a sufficient long-term solution to the security problem. While useful to some extent, it cannot alone withstand the modern levels of intrusion cyber attacks.

On the top of everything else, none of the existing security methods, including encryption, provides protection against denial of service attacks. Protection against denial of service attacks has become a critical aspect of communication system security. All existing log-on security systems, including those using encryption, are practically defenseless against such attacks. Given a malicious intent of a potential attacker, it is reasonable to assume that, even having failed with an intrusion attempt, the attacker is still capable of doing harm by disabling the system with a denial of service attack. Since existing systems by definition have to deal with every log-on attempt, legitimate or not, it is certain that these systems cannot defend themselves against a denial of service attack.

The deficiencies of existing security methods for protecting communications systems leads to the conclusion that a new generation of cyber protection technology is needed to achieve acceptable levels of security in network communications.

Summary of the Invention

It is a primary object of the present invention to provide a novel and improved method of communications, and a novel and improved communication network intrusion protection method and systems and novel and improved intrusion attempt detection method and systems, adapted for use with a wide variety of communication networks including Internet based computers, corporate and organizational computer networks (LANs), e-commerce systems, wireless computer communications networks, telephone dial-up systems, wireless dial-up systems, wireless telephone and computer communications systems, cellular and satellite telephone systems, mobile telephone and mobile communications systems, cable based systems and computer databases, as well as protection of network nodes such as routers, switches, gateways, bridges, and frame relays.

Another object of the present invention is to provide a novel and improved communication network intrusion protection method and system which provides address agility combined with a limited allowable number of log-on attempts.

Yet another object of the present invention is to provide a novel and improved intrusion protection method for a wide variety of communication and other devices which may be accessed by a number, address code, and/or access code. This number, address code, and/or access code is periodically changed and the new number, address code, or access code is provided only to authorized users. The new number, address code, or access code may be provided to a computer or a device for the authorized user and not be accessible to others. This identifier causes the user's computer to transmit the otherwise unknown and inaccessible number, address code, and/or access code.

A still further object of the present invention is to provide a novel and improved communication network intrusion protection method and system wherein a plurality of different cyber coordinates must be correctly provided before access is granted to a protected communications unit or a particular piece of information. If all or some cyber coordinates are not correctly provided, access is denied, an alarm situation is instigated and the affected cyber coordinates may be instantly changed.

For the purposes of this invention cyber coordinates are defined as a set of statements determining location of an object (such as a computer) or a piece of information (such as a computer file) in cyber space. Cyber coordinates include but are not limited to private or public protocol network addresses such as an IP address in the Internet, a computer port number or designator, a computer or database directory, a file name or designator, a telephone number , an access number and/or code, etc.

These and other objects of the present invention are achieved by providing a communication network intrusion protection method and system where a potential intruder must first guess where a target computer such as a host workstation is in cyber space and to predict where the target computer such as a workstation will next be located in cyber space. This is achieved by changing a cyber coordinate (the address) or a plurality of cyber coordinates for the computers such as workstations on a determined or random time schedule and making an unscheduled cyber coordinates change when the system detects an intrusion attempt. A limited number of log-on attempts may be permitted before an intrusion attempt is confirmed and the cyber coordinates are changed. A management unit is provided for generating a random sequence of cyber coordinates and which maintains a series of tables containing current and the next set of addresses. These addresses are distributed to authorized parties, usually with use of an encryption process.

The present invention further provides for a piece of information, a computer or a database intrusion protection method and system where a potential intruder must first guess where a target piece of information such as a computer file or a directory is in cyber space and to predict where the target piece of information will be next in cyber space. This is achieved by changing a cyber coordinate or a plurality of cyber coordinates for the piece of information on a determined or random time schedule and making an unscheduled cyber coordinates change when the system detects an intrusion attempt. A limited number of log-on attempts may be permitted before an intrusion attempt is confirmed and the coordinates changed. A management unit is provided for generating a random sequence of cyber coordinates and which maintains a series of tables containing current and the next set of cyber coordinates. These coordinates are distributed to authorized parties, usually by means of an encryption process.

The intrusion attempt detection methods and systems are provided to the protected devices and pieces of information as described above by means of categorizing a log-on attempt when all or some of the correct cyber coordinates are not present as an intrusion attempt and by instigating an alarm situation.

Brief Description of the Drawings

Figure 1 is a block diagram of the communication network protection system of the present invention;

Figure 2 is a flow diagram showing the operation of the system of Figure 1;

Figure 3 is a block diagram of a second embodiment of the communication network protection system of the present invention;

Figure 4 is a flow diagram showing the operation of the system of Figure 3;

Figure 5 is a block diagram of a third embodiment of the communication network protection system of the present invention;

Figure 6 is a flow diagram showing the operation of the system of Figure 5; and

Figure 7 is a block diagram of a fourth embodiment of the communication network protection system of the present invention.

Description of the Preferred Embodiments

Existing communications systems use fixed coordinates in cyber space for the communications source and communications receiver. Commonly accepted terminology for the Internet refers to these cyber coordinates as source and destination IP addresses. For purposes of an unauthorized intrusion into these communication systems, the situation of a cyber attack might be described in military terms as shooting at a stationary target positioned at known coordinates in cyber space. Obviously, a moving target is more secure than the stationary one, and a moving target with coordinates unknown to the intruder is more secure yet. The method of the present invention takes advantage of the cyber space environment and the fact that the correlation between the physical coordinates of computers or other communication devices and their cyber coordinates is insignificant.

While it is difficult to change the physical coordinates of computers or other communications devices, their cyber coordinates (cyber addresses) can be changed much easier, and in accordance with the present invention, may be variable and changing over time. In addition to varying the cyber coordinates over time, the cyber coordinates can immediately be changed when an attempted intrusion is sensed. Furthermore, making the current cyber coordinates available to only authorized parties makes a computer or other communications device a moving target with cyber coordinates unknown to potential attackers. In effect, this method creates a device which perpetually moves in cyber space.

Considering first the method of the present invention as applied to computers and computer networks, the computer's current cyber address may serve also as its initial log-on password with a difference that this initial log-on password is variable. A user, however, has to deal only with a computer's permanent identifier, which is, effectively its assigned "name" within a corresponding network. Any permanent identifier system can be used, and an alphabetic "name" system seems to be reasonably user-friendly. One of such arrangements would call for using a computer's alphabetic Domain Name System, as a cyber address permanent identifier, while subjecting its numeric, or any other cyber address to a periodic change with regular or irregular intervals. This separation will make the security system transparent to the user, who will have to deal only with the alphabetic addresses. In effect, the user's computer would contain an "address book" where the alphabetic addresses are permanent, and the corresponding variable addresses are more complex and periodically updated by a network's management. While a user is working with other members of the network on the name or the alphabetic address basis, the computer conducts communications based on the corresponding variable numeric or other addresses assigned for that particular time.

A variable address system can relatively easily be made to contain virtually any level of entropy, and certainly enough entropy to defy most sophisticated attacks. Obviously, the level of protection is directly related to the level of entropy contained in the variable address system and to the frequency of the cyber address change.

This scenario places a potential attacker in a very difficult situation when he has to find the target before launching an attack. If a restriction on a number of allowable log-on tries is implemented, it becomes more difficult for an attacker to find the target than to actually attack it. This task of locating the target can be made difficult if a network's cyber address system contains sufficient entropy. This difficulty is greatly increased if the security system also limits the number of allowable log-on tries, significantly raising the entropy density.

For the purpose of this invention, cntropy density is defined as entropy per one attempt to guess a value of a random variable.

Figure 1 illustrates a simple computer intrusion protection system 10 which operates in accordance with the method of the present invention. Here, a remote user's computer 12 is connected to a protected computer 14 by a gateway router or bridge 16. A management system 18 periodically changes the address for the computer 14 by providing a new address from a cyber address book 20 which stores a plurality of cyber addresses. Each new cyber address is provided by the management system 18 to the router 16 and to a user computer address book 22. The address book 22 contains both the alphabetic destination address for the computer 14 which is available to the user and the variable numeric cyber address which is not available to the user. When the user wants to transmit a packet of information with the alphabetic address for the computer 14, this alphabetic address is automatically substituted for the current numerical cyber address and used in the packet.

With the reference to Figures 1 and 2, when a packet is received by the gateway router or bridge 16 as indicated at 24, the cyber address is checked by the gateway router or bridge at 26, and if the destination address is correct, the packet is passed at 28 to the computer 14. If the destination address is not correct, the packet is directed to a security analysis section 30 which, at 32 determines if the packet is retransmitted with a correct address within a limited number of log-in attempts. If this occurs, the security analysis section transmits the packet to the computer 14 at 28. However, if no correct address is received within the allowed limited number of log-in attempts, the packet is not transmitted to the computer 14 and the security analysis section activates an alarm section 34 at 36 which in turn causes the management section to immediately operate at 38 to change the cyber address.

Sophisticated cyber attacks often include intrusion through computer ports other than the port intended for a client log-on. If a system principally described in connection with Figures 1 and 2 is implemented, the port vulnerability still represents an opening for an attack from within the network, that is if an attacker has even a low-level authorized access to a particular computer and thus knows its current variable address.

Computer ports can be protected in a way similar to protection of the computer itself. In this case port assignment for the computer becomes variable and is changed periodically in a manner similar to that described in connection with Figures 1 and 2. Then, a current assignment of a particular port is communicated only to appropriate parties and is not known to others. At the same time, similarly to methods described, a computer user would deal with permanent port assignments, which would serve as the ports' permanent "names".

This arrangement in itself may not be sufficient, however, to reliably protect against a port attack using substantial computing power because of a possible insufficient entropy density. Such a protection can be achieved by implementing an internal computer "port router" which would serve essentially the same role for port identifiers as the common gateway router or bridge 16 serves for computer destination addresses.

With reference to Figures 3 and 4 wherein like reference numerals are used for components and operations which are the same as those previously described in connection with Figures 1 and 2, a port router 40 is provided prior to the protected computer 14, and this port router is provided with a port number or designator by the management unit 18. This port number or designator is also provided to the user address book 22 and will be changed when the cyber address is changed, or separately. Thus, with reference to Figure 4, once the cyber address has been cleared at 26, the port number or designator is examined at 42. If the port number is also correct, the data packet will be passed to the computer 14 at 28. If the port number is initially incorrect, the packet is directed to the security analysis section 30 which at 32 determines if the packet is retransmitted with the correct port number within the limited number of log-in attempts.

The port protection feature can be used independently of other features of the system. It can effectively protect nodes of the infrastructure such as routers, gateways, bridges, and frame relays from unauthorized access. This can protect systems from an attacker staging a cyber attack from such nodes.

The method and system of the present invention may be adapted to provide security for both Internet based computer networks and private computer networks such as LANs.

Internet structure allows the creation of an Internet based Private Cyber Network (PCN) among a number of Internet-connected computers. The main concern for using the Internet for this purpose as an alternative to the actual private networks with dedicated communication channels is security of Internet-based networks.

The present invention facilitates establishment of adequate and controllable level of security for the PCNs. Furthermore, this new technology provides means for flexible structure of a PCN, allowing easy and practically instant changes in its membership. Furthermore, it allows preservation of adequate security in an environment where a computer could be a member of multiple PCNs with different security requirements. Utilizing the described concept, a protected computer becomes a "moving target" for the potential intruders where its cyber coordinates are periodically changed and the new coordinates are communicated on a "need to know" basis only to the other members of the PCN authorized to access this computer along with appropriate routers and gateways. This change of cyber coordinates can be performed either by previous arrangement or by communicating future addresses to the authorized members prior to the change. Feasible frequency of such a change can range from a low extreme of a stationary system changing cyber coordinates only upon detection of a cyber attack to an extremely high frequency such as with every packet. The future coordinates can be transmitted either encrypted or unencrypted. Furthermore, each change of position of each PCN member can be made random in terms of both its current cyber coordinates and the time of the coordinates change. These parameters of a protected PCN member's cyber moves are known only to the PCN management, other PCN members with authorization to communicate with this particular member, and appropriate gateways and routers. PCN management would implement and coordinate periodic cyber coordinates changes for all members of the PCN. While the PCN management is the logical party to make all the notification of the cyber coordinates changes, in certain instances it could be advantageous to shift a part of this task to a PCN member computer itself. With certain limitations, the routers and gateways with the "need to know" the current address of the protected computer are located in cyber space in the general vicinity of the protected computer. In such instances the protected computer could be in a better position to make the mentioned notifications of nearby routers and gateways.

The address changes could be done simultaneously for all the members of the PCN, or separately, particularly if security requirements for the members substantially differ. The latter method is advantageous, for instance, if some of the computers within the PCN are much more likely than others to be targeted by potential intruders. A retail banking PCN could be an example of such an arrangement where the bank's computer is much more likely to be attacked than a customer's computer. It should be noted that, while in certain cases some members of the PCN may not require any protection at all, it still is prudent to provide it as long as the computer belongs to a protected PCN. The correct "signature" of the current "return address" would serve as additional authenticity verification. In the above example of the retail banking, while many customers' computers may not require any protection, assigning variable addresses to them would serve as an additional assurance to the bank that every log-on is authorized. In fact, this system automatically provides two-tier security. In order to reach a protected computer, the client computer has to know the server computer current cyber address in the first place. Then, even if a potential intruder against odds "hits" the correct current address the information packet is screened for the correct "signature" or return address. If that signature does not belong to the list of the PCN's current addresses, the packet is rejected. In high security instances this should trigger an unscheduled address change of the protected computer.

With the reference to Figures 5 and 6 which illustrate this two-tier security system, a network management unit 44 provides different unique cyber coordinates to the address books for each computer in the system (two computers 12 and 14 with address books 22 and 46 respectively being shown). Now when the computer 12 sends a data packet to the computer 14, the gateway router or bridge 16, first checks for the correct current destination address for the computer 14 at 26 in the manner previously described. If the destination address is correct, a source address sensor 48 checks at 50 to determine if the correct source address (i.e. return address) for the computer 12 is also present. If both correct addresses are present, the data packet is passed to the computer 14 at 28, but if the correct source address is not present, the data packet is passed to the security analysis section 30 where at 32 where it is determined if a correct source address is received within the acceptable number of log-on tries. If the correct return address is not received, an alarm situation is activated at 36 and the network management system operates at 38 to change the cyber address of the computer 14

In addition to the penetration (hacking) detection and protection, the system above provides real-time detection of a cyber attack and protection against "flooding" denial of service attacks. A gateway router or bridge 16 filters all the incorrectly addressed packets thus protecting against "flooding". Further yet, since the "address book" of the protected network contains only trusted destinations, this system also protects against instructive viruses or worms if such are present or introduced into the network. For the purpose of this invention, an instructive virus or worm is defined as a foreign unit of software introduced into a computer system so it sends certain computer data to otherwise unauthorized parties outside of the system.

Elements of the system described above are: a gateway router or bridge 16, a computer protection unit, and a management unit. A gateway router or bridge represents an element of collective defense for the network, while the source address filter and the "port router" and filter represent a unit of individual defense for a member computer. This individual defense unit (server unit) can be implemented either as a standalone computer, as a card in the protected computer, as software in the protected computer, or imbedded into the protected computer operating system. For further improvement of the overall security, port assignments can be generated autonomously from the management unit thus creating a "two keys" system in a cryptographic sense. This would allow for security to still be in place even if a security breach happened at the security management level.

The method and system of the present invention minimize human involvement in the system. The system can be configured in such a way that computer users deal only with simple identifiers or names permanently assigned to every computer in the network. All the real (current) cyber coordinates can be stored separately and be inaccessible to the user, and could be available to the appropriate computers only. This approach both enhances security and makes this security system transparent to the user. The user deals only with the simple alphabetic side of the "address book", and is not bothered with the inner workings of the security system. A telephone equivalent of this configuration is an electronic white pages residing in a computerized telephone set, which is automatically updated by the telephone company. The user just has to find a name, and push the "connect" button while the telephone set does the rest of the task.

A numeric cyber address system, based on the Internet host number could be relatively easily utilized for the discussed security purposes, however a limitation exists for this address system in its current form represented by the IPv.4 protocol. This limitation is posed by the fact that the address is represented by a 32-bit number. 32-bit format does not contain sufficient entropy in the address system to enable establishment of adequate security. This is a particularly serious limitation in regard to securing an entire network. The availability of the network numbers are limited to the extent that not only entropy, but a simple permanently assigned number is becoming more and more difficult to obtain with the rapid expansion of the Internet.

If this address system is to be used for the security purposes, than the format of the host number should be adequately expanded to create sufficient size of the address numbers field in the system. If this is done, than the corresponding address in the Domain Name System (DNS) could be conveniently used as permanent identifier for a particular computer and the Internet host number would be variable, creating a moving regime of a protected computer. Currently being implemented IPv.6 (IPNG) protocol solves this problem by providing sufficient entropy.

Another way to achieve the same goal is to use the DNS address as a variable for security purposes. This way, the traditional Internet DNS address system would not be affected and no change in format is required. The relevant part of the protected computer's DNS address would become a variable, utilizing more characters than the alphabet, with a very large number of variations, also creating sufficient level of entropy.

Yet another way to implement the same method is to utilize the geographic zone-based system. While its utilization is somewhat similar to the DNS system, it offers some practical advantages for security use. Naturally, when a computer is protected by a security system, it is still essential to preserve the communication redundancy of the Internet communications. However, the redundancy may suffer if only a limited number of the routers and gateways are informed of the protected computer current cyber address. This effect could be particularly important with the members of a particular protected network vastly remote in geographic terms. The necessary notification of a large number of the routers and gateways can also become problematic, not only technically, but also because it can decrease the level of security. In this sense a geographic zone-based system offers advantages since the variable part of the computer's cyber address could be made to involve only certain geographic locale while initial routing of the information packet could be done by the traditional method. After the packet has been moved to the general vicinity of the addressee computer, it would get into the area of the "informed" routers and gateways. This scheme would simplify the notification process of the routers as well as improve security by limiting the number of the "need to know" parties. It is important to recognize that, after the "general" part of the cyber address caused the information packet to arrive in a cyber vicinity of the addressee, virtually any, even private, address system can be used for the rest of he the delivery. This would further increase the level of underlying entropy in the system.

While certain specific address systems have been discussed, it is an important quality of the present invention that it can be implemented with virtually any address system.

Corporate and organizational computer networks such as LANs or, at least those in closed configurations, do not possess as much vulnerability to cyber attacks as Internet-based networks. However, even in these cases, their remote access security is a subject of concern. This is especially visible when a private network (PN) contains information of different levels of confidentiality with access restricted to appropriate parties. In other words, along with other generally accessible organizational information, an organizational PN can contain information restricted to certain limited groups. Enforcement of these restrictions requires a remote access security system. Usually these security systems employ a password-based scheme of one type or another and, perhaps, a firewall. However, reliance on passwords may not be entirely justified since the passwords can be lost or stolen, giving a malicious insider with a low access level a reasonable chance of access to information intended only for higher levels of access. Furthermore, in some cases use of cracking techniques from such a position is not entirely out of the question. Such an occurrence can relatively easily defeat both the password and the firewall. This would prevent a LAN from a cyber attack launched from within the network.

The present invention provides adequate security to such PCNs without reliance on the passwords and to limit access to only appropriate computers. Then, the task of overall information access security practically would be narrowed down to control of physical access to a particular computer, usually a less complicated feat.

Similarly to the systems described for Internet-based networks, a "closed" LAN as well as an Internet-based LAN can be protected by implementation of periodic changes of the members' network addresses and communicating those changes to the appropriate parties. This way, the lowest access level computers would have the lowest rate of address change. The rate of the address change would increase with the level of access. This system would ensure that all the PCN computers with legitimate access to a particular computer within the PCN would be informed of its location. Furthermore, it will ensure that the current location of a computer with restricted information would be unknown to the parties without the legitimate access clearance. For instance, a superior's computer would be able to access his subordinate's computer but not vice versa.

Also similarly to the systems described for the PCNs, a PCN computer would contain an "address book" where the user can see and use only the permanent side of it with identifiers of all computers accessible to him while the actual communication functions are performed by the computer using the variable side of the "address book" periodically updated by the PN management. To further enhance security, in addition to the computer address system management, the PCN Administrator can implement an automatic security monitoring system where all wrongly addressed log-on attempts would be registered and analyzed for security purposes.

Thus the method and system of the present invention would allow reliable protection against unauthorized remote access to information from within a PN while providing a great deal of flexibility, where the granted access can be revised easily and quickly.

A greatly enhanced intrusion protection system and method can be achieved by combining the operating systems of Figures 1-6. Now an arriving data packet would first be screened by a gateway router or a similar device for a correct destination address. If the destination address is correct, the packet is passed for further processing. If the destination address is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

The packet with correct destination address is then screened for a correct source address. If the source address is correct, the packet is passed to the receiver computer. If the source address is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

Then, the packet with a correct destination address and a correct source address is screened for a correct allowed port coordinate such as port number. If the port coordinate is correct, the packet is passed for further processing. If the port coordinate is incorrect, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

Finally, the packet with a correct destination and source addresses and a correct port designator is screened for data integrity by application of authentication check such as a checksum. If the authentication check is passed, the packet is passed to the addressee computer. If the authentication check is failed, the alarm is triggered and the packet is passed to the network security managing unit for security analysis.

The security managing unit analyses all the alarms and makes decisions on necessary unscheduled changes of addresses for appropriate network servers. Also, it can notify law enforcement and pass appropriate data on to it.

Figure 7 illustrates an enhanced computer intrusion protection system indicated generally at 52 for one or more network computers 54. A gateway router or a bridge 58 includes a destination address filter 60 which receives data packets which pass in through a load distribution switch 62. A non-interrogatable network address book 64 stores current network server addresses for the destination address filter 60, and the destination address filter checks each data packet to determine if a legitimate destination address is present.

Packets with legitimate destination addresses are forwarded to a source address filter 66, while packets with illegitimate destination addresses are sent to a security analysis section 68 in a management unit 70.

When a preset traffic load level is reached indicating that an attempt at flooding is being made, the destination address filter causes the load distribution switch 62 to distribute traffic to one or more parallel gateway routers or bridges which collectively forward legitimate traffic and dump the flooding traffic. An alternative arrangement would call for the load distribution function to be done irrespective of the load, utilizing all the parallel gateways all the time. A source address table 74 stores accessible server's designators and corresponding current addresses for all system servers which may legitimately have access to the computer or computers 54. These addresses are accessed by the source address filter which determines whether or not an incoming data packet with the proper destination address originates from a source with a legitimate source address entered in the source address table 74. If the source address is determined to be legitimate, the data packet is passed to a port address filter 76. Data packets with an illegitimate source address are directed to the security analysis section 68. Alternatively, source address screening can be done at the gateway router or bridge 58 first prior to port filter 76.

A port protection table 78 includes the current port assignments for the computer or computers 54, and these port assignments are accessed by the port designator filter 76 which then determines if an incoming data packet contains legitimate port designation. If it does, it is passed to an actual address translator 80 which forwards the data packet to the specific computer or computers 54 which are to receive thc packet. If an illegitimate port address is found by the port address filter 76, the data packet is transmitted to the security analysis section 68.

The management unit 70 is under the control of a security administrator 82. A network membership master file 84 stores a master list of legitimate server's designators along with respective authorized access lists and corresponding current cyber coordinates. The security administrator can update the master list by adding or removing authorized access for every protected computer. An access authorization unit 86 distributes the upgraded relevant portions of the master lists to the address books of the respective authorized servers.

A random character generator 88 generates random characters for use in forming current port designators, and provides these characters to a port designator forming block 90. This port designator forming block forms the next set of network current port designators in conjunction with the master list and these are incorporated for transmission by a port table block 92. Alternatively, port designators can be formed in the computer unit instead of the management unit.

Similarly, a random character generator 94 generates random characters for use in forming current server addresses, and provides these characters to a server address forming block 96. This server address forming block forms the next set of current network server addresses, and an address table 98 assigns addresses to servers designated on the master list.

A coordinator/dispatcher block 100 coordinates scheduled move of network servers to their next current addresses, provides the next set of network addresses for appropriate servers and routers and coordinates unscheduled changes of addresses on command from the security analysis unit 68. The coordinator/dispatcher block 100 may be connected to an encode/decode block 102 which decodes received address book upgrades from input 104 and encodes new port and server destination addresses to be sent to authorized servers in the system over output 106. Where encoding of new cyber coordinates is used, each authorized computer in the network will have a similar encoding/decoding unit.

The security analysis unit 68 analyses received illegitimate data packets and detects attack attempts. If needed, the security analysis unit orders the coordinator/dispatcher block 100 to provide an unscheduled address change and diverts the attack data packets to an investigation unit 108. This investigation unit simulates the target server keeping a dialog alive with the attacker to permit security personnel to engage and follow the progress of the attacker while tracing the origin of the attack.

Providing security against intrusion for e-commerce systems presents a unique problem, for an important peculiarity of an e-commerce system is that its address must be publicly known. This aspect represents a contradiction to the requirement of the address being known to authorized parties only.. However, the only information intended for the general public usually relates to a company catalog and similar material. The rest of the information on a merchant's network is usually considered private and thus should be protected. Using this distinction, a merchant's e-commerce site should be split into two parts: public and private. The public part is set up on a public "catalog" server with a fixed IP address and should contain only information intended for the general public. The rest of the corporate information should be placed in a separate network and protected as described in relation to Figures 1-7.

When a customer has completed shopping and made purchasing decisions concerning the terms and price of the sale, pertinent for the transaction, information is placed in a separate register. This register is periodically swept by a server handling financial transactions ("financial" server), which belongs to the protected corporate network. In fact, the "catalog" server does not know the current address of thc financial transactions server. Thus, even if an intruder penetrates the "catalog" server, the damage is limited to the contents of the catalog and the intruder cannot get an entry to the protected corporate network.

The financial server, having received pending transaction data, contacts the customer, offering a short-term temporary access for finalizing the transaction. In other words, the customer is allowed access just long enough to communicate pertinent financial data such as a credit card number and to receive a transaction confirmation at which point the session is terminated, the customer is diverted back to the catalog server and the financial server is moved to a new cyber address thus making obtained knowledge of its location during the transaction obsolete.

Dial-up communications systems, in respect to their infrastructure channels susceptibility to transmission intercept by unrelated parties, can be separated into two broad categories: easily interceptable, such as cellular and satellite telephone systems and relatively protected such as conventional land-line based telephone systems. Relatively protected systems such as conventional land-line based telephone systems can be protected in the following way. Phone numbers, assigned by a telephone company to a dial-up telephone-based private network serve as the members' computer addresses. As described previously, such a private network can be protected from unauthorized remote access by implementing periodic changes in the addresses, i.e. telephone numbers assigned to the members for transmission by the network along with other designators such as access codes and communicating the changed numbers to the appropriate parties.

For the conventional land-line dial-up telephone systems, while the "last mile" connection remains constant, the assigned telephone number is periodically changed, making the corresponding computer a moving target for a potential attacker. In this case the telephone company serves as the security system manager. It assigns the current variable telephone numbers to the members of a protected, private network, performs notification of all the appropriate parties, and changes the members' current numbers to a new set at an appropriate time. The telephone company switches naturally serve in the role of routers, and thus they can be programmed to perform surveillance of the system, to detect potential intrusion attacks and to issue appropriate alarms.

Periodically changing the current assigned numbers creates system entropy for a potential intruder, making unauthorized access difficult. Obviously, the implementation of this security system is dependent on availability of sufficient vacant numbers at a particular facility of the telephone company. Furthermore, for a variety of practical reasons it is advisable to keep a just vacated number unassigned for a certain period of time. All this may require additional number capacity at the telephone company facility in order to enable it to provide remote access security to a larger number of personal networks while preserving a comfortable level of system entropy.

If the mentioned additional capacity is not available, or a still higher level of entropy is desired, it could be artificially increased by adding an access code to the assigned number. This would amount to adding virtual capacity to the system, and would make a combination of the phone number and access code an equivalent of a computer's telephone address. In effect, this would make a dialed number larger than the conventional format. This method makes a virtual number capacity practically unlimited and, since the process is handled by computers without human involvement, it should not put any additional burden on a user. With or without a virtual number capacity, utilization of this method allows the intrusion attempts to be easily identified by their wrong number and/or code. At the same time, implementation of this system might require some changes in dialing protocols as well as additional capabilities of the telephone switching equipment.

Entropy density can be increased by limiting the number of allowable connection attempts. Similarly to the method described previously, telephone company switching equipment can be made to perform a role of an outside security barrier for the private network. In this case wrongly addressed connection attempts should be analyzed in order to detect possible "sweeping". If such an attempt is detected, tracing the origin of the attempt and notifying the appropriate phone company should not present a problem even with the existing technology.

The simplest form of private network protection under the proposed method and system is when at a predetermined time all the members of a particular network are switched to the new "telephone book" of the network. However, in some cases required level of security for some members of the same private network could substantially differ, or they may face different levels of security risk. In such cases frequency of the phone number change could be set individually with appropriate notification of the other members of the network. This differentiation enables the telephone company to offer differentiated levels of security protection to its customers even within the same private network.

A telephone company can also offer its customers protected voice private networks which would provide a higher level of privacy protection than the presently used "unlisted numbers." In this configuration the customers' telephone sets are equipped with a computerized dialing device with remotely upgradeable memory which would allow each member of a protected voice network to contain the network "telephone book" and that book is periodically updated by the telephone company.

The telephone company would periodically change the assigned telephone numbers of a protected network to a new set of current numbers. These new numbers would be communicated to the members of a protected voice network through updating their computerized dialing devices.

As a derivative of the described system, an updateable electronic telephone directory system can be also implemented. In this case a customer's phone set would include a computerized dialing device with electronic memory containing a conventional telephone directory and a personal directory as well. This telephone directory can be periodically updated on-line by the telephone company.

Easily interceptable systems such as cellular and satellite telephone systems, in addition to the protection described above, can be protected from "cloning" when their signals can be intercepted and the "identity" of the phone can be cloned for gaining unauthorized access and use of the system by unauthorized parties.

Mobile telephone and mobile communications systems are protected in a manner similar to networks or land based telephone systems. In this instance, the novel and improved method of changing cyber coordinates is designed to reliably protect mobile phone systems from unauthorized use commonly known as cloning as well as to make intercept of wireless communications more difficult than it is at present. With this system the static wireless phone number or other similar identifier is not used for identification and authorization. Instead, a set of private identifiers is generated known only to the phone company and base stations controlling mobile phone calls and used to continually update the mobile phone and base station directories with current valid identifiers. This approach provides vastly superior protection over current methods requiring that each call be intercepted in order to track and keep current with changing identifiers. Immediate detection of unauthorized attempts to use a cloned phone is realized and law enforcement may be notified in near real time for appropriate action.

Other electronic devices using wireless communications can be protected by the methods and systems described above.

Finally, computers often contain databases with a variety of information. That information in a database often has wide-ranging levels of sensitivity or commercial value. This creates a situation when large computers serve multiple users with vastly different levels of access. Furthermore, even within the same level of access, security considerations require compartmentalization of information when each user has to have access to only a small portion of the database.

The existing systems try to solve this situation by utilizing passwords and internal firewalls. As it was mentioned earlier, password-based systems and firewalls are not sufficient against computerized attacks. In practical terms it means that a legitimate user with a low level of access, utilizing hacking techniques from his station, potentially can break into even the most restricted areas of the database.

This problem can be solved by using the method of the present invention. A piece of information such as a file or a directory in a computer exists in cyber space. Accordingly, it has its cyber address, usually expressed as a directory and/or a file name which defines its position in a particular computer file system. This, in effect, represents the cyber coordinates of that piece of information within a computer.

As described earlier, information security can be provided if a system manager periodically changes the directories and/or file names in the system, i.e. the cyber addresses of the information, and notifies only appropriate parties of the current file names. This method would ensure that each user computer knows locations of only files to which it has legitimate access. Furthermore, a user would not even know of existence of the files to which he has no access.

To further strengthen the system and make it user-friendly, the user would have a personal directory similar to an address book, where only permanent directory and/or file names are accessible to him, while the variable side of the "address book" would be accessible only to the system manager and upgraded periodically. In this arrangement variable directory and/or file names can contain any required level of entropy, further increasing resistance to attacks from within the system. Additionally, an internal "router" or "filter" can also perform information security monitoring functions, detect intrusion attempts and issue appropriate alarms in real time.

Obviously, in order to ensure information security in such arrangement any computer-wide search by keywords or subject should be disabled and substituted with a search within specific clients' "address books".

The systems and methods described above allow for creation of a feasible infrastructure protection system such as a national or international infrastructure protection system. When detected at specific points cyber attacks are referred to such a system for further analysis and a possible action by law enforcement authorities.

I claim:

1. A method for protecting a communications device which is connected to a communications system against an unauthorized intrusion which includes:

providing the communications device with at least one identifier,

providing the at least one identifier for use in accessing the communications device to entities authorized to access said communications device,

sensing the presence or absence of said identifier before granting access to said communications device,

providing access to said communications device when the use of said at least one correct identifier is sensed

denying access to said communications device and providing said communications device with at least one new identifier when the absence of the correct at least one identifier is sensed during an attempt to access said communications device, and providing said at least one new identifier to entities authorized to access said communications device.

2. The method of claim 1 which includes periodically changing the at least one identifier and providing the changed at least one identifier to the entities authorized to access said communications device.

3. The method of claim 1 which includes providing said communications device with a plurality of separate identifiers,

sensing the presence or absence of all of said plurality of identifiers before granting access to said communications device,

providing access to said communications device when the use of all of said identifiers is sensed, and

denying access to said communications device and providing said communications device with a new plurality of identifiers to replace the previous plurality of identifiers when the absence of any one of the correct identifiers is sensed.

4. The method of claim 3 which includes periodically changing said plurality of

separate identifiers and providing the changed identifiers to the entities authorized to access said communications device.

5. The method of claim 1 which includes permitting a predetermined number of attempts to access said communications device with a correct at least one identifier after the absence of the correct at least one identifier is sensed before providing said communications device with at least one new identifier,

and providing access to said communications device if the correct at least one identifier is sensed during the predetermined number of attempts to access.

6. The method of claim 2 wherein said communications system is a telephone system and said communications device is a telephone.

7. The method of claim 1 wherein said communications system is a computer network with said entities authorized to access said communications device being authorized computers having access to said computer network, said communications device including at least one host computer having access to said computer network.

8. The method of claim 7 which includes periodically changing the at least one identifier for the host computer and providing the changed at least one identifier to the authorized computers.

9. The method of claim 7 which includes providing the authorized computers with an unchangeable, accessible address for the host computer which is used by the authorized computer to activate and transmit the at least one identifier for the host computer when the authorized computer initiates access to the host computer.

10. The method of claim 8 which includes providing each authorized computer with an authorized computer identifier,

providing the host computer with a destination identifier,

causing each authorized computer to access said host computer with at least a host computer destination identifier and the authorized computer identifier,

sensing the presence or absence of both said host computer destination identifier and an authorized computer identifier before granting access to said host computer,

providing access to said host computer when the use of both a correct host computer destination identifier and an authorized computer identifier is sensed, and

denying access to said host computer and providing said host computer with a new host computer destination identifier when the absence of either a correct host computer destination identifier or a correct authorized computer identifier is sensed.

11. The method of claim 10 which includes permitting a predetermined number of attempts to access said host computer with both a correct host computer destination identifier and an authorized computer identifier after the absence of a correct host computer destination identifier or an authorized computer identifier is sensed before providing said host computer with a new host computer destination identifier, and

providing access to said host computer if correct host computer destination and authorized computer identifier are sensed during the predetermined number of attempts to access the host computer.

12. The method of claim 11 which includes storing said host computer destination identifier as an inaccessible identifier in said authorized computers, and providing said authorized computers with an unchangeable, accessible host computer address, which will activate and transmit the host computer destination identifier when an authorized computer initiates access to the host computer.

13. The method of claim 8 which includes providing said host computer with a host computer destination identifier and a host computer port identifier,

causing each authorized computer to access said host computer with at least the host computer destination identifier and the host computer port identifier,

sensing the presence or absence of both said host computer destination identifier and said host computer port identifier before granting access to said host computer,

providing access to said host computer when the use of both a correct host computer destination identifier and a correct host computer port identifier are sensed, and

denying access to said host computer and providing said host computer with a new destination identifier and port identifier when the absence of either or both of a correct host computer destination or port identifier is sensed.

14. The method of claim 13 which includes permitting a predetermined number of attempts to access said host computer with both a correct host computer destination and port identifier when either or both an incorrect host computer destination or port identifier is sensed before providing said host computer with a new destination and port identifier, and

providing access to said host computer if both correct host computer destination and port identifiers are sensed during the predetermined number of attempts to access said host computer.

15. The method of claim 14 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computers and providing said authorized computers with an unchangeable, accessible host computer address which will activate and transmit the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

16. An intrusion protection method for protecting a host computer connected to a computer communications system which includes one or more authorized computers having access to said computer communications system which are authorized to access said host computer which includes:

providing each authorized computer with an authorized computer identifying address,

providing said host computer with a host computer destination identifier and a host computer port identifier,

providing said host computer destination identifier and said host computer port identifier to said authorized computers,

causing each authorized computer to access said host computer with the host computer destination and port identifiers and said authorized computer identifying address,

sensing the presence or absence of said host computer destination and port identifiers and said authorized computer identifying address before granting access to said host computer,

providing access to said host computer when the use of correct computer destination and port identifiers and a correct authorized computer identifying address is sensed, and

denying immediate access to said host computer when the absence of any one or more of the correct host computer destination and port identifiers or the authorized computer identifying address is sensed.

17. The method of claim 16 which includes periodically changing the host computer destination and port identifiers and providing these changes to the authorized computers.

18. The method of claim 17 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computer and providing said authorized computers with an unchangeable, accessible host computer address which will activate and transmit the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

19. The method of claim 16 which includes changing the host computer destination and port identifiers when access is denied to said host computer after at least one access attempt has been made and providing these changed identifiers to the authorized computers.

20. The method of claim 16 which includes permitting a predetermined number of attempts to access said host computer with correct host computer destination and port identifiers and a correct authorized computer identifying address after the absence of at least a correct one of said identifiers and authorized computer identifying address is sensed by the host computer and

providing access to said host computer if correct host computer destination and port identifiers and a correct authorized computer identifying address are sensed during the predetermined number of attempts to access said host computer.

21. The method of claim 19 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computer and providing said authorized computers with an unchangeable, accessible host computer address which will activate and cause transmission of the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

22. The method of claim 20 which includes changing the host computer destination and port identifiers when access is denied to said host computer after at least one access attempt has been made and providing these changed identifiers to the authorized computers.

23. The method of claim 22 which includes storing said host computer destination and port identifiers as inaccessible identifiers in said authorized computer and providing said authorized computers with an unchangeable, accessible host computer address which will activate and cause transmission of the host computer destination and port identifiers when an authorized computer initiates access to said host computer.

24. A method of communication with a remote entity over a communication system which includes

providing the remote entity with at least one remote entity cyber coordinate identifier,

providing the remote entity cyber coordinate identifier to one or more base entities authorized to communicate with said remote entity,

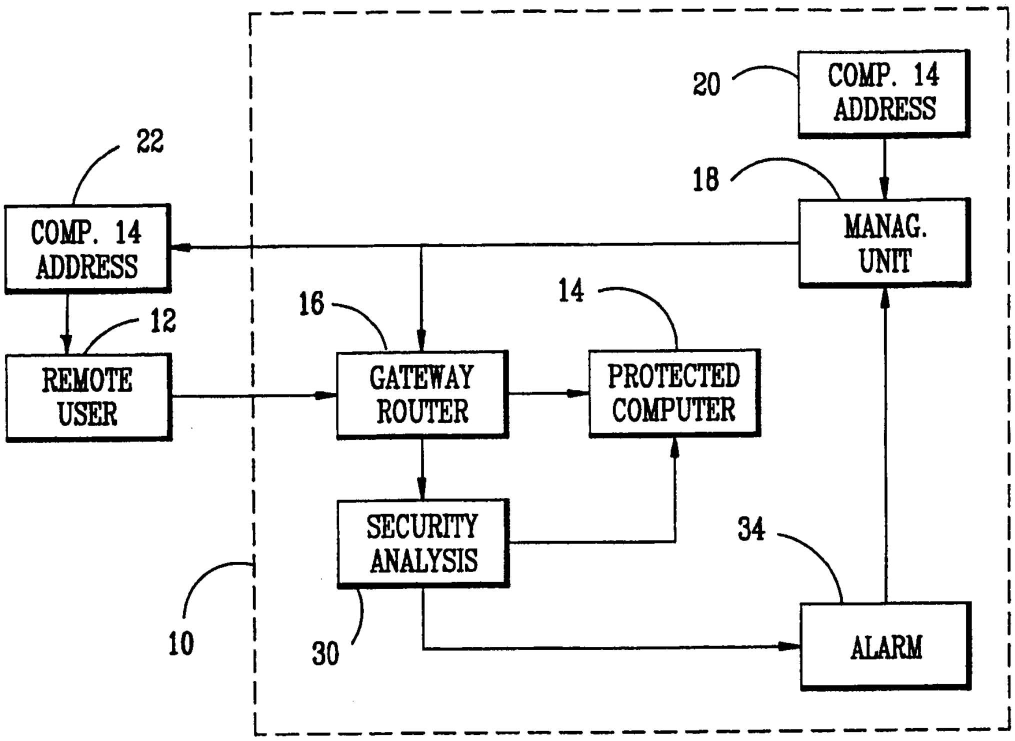
periodically changing the remote entity cyber coordinate identifier to a new remote entity cyber coordinate identifier and

providing the new remote entity cyber coordinate identifier to said one or more base entities.

25. The method of claim 24 which includes changing the remote entity cyber coordinate identifier to a new cyber coordinate identifier in response to an attempt to communicate with said remote entity with an incorrect remote entity cyber coordinate identifier and

providing the new remote entity cyber coordinate identifier to said one or more base entities.

FIG. 1


COMP. 14 ADDRESS
20
22
18
COMP. 14 ADDRESS
MANAG. UNIT
12
16
14
REMOTE USER
GATEWAY ROUTER
PROTECTED COMPUTER
SECURITY ANALYSIS
34
10
30
ALARM

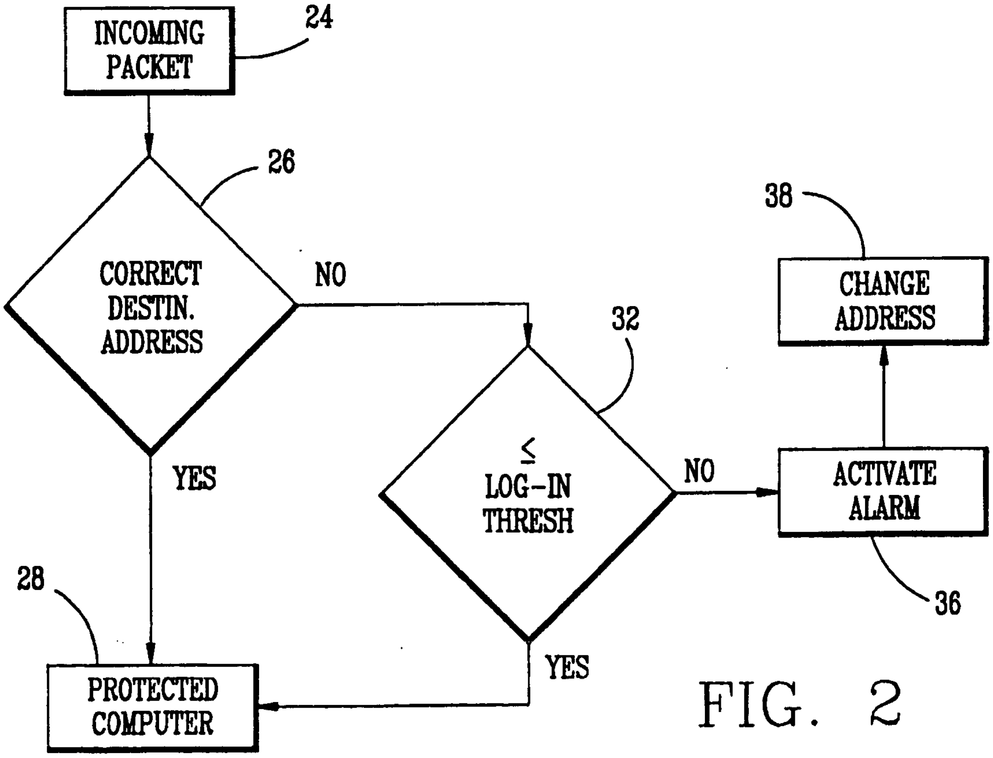

INCOMING PACKET
24
26
CORRECT DESTIN. ADDRESS
NO
38
CHANGE ADDRESS
32
≤ LOG-IN THRESH
NO
ACTIVATE ALARM
YES
36
28
YES
PROTECTED COMPUTER

FIG. 2

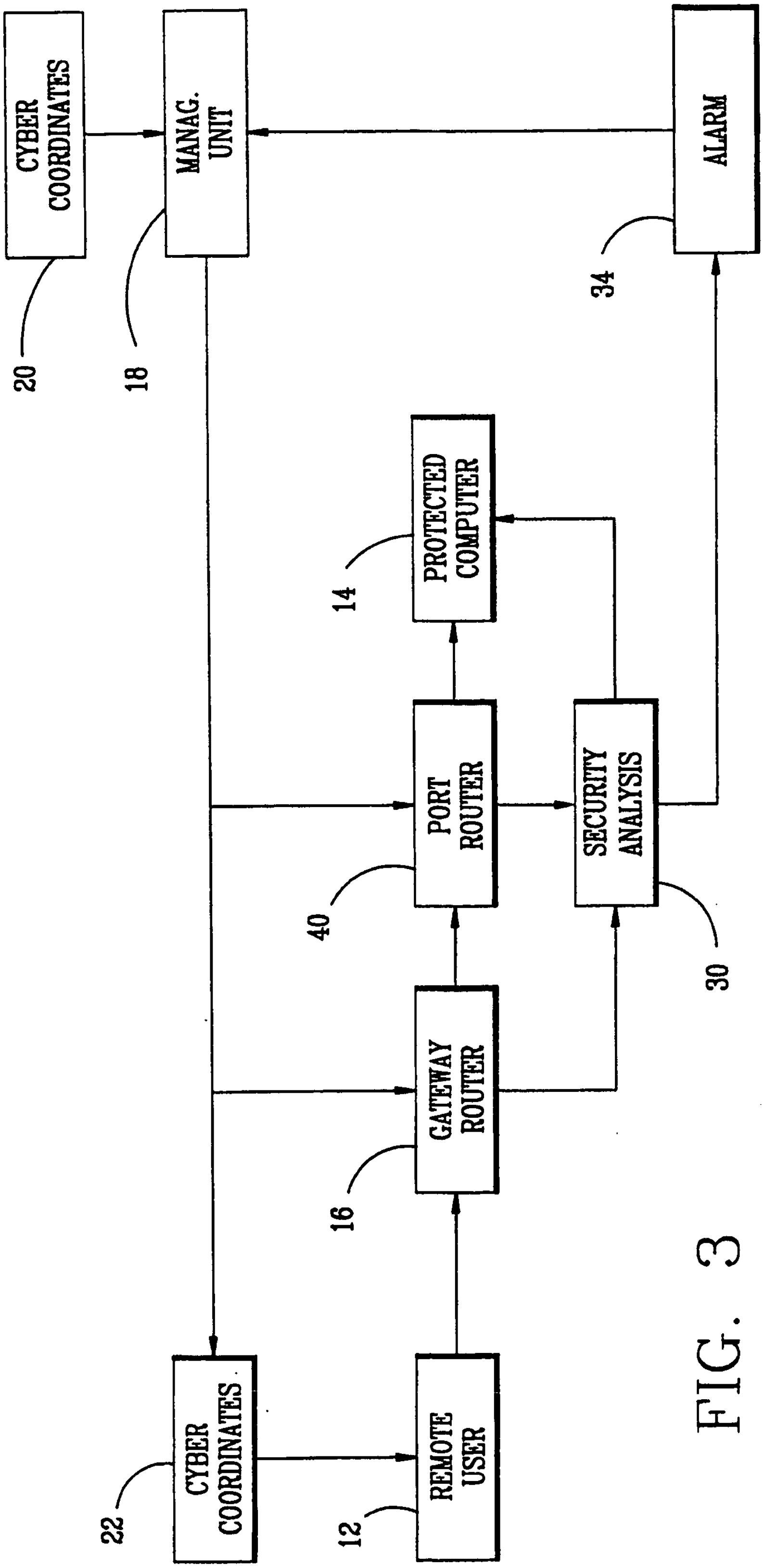

CYBER COORDINATES
20
MANAG. UNIT
18
ALARM
34
PROTECTED COMPUTER
14
PORT ROUTER
40
SECURITY ANALYSIS
30
GATEWAY ROUTER
16
CYBER COORDINATES
22
REMOTE USER
12

FIG. 3

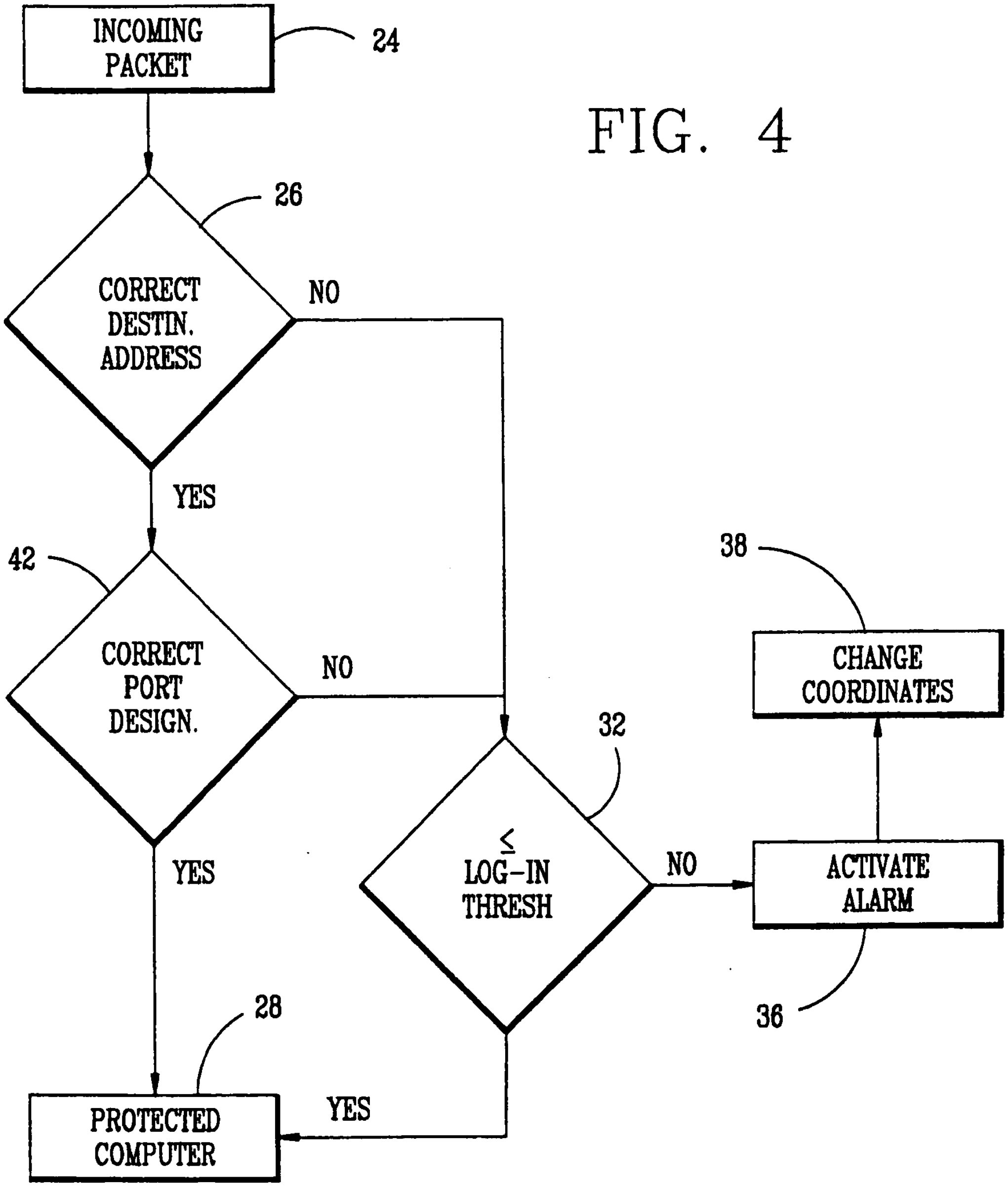

INCOMING PACKET
24
26
CORRECT DESTIN. ADDRESS
NO
YES
42
CORRECT PORT DESIGN.
NO
YES
32
≤ LOG-IN THRESH
NO
YES
ACTIVATE ALARM
36
CHANGE COORDINATES
38
28
PROTECTED COMPUTER

FIG. 4

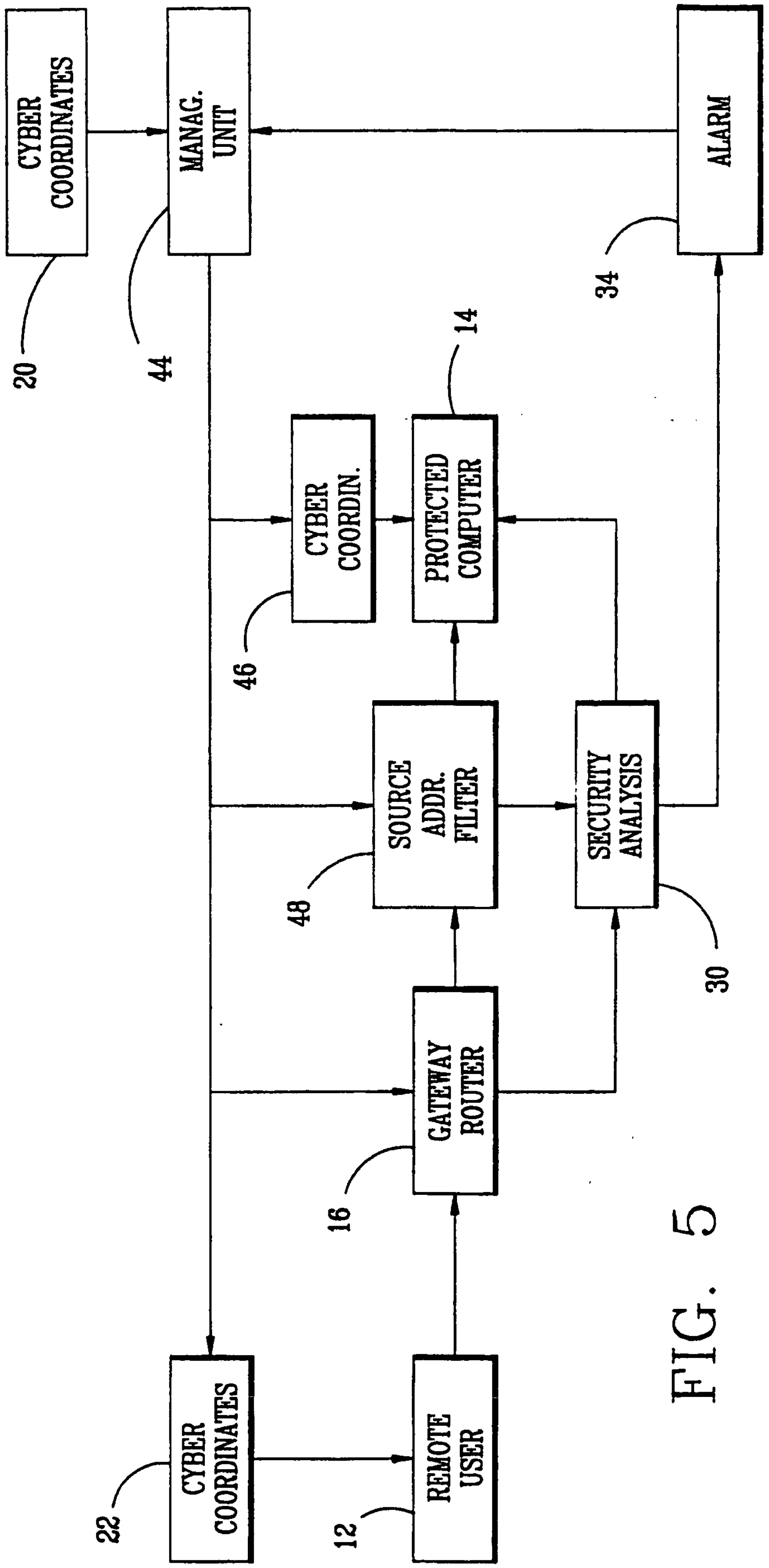

CYBER COORDINATES
MANAG. UNIT
ALARM
20
44
34
14
CYBER COORDIN.
PROTECTED COMPUTER
46
SOURCE ADDR. FILTER
SECURITY ANALYSIS
48
30
GATEWAY ROUTER
16
CYBER COORDINATES
REMOTE USER
22
12

FIG. 5

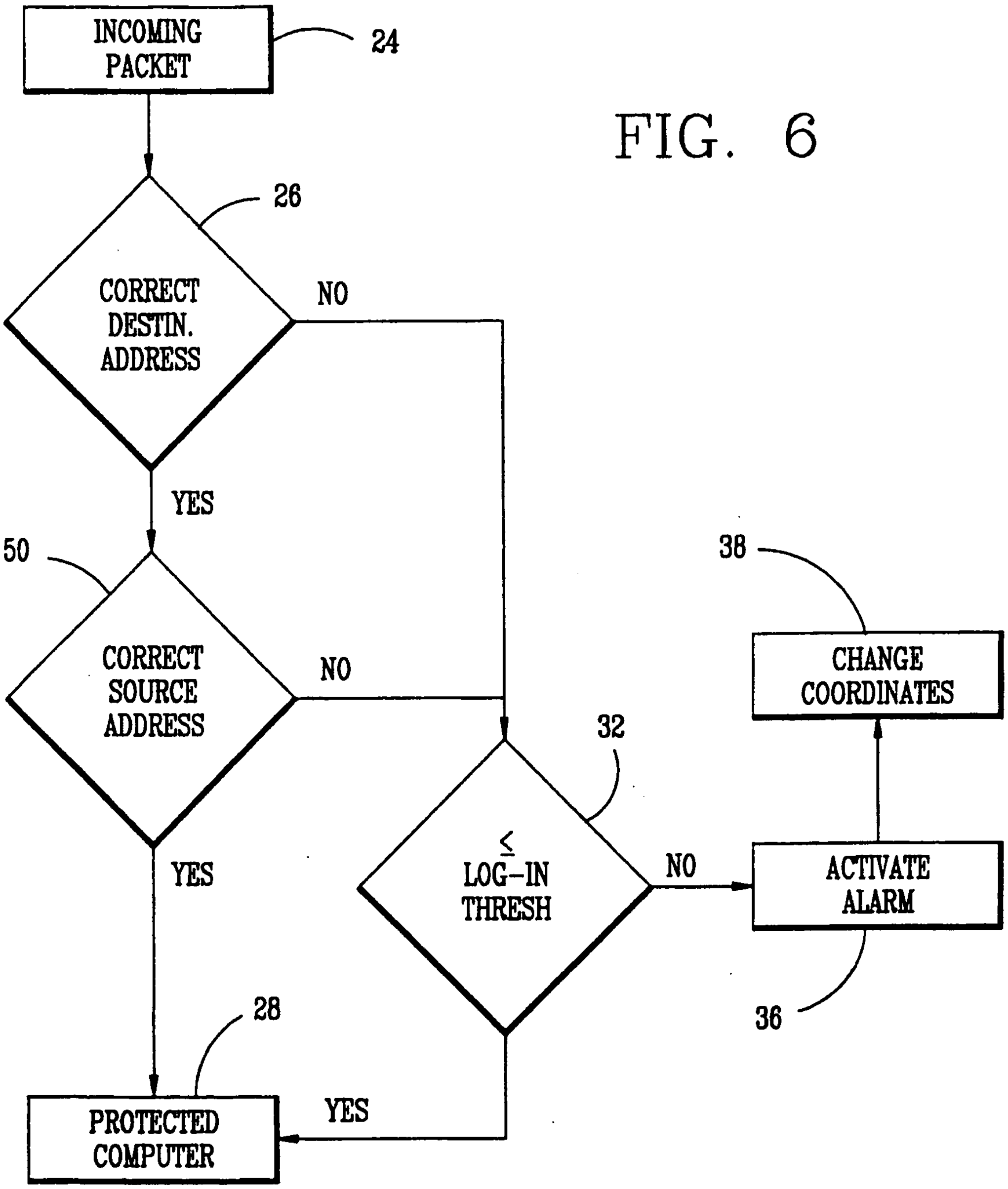
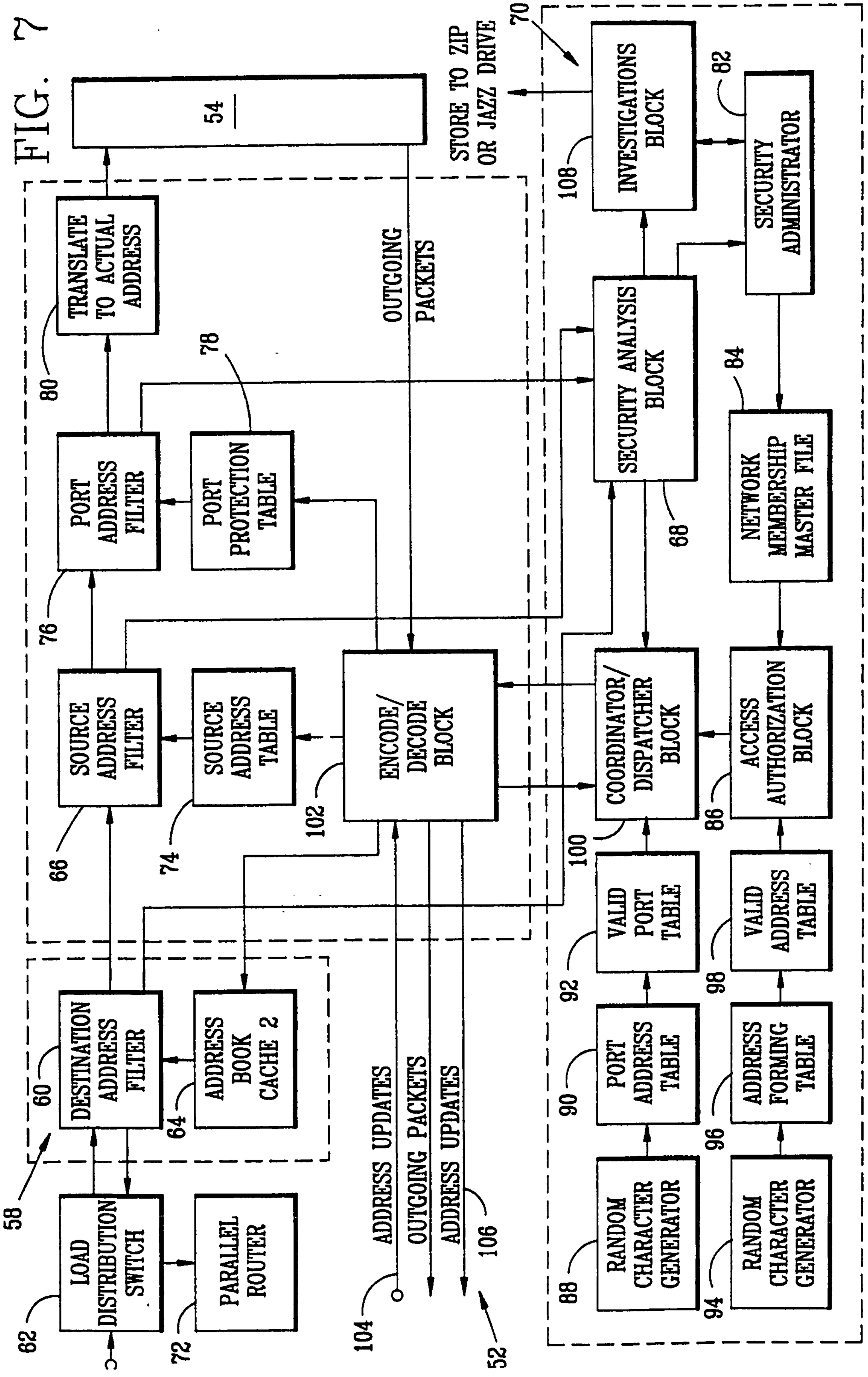

INCOMING PACKET
24
26
CORRECT DESTIN. ADDRESS
NO
YES
50
CORRECT SOURCE ADDRESS
NO
YES
32
≤ LOG-IN THRESH
NO
YES
38
CHANGE COORDINATES
ACTIVATE ALARM
36
28
PROTECTED COMPUTER

FIG. 6

FIG. 7


54
TRANSLATE TO ACTUAL ADDRESS
80
PORT ADDRESS FILTER
76
PORT PROTECTION TABLE
78
SOURCE ADDRESS FILTER
66
SOURCE ADDRESS TABLE
74
ENCODE/ DECODE BLOCK
102
OUTGOING PACKETS
DESTINATION ADDRESS FILTER
60
ADDRESS BOOK CACHE 2
64
58
LOAD DISTRIBUTION SWITCH
62
PARALLEL ROUTER
72
ADDRESS UPDATES
OUTGOING PACKETS
ADDRESS UPDATES
104
106
52
STORE TO ZIP OR JAZZ DRIVE
70
INVESTIGATIONS BLOCK
108
SECURITY ADMINISTRATOR
82
SECURITY ANALYSIS BLOCK
68
NETWORK MEMBERSHIP MASTER FILE
84
COORDINATOR/ DISPATCHER BLOCK
100
ACCESS AUTHORIZATION BLOCK
86
VALID PORT TABLE
92
VALID ADDRESS TABLE
98
PORT ADDRESS TABLE
90
ADDRESS FORMING TABLE
96
RANDOM CHARACTER GENERATOR
88
RANDOM CHARACTER GENERATOR
94

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/08219

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 11/00
US CL : 713/201
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)

U.S. : 713/201,200,202; 340/825.31,825.34; 380/255;

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS US PATENT FILE; WEST; JPAB; EPAB; DWPI; TDBD;

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,805,801 A (HOLLOWAY ET AL) 08 SEPTEMBER 1998, Entire document.	1-25
Y	US 5,796,942 A (ESBENSEN) 18 AUGUST 1998, Entire document.	1-25
Y,P	US 5,905,859 A (HOLLOWAY ET AL) 18 MAY 1999, Entire document.	1-25
Y	US 5,892,903 A (KLAUS) 06 APRIL 1999, Entire document.	1-25
A	US 5,537,099 A (LIANG) 16 JULY 1996, Entire document.	1-25
A	US 5,278,901 A (SHIEH ET AL) 11 JANUARY 1994, Entire document.	1-25

☒ Further documents are listed in the continuation of Box C. ☐ 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 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

"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

"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 20 JULY 2000	Date of mailing of the international search report 22 AUG 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Eugenia Logan NADEEM IQBAL Telephone No. (703) 308-5228

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/08219

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 5,991,881 A (CONKLIN ET AL) 23 NOVEMBER 1999, Entire document.	1-25

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

B1002

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 March 2001 (08.03.2001)

PCT

(10) International Publication Number
WO 01/016766 A1

(51) International Patent Classification⁷: G06F 13/00

(21) International Application Number: PCT/US00/23774

(22) International Filing Date: 31 August 2000 (31.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/151,563 31 August 1999 (31.08.1999) US

(71) Applicant: SCIENCE APPLICATIONS INTERNATIONAL CORPORATION [US/US]; 10260 Campus Point Drive, San Diego, CA 92121 (US).

(72) Inventors: WHITTLE, Bryan; 73 Zion-Wertsville Road, Skillman, NJ 08558 (US). TESINK, Kaj; 140 Park Road, Fair Haven, NJ 07704 (US).

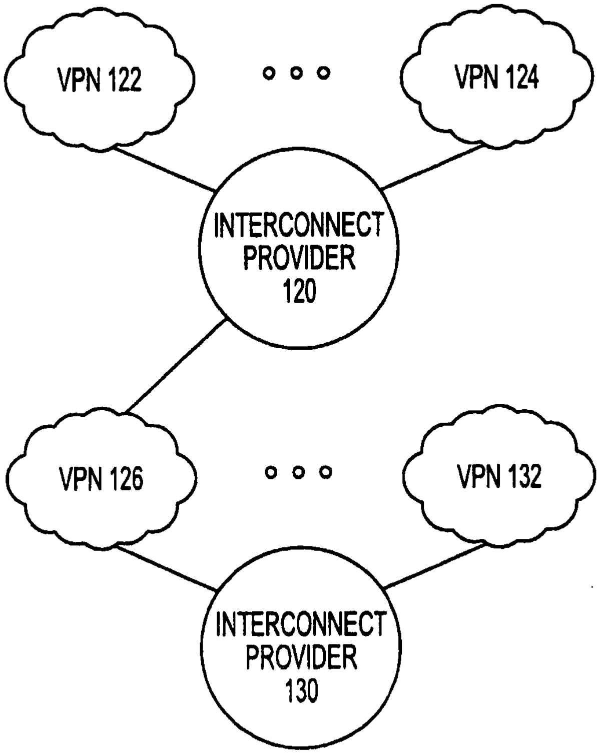
(74) Agents: ROBINSON, Douglas, W. et al.; Banner & Witcoff, Ltd., Eleventh Floor, 1001 G Street, N.W., Washington, D.C 20001-4597 (US).

(81) Designated States *(national)*: 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.

(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 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).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR INTERCONNECTING MULTIPLE VIRTUAL PRIVATE NETWORKS



(57) Abstract: A system and method for interconnecting multiple VPNs (122, 124, 126, 132), each using multiple service providers (120, 130), while offering a minimum standard of end-to-end connection quality and reliability. The system and method utilizes an overseer that resolves end-to-end issues across multiple interconnected virtual private networks (122, 124, 126, 132). When connecting multiple virtual private networks (122, 124, 126, 132) multiple interconnect providers (120, 130) are interconnected so that the end-to-end service quality standard. The certification of service providers, exchange points, transit service providers and IPSec devices permits interoperability for encryption, integrity and authentication across the product of all IPSec vendors. When two subscribers both use certified IPSec equipment then they can provide each other with controlled access to each other's networks.

WO 01/016766 A1

Published:

— *with international search report*

(48) Date of publication of this corrected version:
12 September 2002

(15) Information about Correction:
see PCT Gazette No. 37/2002 of 12 September 2002, Section II

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.

SYSTEM AND METHOD FOR INTERCONNECTING MULTIPLE VIRTUAL PRIVATE NETWORKS

This application claims priority to the following provisional patent applications, which are incorporated herein by reference in their entireties:

(1) Provisional Application Serial No. 60/151,563, titled "Method & Apparatus For a Globalized Automotive Network & Exchange," filed on August 31, 1999, and having reference no. 99,532 (479.83581).

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to virtual private networks. More particularly, the present invention relates to virtual private networks wherein in each virtual private network, multiple service providers can be utilized by the trading partners of the virtual private network. The end-to-end service quality of the connection within the virtual private network is guaranteed to meet minimum requirements. The end-to-end service quality encompasses numerous factors including: network services; interoperability; performance; reliability; disaster recovery and business continuity; security; customer care; and trouble handling. The system and method of the present invention is directed to the interconnection of multiple virtual private networks each having multiple service providers. Furthermore the present invention encompasses a system and method for interconnecting multiple interconnect providers, such as exchange points, exchange networks, direct connect or transit service providers, between the multiple virtual private networks. Finally, the present invention employs an end-to-end overseer across the multiple virtual private networks.

Description of the Related Art

Early in 1994, the automotive industry recognized the need for global network services that would support more new demanding automotive business applications. The purpose of this network service was to simplify complex, redundant, outdated connection methods while minimizing costs and ensuring the management, security, reliability, and performance essential to the automotive industry. Transport Control Protocol/Internet Protocol (TCP/IP) was endorsed as the standard suite for electronic data communications.

Ultimately in 1995, the industry formed a Telecommunications Project Team to oversee the design and development of a common global communication infrastructure supporting automotive industry application initiatives (later called the Automotive Network eXchange (ANX) Implementation Task Force). The Task Force, in June 1997, published the initial results of the technical design process for this new network service, called the Automotive Network eXchange (ANX), in "ANX Release 1 Draft Document Publication" (TEL-2 01.00). This reference is incorporated herein by reference in its entirety. The TEL-2 specification undergoes constant updating and correction.

The ANX system is a business-to-business communications infrastructure that provides a uniform, secured link between trading partners, such as manufacturers and suppliers, in the automotive industry. The ANX is a subscription-based network composed of Certified Service Providers (CSP). CSPs are providers of IP network service that have satisfied certain service end-to-end quality. CASPs are certificate authority service providers. The Certified Exchange Point Operator (CEPO) provides services to interconnect CSPs. CEPOs also must satisfy certain end-to-end service quality requirements.

Trading Partners (TP) are registered end users, or subscribers, of the ANX system such as automotive parts manufacturers, suppliers, original equipment manufacturers, and car manufacturers. The ANX system allows TPs to communicate, exchange information, and transact business with other TPs over the ANX network. The TP may utilize any TCP/IP-compliant application program to exchange information with other TPs. The registered TP selects the TPs with which it wants to communicate and thereafter may gain access to and receive communications from those selected TPs. As a result, the ANX system allows each TP to develop its own virtual private network with its customers and vendors.

The ANX system significantly reduces the complexity of connecting to multiple trading partners. Since there are diverse communication protocols for the trading partners, separate links are required to access each trading partner.

By having a single private network operated under a uniform protocol, interconnectivity between various trading partners is substantially simplified. In addition, ANX offers improved end-to-end service quality. For example, if an auto manufacturer needs to place with its parts supplier an order for car seats, the manufacturer may submit over the ANX system its confidential CAD drawings directly to the supplier. The manufacturer may also fill out the order form that the supplier may have for filling orders and timely submit over the ANX system due to its high reliability and performance.

The CSP and the CEPO must satisfy certain performance and security requirements in order to be certified under the ANX. The certification process is disclosed in ANX Release 1 Document Publication (TEL-2 02.00), which is incorporated herein by reference in its entirety.

The ANX VPN permits the use of a plurality of different IPSec devices. By virtue of the TEL-2 specification and the certification process all of the designated IPSec device are guaranteed to communicate with one another across the ANX VPN.

While the ANX was originated out of the need to interconnect automotive related companies, it is not limited to that industry. Any company/industry may become a TP, e.g. an aerospace company, a healthcare company, etc. ANX has become known as the Advanced Network eXchange.

With the advent of the Internet, global communication has become a reality. While the Internet works well for non-mission critical applications, such as transmitting and receiving e-mail and hosting websites, it has some drawbacks for business-to-business commerce and communication that require stringent end-to–end service quality. Quality concerns are in the area of end-to-end service quality as explained previously.

For example, when two companies want to communicate over the Internet, the lag between the systems at each company will be different virtually every time. The connection each has through their service provider, i.e. 14.4K, 28.8K, 56K, ISDN, DSL, T1, etc., plus the number of servers through which the connection is directed contribute to the resulting time lag between the two companies. Depending upon the type of information transmitted, the two parties may require a maximum acceptable time lag. Due to the nature of the Internet, it cannot guarantee such a maximum time lag. Furthermore, the two companies may desire that service assistance be available at certain times or 24 hours a day. The Internet has no such guarantees for help availability in a multi-provider environment. Such a lack of guaranteed bandwidth, latency and reliability are major impediments to business-to-business commerce and communication over the Internet.

In recent years the number of electronic viruses and hacker attacks has increased dramatically. A company considering conducting business-to-business commerce over the Internet runs the risk of making their intranet vulnerable to such viruses and attacks with the potential related loss of data.

In order to address the security issue, some companies have developed virtual private networks (VPNs). Secure VPNs permit a company to communicate with any other entity on the network without the risk of increased vulnerability to viruses and hackers. However, while VPNs can connect to other VPNs over the Internet by providing authentication, access control, confidentiality and data integrity, there is still no way the end-to-end quality of the connection can be guaranteed to meet a required set of minimum standards in a multi-provider setting.

A secure VPN is a communication network that is secured with encryption and authentication. Secure VPNs are based on multiple technologies, for example IPSec, tunneling, certification and shared secret authentication. IPSec is the security standard established by the Internet Engineering task Force (IETF). Tunneling permits private networks to cross the Internet using unregistered IP addresses.

SUMMARY OF THE INVENTION

From the foregoing, it is desirable to provide a system and method for interconnecting multiple VPNs each using multiple service providers while offering a minimum standard of end-to-end service quality.

The system and method of the present invention utilizes an overseer that defines the service quality, continually qualifies service providers as meeting that service quality, and resolves end-to-end issues across multiple interconnected virtual private networks, such as the ANX. When connecting multiple virtual private networks according to the system and method of the present invention multiple interconnect providers are interconnected, and the manner in which these interconnect providers are interconnected so that the quality and reliability standards is met are another aspect of the present invention.

Certification of IPSec devices permits interoperability for encryption, integrity and authentication across the product of all IPSec vendors. When two subscriber companies both use certified IPSec equipment then they can provide each other with controlled access to each other's networks.

Based on the foregoing, an object of the present invention is to provide a system and method of interconnecting multiple VPNs each using multiple service providers while offering a minimum standard of end-to-end connection quality and reliability.

Another object of the present invention is to provide a system and method of interconnecting multiple VPNs having an overseer that resolves end-to-end issues across multiple virtual private networks.

Still another object of the present invention is to provide a system and method of connecting multiple virtual private networks in which multiple interconnect providers are interconnected so that the end-to-end service quality is met.

DETAILED DESCRIPTION OF THE DRAWINGS

The foregoing and other attributes of the present invention will be described with respect to the following drawings in which:

Fig. 1 is a block diagram of two interconnected virtual private networks according to the present invention;

Fig. 2 is a configuration of governance and management of separate virtual private networks;

Fig. 3 is a configuration of governance and management of interconnected virtual private networks according to the present invention;

Fig. 4 is an interconnection configuration for governance of multiple interconnected virtual private networks according to the present invention;

Fig. 5 is a flow chart showing contractual obligations according to the present invention;

Fig. 6 is a diagram illustrating end-to-end latency in a virtual private network having multiple service providers;

Fig. 7 is a diagram illustrating end-to-end availability in a virtual private network having multiple service providers;

Fig. 8 is a diagram illustrating trouble handling in a virtual private network having multiple service providers;

Fig. 9 is a diagram illustrating an accountability model for a single virtual private network having multiple service providers;

Fig. 10 is a diagram illustrating an accountability model for multiple virtual private networks having multiple service providers according to the present invention;

Fig. 11 is a diagram illustrating end-to-end interconnection of two virtual private networks according to the present invention;

Fig. 12 is a diagram illustrating a trouble escalation model for interconnection of two virtual private networks according to the present invention;

Fig. 13 is a diagram illustrating a multiple virtual private network fee model for interconnection of two virtual private networks according to the present invention; is a diagram illustrating interconnection of two virtual private networks using a multiple transit certified service providers according to the present invention;

Fig. 14 is a diagram illustrating interconnection of two virtual private networks using a single transit certified service provider according to the present invention;

Fig. 15 is a diagram illustrating interconnection of two virtual private networks using a multiple transit certified service providers according to the present invention;

Figs. 16 is a diagram illustrating interconnection of multiple virtual private networks using a multiple transit certified service providers, where no single transit certified service provider connects all of the virtual private networks according to the present invention; and

Figs. 17a - c are alternative configurations for interconnecting multiple virtual private networks according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 1 shows a block diagram of two interconnected virtual private networks 20 and 22. The present system and method of the interconnecting multiple virtual private networks is not intended to be limited to only these types of networks and has applicability to a wide variety of virtual private networks.

Each virtual private network 20 and 22 is shown having a trading partner (TP) 24 and 26, respectively. While Fig. 1 shows only one TP 24 and 26 for each virtual private network, there can in fact be hundred or thousands of such TPs for each virtual private network. Fig. 1 is intended to define the end-to-end service quality concept, and for such a purpose, only one TP 24 and 26 is need for each virtual private network 20 and 22.

The end-to-end service quality, provided by the present system and method of interconnecting multiple virtual private networks, cannot be achieved by simply interconnecting two virtual private networks, such as 20 and 22, with a wire. The end-to-end service quality incorporates a user-centric philosophy, where the user is the TP or subscriber. The user is guaranteed a minimum level of service encompassing factors that include: network services; interoperability; performance; reliability; disaster recovery and business continuity; security; customer care; and trouble handling. Simply connecting the two virtual private networks 20 and 22 with a wire will not achieve the minimum satisfactory levels for these factors.

To achieve such minimum levels of satisfactory performance for these factors the system and method must include a way to resolve disputes between the two virtual private networks. Referring to Fig. 2, each VPN 20 and 22 is shown as having its own governance, program management, coopetition policy, contracts, service assurance, and service description. While each virtual private network can operate with a successful level of end-to-end service quality when each VPN is not interconnected to another VPN, the governance, program management, coopetition policy, contracts, service assurance, and service description may need to be revised when interconnecting two or more VPNs in order to maintain the end-to-end service quality. It will be appreciated that at the very least the interconnection of at least two VPNs adds at least one additional level of complexity with regard to service between the VPNs.

One resolution is shown in Fig. 3, in which each VPN 20 and 22 maintain their own governance, but the program management, coopetition policy, contracts, service assurance, and service description for the two VPNs 20 and 22 are unified. Such unification means that where the parameters for the program management, coopetition policy, contracts, service assurance, and service description of the two VPNs 20 and 22 are different, the parameter used in one of the networks is chosen as the acceptable minimum standard or a compromise parameter different from the parameter used in each or the VPNs is agreed upon. It is possible that the parameters for communication within each VPN need not change, while the new parameters are used only when communicating between VPNs. Fig. 3 further shows that the system and method contemplate connecting more than two VPNs.

One configuration for governance of multiple interconnected VPNs is shown in Fig. 4. In this scenario each VPN has its own program overseer (POVER) 30, and a global, or multiple virtual private network, overseer 32 is provided to resolve issues between the POVERs 30. Arrows are shown between the POVERs 30 indicating that the POVERs 30 are free to resolve their issues without requiring the GOVER 32. The GOVER is called on when direct POVER-to-POVER resolution fails. Each of the POVERs 30 governs one of the regional VPNs, while the GOVER 32 oversees the interconnection of the VPNs.

The GOVER is responsible for end-to-end quality assurance, and in particular acts as an inter-VPN interconnection certifier. The GOVER certifies interconnection facilities, and certifies a global CASP-CASP trust model. The GOVER also is an inter-VPN arbitrator that steps in when POVERs cannot resolve trouble between them.

Since the VPNs are used to running their networks in isolation, the interconnection of multiple VPNs has unique issues such as resolving trouble and conflicts between the VPNs and maintenance of minimum end-to-end service quality across the multiple programs. Since the system and method of the present invention are directed to providing specific end-to-end service quality, it must be possible for TPs to quantify the end-to-end service quality levels, and these service quality levels must be sufficient to allow applications to work across the multiple VPNs. Therefore, a high level of metric compatibility and measurement techniques are required.

In the ANX type VPN each TP, CSP and CEP must meet specified criteria to become certified and to maintain that certification. The certification provides the TPs or subscribers with confidence that the level or transport and security will meet their business needs. The ANX type VPN utilizes multiple CSPs. On one level it is easier to run a VPN where all TPs are required to use a single CSP. The use of multiple CSPs in the ANX type VPN fosters competition between the CSPs and allows the VPN to reach TPs that may not be serviced by a single CSP. The implementation of multiple CSPs, however, brings with it the drawback of insuring that the CSPs can talk to one another. Whether the connection from one TP to another TP within the same VPN is through a single CSP of two CSPs should be invisible to the TPs. The TPs need never know when one or more CSPs are used for any particular connection. The certification process ensures that the TPs use one of the certified IPSec devices at their premises, and that the CSPs will utilize certified equipment and meet certain metrics so as to achieve the end-to-end service quality guaranteed to the TPs. In this manner, the multiple CSPs will be able to communicate with one another. The CSPs must meet business criteria, technical metrics, ongoing monitoring, trouble-handling criteria, routing registry criteria, and domain name registry criteria to achieve and maintain certification.

Fig. 5 shows the contractual obligations of the members of an ANX-type VPN. The TPs 40 contract with the VPN, as denoted in Fig. 5 by the arrows to the overseer 50, and contract with one of the multiple CSPs 42. The CSPs contract with the VPN and with the CEPO 44. The CEPO 44 contracts with the VPN. Each entity is responsible for the services that that entity provides.

The technical metrics for achieving end-to-end service quality in the ANX-type network include among other metrics, latency and availability. Fig. 6 illustrates the end-to-end latency within the ANX network. The TP1 router 60 is connected to ANX CSP_1 62, which in turn is connected to ANX CEPO 64. TP2 router 66 is connected to ANX CSP_2 68, which is connected to ANX CEPO 64. The packet latency from each router 60 and 66 through the corresponding CSP is 125 msec. The latency through the ANX CEPO is on the order of microseconds. The total packet latency through the network is therefore only slightly more than 250 msec.

Fig. 7 illustrates the end-to-end availability metric. The Access network between the TP1 router 60 and the ANX CSP_1 62 is permitted to be unavailable 43.80

hours/year. The ANX CSP$_1$ 62 may only be unavailable 2.63 hrs./year. The trunk 65 between the ANX CSP$_1$ 62 and the ANX CEPO may only be unavailable 1.76 hrs./year. The ANX CEPO may only be unavailable 0.44 hours/year. The foregoing availabilities yield a total of 99.895% availability or 9.22 hours per year downtime.

The outline for how trouble is handled within the ANX-type VPN is shown in Fig. 8. There are effectively five layers of trouble handling. At the first level trouble between TPs is handled directly between the two TPs. Similarly, issues between the TPs and the CSPs are handled between the two parties. CSPs and the CEPOs also resolve their troubles between the troubled parties. A network overseer is provided to handle troubles that cannot be handled in the foregoing scenarios. The overseer can take complaints from the TPS, the CSPs, and the CEPOs.

A key to providing predictable end-to-end service quality is that the TPs must know the level of service they receive. To this end four service provider accountability levels exist. First, service providers, both interconnect providers and CSPs, must timely fix infrequent service provider troubles. Second, there must be end-to-end service provider cooperation to handle any troubles. Third, recourse must be provided to resolve disputes in the event of disagreement between CSPs and/or interconnect providers. Fourth, recourse must be provided to resolve continued non-compliance with the end-to-end service quality.

Referring to Figs. 9 and 10, charts for single VPN and interconnected VPNs are shown, respectively. In Fig. 9, the CSPs 70, CEPOs 72 and CASPs 74 are accountable to the POVER 76. The POVER 76 is accountable to the body 78 representing the TPs. The body 78 is accountable a regional/national arbitration body 80. Where multiple VPNs are interconnected in Fig. 10, the CSPs 70, the CEPOs 72, and CASPs 74 are accountable to the POVERs 76. The POVERs 76 are accountable to a GOVER 77, which in turn is accountable to the body 78. The body 78, instead of being accountable to the regional/national arbitration body 80, is accountable to an international arbitration body 82.

The GOVER/POVER model is but one way to oversee ensuring of the end-to-end service quality and metric compatibility. How the ANX-type networks are connected will be discussed below. In this context there must be five key types of end-to-end technology compatibility: 1 network interconnection that ensures a trading partner on one VPN can reach any trading partner on the other VPN; 2 routing compatibility that ensures any trading partner on one VPN can logically reach nay TP on the other VPN; 3 naming compatibility, e.g. so the web names or e-mail names of any trading partner on one VPN can be resolved to an address that is routable over the two VPNs; 4 IPSec compatibility; and 5 digital security certificate compatibility across multiple VPNs. While Figs. 9 and 10 refer to regional/national VPNs and international arbitration, the VPNs need not be limited to a specific country or geographical area. Any ANX-type VPN, regardless of the location of its subscribers could be interconnected.

While Fig. 1 illustrated the interconnection of two VPNs 20 and 22, a significant element is missing. Fig. 11 shows two VPNs, that have multiple service providers, which are connected through an inter-program service provider, also called an interconnect provider. The Tel-2 specification is still used as the basic guide in determining the end-to-end service quality, however regional or particular VPN peculiarities, referred to as deltas, must be considered when establishing the interconnected end-to-end service quality standards.

Returning to the GOVER/POVER model for overseeing interconnected VPNs; Fig. 12 illustrates an end-to-end trouble escalation model. It is expected that CSPs will work together to resolve trouble before contacting a POVER. Similarly, the POVERs and/or the POVERS and the interconnect provider are expected to work together to resolve trouble before contacting the GOVER.

When expanding from a single VPN to interconnected VPNs the inherent costs of running the system naturally increase. How such costs are distributed is an important part of the system. As shown in Fig. 13, the POVERs 100 pay fees to the GOVER to offset the costs of maintaining the GOVER. The VPNs having multiple service providers in turn pay fees to support the POVER. Furthermore the interconnect providers pay a certification fee to the GOVER for certification as a interconnect provider between VPNs.

There are multiple methods of interconnecting multiple VPNs with interconnect providers. As shown in Fig. 14, all the VPNs, having multiple service providers, can be interconnected using a single interconnect provider. Alternatively, all the VPNs can be interconnected by multiple interconnect providers, as shown in Fig. 15, thereby creating competition between the interconnect providers, just as there is competition between the CSPs in a single xNX-type VPN. Finally, as shown in

Fig. 16, where no suitable interconnect provider is available to connect all he VPNs having multiple service providers, multiple interconnect providers are used. These interconnect providers service different combinations of VPNs. In Fig. 16, interconnect provider 120 interconnects VPNs having multiple service providers 122, 124, and 126. Interconnect provider 130 interconnects VPNs having multiple service providers 132 and 126. As a result, a TP of VPN 132 must connect through both Interconnect provider 130 and Interconnect provider 120 to reach TPs of either VPN 122 or 124.

How the multiple VPNs interconnect will directly affect the resulting end-to-end service quality. Figs. 17a-c illustrate potential configurations of multiple VPNs. In Fig. 17a a first TP 200 connects to a first CSP 210. The CSP210 connects to a first exchange point 220. The TP 200, CSP 210, and the exchange point 220 are within a first VPN 240. A second TP 250 connects to a second CSP 260, which connects to a second exchange point 270. The TP 250, CSP 260 and exchange point 270 are within a second VPN 280. The two VPNs 240 and 280 are interconnected by an Interconnect provider 300, which is connected to the exchange points 220 and 270.

In Fig. 17b TP 200, CSP 210, exchange point 220 and Interconnect provider 300 are connected in the same manner shown in Fig. 17a. While the second TP 250 is connected to the CSP 260, the exchange point 270 is not provided. Instead CSP 260 is shown as connecting directly to the Interconnect provider 300. This embodiment encompasses the situation where the Interconnect provider 300 and CSP 260 are the same entity or are directly wired. Fig. 17c is similar to Fig. 16b,
Except that the interconnect provider also acts as a CSP 320, and a third TP 310 is connected directly to the Interconnect provider 300/CSP 320.

As stated previously, while the end-to-end service quality is based upon the TEL-2 specification, the degree to which the TEL-2 specification needs to be modified to interconnect multiple VPNs depends upon the chosen complexity of the interconnection. An xNX-type VPN uses a maximum of two CSPs between any two TPS. A larger value, either three or four, is needed for multiple VPNs. The Interconnect provider will account for one additional CSP, and for configuration set forth in Fig. 16, two Interconnect providers are employed in addition to the two CSPs yielding four CSPs.

Having described several embodiments of the system and method for interconnecting multiple virtual private networks in accordance with the present invention, it is believed that other modifications, variations and changes will be suggested to those skilled in the art in view of the description set forth above. It is therefore to be understood that all such variations, modifications and changes are believed to fall within the scope of the present invention as defined in the appended claims.

What is claimed is:

1. A system of interconnecting multiple virtual private networks, each of said multiple private networks having multiple service providers, comprising:

at least one interconnect provider for connecting said multiple virtual private networks,

said multiple virtual private networks connected through said at least one interconnect provider having minimum standards for cross network services, virtual private network interoperability, inter–network performance, inter-network reliability, disaster recovery and business continuity, inter-network security, inter-network customer care, and inter-network trouble handling.

2. A system as recited in claim 1, further comprising a maximum acceptable latency between subscribers to different ones of said multiple virtual private networks.

3. A system as recited in claim 1, further comprising a maximum acceptable number of service providers between subscribers to different ones of said multiple virtual private networks.

4. A system as recited in claim 1, further comprising a minimum acceptable period of unavailability of interconnected multiple virtual private networks.

5. A system as recited in claim 1, wherein each of said multiple virtual private networks comprises a program overseer to ensure end-to-end service quality across each of said multiple virtual private networks.

6. A system as recited in claim 5, further comprising a global overseer to ensure end-to-end service quality across multiple ones of said multiple virtual private networks.

7. A system as recited in claim 6, wherein said global overseer resolves disputes between ones of said program overseers for said multiple virtual private networks or said program overseers and said at least one interconnect provider.

8. A system as recited in claim 5, wherein said program overseer for each one of said multiple virtual private networks resolves disputes between service providers within said one of said multiple virtual private networks.

9. A system as recited in claim 6, wherein each of said program overseers and said multiple interconnect providers provides financial support to run said global overseer.

10. A system as recited in claim 1, wherein management of said multiple virtual private networks, contracts by between service providers and interconnect providers, service assurance, service description and how service providers and interconnect providers collaborate and compete are unified across said multiple virtual private networks to ensure end-to-end service quality.

11. A system as recited in claim 1, comprising multiple interconnect providers, wherein no one interconnect provider services all of said multiple virtual private networks.

12. A method of interconnecting multiple interconnection providers between multiple virtual private networks, each of said virtual private networks having multiple subscribers, multiple service providers and at least one exchange point interconnecting said multiple service providers, with guaranteed end-to-end service quality, comprising the steps of:

providing at least one interconnect provider disposed between a first set of said multiple service providers in one of said multiple virtual private networks and a second set of multiple service providers in a second one of said multiple virtual private networks.

13. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 12, wherein one of said at least one transit service providers is also one of said multiple service providers within at least one of said multiple virtual private networks.

14. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 12, further comprising the step of certifying all of said multiple service providers in all of said multiple virtual private networks, said multiple transit service providers, and said exchange points to ensure minimum end-to-end quality and security levels are maintained.

15. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 12, comprising the further step of providing at least one exchange point between a first set of said multiple service providers in one of said multiple virtual private networks and said at least one interconnect service provider.

16. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 12, wherein a maximum number of service providers between two subscribers within one of said multiple virtual private networks is two, and the maximum number of said service providers and transit service providers between subscribers of different ones of said multiple virtual private networks is three.

17. A method of interconnecting multiple interconnection providers between multiple virtual private networks as recited in claim 15, further comprising the step of providing at least one second exchange point between a second set of said multiple service providers in another one of said multiple virtual private networks and said at least one transit service provider.

18. A system of interconnecting multiple virtual private networks, each of said multiple private networks having multiple service providers, comprising:

at least one interconnect provider for connecting said multiple virtual private networks,

each of said multiple virtual private networks comprising a program overseer to ensure end-to-end service quality across each of said multiple virtual private networks, and a global overseer to ensure end-to-end service quality across multiple ones of said multiple virtual private networks,

said multiple virtual private networks connected through said at least one interconnect provider have: minimum standards for cross network services; virtual private network interoperability; inter–network performance; inter-network reliability; disaster recovery and business continuity; inter-network security; inter-network customer care; and inter-network trouble handling.

19. A system as recited in claim 18, further comprising a maximum acceptable latency between subscribers to different ones of said multiple virtual private networks.

20. A system as recited in claim 18, further comprising a maximum acceptable number of service providers between subscribers to different ones of said multiple virtual private networks.

21. A system as recited in claim 18, further comprising a minimum acceptable period of unavailability of interconnected multiple virtual private networks.

22. A system as recited in claim 18, wherein said global overseer resolves disputes between ones of said program overseers for said multiple virtual private networks or said program overseers and said at least one interconnect provider.

23. A system as recited in claim 18, wherein said program overseer for each one of said multiple virtual private networks resolves disputes between service providers within said one of said multiple virtual private networks.

24. A system as recited in claim 18, wherein each of said program overseers and said multiple interconnect providers provides financial support to run said global overseer.

25. A system as recited in claim 18, wherein management of said multiple virtual private networks, contracts by between service providers and interconnect

providers, service assurance, service description and how service providers and interconnect providers collaborate and compete are unified across said multiple virtual private networks to ensure end-to-end service quality.

26. A system as recited in claim 18, comprising multiple interconnect providers, wherein no one interconnect provider services all of said multiple virtual private networks.

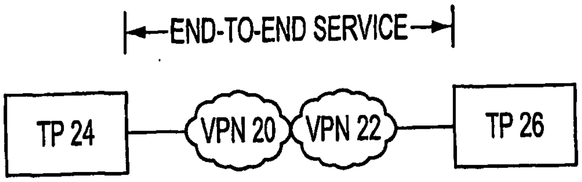


FIG. 1

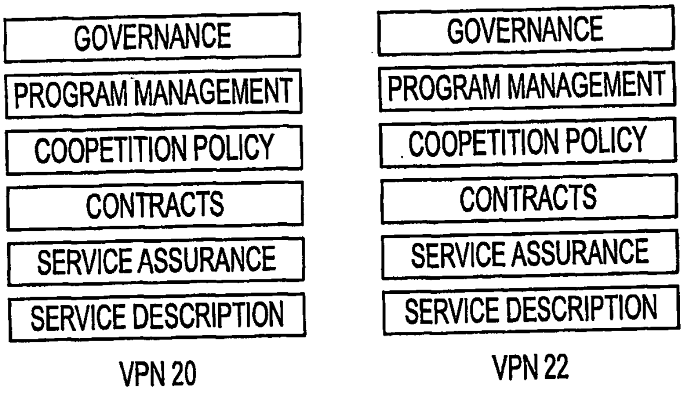


FIG. 2

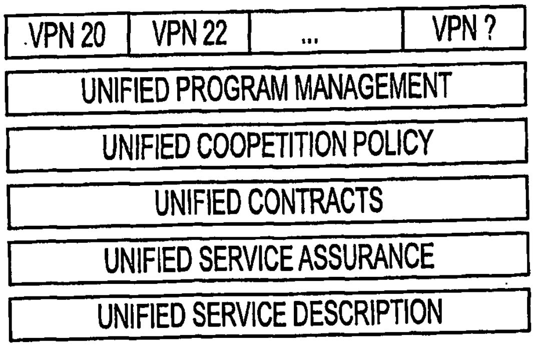

VPN 20
VPN 22
...
VPN ?
UNIFIED PROGRAM MANAGEMENT
UNIFIED COOPETITION POLICY
UNIFIED CONTRACTS
UNIFIED SERVICE ASSURANCE
UNIFIED SERVICE DESCRIPTION

FIG. 3

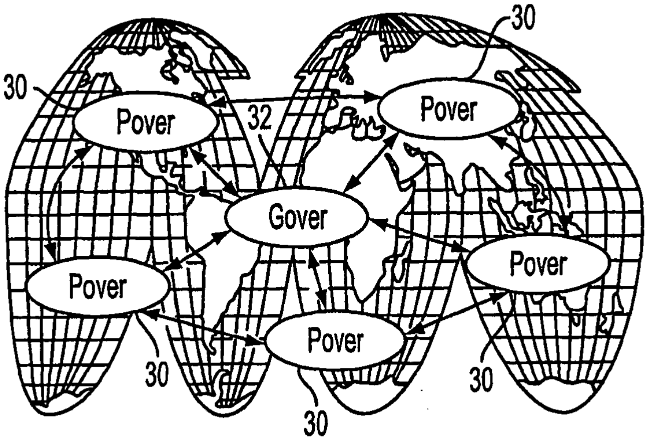

30
30
32
Pover
Pover
Gover
Pover
Pover
Pover
30
30
30
30

FIG. 4

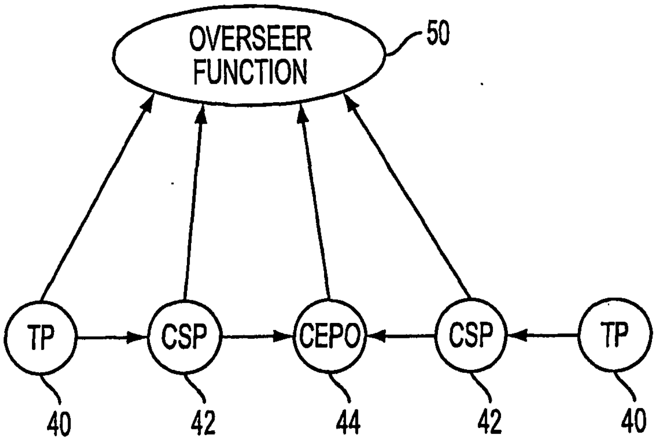

OVERSEER FUNCTION
50
TP
CSP
CEPO
CSP
TP
40
42
44
42
40

FIG. 5

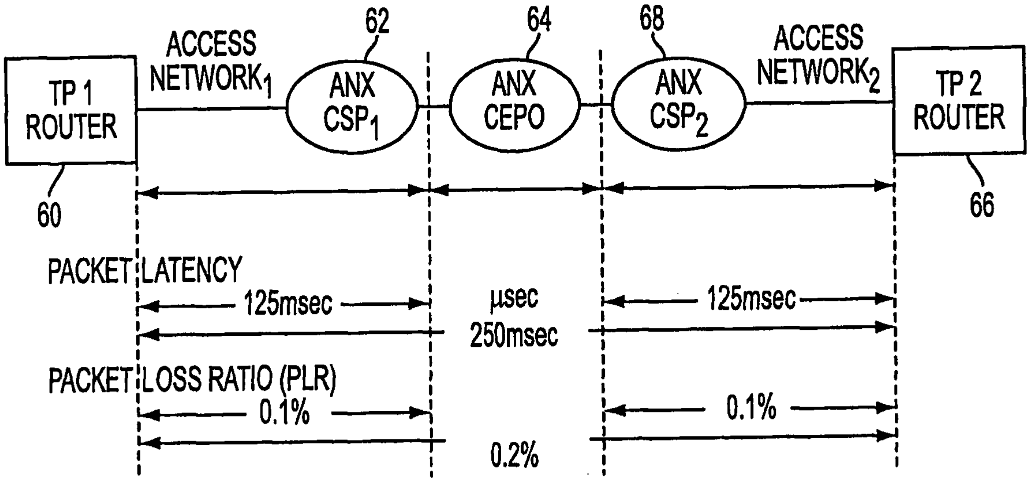


FIG. 6

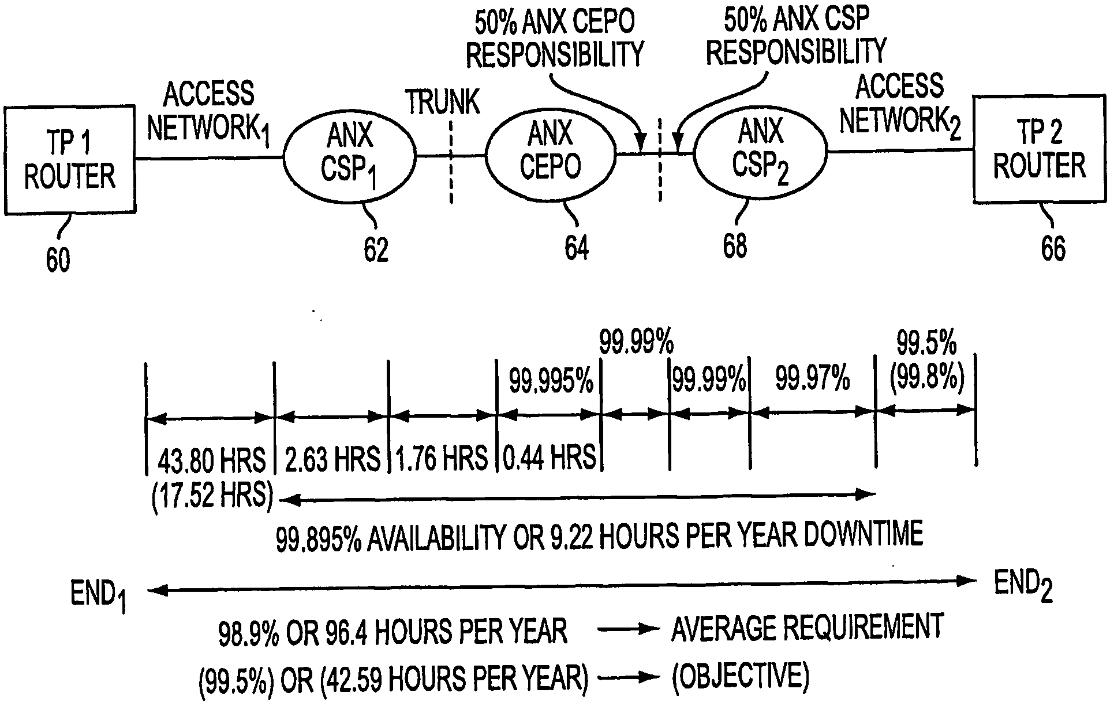


FIG. 7

SUBSTITUTE SHEET (RULE 26)

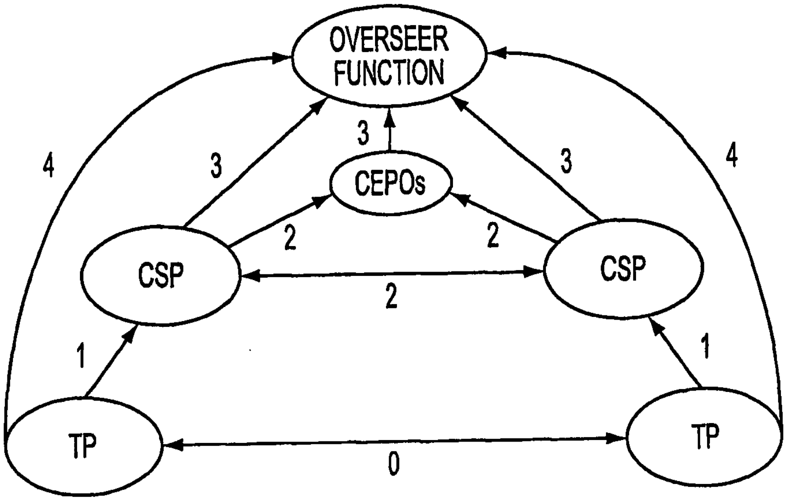

OVERSEER FUNCTION
4
3
3
CEPOs
3
4
2
2
CSP
CSP
2
1
1
TP
TP
0

FIG. 8

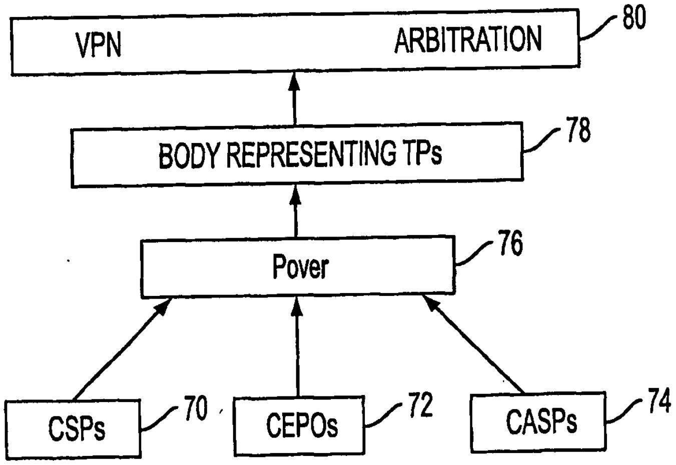

VPN ARBITRATION
80
BODY REPRESENTING TPs
78
Pover
76
CSPs
70
CEPOs
72
CASPs
74

FIG. 9

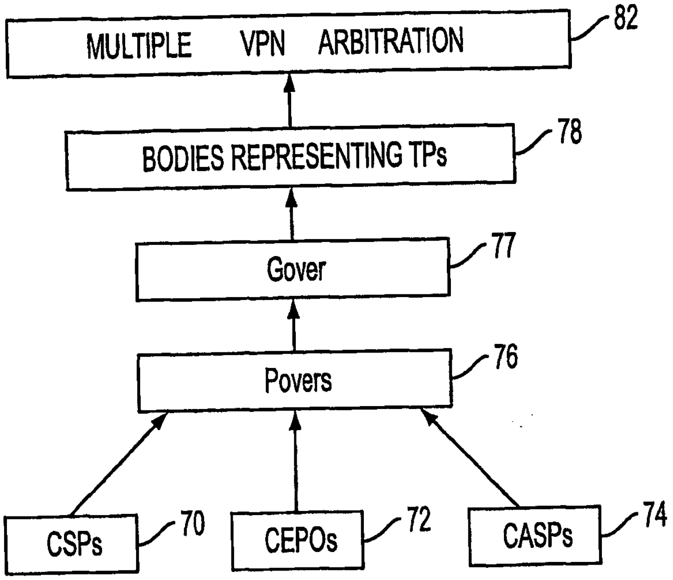

MULTIPLE VPN ARBITRATION
82
BODIES REPRESENTING TPs
78
Gover
77
Povers
76
CSPs
70
CEPOs
72
CASPs
74

FIG. 10

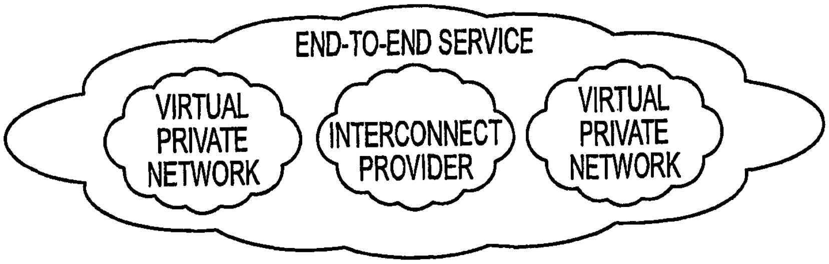

END-TO-END SERVICE
VIRTUAL PRIVATE NETWORK
INTERCONNECT PROVIDER
VIRTUAL PRIVATE NETWORK

FIG. 11

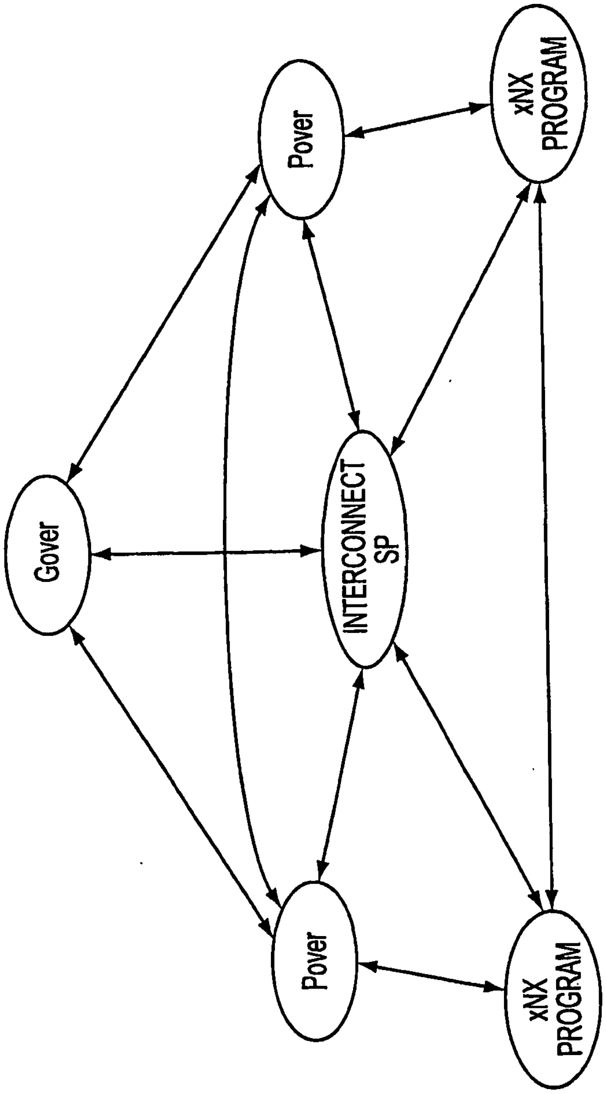


FIG. 12

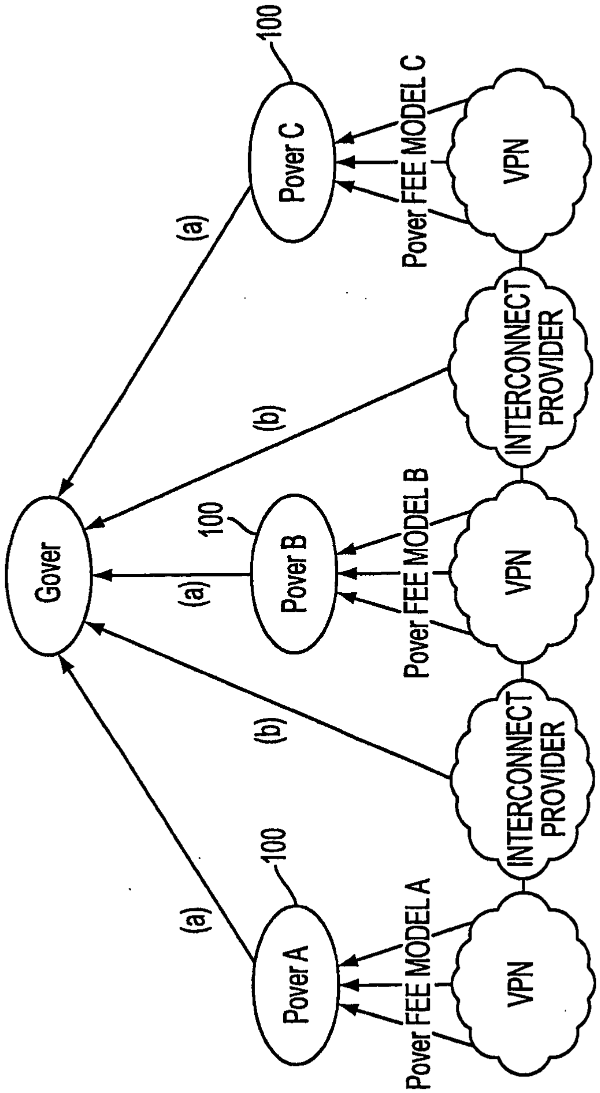

Gover
(a)
(b)
(a)
(b)
(a)
Pover A
100
Pover B
100
Pover C
100
Pover FEE MODEL A
Pover FEE MODEL B
Pover FEE MODEL C
VPN
INTERCONNECT PROVIDER
VPN
INTERCONNECT PROVIDER
VPN

FIG. 13

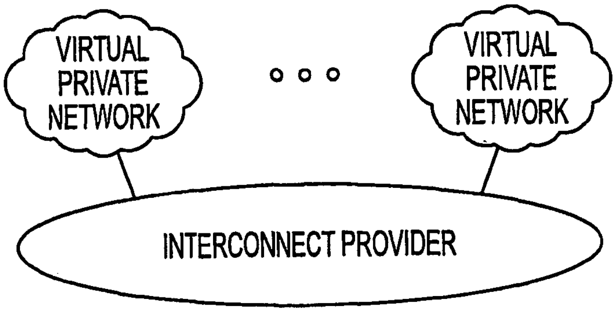

VIRTUAL PRIVATE NETWORK
○ ○ ○
VIRTUAL PRIVATE NETWORK
INTERCONNECT PROVIDER

FIG. 14

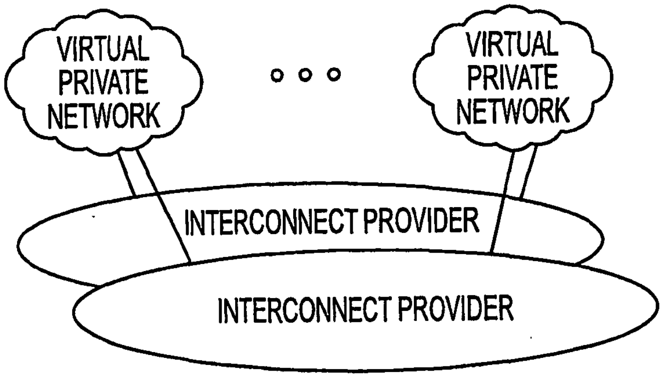

VIRTUAL PRIVATE NETWORK
○ ○ ○
VIRTUAL PRIVATE NETWORK
INTERCONNECT PROVIDER
INTERCONNECT PROVIDER

FIG. 15

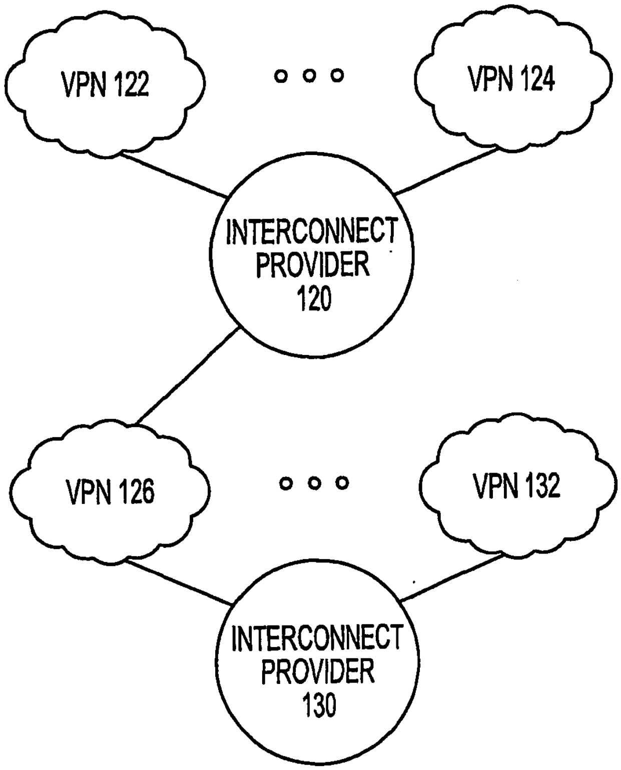

VPN 122
o o o
VPN 124
INTERCONNECT PROVIDER 120
VPN 126
o o o
VPN 132
INTERCONNECT PROVIDER 130

FIG. 16

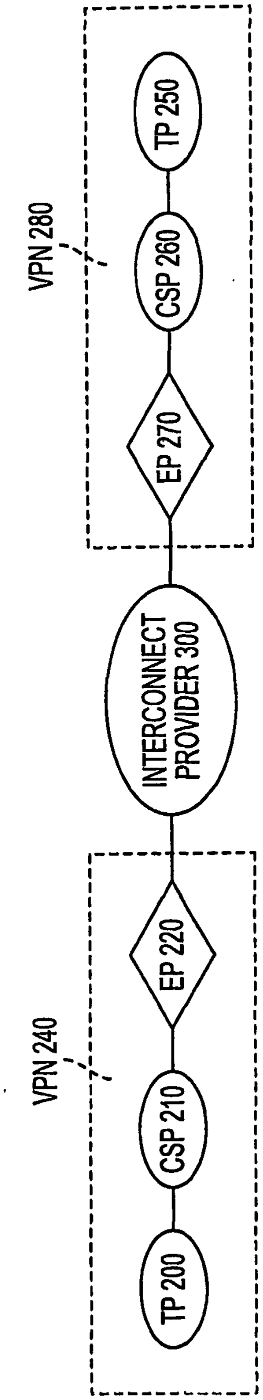


FIG. 17A

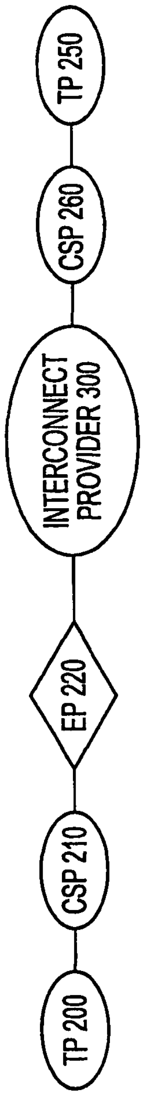


FIG. 17B

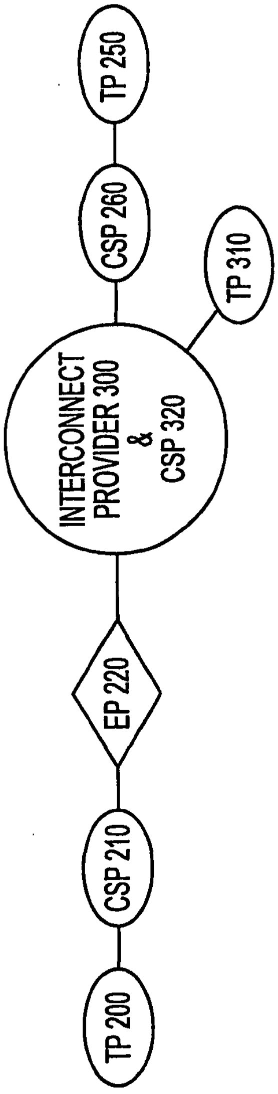


FIG. 17C

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/23774

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G06F 13/00
US CL : 709/201, 220, 221, 223, 227, 228, 236, 238
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)

U.S. : 709/201, 220, 221, 223, 227, 228, 236, 238

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CAS ONLINE
service(1w)providers, private(1w)(networks or lans), interconnection(1w)provider

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, P	US 6,104,701 A (AVARGUES et al) 15 August 2000, Figs 1-3, col 1, lines 60-67, col 2, lines 1-6, lines 22-67, col 3, lines 1-6, col 6, lines 20-67, col 7, lines 1-26.	1-26

□ Further documents are listed in the continuation of Box C. □ 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 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
"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
"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

10 OCTOBER 2000

Date of mailing of the international search report

26 OCT 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer Peggy Harrod
MOUSTAFA M. MEKY
Telephone No. (703) 305-9697

5-20-09

JFW

Docket No.: 077580-0063

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Victor Larson, et al.	Customer No.: 23630
Appl. No.:	11/840,560	Confirmation No.: 1537
Filed:	August 17, 2007	
Title:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	
Grp./A.U.	2157	
Examiner:	VU, Kim Y.	

CERTIFICATE OF MAILING (37 CFR. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail under 37 CFR 1.8(a) in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on May 19, 2009.

Jacqueline Andreu

Jacqueline Andreu

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

Enclosed for filing in connection with the above-referenced patent application are the following documents:

1) Information Disclosure Statement (2 pages)
2) Information Disclosure Statement by Applicant (Form 1449) (17 pages);
3) 6 Boxes of cited references B1000-B1002 and C998-C1226;
    - (Please note that references are arranged in order starting from Box 1)
4) Return receipt postcard.

There are no fees due with the filing of this Information Disclosure Statement. However, the Commissioner is hereby authorized to charge any additional fees that may be required, or credit any overpayment, to our Deposit Account No. 50-1133.

Respectfully submitted,

Date: May 19, 2009

Toby H. Kusmer, Reg. No.: 26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4065
Facsimile: (617) 535-3800

Docket No.: 077580-0063

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Victor Larson, et al.	Customer No.: 23630
Appl. No.:	11/840,560	Confirmation No.: 1537
Filed:	August 17, 2007	
Title:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	
Grp./A.U.	2157	
Examiner:	VU, Kim Y.	

CERTIFICATE OF MAILING (37 CFR. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage via Express Mail under 37 CFR 1.8(a) in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on May 19, 2009.

Jacqueline Andreu

Jacqueline Andreu

Mail Stop: Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Dear Sir:

In accordance with the provisions of 37 C.F.R. 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the documents listed on the attached form PTO-1449. It is respectfully requested that the documents be expressly considered during the prosecution of this application, and that the documents be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is being filed before the receipt of a First Office Action on the merits for above-referenced application; therefore, no fees are believed to be due with the filing of this paper.

All of the documents herein submitted have been produced by Microsoft Corp. in VirnetX Inc. and Science Applications International Corp. v. Microsoft Corp. civil action currently pending before the U.S. District Court for the Eastern District of Texas. Although the undersigned attorney has not reviewed these documents to assess their materiality, these documents are submitted under the assumption that they may be material to the patentability of the claims pending in this application. As indicated in form 1449 enclosed herewith, the hard copies of some of the documents listed have not been located and therefore are not included with this IDS submission. The undersigned attorney will file the missing documents with the U.S. Patent Office if or as soon as they become available. The Examiner is invited to call the undersigned attorney for any questions regarding the missing documents.

This Statement is not to be interpreted as a representation that the cited publications are material, or that no other relevant information exists. Nor shall the citation of any publication herein be construed *per se* as a representation that such publication is prior art. Moreover, the Applicant understands that the Examiner will make an independent evaluation of the cited publications.

If the Examiner applies any of the documents as prior art against any claim in the application and applicants determine that the cited document does not constitute "prior art" under United States law, applicant reserves the right to present to the office the relevant facts and law regarding the appropriate status of such documents. Applicants further reserve the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims of the present application.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1133 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Toby H. Kusmer
Registration No. 26,418
28 State Street
Boston, MA 02109
Phone: 617-535-4065
Facsimile: 617-535-3800
Date: May 19, 2009

Please recognize our Customer No. 23630 as our correspondence address.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	11840560
	Filing Date	2007-08-17
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-063(VRNK-1CP3CN2)

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5771239		1998-06-23	Moroney, et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		11840560
	Filing Date		2007-08-17
	First Named Inventor	Larson, et al.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		077580-063(VRNK-1CP3CN2)

	1	FASBENDER, A., et al., Variable and Scalable Security: Protection of Location Information in Mobile IP, IEEE VTS, 46th, 1996, 5 pp.	□

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number		11840560
	Filing Date		2007-08-17
	First Named Inventor	Larson, et al.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		077580-063(VRNK-1CP3CN2)

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ 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

☐ 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).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ 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	/ARR/	Date (YYYY-MM-DD)	2009-02-24
Name/Print	Atabak R. Royaee	Registration Number	59,037

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 record s.

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.

Electronic Acknowledgement Receipt

EFS ID:	4848196
Application Number:	11840560
International Application Number:	
Confirmation Number:	1537
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royaee/Erin Shea
Filer Authorized By:	Atabak R Royaee
Attorney Docket Number:	077580-0063 (VRNK-1CP3CN2
Receipt Date:	24-FEB-2009
Filing Date:	17-AUG-2007
Time Stamp:	15:33:46
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) Filed (SB/08)	77580_063_US_IDS_Form__SB_08a.pdf	608138 7eeaf855c5255e7f9b1c625ed840cc70d91718ab	no	4

Warnings:

Information:

2	NPL Documents	VRNK_NPLREFERENCE.PDF	731920 7e1f64823a0ad0d6d42fb2b62ae80e8c05c3f713	no	5
Warnings:					
Information:					
		Total Files Size (in bytes):	1340058		

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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	11840560
	Filing Date	2007-08-17
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-063(VRNK-1CP3CN2)

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5303302		1994-04-12	Burrows	
	2	5629984		1997-05-13	McManis	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] ¡	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	11840560
	Filing Date	2007-08-17
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-063(VRNK-1CP3CN2)

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1		□

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT **(Not for submission under 37 CFR 1.99)**	Application Number		11840560
	Filing Date		2007-08-17
	First Named Inventor	Larson, et al.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		077580-063(VRNK-1CP3CN2)

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☒ 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

□ 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).

□ See attached certification statement.

□ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

□ 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	/ARR/	Date (YYYY-MM-DD)	2009-01-22
Name/Print	Atabak R. Royaee	Registration Number	59,037

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 record s.

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.

Electronic Acknowledgement Receipt

EFS ID:	4656424
Application Number:	11840560
International Application Number:	
Confirmation Number:	1537
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royaee/Erin Shea
Filer Authorized By:	Atabak R Royaee
Attorney Docket Number:	077580-0063 (VRNK-1CP3CN2
Receipt Date:	22-JAN-2009
Filing Date:	17-AUG-2007
Time Stamp:	13:46:38
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) Filed (SB/08)	77580_063_US_IDS_Form__SB_08a.pdf	607962 04ffe30bd786d35c0b91d77bb84e635f2ae13a81	no	4

Warnings:

Information:

Total Files Size (in bytes):	607962

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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	11840560
	Filing Date	2007-08-17
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-063(VRNK-1CP3CN2)

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code1	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5384848		1995-01-00	Kikuchi	
	2	6223287		2001-04-00	Douglas, et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code1	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number3	Country Code2 i	Kind Code4	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T5
	1							□

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number		11840560
	Filing Date		2007-08-17
	First Named Inventor	Larson, et al.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		077580-063(VRNK-1CP3CN2)

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1		□

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	11840560
	Filing Date	2007-08-17
	First Named Inventor	Larson, et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	077580-063(VRNK-1CP3CN2)

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

□ 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

□ 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).

□ See attached certification statement.

□ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ 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	/THK/	Date (YYYY-MM-DD)	2008-12-16
Name/Print	Toby H. Kusmer	Registration Number	26,418

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 record s.

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.

Electronic Acknowledgement Receipt

EFS ID:	4461869
Application Number:	11840560
International Application Number:	
Confirmation Number:	1537
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Toby H. Kusmer./Erin Shea
Filer Authorized By:	Toby H. Kusmer.
Attorney Docket Number:	077580-0063 (VRNK-1CP3CN2
Receipt Date:	16-DEC-2008
Filing Date:	17-AUG-2007
Time Stamp:	11:22:27
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) Filed (SB/08)	77580_063_US_IDS_Form__SB_08a.pdf	608039 d49a887728d7b4b7c415926546012a7c0f980342	no	4

Warnings:

Information:

Total Files Size (in bytes):	608039

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

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/840,560	08/17/2007	Victor Larson	077580-0063 (VRNK-1CP3CN2

CONFIRMATION NO. 1537

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA02109-1775

Title: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Publication No. US-2008-0040792-A1
Publication Date: 02/14/2008

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.

Pre-Grant Publication Division, 703-605-4283

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	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
11/840,560	08/17/2007	2157	1130	077580-0063 (VRNK-1CP3CN2	3	3

CONFIRMATION NO. 1537

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA 02109-1775

UPDATED FILING RECEIPT

OC000000026652054

Date Mailed: 11/08/2007

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 write to the Office of Initial Patent Examination's Filing Receipt Corrections. 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**

Applicant(s)

Victor Larson, Fairfax, VA;
Robert Dunham Short III, Leesburg, VA;
Edmund Colby Munger, Crownsville, MD;
Michael Williamson, South Riding, VA;

Assignment For Published Patent Application

VirnetX, Inc., Scotts Valley, CA

Power of Attorney: The patent practitioners associated with Customer Number 23630

Domestic Priority data as claimed by applicant

This application is a CON of 10/714,849 11/18/2003
which is a CON of 09/558,210 04/26/2000 ABN
which is a CIP of 09/504,783 02/15/2000 PAT 6,502,135
which is a CIP of 09/429,643 10/29/1999 PAT 7,010,604
which claims benefit of 60/106,261 10/30/1998
and claims benefit of 60/137,704 06/07/1999

Foreign Applications

If Required, Foreign Filing License Granted: 08/29/2007

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 11/840,560**

Projected Publication Date: 02/14/2008

Non-Publication Request: No

Early Publication Request: No
Title

AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Preliminary Class

709

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 (1-866-999-4158).

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 AssetsControl, 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).

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
11/840,560	08/17/2007	Victor Larson	077580-0063 (VRNK-1CP3CN2

CONFIRMATION NO. 1537

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA 02109-1775

POA ACCEPTANCE LETTER

OC000000026505880

Date Mailed: 10/31/2007

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/22/2007.

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.

/snguyen/

Office of Initial Patent Examination (571) 272-4000 or 1-800-PTO-9199

10-29-07

Page 1 of 2

1FW

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	ATTORNEY DOCKET NUMBER
11/840,560	08/17/2007	Victor Larson	077580-0063 (VRNK-1CP3CN2

CONFIRMATION NO. 1537

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA 02109-1775

FORMALITIES LETTER

Date Mailed: 08/30/2007

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is missing. *A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.* *Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.*

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee, or oath or declaration) as set forth in 37 CFR 1.16(f) of $130 for a non-small entity, must be submitted with the missing items identified in this notice.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$130** for a non-small entity

- **$130** Surcharge.

Replies should be mailed to: Mail Stop Missing Parts

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199
PART 1 - ATTORNEY/APPLICANT COPY

PATENT
077580-0063 (VRNK-1CP3CN2)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor Larson et al.
Serial No: 11/840,560
Filing Date: August 17, 2007
Group Art Unit: 2157
Examiner: To Be Determined
Title: AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
Docket No: 77580-0063 (VRNK-1CP3CN2)

CERTIFICATE UNDER 37 CFR § 1.10 OF MAILING BY "EXPRESS MAIL"
EV 942454832 US Date

I hereby certify that this correspondence is being deposited with the United States Postal Services "Express Mail Post Office to Addressee" service under 37 CFR § 1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: 10.26.07

Cynthia Joseph
Cynthia Joseph

Mail Stop: Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

Enclosed herewith for filing in the above-identified patent application please find the following:

1. Response to Notice to File Missing Parts;
2. Statement Under 37 C.F.R. §1.63(d)(1)(iv);
3. Joint Declaration And Power of Attorney for Patent Application;
4. The Change in Power of Attorney and Correspondence Address Under 37 C.F.R. §1.63(d)(4);
5. Copy of Notice to File Missing Parts of Nonprovisional Application; and
6. Return Postcard.

In connection with the foregoing matter, please charge any additional fees which may be due, or credit any overpayment, to Deposit Account Number 50-1133. A duplicate copy of this letter is provided for this purpose.

Date: 10-26-07

Respectfully submitted,

Toby H. Kusmer, Esq.
Registration Number 26,418
McDermott, Will & Emery LLP
28 State Street
Boston, MA 02109-1775
Telephone: (617) 535-4000
Facsimile: (617) 535-3800
E-mail: tkusmer@mwe.com

PATENT
077580-0063 (VRNK-1CP3CN2)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor Larson et al.
Serial No: 11/840,560
Filing Date: August 17, 2007
Group Art Unit: 2157
Examiner: To Be Determined
Title: AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
Docket No: 77580-0063 (VRNK-1CP3CN2)

CERTIFICATE UNDER 37 CFR § 1.10 OF MAILING BY "EXPRESS MAIL"

EV 942454832 US Date

I hereby certify that this correspondence is being deposited with the United States Postal Services "Express Mail Post Office to Addressee" service under 37 CFR § 1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: 10·26·07

Cynthia Joseph
Cynthia Joseph

Mail Stop: Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO NOTICE TO FILE MISSING PARTS

Sir:

In response to the Notice to File Missing Parts of Non-Provisional Application, dated August 30, 2007, Applicant submits the required executed Declaration under 37 C.F.R. § 1.63(d)(1)(iv).

The Commissioner is also authorized to charge the surcharge fee of $130.00 and/or any further fees which may be due, and/or credit any overpayment to Deposit Account Number 50-1133.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Date: 10·26·07

Toby H. Kusmer, P.C.
Reg. No. 26,418
28 State Street
Boston, MA 02109-1775
DD Telephone: (617) 535-4065
Facsimile: (617)535-3800
e-mail: tkusmer@mwe.com

PATENT
077580-0063 (VRNK-1CP3CN2)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Victor Larson et al.
Serial No:	11/840,560
Filing Date:	August 17, 2007
Group Art Unit:	2157
Examiner:	To Be Determined
Title:	AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
Docket No:	77580-0063 (VRNK-1CP3CN2)

CERTIFICATE UNDER 37 CFR § 1.10 OF MAILING BY "EXPRESS MAIL"
EV 942454832 US Date

I hereby certify that this correspondence is being deposited with the United States Postal Services "Express Mail Post Office to Addressee" service under 37 CFR § 1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: 10-26-07

Cynthia Joseph

Mail Stop: Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

STATEMENT UNDER 37 C.F.R. § 1.63(d)(1)(iv)

Sir:

In accordance with 37 C.F.R. § 1.63(d)(1)(iv), for the above-identified continuation application, Applicants hereby submit a copy of the original Declaration filed in the prior application. The above-identified application is a continuation of U.S. Application Serial No. 10/714,849, filed November 18, 2003, which is a continuation of U.S. Application Serial No. 09/558,210, filed April 26, 2000, which is a continuation-in-part of U.S. Application No. 09/504,783, filed February 15, 2000, which is a continuation-in-part of U.S. Application No. 09/429,643, filed October 29, 1999, which claims the benefit under 35 U.S.C. 119(e) to U.S. Provisional Application Nos. 60/106,261, filed October 30, 1998, and 60/137,704, filed June 7, 1999.

The Commissioner is hereby authorized to charge any fees due with the filing of this paper to Deposit Account No. 50-1133.

Respectfully submitted,
McDERMOTT WILL & EMERY LLP

Date: 10·26·07

Toby H. Kusmer, P.C.
Reg. No. 26,418
28 State Street
Boston, MA 02109-1775
DD Telephone: (617) 535-4065
Facsimile: (617)535-3800
e-mail: tkusmer@mwe.com

Banner & Witcoff Ref. No. 00479.00111
Client Ref. No. 10007-Cont.

JOINT DECLARATION FOR PATENT APPLICATION

As the below named inventors, we hereby declare that:

Our residence, post office address and citizenship are as stated below next to our names;

We believe we are the original, first and joint inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES, the specification of which

☒ is attached hereto.

☐ was filed on ______ as Application Serial Number ______ and was amended on _________ (if applicable).

☐ was filed under the Patent Cooperation Treaty (PCT) and accorded International Application No. __________, filed _______, and amended on _______ (if any).

We hereby state that we have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

We hereby acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Prior Foreign Application(s)

We hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Country	Application No.	Date of Filing (day month year)	Date of Issue (day month year)	Priority Claimed Under 35 U.S.C. §119

Prior United States Provisional Application(s)

We hereby claim priority benefits under Title 35, United States Code, §119(e)(1) of any U.S. provisional application listed below:

U.S. Provisional Application No.	Date of Filing (day month year)	Priority Claimed Under 35 U.S.C. §119(e)(1)
60/106,261	30 October 1998	Yes
60/137,704	7 June 1999	Yes

Prior United States Application(s)

We hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, we acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Banner & Witcoff Ref. No. 00479.000111
Client Ref. No. 10007-Cont.

Application Serial No.	Date of Filing (Day, Month, Year)	Status — Patented, Pending, Abandoned
09/558,210	26 April 2000	Pending
09/504,783	15 February 2000	Patented
09/429,643	29 October 1999	Pending

Power of Attorney

And we hereby appoint, both jointly and severally, as our attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith the practitioners at:

Customer Number: 22907 (WDC)

Please address all correspondence and telephone communications to the address and telephone number for this Customer Number.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made 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 so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature Victor Larson Date 11/10/2003
Full Name of First Inventor Larson Victor
Family Name First Given Name Second Given Name
Residence Fairfax, Virginia Citizenship USA
Post Office Address 12026 Lisa Marie Court, Fairfax, Virginia 22033

Signature Date
Full Name of Second Inventor Short, III Robert Dunham
Family Name First Given Name Second Given Name
Residence Leesburg, Virginia Citizenship USA
Post Office Address 38710 Goose Creek Lane, Leesburg, Virginia 20175

Signature Date
Full Name of Third Inventor Munger Edmund Colby
Family Name First Given Name Second Given Name
Residence Crownsville, Maryland Citizenship USA
Post Office Address 1101 Opaca Court, Crownsville, Maryland 21032

Signature Date Nov 10 2003
Full Name of Fourth Inventor Williamson Michael
Family Name First Given Name Second Given Name
Residence South Riding, Virginia Citizenship USA
Post Office Address 26203 Ocala Circle, South Riding, Virginia 20152

Banner & Witcoff Ref. No. 000479.00111
Client Ref. No. 10007-Cont.

JOINT DECLARATION FOR PATENT APPLICATION

As the below named inventors, we hereby declare that:

Our residence, post office address and citizenship are as stated below next to our names;

We believe we are the original, first and joint inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES, the specification of which

☒ is attached hereto.

□ was filed on ______as Application Serial Number ______and was amended on _________ (if applicable).

□ was filed under the Patent Cooperation Treaty (PCT) and accorded International Application No. __________, filed _______, and amended on _______ (if any).

We hereby state that we have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

We hereby acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Prior Foreign Application(s)

We hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Country	Application No.	Date of Filing (day month year)	Date of Issue (day month year)	Priority Claimed Under 35 U.S.C. §119

Prior United States Provisional Application(s)

We hereby claim priority benefits under Title 35, United States Code, §119(e)(1) of any U.S. provisional application listed below:

U.S. Provisional Application No.	Date of Filing (day month year)	Priority Claimed Under 35 U.S.C. §119(e)(1)
60/106,261	30 October 1998	Yes
60/137,704	7 June 1999	Yes

Prior United States Application(s)

We hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, we acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Banner & Witcoff Ref. No. 000479.000111
Client Ref. No. 10007-Cont.

Application Serial No.	Date of Filing (Day, Month, Year)	Status — Patented, Pending, Abandoned
09/558,210	26 April 2000	Pending
09/504,783	15 February 2000	Patented
09/429,643	29 October 1999	Pending

Power of Attorney

And we hereby appoint, both jointly and severally, as our attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith the practitioners at:

Customer Number: 22907 (WDC)

Please address all correspondence and telephone communications to the address and telephone number for this Customer Number.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made 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 so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature__________ Date__________
Full Name of First Inventor Larson Victor
Family Name First Given Name Second Given Name
Residence Fairfax, Virginia Citizenship USA
Post Office Address 12026 Lisa Marie Court, Fairfax, Virginia 22033

Signature__________ Date 11/7/03
Full Name of Second Inventor Short, III Robert Dunham
Family Name First Given Name Second Given Name
Residence Leesburg, Virginia Citizenship USA
Post Office Address 38710 Goose Creek Lane, Leesburg, Virginia 20175

Signature__________ Date__________
Full Name of Third Inventor Munger Edmund Colby
Family Name First Given Name Second Given Name
Residence Crownsville, Maryland Citizenship USA
Post Office Address 1101 Opaca Court, Crownsville, Maryland 21032

Signature__________ Date__________
Full Name of Fourth Inventor Williamson Michael
Family Name First Given Name Second Given Name
Residence South Riding, Virginia Citizenship USA
Post Office Address 26203 Ocala Circle, South Riding, Virginia 20152

Banner & Witcoff Ref. No. 000479.00[illegible]1
Client Ref. No. 10007-Cont.

JOINT DECLARATION FOR PATENT APPLICATION

As the below named inventors, we hereby declare that:

Our residence, post office address and citizenship are as stated below next to our names;

We believe we are the original, first and joint inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES, the specification of which

☒ is attached hereto.
□ was filed on ______as Application Serial Number ______and was amended on _________ (if applicable).
□ was filed under the Patent Cooperation Treaty (PCT) and accorded International Application No. _________, filed _______, and amended on _______ (if any).

We hereby state that we have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

We hereby acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Prior Foreign Application(s)

We hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Country	Application No.	Date of Filing (day month year)	Date of Issue (day month year)	Priority Claimed Under 35 U.S.C. §119

Prior United States Provisional Application(s)

We hereby claim priority benefits under Title 35, United States Code, §119(e)(1) of any U.S. provisional application listed below:

U.S. Provisional Application No.	Date of Filing (day month year)	Priority Claimed Under 35 U.S.C. §119(e)(1)
60/106,261	30 October 1998	Yes
60/137,704	7 June 1999	Yes

Prior United States Application(s)

We hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, we acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Banner & Witcoff Ref. No. 000479.000111
Client Ref. No. 10007-Cont.

Application Serial No.	Date of Filing (Day, Month, Year)	Status — Patented, Pending, Abandoned
09/558,210	26 April 2000	Pending
09/504,783	15 February 2000	Patented
09/429,643	29 October 1999	Pending

Power of Attorney

And we hereby appoint, both jointly and severally, as our attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith the practitioners at:

Customer Number: 22907 (WDC)

Please address all correspondence and telephone communications to the address and telephone number for this Customer Number.

We hereby declare that all statements made herein of our own knowledge are true and that all statements made 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 so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature________________ Date________________
Full Name of First Inventor Larson Victor
Family Name First Given Name Second Given Name
Residence Fairfax, Virginia Citizenship USA
Post Office Address 12026 Lisa Marie Court, Fairfax, Virginia 22033

Signature________________ Date________________
Full Name of Second Inventor Short, III Robert Dunham
Family Name First Given Name Second Given Name
Residence Leesburg, Virginia Citizenship USA
Post Office Address 38710 Goose Creek Lane, Leesburg, Virginia 20175

Signature Edmund Colby Munger Date 11 November 2003
Full Name of Third Inventor Munger Edmund Colby
Family Name First Given Name Second Given Name
Residence Crownsville, Maryland Citizenship USA
Post Office Address 1101 Opaca Court, Crownsville, Maryland 21032

Signature________________ Date________________
Full Name of Fourth Inventor Williamson Michael
Family Name First Given Name Second Given Name
Residence South Riding, Virginia Citizenship USA
Post Office Address 26203 Ocala Circle, South Riding, Virginia 20152

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Victor Larson et al.
Serial No: 11/840,560
Filing Date: August 17, 2007
Group Art Unit: 2157
Examiner: To Be Determined
Title: AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
Docket No: 77580-0063 (VRNK-1CP3CN2)

CERTIFICATE UNDER 37 CFR § 1.10 OF MAILING BY "EXPRESS MAIL"
EV 942454832 US Date

I hereby certify that this correspondence is being deposited with the United States Postal Services "Express Mail Post Office to Addressee" service under 37 CFR § 1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: 10.26.07 Cynthia Joseph
Cynthia Joseph

Mail Stop: Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

THE CHANGE IN POWER OF ATTORNEY AND CORRESPONDENCE ADDRESS UNDER 37 C.F.R. § 1.63 (d)(4)

Dear Sir:

In accordance with 37 C.F.R. § 1.63 (d)(4) and pursuant to the Power of Attorney and Change of Correspondence Address filed on October 22, 2007, Applicants in the above-identified patent application have revoked all powers of attorney previously given in connection with the prior application and have appointed the following attorneys, with full power of substitution, to transact all business in the Patent and Trademark Office connected therewith:

All attorneys associated with CUSTOMER NUMBER 23630

It is requested that all correspondence regarding this patent application be directed to:

Toby H. Kusmer, P.C.
McDermott Will & Emery LLP
28 State Street
Boston, Massachusetts 02109-1775
Telephone: (617) 535-4065
Facsimile: (617) 535-3800
E-mail: tkusmer@mwe.com

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Date: 10.26.07

Toby H. Kusmer, P.C.
Reg. No. 26,418
28 State Street
Boston, MA 02109-1775
DD Telephone: (617) 535-4065
Facsimile: (617)535-3800
e-mail: tkusmer@mwe.com

PTO/SB/21 (10-07)
Approved for use through 10/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
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.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	11/840,560
Filing Date	August 17, 2007
First Named Inventor	Victor Larson
Art Unit	2157
Examiner Name	Not Yet Assigned
Total Number of Pages in This Submission	3
Attorney Docket Number	077580-0063 (VRNK-1CP3CN2)

ENCLOSURES (*Check all that apply*)

- □ Fee Transmittal Form
  - □ Fee Attached
- □ Amendment/Reply
  - □ After Final
  - □ Affidavits/declaration(s)
- □ Extension of Time Request
- □ Express Abandonment Request
- □ Information Disclosure Statement
- □ Certified Copy of Priority Document(s)
- □ Reply to Missing Parts/ Incomplete Application
  - □ Reply to Missing Parts under 37 CFR 1.52 or 1.53

- □ Drawing(s)
- □ Licensing-related Papers
- □ Petition
- □ Petition to Convert to a Provisional Application
- ☑ Power of Attorney, Revocation Change of Correspondence Address
- □ Terminal Disclaimer
- □ Request for Refund
- □ CD, Number of CD(s) _____________
  - □ Landscape Table on CD

- □ After Allowance Communication to TC
- □ Appeal Communication to Board of Appeals and Interferences
- □ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- □ Proprietary Information
- □ Status Letter
- □ Other Enclosure(s) (please Identify below):

Remarks

No fees are believed to be due with the filing of this paper; however, the commissioner is hereby authorized to charge any necessary fees in relation to this filing to Deposit Account No. 50-1133.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	McDERMOTT WILL & EMERY LLP		
Signature	/ATABAK R. ROYAEE/		
Printed name	ATABAK R. ROYAEE		
Date	October 22, 2007	Reg. No.	59,037

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	/ATABAK R. ROYAEE/		
Typed or printed name	ATABAK R. ROYAEE	Date	October 22, 2007

This collection of information is required by 37 CFR 1.5. 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 and1.14. This collection is estimated to 2 hours 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.

Doc Code: **077580** – CC63

PTO/SB/80 (01-06)
Approved for use through 12/31/2008. OMB 0651-0035
U S. Patent and Trademark Office; U S DEPARTMENT OF COMMERCE
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.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☒ Practitioners associated with the Customer **23,630**

OR

☐ Practitioner(s) named below (if more then ten practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☒ The address associated with Customer **23,630**

OR

☒ Firm or Individual Name	**McDermott Will & Emery LLP**		
Address	**28 State Street**		
City	**Boston**	State **MA**	Zip **02109**
Country	**U.S.A.**		
Telephone	**(617) 535-4065**	Email **tkusmer@mwe.com**	

Assignee Name and Address:
VIRNETX, INC.
5615 SCOTTS VALLEY DRIVE, SUITE 110
SCOTTS VALLEY, CALIFORNIA 95066

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	10/19/07
Name	Randall Larson	Telephone	831.688.5698
Title	President		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. 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 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.

PTO/SB/96 (04-07)
Approved for use through 09/30/2007. OMB 0651-0031
U S Patent and Trademark Office; U S DEPARTMENT OF COMMERCE
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.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: VIRNETX, INC.

Application No./Patent No.: 11/840,560 Filed/Issue Date: AUGUST 17, 2007

Entitled: AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

VIRNETX, INC, a CORPORATION
(Name of Assignee) (Type of Assignee, e g , corporation, partnership, university, government agency, etc)

states that it is:

1. ☑ the assignee of the entire right, title, and interest; or

2. □ an assignee of less than the entire right, title and interest
(The extent (by percentage) of its ownership interest is ________ %)

in the patent application/patent identified above by virtue of either:

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 ________, Frame ________, or for which a copy thereof is attatched.

OR

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Victor Larson, et al. To: Science Applications International Corporation
The document was recorded in the United States Patent and Trademark Office at
Reel 019722, Frame 0321, or for which a copy thereof is attached.

2. From: Science Applications International Corporation To: VirnetX, Inc
The document was recorded in the United States Patent and Trademark Office at
Reel 019722, Frame 0525, or for which a copy thereof is attached.

3. From: N/A 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.

□ As required by 37 CFR 3.73(b)(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.

Signature

10/19/07
Date

Kendall Larsen
Printed or Typed Name

831·608·5698
Telephone number

President
Title

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.

Electronic Acknowledgement Receipt

EFS ID:	2348564
Application Number:	11840560
International Application Number:	
Confirmation Number:	1537
Title of Invention:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES
First Named Inventor/Applicant Name:	Victor Larson
Customer Number:	23630
Filer:	Atabak R Royaee
Filer Authorized By:	
Attorney Docket Number:	077580-0063 (VRNK-1CP3CN2
Receipt Date:	22-OCT-2007
Filing Date:	17-AUG-2007
Time Stamp:	10:51:50
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	Miscellaneous Incoming Letter	Transmittal_63.pdf	46816 6d30f8771d9f05a27e6d9d24aec43c64078c65d4	no	1
Warnings:					

Information:					
2	Power of Attorney	POA_63.pdf	356731 0a89bdf2a8b24ab1c15df09875b96b796108dc15	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			403547		

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.

McDermott
Will&Emery

Boston Brussels Chicago Düsseldorf London Los Angeles Miami Munich
New York Orange County Rome San Diego Silicon Valley Washington, D.C.
Strategic alliance with MWE China Law Offices (Shanghai)

FACSIMILE

Date:	October 4, 2007	**Time Sent:**	

To:	**Company:**	**Facsimile No:**	**Telephone No:**
Commissioner for Patents	U.S. Patent and Trademark Office	1.571.273.8300	

From:	Toby H. Kusmer, P.C.	*Direct Phone:*	617.535.4065
E-Mail:	tkusmer@mwe.com	*Direct Fax:*	617.535.3800
Sent By:	Cynthia Joseph	*Direct Phone:*	617.535.4111
Client/Matter/Tkpr:	77580-063/5496	*Original to Follow by Mail:*	No
		Number of Pages, Including Cover:	2

Re: In re Application of: Victor Larson, et al.
Serial No.: 11/840,560
Filing Date: August 17, 2007
Title: An Agile Network Protocol For Secure Communications Using Secure Domain Names
Docket No.: 77580-063 (VRNK-1CP3CN2)

Message:

Please enter the attached Status Inquiry.

The information contained in this facsimile message is legally privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copy of this facsimile is strictly prohibited. If you have received this facsimile in error, please notify us immediately by telephone and return the original message to us at the below address by mail. Thank you.

IF YOU DO NOT RECEIVE ALL OF THE PAGES, PLEASE CALL AS SOON AS POSSIBLE.

Main Facsimile: 617.535.3800 Facsimile Operator: 617.535.4000

U.S. practice conducted through McDermott Will & Emery LLP.
28 State Street Boston, Massachusetts 02109-1775 Telephone: 617.535.4000

BST99 1553854-1.077580.0063

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Victor Larson, et al.
Serial No:	11/840,560
Filing Date:	August 17, 2007
Title:	An Agile Network Protocol For Secure Communications Using Secure Domain Names
Group Art Unit:	2157
Confirmation No.:	1537
Docket No:	77580-063 (VRNK-1CP3CN2)

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

STATUS INQUIRY

Applicants make a request as to the status of the above-identified application and for information as to when they might expect to receive an Office Action.

Respectfully submitted,

Toby H. Kusmer, P.C.
Registration Number 26,418
McDermott Will & Emery LLP
28 State Street
Boston, Massachusetts 02109-1775
Telephone: (617) 535-4065
Facsimile: (617) 535-3800
e-mail: tkusmer@mwe.com

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being facsimile transmitted, via Facsimile No. 571.273.8300, to the U.S. Patent and Trademark Office and is addressed to: Commissioner For Patents, P. O. Box 1450, Alexander, VA 22313-1450 on the date indicated below.

Date: October 4, 2007

Cynthia Joseph
Cynthia Joseph

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	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
11/840,560	08/17/2007	2157	1000	077580-0063 (VRNK-1CP3CN2	3	3

CONFIRMATION NO. 1537

FILING RECEIPT

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA02109-1775

Date Mailed: 08/30/2007

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 write to the Office of Initial Patent Examination's Filing Receipt Corrections. 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**

Applicant(s)

Victor Larson, Fairfax, VA;
Robert Dunham Short III, Leesburg, VA;
Edmund Colby Munger, Crownsville, MD;
Michael Williamson, South Riding, VA;

Assignment For Published Patent Application

VirnetX, Inc., Scotts Valley, CA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 10/714,849 11/18/2003
which is a CON of 09/558,210 04/26/2000 ABN
which is a CIP of 09/504,783 02/15/2000 PAT 6,502,135
which is a CIP of 09/429,643 10/29/1999 PAT 7,010,604
which claims benefit of 60/106,261 10/30/1998
and claims benefit of 60/137,704 06/07/1999

Foreign Applications

If Required, Foreign Filing License Granted: 08/29/2007

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is
US11/840,560

Projected Publication Date: To Be Determined - pending completion of Missing Parts

Non-Publication Request: No

Early Publication Request: No

Title

AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

Preliminary Class

709

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 (1-866-999-4158).

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 AssetsControl, 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).

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	ATTORNEY DOCKET NUMBER
11/840,560	08/17/2007	Victor Larson	077580-0063 (VRNK-1CP3CN2

CONFIRMATION NO. 1537

23630
MCDERMOTT WILL & EMERY LLP
28 STATE STREET
BOSTON, MA 02109-1775

FORMALITIES LETTER

Date Mailed: 08/30/2007

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is missing. *A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.*
  Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee, or oath or declaration) as set forth in 37 CFR 1.16(f) of $130 for a non-small entity, must be submitted with the missing items identified in this notice.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$130** for a non-small entity

- **$130** Surcharge.

Replies should be mailed to: Mail Stop Missing Parts

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199
PART 3 - OFFICE COPY

Express Mail Label No.

UTILITY PATENT APPLICATION TRANSMITTAL (Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
077580-0063 (VRNK-1CP3CN2)

Total Pages in this Submission

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

and invented by:

Victor Larson, Robert Dunham Short III, Edmund Colby Munger and Michael Williamson

If a CONTINUATION APPLICATION, *check appropriate box and supply the requisite information:*

☒ **Continuation** □ **Divisional** □ **Continuation-in-part (CIP)** of prior application No.: 10/714,849

Which is a:

☒ **Continuation** □ **Divisional** □ **Continuation-in-part (CIP)** of prior application No.: 09/558,210

Which is a:

□ **Continuation** □ **Divisional** ☒ **Continuation-in-part (CIP)** of prior application No.: 09/504,783

Enclosed are:

Application Elements

1. □ Filing fee as calculated and transmitted as described below

2. ☒ Specification having 83 pages and including the following:

   a. ☒ Descriptive Title of the Invention

   b. ☒ Cross References to Related Applications *(if applicable)*

   c. □ Statement Regarding Federally-sponsored Research/Development *(if applicable)*

   d. □ Reference to Sequence Listing, a Table, or a Computer Program Listing Appendix

   e. ☒ Background of the Invention

   f. ☒ Brief Summary of the Invention

   g. ☒ Brief Description of the Drawings *(if filed)*

   h. ☒ Detailed Description

   i. ☒ Claim(s) as Classified Below

   j. ☒ Abstract of the Disclosure

UTILITY PATENT APPLICATION TRANSMITTAL **(Large Entity)** *(Only for new nonprovisional applications under 37 CFR 1.53(b))*	Docket No. 077580-0063 (VRNK-1CP3CN2)
	Total Pages in this Submission

Application Elements (Continued)

3. ☒ Drawing(s) *(when necessary as prescribed by 35 USC 113)*

a. ☒ Formal Number of Sheets 40

b. □ Informal Number of Sheets ____________

4. □ Oath or Declaration

a. □ Newly executed *(original or copy)* □ Unexecuted

b. □ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional application only)*

c. □ With Power of Attorney □ Without Power of Attorney

d. □ *DELETION OF INVENTOR(S)*
Signed statement attached deleting inventor(s) named in the prior application,
see 37 C.F.R. 1.63(d)(2) and 1.33(b).

5. ☒ Incorporation By Reference *(usable if Box 4b is checked)*
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. □ CD ROM or CD-R in duplicate, large table or Computer Program (Appendix)

7. ☒ Application Data Sheet (See 37 CFR 1.76)

8. □ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all must be included)*

a. □ Computer Readable Form (CRF)

b. □ Specification Sequence Listing on:

i. □ CD-ROM or CD-R (2 copies); or

ii. □ Paper

c. □ Statement(s) Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

9. □ Assignment Papers *(cover sheet & document(s))*

10. □ 37 CFR 3.73(B) Statement *(when there is an assignee)*

11. □ English Translation Document *(if applicable)*

12. □ Information Disclosure Statement/PTO-1449 □ Copies of IDS Citations

13. □ Preliminary Amendment

14. □ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*

15. □ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*

16. □ Certificate of Mailing

□ First Class □ Express Mail *(Specify Label No.)*: ____________

UTILITY PATENT APPLICATION TRANSMITTAL (Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No. 077580-0063 (VRNK-1CP3CN2)
Total Pages in this Submission

Accompanying Application Parts (Continued)

17. □ Additional Enclosures *(please identify below)*:

Request That Application Not Be Published Pursuant To 35 U.S.C. 122(b)(2)

18. □ Pursuant to 35 U.S.C. 122(b)(2), Applicant hereby requests that this patent application not be published pursuant to 35 U.S.C. 122(b)(1). Applicant hereby certifies that the invention disclosed in this 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 of applications 18 months after filing of the application.

Warning

An applicant who makes a request not to publish, but who subsequently files in a foreign country or under a multilateral international agreement specified in 35 U.S.C. 122(b)(2)(B)(i), must notify the Director of such filing not later than 45 days after the date of the filing of such foreign or international application. A failure of the applicant to provide such notice within the prescribed period shall result in the application being regarded as abandoned, unless it is shown to the satisfaction of the Director that the delay in submitting the notice was unintentional.

19. ☒ Other:

Additional priority information is provided in the Application Data Sheet.

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
077580-0063 (VRNK-1CP3CN2)

Total Pages in this Submission

Fee Calculation and Transmittal

CLAIMS AS FILED					
For	#Filed	#Allowed	#Extra	Rate	Fee
Total Claims	3	- 20 =	0	x $50.00	$0.00
Indep. Claims	1	- 3 =	0	x $200.00	$0.00
Multiple Dependent Claims (check if applicable) □					$0.00
Total # of Pages in Specification	83	Total # of Drawing Sheets	40		
Total # of Sheets	123			Application Size Fee	$250.00
				Basic Fee	$300.00
				Search Fee	$500.00
				Examination Fee	$200.00
OTHER FEE *(specify purpose)*					$0.00
				TOTAL FILING FEE	$1,250.00

□ A check in the amount of to cover the filing fee is enclosed.

☒ The Director is hereby authorized to charge and credit Deposit Account No. **50-1133** as described below.

- ☒ Charge the amount of **$1,450.00** as filing fee.
- ☒ Credit any overpayment.
- ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
- □ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

□ Payment by credit card. Form PTO-2038 is attached.
WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Dated: **August 17, 2007**

Signature

Toby H. Kusmer, P.C.
Reg. No. 26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Telephone: 617-535-4065
Facsimile: 617-535-3800
e-mail: tkusmer@mwe.com

Customer Number: **23,630**

cc:

Express Mail Label No.

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
077580-0063 (VRNK-1CP3CN2)

Total Pages in this Submission

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

and invented by:

Victor Larson, Robert Dunham Short III, Edmund Colby Munger and Michael Williamson

If a CONTINUATION APPLICATION, *check appropriate box and supply the requisite information:*

☒ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: 10/714,849

Which is a:

☒ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: 09/558,210

Which is a:

☐ **Continuation** ☐ **Divisional** ☒ **Continuation-in-part (CIP)** of prior application No.: 09/504,783

Enclosed are:

Application Elements

1. ☐ Filing fee as calculated and transmitted as described below

2. ☒ Specification having 83 pages and including the following:

   a. ☒ Descriptive Title of the Invention

   b. ☒ Cross References to Related Applications *(if applicable)*

   c. ☐ Statement Regarding Federally-sponsored Research/Development *(if applicable)*

   d. ☐ Reference to Sequence Listing, a Table, or a Computer Program Listing Appendix

   e. ☒ Background of the Invention

   f. ☒ Brief Summary of the Invention

   g. ☒ Brief Description of the Drawings *(if filed)*

   h. ☒ Detailed Description

   i. ☒ Claim(s) as Classified Below

   j. ☒ Abstract of the Disclosure

UTILITY PATENT APPLICATION TRANSMITTAL (Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
077580-0063 (VRNK-1CP3CN2)

Total Pages in this Submission

Application Elements (Continued)

3. ☒ Drawing(s) *(when necessary as prescribed by 35 USC 113)*
   - a. ☒ Formal Number of Sheets 40
   - b. ☐ Informal Number of Sheets ______
4. ☐ Oath or Declaration
   - a. ☐ Newly executed *(original or copy)* ☐ Unexecuted
   - b. ☐ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional application only)*
   - c. ☐ With Power of Attorney ☐ Without Power of Attorney
   - d. ☐ *DELETION OF INVENTOR(S)*
     Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. 1.63(d)(2) and 1.33(b).
5. ☒ Incorporation By Reference *(usable if Box 4b is checked)*
   The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. ☐ CD ROM or CD-R in duplicate, large table or Computer Program (Appendix)
7. ☒ Application Data Sheet (See 37 CFR 1.76)
8. ☐ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all must be included)*
   - a. ☐ Computer Readable Form (CRF)
   - b. ☐ Specification Sequence Listing on:
     - i. ☐ CD-ROM or CD-R (2 copies); or
     - ii. ☐ Paper
   - c. ☐ Statement(s) Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

9. ☐ Assignment Papers *(cover sheet & document(s))*
10. ☐ 37 CFR 3.73(B) Statement *(when there is an assignee)*
11. ☐ English Translation Document *(if applicable)*
12. ☐ Information Disclosure Statement/PTO-1449 ☐ Copies of IDS Citations
13. ☐ Preliminary Amendment
14. ☐ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. ☐ Certificate of Mailing
    ☐ First Class ☐ Express Mail *(Specify Label No.)*: ______

UTILITY PATENT APPLICATION TRANSMITTAL **(Large Entity)** *(Only for new nonprovisional applications under 37 CFR 1.53(b))*	Docket No. 077580-0063 (VRNK-1CP3CN2) Total Pages in this Submission

Accompanying Application Parts (Continued)

17. □ Additional Enclosures *(please identify below):*

Request That Application Not Be Published Pursuant To 35 U.S.C. 122(b)(2)

18. □ Pursuant to 35 U.S.C. 122(b)(2), Applicant hereby requests that this patent application not be published pursuant to 35 U.S.C. 122(b)(1). Applicant hereby certifies that the invention disclosed in this 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 of applications 18 months after filing of the application.

Warning

An applicant who makes a request not to publish, but who subsequently files in a foreign country or under a multilateral international agreement specified in 35 U.S.C. 122(b)(2)(B)(i), must notify the Director of such filing not later than 45 days after the date of the filing of such foreign or international application. A failure of the applicant to provide such notice within the prescribed period shall result in the application being regarded as abandoned, unless it is shown to the satisfaction of the Director that the delay in submitting the notice was unintentional.

19. ☒ Other:

Additional priority information is provided in the Application Data Sheet.

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
077580-0063 (VRNK-1CP3CN2)

Total Pages in this Submission

Fee Calculation and Transmittal

CLAIMS AS FILED					
For	#Filed	#Allowed	#Extra	Rate	Fee
Total Claims	3	- 20 =	0	x $50.00	$0.00
Indep. Claims	1	- 3 =	0	x $200.00	$0.00
Multiple Dependent Claims (check if applicable) □					$0.00
Total # of Pages in Specification	83	Total # of Drawing Sheets	40		
Total # of Sheets	123			Application Size Fee	$250.00
				Basic Fee	$300.00
				Search Fee	$500.00
				Examination Fee	$200.00
OTHER FEE *(specify purpose)*					$0.00
				TOTAL FILING FEE	$1,250.00

□ A check in the amount of to cover the filing fee is enclosed.

☒ The Director is hereby authorized to charge and credit Deposit Account No. **50-1133** as described below.

- ☒ Charge the amount of **$1,450.00** as filing fee.
- ☒ Credit any overpayment.
- ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
- □ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

□ Payment by credit card. Form PTO-2038 is attached.
WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Dated: **August 17, 2007**

Signature

**Toby H. Kusmer, P.C.
Reg. No. 26,418
McDermott Will & Emery LLP
28 State Street
Boston, MA 02109
Telephone: 617-535-4065
Facsimile: 617-535-3800
e-mail: tkusmer@mwe.com**

Customer Number: **23,630**

cc:

Application Data Sheet

Application Information

Application Number::	not assigned
Filing Date::	August 17, 2007
Application Type::	Continuation
Subject Matter::	Utility
Suggested Classification	
Suggested Group Art Unit	
CD-ROM or CD-R	
Number of CD Disks	
Number of copies of CDs	
Sequence Submission	
Computer Readable Form (CRF)	
Number of copies of CRF	
Title::	An Agile Network Protocol For Secure Communications Using Secure Domain Names
Attorney Docket Number::	077580-0063 (VRNK-1CP3CN2)
Request for Early Publication::	No
Request for Non-Publication::	No
Suggested Drawing Figure::	1
Total Drawing Sheets::	40
Small Entity::	No
Latin Name	
Variety Denomination Name	
Petition Included::	
Petition Type::	
Licensed US Govt. Agency::	
Contract or Grant Numbers::	
Secrecy Order in Parent Appl.::	

Applicant Information

Applicant Authority Type::	Inventor **1**
Primary Citizenship Country::	U.S.
Status::	Full Capacity
Given Name::	Victor
Middle Name::	
Family Name::	Larson
Name Suffix::	
City of Residence::	Fairfax

State or Province of Residence::	VA
Country of Residence::	U.S.
Street of mailing address::	12026 Lisa Marie Court
City of mailing address::	Fairfax
State or Province of mailing address::	VA
Country of mailing address::	U.S.
Postal or Zip Code of mailing address::	22033
Applicant Authority Type::	Inventor **2**
Primary Citizenship Country::	U.S.
Status::	Full Capacity
Given Name::	Robert
Middle Name::	Dunham
Family Name::	Short
Name Suffix::	III
City of Residence::	Leesburg
State or Province of Residence::	VA
Country of Residence::	U.S.
Street of mailing address::	38710 Goose Creek Lane
City of mailing address::	Leesburg
State or Province of mailing address::	VA
Country of mailing address::	U.S.
Postal or Zip Code of mailing address::	20175
Applicant Authority Type::	Inventor **3**
Primary Citizenship Country::	U.S.
Status::	Full Capacity
Given Name::	Edmund
Middle Name::	Colby
Family Name::	Munger
Name Suffix::	
City of Residence::	Crownsville
State or Province of Residence::	MD
Country of Residence::	U.S.
Street of mailing address::	1101 Opaca Court
City of mailing address::	Crownsville
State or Province of mailing address::	MD
Country of mailing address::	U.S.
Postal or Zip Code of mailing address::	21032

Applicant Authority Type	Inventor **4**
Primary Citizenship Country	U.S.
Status	Full Capacity
Given Name	Michael
Middle Name	
Family Name	Williamson
Name Suffix	
City of Residence	South Riding
State or Province of Residence	VA
Country of Residence	U.S.
Street of Mailing Address	26203 Ocala Circle
City of Mailing Address	South Riding
State or Province of Mailing Address	VA
Country of Mailing Address	U.S.
Postal or Zip Code of Mailing Address	20152

Correspondence Information

Correspondence Customer Number::	23630

Representative Information

Representative Customer Number::	23630

Domestic Priority Information

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
This application	is a continuation of	10/714,849	November 18, 2003
10/714,849	is a continuation of	09/558,210	April 26, 2000
09/558,210	Is a continuation-in-part of	09/504,783	February 15, 2000
09/504,783	Is a continuation-in-part of	09/429,643	October 29, 1999
09/429,643	Claims the benefit under 35 U.S.C. 119(e) to	60/106,261	October 30, 1998
09/429,643	Claims the benefit under 35 U.S.C. 119(e) to	60/137,704	June 7, 1999

Foreign Priority Information

Country::	Application number::	Filing Date::	Priority Claimed::

Assignee Information

Assignee Name::	VirnetX, Inc.
Street of mailing address::	5615 Scotts Valley Drive, Suite 110
City of mailing address::	Scotts Valley
State or Province of mailing address::	CA
Country of mailing address::	U.S.
Postal or Zip Code of mailing address::	95066

Attorney Docket No. 077580-0063 (VRNK-1CP3CN2)

AN AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority from and is a continuation of a co-pending U.S. application serial number 10/714,849, filed November 18, 2003, which is a continuation of U.S. application serial number 09/558,210, filed April 26, 2000, now abandoned, which is a continuation-in-part of previously-filed U.S. application serial number 09/504,783, filed on February 15, 2000, now U.S. Patent No. 6,502,135, issued December 31, 2002, which claims priority from and is a continuation-in-part patent application of previously-filed U.S. application serial number 09/429,643, filed on October 29, 1999, now U.S. Patent No. 7,010,604, issued March 07, 2006. The subject matter of U.S. application serial number 09/429,643, which is bodily incorporated herein, derives from provisional U.S. application numbers 60/106,261 (filed October 30, 1998) and 60/137,704 (filed June 7, 1999). The present application is also related to U.S. application serial number 09/558,209, filed April 26, 2000, now abandoned, and which is incorporated by reference herein.

BACKGROUND OF THE INVENTION

[0002] A tremendous variety of methods have been proposed and implemented to provide security and anonymity for communications over the Internet. The variety stems, in part, from the different needs of different Internet users. A basic heuristic framework to aid in discussing these different security techniques is illustrated in FIG. 1. Two terminals, an originating terminal 100 and a destination terminal 110 are in communication over the Internet. It is desired for the communications to be secure, that is, immune to eavesdropping. For example, terminal 100 may transmit secret information to terminal 110 over the Internet 107. Also, it may be desired to prevent an eavesdropper from discovering that terminal 100 is in communication with terminal 110. For example, if terminal 100 is a user and terminal 110 hosts a web site, terminal 100's user may not want anyone in the intervening networks to know what web sites he is "visiting." Anonymity would thus be an issue, for example, for companies that want to keep their market research interests private and thus would prefer to prevent outsiders from knowing which web- sites or other Internet resources they are "visiting." These two security issues may be called data security and anonymity, respectively.

[0003] Data security is usually tackled using some form of data encryption. An encryption key 48 is known at both the originating and terminating terminals 100 and 110. The keys may be private and public at the originating and destination terminals 100 and 110, respectively or they may be symmetrical keys (the same key is used by both parties to encrypt and decrypt). Many encryption methods are known and usable in this context.

[0004] To hide traffic from a local administrator or ISP, a user can employ a local proxy server in communicating over an encrypted channel with an outside proxy such that the local administrator or ISP only sees the encrypted traffic. Proxy servers prevent destination servers from determining the identities of the originating clients. This system employs an intermediate server interposed between client and destination server. The destination server sees only the Internet Protocol (IP) address of the proxy server and not the originating client. The target server only sees the address of the outside proxy. This scheme relies on a trusted outside proxy server. Also, proxy schemes are vulnerable to traffic analysis methods of determining identities of transmitters and receivers. Another important limitation of proxy servers is that the server knows the identities of both calling and called parties. In many instances, an originating terminal, such as terminal A, would prefer to keep its identity concealed from the proxy, for example, if the proxy server is provided by an Internet service provider (ISP).

[0005] To defeat traffic analysis, a scheme called Chaum's mixes employs a proxy server that transmits and receives fixed length messages, including dummy messages. Multiple originating terminals are connected through a mix (a server) to multiple target servers. It is difficult to tell which of the originating terminals are communicating to which of the connected target servers, and the dummy messages confuse eavesdroppers' efforts to detect communicating pairs by analyzing traffic. A drawback is that there is a risk that the mix server could be compromised. One way to deal with this risk is to spread the trust among multiple mixes. If one mix is compromised, the identities of the originating and target terminals may remain concealed. This strategy requires a number of alternative mixes so that the intermediate servers interposed between the originating and target terminals are not determinable except by compromising more than one mix. The strategy wraps the message with multiple layers of encrypted addresses. The first mix in a sequence can decrypt only the outer layer of the message to reveal the next destination mix in sequence. The second mix can decrypt the message to reveal the next mix and so on. The target server receives the message and, optionally, a multi-layer encrypted payload containing return information to send data back in the same fashion. The only way to defeat such a mix scheme is to collude among mixes. If the packets are all fixed-length and intermixed with dummy packets, there is no way to do any kind of traffic analysis.

[0006] Still another anonymity technique, called ‘crowds,’ protects the identity of the originating terminal from the intermediate proxies by providing that originating terminals belong to groups of proxies called crowds. The crowd proxies are interposed between originating and target terminals. Each proxy through which the message is sent is randomly chosen by an upstream proxy. Each intermediate proxy can send the message either to another randomly chosen proxy in the “crowd” or to the destination. Thus, even crowd members cannot determine if a preceding proxy is the originator of the message or if it was simply passed from another proxy.

[0007] ZKS (Zero-Knowledge Systems) Anonymous IP Protocol allows users to select up to any of five different pseudonyms, while desktop software encrypts outgoing traffic and wraps it in User Datagram Protocol (UDP) packets. The first server in a 2+-hop system gets the UDP packets, strips off one layer of encryption to add another, then sends the traffic to the next server, which strips off yet another layer of encryption and adds a new one. The user is permitted to control the number of hops. At the final server, traffic is decrypted with an untraceable IP address. The technique is called onion-routing. This method can be defeated using traffic analysis. For a simple example, bursts of packets from a user during low-duty periods can reveal the identities of sender and receiver.

[0008] Firewalls attempt to protect LANs from unauthorized access and hostile exploitation or damage to computers connected to the LAN. Firewalls provide a server through which all access to the LAN must pass. Firewalls are centralized systems that require administrative overhead to maintain. They can be compromised by virtual-machine applications (“applets”). They instill a false sense of security that leads to security breaches for example by users sending sensitive information to servers outside the firewall or encouraging use of modems to sidestep the firewall security. Firewalls are not useful for distributed systems such as business travelers, extranets, small teams, etc.

SUMMARY OF THE INVENTION

[0009] A secure mechanism for communicating over the internet, including a protocol referred to as the Tunneled Agile Routing Protocol (TARP), uses a unique two-layer encryption format and special TARP routers. TARP routers are similar in function to regular IP routers. Each TARP router has one or more IP addresses and uses normal IP protocol to send IP packet messages ("packets" or "datagrams"). The IP packets exchanged between TARP terminals via TARP routers are actually encrypted packets whose true destination address is concealed except to TARP routers and servers. The normal or "clear" or "outside" IP header attached to TARP IP packets contains only the address of a next hop router or destination server. That is, instead of indicating a final destination in the destination field of the IP header, the TARP packet's IP header always points to a next-hop in a series of TARP router hops, or to the final destination. This means there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet since the destination could always be next-hop TARP router as well as the final destination.

[0010] Each TARP packet's true destination is concealed behind a layer of encryption generated using a link key. The link key is the encryption key used for encrypted communication between the hops intervening between an originating TARP terminal and a destination TARP terminal. Each TARP router can remove the outer layer of encryption to reveal the destination router for each TARP packet. To identify the link key needed to decrypt the outer layer of encryption of a TARP packet, a receiving TARP or routing terminal may identify the transmitting terminal by the sender/receiver IP numbers in the cleartext IP header.

[0011] Once the outer layer of encryption is removed, the TARP router determines the final destination. Each TARP packet 140 undergoes a minimum number of hops to help foil traffic analysis. The hops may be chosen at random or by a fixed value. As a result, each TARP packet may make random trips among a number of geographically disparate routers before reaching its destination. Each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined. This feature is called *agile routing*. The fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. The associated advantages have to do with the inner layer of encryption discussed below. Agile routing is combined with another feature that furthers this purpose; a feature that ensures that any message is broken into multiple packets.

[0012] The IP address of a TARP router can be changed, a feature called *IP agility*. Each TARP router, independently or under direction from another TARP terminal or router, can change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs.

[0013] The message payload is hidden behind an inner layer of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the intervening TARP routers. The session key is used to decrypt the payloads of the TARP packets permitting the data stream to be reconstructed.

[0014] Communication may be made private using link and session keys, which in turn may be shared and used according to any desired method. For example, public/private keys or symmetric keys may be used.

[0015] To transmit a data stream, a TARP originating terminal constructs a series of TARP packets from a series of IP packets generated by a network (IP) layer process. (Note that the terms "network layer," "data link layer," "application layer," etc. used in this specification correspond to the Open Systems Interconnection (OSI) network terminology.) The payloads of these packets are assembled into a block and chain-block encrypted using the session key. This assumes, of course, that all the IP packets are destined for the same TARP terminal. The block is then interleaved and the interleaved encrypted block is broken into a series of payloads, one for each TARP packet to be generated. Special TARP headers IP_T are then added to each payload using the IP headers from the data stream packets. The TARP headers can be identical to normal IP headers or customized in some way. They should contain a formula or data for deinterleaving the data at the destination TARP terminal, a time-to-live (TTL) parameter to indicate the number of hops still to be executed, a data type identifier which indicates whether the payload contains, for example, TCP or UDP data, the sender's TARP address, the destination TARP address, and an indicator as to whether the packet contains real or decoy data or a formula for filtering out decoy data if decoy data is spread in some way through the TARP payload data.

[0016] Note that although chain-block encryption is discussed here with reference to the session key, any encryption method may be used. Preferably, as in chain block encryption, a method should be used that makes unauthorized decryption difficult without an entire result of the encryption process. Thus, by separating the encrypted block among multiple packets and making it difficult for an interloper to obtain access to all of such packets, the contents of the communications are provided an extra layer of security.

[0017] Decoy or dummy data can be added to a stream to help foil traffic analysis by reducing the peak-to-average network load. It may he desirable to provide the TARP process with an ability to respond to the time of day or other criteria to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints.

[0018] Dummy data also helps to break the data into a larger number of inconspicuously-sized packets permitting the interleave window size to be increased while maintaining a reasonable size for each packet. (The packet size can be a single standard size or selected from a fixed range of sizes.) One primary reason for desiring for each message to be broken into multiple packets is apparent if a chain block encryption scheme is used to form the first encryption layer prior to interleaving. A single block encryption may be applied to a portion, or entirety, of a message, and that portion or entirety then interleaved into a number of separate packets. Considering the agile IP routing of the packets, and the attendant difficulty of reconstructing an entire sequence of packets to form a single block-encrypted message element, decoy packets can significantly increase the difficulty of reconstructing an entire data stream.

[0019] The above scheme may he implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Because the encryption system described above is insertable between the data link and network layers, the processes involved in supporting the encrypted communication may be completely transparent to processes at the IP (network) layer and above. The TARP processes may also be completely transparent to the data link layer processes as well. Thus, no operations at or above the Network layer, or at or below the data link layer, are affected by the insertion of the TARP stack. This provides additional security to all processes at or above the network layer, since the difficulty of unauthorized penetration of the network layer (by, for example, a hacker) is increased substantially. Even newly developed servers running at the session layer leave all processes below the session layer vulnerable to attack. Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over the Internet without any compromise in security.

[0020] IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of "attacks." The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing.

[0021] As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicating that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. In addition, it may create a subprocess that maintains the original IP address and continues interacting with the attacker in some manner.

[0022] Decoy packets may be generated by each TARP terminal on some basis determined by an algorithm. For example, the algorithm may be a random one which calls for the generation of a packet on a random basis when the terminal is idle. Alternatively, the algorithm may be responsive to time of day or detection of low traffic to generate more decoy packets during low traffic times. Note that packets are preferably generated in groups, rather than one by one, the groups being sized to simulate real messages. In addition, so that decoy packets may be inserted in normal TARP message streams, the background loop may have a latch that makes it more likely to insert decoy packets when a message stream is being received. Alternatively, if a large number of decoy packets is received along with regular TARP packets, the algorithm may increase the rate of dropping of decoy packets rather than forwarding them. The result of dropping and generating decoy packets in this way is to make the apparent incoming message size different from the apparent outgoing message size to help foil traffic analysis.

[0023] In various other embodiments of the invention, a scalable version of the system may be constructed in which a plurality of IP addresses are preassigned to each pair of communicating nodes in the network. Each pair of nodes agrees upon an algorithm for "hopping" between IP addresses (both sending and receiving), such that an eavesdropper sees apparently continuously random IP address pairs (source and destination) for packets transmitted between the pair. Overlapping or "reusable" IP addresses may be allocated to different users on the same subnet, since each node merely verifies that a particular packet includes a valid source/destination pair from the agreed-upon algorithm. Source/destination pairs are preferably not reused between any two nodes during any given end-to-end session, though limited IP block sizes or lengthy sessions might require it.

[0024] Further improvements described in this continuation-in-part application include: (1) a load balancer that distributes packets across different transmission paths according to transmission path quality; (2) a DNS proxy server that transparently creates a virtual private network in response to a domain name inquiry; (3) a large-to-small link bandwidth management feature that prevents denial-of service attacks at system chokepoints; (4) a traffic limiter that regulates incoming packets by limiting the rate at which a transmitter can be synchronized with a receiver; and (5) a signaling synchronizer that allows a large number of nodes to communicate with a central node by partitioning the communication function between two separate entities.

[0025] The present invention provides key technologies for implementing a secure virtual Internet by using a new agile network protocol that is built on top of the existing Internet protocol (IP). The secure virtual Internet works over the existing Internet infrastructure, and interfaces with client applications the same way as the existing Internet. The key technologies provided by the present invention that support the secure virtual Internet include a "one-click" and "no-click" technique to become part of the secure virtual Internet, a secure domain name service (SDNS) for the secure virtual Internet, and a new approach for interfacing specific client applications onto the secure virtual Internet. According to the invention, the secure domain name service interfaces with existing applications, in addition to providing a way to register and serve domain names and addresses.

[0026] According to one aspect of the present invention, a user can conveniently establish a VPN using a "one-click" or a "no-click" technique without being required to enter user identification information, a password and/or an encryption key for establishing a VPN. The advantages of the present invention are provided by a method for establishing a secure communication link between a first computer and a second computer over a computer network, such as the Internet. In one embodiment, a secure communication mode is enabled at a first computer without a user entering any cryptographic information for establishing the secure communication mode of communication, preferably by merely selecting an icon displayed on the first computer. Alternatively, the secure communication mode of communication can be enabled by entering a command into the first computer. Then, a secure communication link is established between the first computer and a second computer over a computer network based on the enabled secure communication mode of communication. According to the invention, it is determined whether a secure communication software module is stored on the first computer in response to the step of enabling the secure communication mode of communication. A predetermined computer network address is then accessed for loading the secure communication software module when the software module is not stored on the first computer. Subsequently, the proxy software module is stored in the first computer. The secure communication link is a virtual private network communication link over the computer network. Preferably, the virtual private network can be based on inserting into each data packet one or more data values that vary according to a pseudo-random sequence. Alternatively, the virtual private network can be based on a computer network address hopping regime that is used to pseudorandomly change computer network addresses or other data values in packets transmitted between the first computer and the second computer, such that the second computer compares the data values in each data packet transmitted between the first computer and the second computer to a moving window of valid values. Yet another alternative provides that the virtual private network can be based on a comparison between a discriminator field in each data packet to a table of valid discriminator fields maintained for the first computer.

[0027] According to another aspect of the invention, a command is entered to define a setup parameter associated with the secure communication link mode of communication. Consequently, the secure communication mode is automatically established when a communication link is established over the computer network.

[0028] The present invention also provides a computer system having a communication link to a computer network, and a display showing a hyperlink for establishing a virtual private network through the computer network. When the hyperlink for establishing the virtual private network is selected, a virtual private network is established over the computer network. A non-standard top-level domain name is then sent over the virtual private network communication to a predetermined computer network address, such as a computer network address for a secure domain name service (SDNS).

[0029] The present invention provides a domain name service that provides secure computer network addresses for secure, non-standard top-level domain names. The advantages of the present invention are provided by a secure domain name service for a computer network that includes a portal connected to a computer network, such as the Internet, and a domain name database connected to the computer network through the portal. According to the invention, the portal authenticates a query for a secure computer network address, and the domain name database stores secure computer network addresses for the computer network. Each secure computer network address is based on a non-standard top-level domain name, such as .scom, .sorg, .snet, .snet, .sedu, .smil and .sint.

[0030] The present invention provides a way to encapsulate existing application network traffic at the application layer of a client computer so that the client application can securely communicate with a server protected by an agile network protocol. The advantages of the present invention are provided by a method for communicating using a private communication link between a client computer and a server computer over a computer network, such as the Internet. According to the invention, an information packet is sent from the client computer to the server computer over the computer network. The information packet contains data that is inserted into the payload portion of the packet at the application layer of the client computer and is used for forming a virtual private connection between the client computer and the server computer. The modified information packet can be sent through a firewall before being sent over the computer network to the server computer and by working on top of existing protocols (i.e., UDP, ICMP and TCP), the present invention more easily penetrates the firewall. The information packet is received at a kernel layer of an operating system on the server side. It is then determined at the kernel layer of the operating system on the host computer whether the information packet contains the data that is used for forming the virtual private connection. The server side replies by sending an information packet to the client computer that has been modified at the kernel layer to containing virtual private connection information in the payload portion of the reply information packet. Preferably, the information packet from the client computer and the reply information packet from the server side are each a UDP protocol information packet. Alternative, both information packets could be a TCP/IP protocol information packet, or an ICMP protocol information packet.

BRIEF DESCRIPTION OF THE DRAWINGS

[0031] FIG. 1 is an illustration of secure communications over the Internet according to a prior art embodiment.

[0032] FIG. 2 is an illustration of secure communications over the Internet according to a an embodiment of the invention.

[0033] FIG. 3a is an illustration of a process of forming a tunneled IP packet according to an embodiment of the invention.

[0034] FIG. 3b is an illustration of a process of forming a tunneled IP packet according to another embodiment of the invention.

[0035] FIG. 4 is an illustration of an OSI layer location of processes that may be used to implement the invention.

[0036] FIG. 5 is a flow chart illustrating a process for routing a tunneled packet according to an embodiment of the invention.

[0037] FIG. 6 is a flow chart illustrating a process for forming a tunneled packet according to an embodiment of the invention.

[0038] FIG. 7 is a flow chart illustrating a process for receiving a tunneled packet according to an embodiment of the invention.

[0039] FIG. 8 shows how a secure session is established and synchronized between a client and a TARP router.

[0040] FIG, 9 shows an IP address hopping scheme between a client computer and TARP router using transmit and receive tables in each computer.

[0041] FIG. 10 shows physical link redundancy among three Internet Service Providers (ISPs) and a client computer.

[0042] FIG. 11 shows how multiple IP packets can be embedded into a single “frame” such as an Ethernet frame, and further shows the use of a discriminator field to camouflage true packet recipients.

[0043] FIG. 12A shows a system that employs hopped hardware addresses, hopped IP addresses, and hopped discriminator fields.

[0044] FIG. 12B shows several different approaches for hopping hardware addresses, IP addresses, and discriminator fields in combination.

[0045] FIG. 13 shows a technique for automatically re-establishing synchronization between sender and receiver through the use of a partially public sync value.

[0046] FIG. 14 shows a "checkpoint" scheme for regaining synchronization between a sender and recipient.

[0047] FIG. 15 shows further details of the checkpoint scheme of FIG. 14.

[0048] FIG. 16 shows how two addresses can be decomposed into a plurality of segments for comparison with presence vectors.

[0049] FIG. 17 shows a storage array for a receiver's active addresses.

[0050] FIG. 18 shows the receiver's storage array after receiving a sync request.

[0051] FIG. 19 shows the receiver's storage array after new addresses have been generated. FIG. 20 shows a system employing distributed transmission paths.

[0052] FIG, 21 shows a plurality of link transmission tables that can be used to route packets in the system of FIG. 20.

[0053] FIG. 22A shows a flowchart for adjusting weight value distributions associated with a plurality of transmission links.

[0054] FIG. 22B shows a flowchart for setting a weight value to zero if a transmitter turns off.

[0055] FIG. 23 shows a system employing distributed transmission paths with adjusted weight value distributions for each path.

[0056] FIG. 24 shows an example using the system of FIG. 23.

[0057] FIG. 25 shows a conventional domain-name look-up service.

[0058] FIG. 26 shows a system employing a DNS proxy server with transparent VPN creation.

[0059] FIG. 27 shows steps that can be carried out to implement transparent VPN creation based on a DNS look-up function.

[0060] FIG. 28 shows a system including a link guard function that prevents packet overloading on a low-bandwidth link LOW BW.

[0061] FIG. 29 shows one embodiment of a system employing the principles of FIG. 28.

[0062] FIG. 30 shows a system that regulates packet transmission rates by throttling the rate at which synchronizations are performed.

[0063] FIG. 31 shows a signaling server 3101 and a transport server 3102 used to establish a VPN with a client computer.

[0064] FIG. 32 shows message flows relating to synchronization protocols of FIG. 31.

[0065] FIG. 33 shows a system block diagram of a computer network in which the "one-click" secure communication link of the present invention is suitable for use.

[0066] FIG. 34 shows a flow diagram for installing and establishing a "one-click" secure communication link over a computer network according to the present invention.

[0067] FIG. 35 shows a flow diagram for registering a secure domain name according to the present invention.

[0068] FIG. 36 shows a system block diagram of a computer network in which a private connection according to the present invention can be configured to more easily traverse a firewall between two computer networks.

[0069] FIG. 37 shows a flow diagram for establishing a virtual private connection that is encapsulated using an existing network protocol.

DETAILED DESCRIPTION OF THE INVENTION

[0070] Referring to FIG. 2, a secure mechanism for communicating over the internet employs a number of special routers or servers, called TARP routers 122-127 that are similar to regular IP routers 128-132 in that each has one or more IP addresses and uses normal IP protocol to send normal-looking IP packet messages, called TARP packets 140. TARP packets 140 are identical to normal IP packet messages that are routed by regular IP routers 128-132 because each TARP packet 140 contains a destination address as in a normal IP packet. However, instead of indicating a final destination in the destination field of the IP header, the TARP packet's 140 IP header always points to a next-hop in a series of TARP router hops, or the final destination, TARP terminal 110. Because the header of the TARP packet contains only the next-hop destination, there is no overt indication from an intercepted TARP packet of the true destination of the TARP packet 140 since the destination could always be the next-hop TARP router as well as the final destination, TARP terminal 110.

[0071] Each TARP packet's true destination is concealed behind an outer layer of encryption generated using a link key 146. The link key 146 is the encryption key used for encrypted communication between the end points (TARP terminals or TARP routers) of a single link in the chain of hops connecting the originating TARP terminal 100 and the destination TARP terminal 110. Each TARP router 122-127, using the link key 146 it uses to communicate with the previous hop in a chain, can use the link key to reveal the true destination of a TARP packet. To identify the link key needed to decrypt the outer layer of encryption of a TARP packet, a receiving TARP or routing terminal may identify the transmitting terminal (which may indicate the link key used) by the sender field of the clear IP header. Alternatively, this identity may be hidden behind another layer of encryption in available bits in the clear IP header. Each TARP router, upon receiving a TARP message, determines if the message is a TARP message by using authentication data in the TARP packet. This could be recorded in available bytes in the TARP packet's IP header. Alternatively, TARP packets could be authenticated by attempting to decrypt using the link key 146 and determining if the results are as expected. The former may have computational advantages because it does not involve a decryption process.

[0072] Once the outer layer of decryption is completed by a TARP router 122-127, the TARP router determines the final destination. The system is preferably designed to cause each TARP packet 140 to undergo a minimum number of hops to help foil traffic analysis. The time to live counter in the IP header of the TARP message may be used to indicate a number of TARP router hops yet to be completed. Each TARP router then would decrement the counter and determine from that whether it should forward the TARP packet 140 to another TARP router 122-127 or to the destination TARP terminal 110. If the time to live counter is zero or below zero after decrementing, for an example of usage, the TARP router receiving the TARP packet 140 may forward the TARP packet 140 to the destination TARP terminal 110. If the time to live counter is above zero after decrementing, for an example of usage, the TARP router receiving the TARP packet 140 may forward the TARP packet 140 to a TARP router 122-127 that the current TARP terminal chooses at random. As a result, each TARP packet 140 is routed through some minimum number of hops of TARP routers 122-127 which are chosen at random.

[0073] Thus, each TARP packet, irrespective of the traditional factors determining traffic in the Internet, makes random trips among a number of geographically disparate routers before reaching its destination and each trip is highly likely to be different for each packet composing a given message because each trip is independently randomly determined as described above. This feature is called *agile routing*. For reasons that will become clear shortly, the fact that different packets take different routes provides distinct advantages by making it difficult for an interloper to obtain all the packets forming an entire multi-packet message. Agile routing is combined with another feature that furthers this purpose, a feature that ensures that any message is broken into multiple packets.

[0074] A TARP router receives a TARP packet when an IP address used by the TARP router coincides with the IP address in the TARP packet's IP header IPc. The IP address of a TARP router, however, may not remain constant. To avoid and manage attacks, each TARP router, independently or under direction from another TARP terminal or router, may change its IP address. A separate, unchangeable identifier or address is also defined. This address, called the TARP address, is known only to TARP routers and terminals and may be correlated at any time by a TARP router or a TARP terminal using a Lookup Table (LUT). When a TARP router or terminal changes its IP address, it updates the other TARP routers and terminals which in turn update their respective LUTs. In reality, whenever a TARP router looks up the address of a destination in the encrypted header, it must convert a TARP address to a real IP address using its LUT.

[0075] While every TARP router receiving a TARP packet has the ability to determine the packet's final destination, the message payload is embedded behind an inner layer of encryption in the TARP packet that can only be unlocked using a session key. The session key is not available to any of the TARP routers 122-127 intervening between the originating 100 and destination 110 TARP terminals. The session key is used to decrypt the payloads of the TARP packets 140 permitting an entire message to be reconstructed.

[0076] In one embodiment, communication may be made private using link and session keys, which in turn may be shared and used according any desired method. For example, a public key or symmetric keys may be communicated between link or session endpoints using a public key method. Any of a variety of other mechanisms for securing data to ensure that only authorized computers can have access to the private information in the TARP packets 140 may be used as desired.

[0077] Referring to FIG. 3a, to construct a series of TARP packets, a data stream 300 of IP packets 207a, 207b, 207c, etc., such series of packets being formed by a network (IP) layer process, is broken into a series of small sized segments. In the present example, equal-sized segments 1-9 are defined and used to construct a set of interleaved data packets A, B, and C. Here it is assumed that the number of interleaved packets A, B, and C formed is three and that the number of IP packets 207a-207c used to form the three interleaved packets A, B, and C is exactly three. Of course, the number of IP packets spread over a group of interleaved packets may be any convenient number as may be the number of interleaved packets over which the incoming data stream is spread. The latter, the number of interleaved packets over which the data stream is spread, is called the *interleave window*.

[0078] To create a packet, the transmitting software interleaves the normal IP packets 207a *et. seq, to* form a new set of interleaved payload data 320. This payload data 320 is then encrypted using a session key to form a set of session-key-encrypted payload data 330, each of which, A, B, and C, will form the payload of a TARP packet. Using the IP header data, from the original packets 207a-207c, new TARP headers IPT are formed. The TARP headers IPT can be identical to normal IP headers or customized in some way. In a preferred embodiment, the TARP headers IPT are IP headers with added data providing the following information required for routing and reconstruction of messages, some of which data is ordinarily, or capable of being, contained in normal IP headers:

1. A window sequence number — an identifier that indicates where the packet belongs in the original message sequence.

2. An interleave sequence number — an identifier that indicates the interleaving sequence used to form the packet so that the packet can be deinterleaved along with other packets in the interleave window.

3. A time-to-live (TTL) datum — indicates the number of TARP-router-hops to be executed before the packet reaches its destination. Note that the TTL parameter may provide a

datum to be used in a probabilistic formula for determining whether to route the packet to the destination or to another hop.

4. Data type identifier — indicates whether the payload contains, for example, TCP or UDP data.

5. Sender's address — indicates the sender's address in the TARP network.

6. Destination address — indicates the destination terminal's address in the TARP network.

7. Decoy/Real — an indicator of whether the packet contains real message data or dummy decoy data or a combination.

[0079] Obviously, the packets going into a single interleave window must include only packets with a common destination. Thus, it is assumed in the depicted example that the IP headers of IP packets 207a-207c all contain the same destination address or at least will be received by the same terminal so that they can be deinterleaved. Note that dummy or decoy data or packets can be added to form a larger interleave window than would otherwise be required by the size of a given message. Decoy or dummy data can be added to a stream to help foil traffic analysis by leveling the load on the network. Thus, it may be desirable to provide the TARP process with an ability to respond to the time of day or other criteria to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints.

[0080] Dummy data also helps to break the data into a larger number of inconspicuously-sized packets permitting the interleave window size to be increased while maintaining a reasonable size for each packet. (The packet size can be a single standard size or selected from a fixed range of sizes.) One primary reason for desiring for each message to be broken into multiple packets is apparent if a chain block encryption scheme is used to form the first encryption layer prior to interleaving. A single block encryption may be applied to a portion, or the entirety, of a message, and that portion or entirety then interleaved into a number of separate packets.

[0081] Referring to FIG. 3b, in an alternative mode of TARP packet construction, a series of IP packets are accumulated to make up a predefined interleave window. The payloads of the packets are used to construct a single block 520 for chain block encryption using the session key. The payloads used to form the block are presumed to be destined for the same terminal. The block size may coincide with the interleave window as depicted in the example embodiment of FIG. 3b. After encryption, the encrypted block is broken into separate payloads and segments which are interleaved as in the embodiment of Fig 3a. The resulting interleaved packets A, B, and C, are then packaged as TARP packets with TARP headers as in the Example of FIG. 3a. The remaining process is as shown in, and discussed with reference to, FIG. 3a.

[0082] Once the TARP packets 340 are formed, each entire TARP packet 340, including the TARP header IPT, is encrypted using the link key for communication with the first-hop-TARP router. The first hop TARP router is randomly chosen. A final unencrypted IP header IPc is added to each encrypted TARP packet 340 to form a normal IP packet 360 that can be transmitted to a TARP router. Note that the process of constructing the TARP packet 360 does not have to be done in stages as described. The above description is just a useful heuristic for describing the final product, namely, the TARP packet.

[0083] Note that, TARP header IP_T could be a completely custom header configuration with no similarity to a normal IP header except that it contain the information identified above. This is so since this header is interpreted by only TARP routers.

[0084] The above scheme may be implemented entirely by processes operating between the data link layer and the network layer of each server or terminal participating in the TARP system. Referring to FIG. 4, a TARP transceiver 405 can be an originating terminal 100, a destination terminal 110, or a TARP router 122-127. In each TARP Transceiver 405, a transmitting process is generated to receive normal packets from the Network (IP) layer and generate TARP packets for communication over the network. A receiving process is generated to receive normal IP packets containing TARP packets and generate from these normal IP packets which are "passed up" to the Network (IP) layer. Note that where the TARP Transceiver 405 is a router, the received TARP packets 140 are not processed into a stream of IP packets 415 because they need only be authenticated as proper TARP packets and then passed to another TARP router or a TARP destination terminal 110. The intervening process, a "TARP Layer" 420, could be combined with either the data link layer 430 or the Network layer 410. In either case, it would intervene between the data link layer 430 so that the process would receive regular IP packets containing embedded TARP packets and "hand up" a series of reassembled IP packets to the

Network layer 410. As an example of combining the TARP layer 420 with the data link layer 430, a program may augment the normal processes running a communications card, for example, an Ethernet card. Alternatively, the TARP layer processes may form part of a dynamically loadable module that is loaded and executed to support communications between the network and data link layers.

[0085] Because the encryption system described above can be inserted between the data link and network layers, the processes involved in supporting the encrypted communication may be completely transparent to processes at the IP (network) layer and above. The TARP processes may also be completely transparent to the data link layer processes as well. Thus, no operations at or above the network layer, or at or below the data link layer, are affected by the insertion of the TARP stack. This provides additional security to all processes at or above the network layer, since the difficulty of unauthorized penetration of the network layer (by, for example, a hacker) is increased substantially. Even newly developed servers running at the session layer leave all processes below the session layer vulnerable to attack. Note that in this architecture, security is distributed. That is, notebook computers used by executives on the road, for example, can communicate over the Internet without any compromise in security.

[0086] Note that IP address changes made by TARP terminals and routers can be done at regular intervals, at random intervals, or upon detection of "attacks." The variation of IP addresses hinders traffic analysis that might reveal which computers are communicating, and also provides a degree of immunity from attack. The level of immunity from attack is roughly proportional to the rate at which the IP address of the host is changing.

[0087] As mentioned, IP addresses may be changed in response to attacks. An attack may be revealed, for example, by a regular series of messages indicates that a router is being probed in some way. Upon detection of an attack, the TARP layer process may respond to this event by changing its IP address. To accomplish this, the TARP process will construct a TARP-formatted message, in the style of Internet Control Message Protocol (ICMP) datagrarns as an example; this message will contain the machine's TARP address, its previous IP address, and its new IP address. The TARP layer will transmit this packet to at least one known TARP router; then upon receipt and validation of the message, the TARP router will update its LUT with the new IP address for the stated TARP address. The TARP router will then format a similar message, and broadcast it to the other TARP routers so that they may update their LUTs. Since the total number of TARP routers on any given subnet is expected to be relatively small, this process of updating the LUTs should be relatively fast. It may not, however, work as well when there is a relatively large number of TARP routers and/or a relatively large number of clients; this has motivated a refinement of this architecture to provide scalability; this refinement has led to a second embodiment, which is discussed below.

[0088] Upon detection of an attack, the TARP process may also create a subprocess that maintains the original IP address and continues interacting with the attacker. The latter may provide an opportunity to trace the attacker or study the attacker's methods (called "fishbowling" drawing upon the analogy of a small fish in a fish bowl that "thinks" it is in the ocean but is actually under captive observation). A history of the communication between the attacker and the abandoned (fishbowled) IP address can be recorded or transmitted for human analysis or further synthesized for purposes of responding in some way.

[0089] As mentioned above, decoy or dummy data or packets can be added to outgoing data streams by TARP terminals or routers. In addition to making it convenient to spread data over a larger number of separate packets, such decoy packets can also help to level the load on inactive portions of the Internet to help foil traffic analysis efforts.

[0090] Decoy packets may be generated by each TARP terminal 100, 110 or each router 122-127 on some basis determined by an algorithm. For example, the algorithm may be a random one which calls for the generation of a packet on a random basis when the terminal is idle. Alternatively, the algorithm may be responsive to time of day or detection of low traffic to generate more decoy packets during low traffic times. Note that packets are preferably generated in groups, rather than one by one, the groups being sized to simulate real messages. In addition, so that decoy packets may be inserted in normal TARP message streams, the background loop may have a latch that makes it more likely to insert decoy packets when a message stream is being received. That is, when a series of messages are received, the decoy packet generation rate may be increased. Alternatively, if a large number of decoy packets is received along with regular TARP packets, the algorithm may increase the rate of dropping of decoy packets rather than forwarding them. The result of dropping and generating decoy packets in this way is to make the apparent incoming message size different from the apparent outgoing message size to help foil traffic analysis. The rate of reception of packets, decoy or otherwise, may be indicated to the decoy packet dropping and generating processes through perishable decoy and regular packet counters. (A perishable counter is one that resets or decrements its value in response to time so that it contains a high value when it is incremented in rapid succession and a small value when incremented either slowly or a small number of times in rapid succession.) Note that destination TARP terminal 110 may generate decoy packets equal in number and size to those TARP packets received to make it appear it is merely routing packets and is therefore not the destination terminal.

[0091] Referring to FIG. 5, the following particular steps may be employed in the above- described method for routing TARP packets.

- S0. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.
- S2. The TARP packet may be probed in some way to authenticate the packet before attempting to decrypt it using the link key. That is, the router may determine that the packet is an authentic TARP packet by performing a selected operation on some data included with the clear IP header attached to the encrypted TARP packet contained in the payload. This makes it possible to avoid performing decryption on packets that are not authentic TARP packets.
- S3. The TARP packet is decrypted to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.
- S4. If the packet is a decoy packet, the perishable decoy counter is incremented.
- S5. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the router may choose to throw it away. If the received packet is a decoy packet and it is determined that it should be thrown away (S6), control returns to step S0.
- S7. The TTL parameter of the TARP header is decremented and it is determined if the TTL parameter is greater than zero.
- S8. If the TTL parameter is greater than zero, a TARP address is randomly chosen from a list of TARP addresses maintained by the router and the link key and IP address corresponding

to that TARP address memorized for use in creating a new IP packet containing the TARP packet.

- S9. If the TTL parameter is zero or less, the link key and IP address corresponding to the TARP address of the destination are memorized for use in creating the new IP packet containing the TARP packet.
- S 10. The TARP packet is encrypted using the memorized link key.
- S 11. An IP header is added to the packet that contains the stored IP address, the encrypted TARP packet wrapped with an IP header, and the completed packet transmitted to the next hop or destination.

[0092] Referring to FIG. 6, the following particular steps may be employed in the above- described method for generating TARP packets.

- S20. A background loop operation applies an algorithm that determines the generation of decoy IP packets. The loop is interrupted when a data stream containing IP packets is received for transmission.
- S21. The received IP packets are grouped into a set consisting of messages with a constant IP destination address. The set is further broken down to coincide with a maximum size of an interleave window The set is encrypted, and interleaved into a set of payloads destined to become TARP packets.
- S22. The TARP address corresponding to the IP address is determined from a lookup table and stored to generate the TARP header. An initial TTL count is generated and stored in the header. The TTL count may be random with minimum and maximum values or it may be fixed or determined by some other parameter.
- S23. The window sequence numbers and interleave sequence numbers are recorded in the TARP headers of each packet.
- S24. One TARP router address is randomly chosen for each TARP packet and the IP address corresponding to it stored for use in the clear IP header. The link key corresponding to this router is identified and used to encrypt TARP packets containing interleaved and encrypted data and TARP headers.

- S25. A clear IP header with the first hop router's real IP address is generated and added to each of the encrypted TARP packets and the resulting packets.

[0093] Referring to FIG. 7, the following particular steps may be employed in the above- described method for receiving TARP packets.

- S40. A background loop operation is performed which applies an algorithm which determines the generation of decoy IP packets. The loop is interrupted when an encrypted TARP packet is received.
- S42. The TARP packet may be probed to authenticate the packet before attempting to decrypt it using the link key.
- S43. The TARP packet is decrypted with the appropriate link key to expose the destination TARP address and an indication of whether the packet is a decoy packet or part of a real message.
- S44. If the packet is a decoy packet, the perishable decoy counter is incremented.
- S45. Based on the decoy generation/dropping algorithm and the perishable decoy counter value, if the packet is a decoy packet, the receiver may choose to throw it away.
- S46. The TARP packets are cached until all packets forming an interleave window are received.
- S47. Once all packets of an interleave window are received, the packets are deinterleaved.
- S48. The packets block of combined packets defining the interleave window is then decrypted using the session key.
- S49. The decrypted block is then divided using the window sequence data and the IP_T headers are converted into normal IP_C headers. The window sequence numbers are integrated in the IP_C headers.
- S50. The packets are then handed up to the IP layer processes.

I . SCALABILITY ENHANCEMENTS

[0094] The IP agility feature described above relies on the ability to transmit IP address changes to all TARP routers. The embodiments including this feature will be referred to as "boutique" embodiments due to potential limitations in scaling these features up for a large network, such as the Internet. (The "boutique" embodiments would, however, be robust for use in smaller networks, such as small virtual private networks, for example). One problem with the boutique embodiments is that if IP address changes are to occur frequently, the message traffic required to update all routers sufficiently quickly creates a serious burden on the Internet when the TARP router and/or client population gets large. The bandwidth burden added to the networks, for example in ICMP packets, that would be used to update all the TARP routers could overwhelm the Internet for a large scale implementation that approached the scale of the Internet. In other words, the boutique system's scalability is limited.

[0095] A system can be constructed which trades some of the features of the above embodiments to provide the benefits of IP agility without the additional messaging burden. This is accomplished by IP address-hopping according to shared algorithms that govern IP addresses used between links participating in communications sessions between nodes such as TARP nodes. (Note that the IP hopping technique is also applicable to the boutique embodiment.) The IP agility feature discussed with respect to the boutique system can be modified so that it becomes decentralized under this scalable regime and governed by the above-described shared algorithm. Other features of the boutique system may be combined with this new type of IP-agility.

[0096] The new embodiment has the advantage of providing IP agility governed by a local algorithm and set of IP addresses exchanged by each communicating pair of nodes. This local governance is session-independent in that it may govern communications between a pair of nodes, irrespective of the session or end points being transferred between the directly communicating pair of nodes.

[0097] In the scalable embodiments, blocks of IP addresses are allocated to each node in the network. (This scalability will increase in the future, when Internet Protocol addresses are increased to 128-bit fields, vastly increasing the number of distinctly addressable nodes). Each node can thus use any of the IP addresses assigned to that node to communicate with other nodes in the network. Indeed, each pair of communicating nodes can use a plurality of source IP addresses and destination IP addresses for communicating with each other.

[0098] Each communicating pair of nodes in a chain participating in any session stores two blocks of IP addresses, called netblocks, and an algorithm and randomization seed for selecting, from each netblock, the next pair of source/destination IP addresses that will be used to transmit the next message. In other words, the algorithm governs the sequential selection of IP-address pairs, one sender and one receiver IP address, from each netblock. The combination of algorithm, seed, and netblock (IP address block) will be called a "hopblock." A router issues separate transmit and receive hopblocks to its clients. The send address and the receive address of the IP header of each outgoing packet sent by the client are filled with the send and receive IP addresses generated by the algorithm. The algorithm is "clocked" (indexed) by a counter so that each time a pair is used, the algorithm turns out a new transmit pair for the next packet to be sent.

[0099] The router's receive hopblock is identical to the client's transmit hopblock. The router uses the receive hopblock to predict what the send and receive IP address pair for the next expected packet from that client will be. Since packets can be received out of order, it is not possible for the router to predict with certainty what IP address pair will be on the next sequential packet. To account for this problem, the router generates a range of predictions encompassing the number of possible transmitted packet send/receive addresses, of which the next packet received could leap ahead. Thus, if there is a vanishingly small probability that a given packet will arrive at the router ahead of 5 packets transmitted by the client before the given packet, then the router can generate a series of 6 send/receive IP address pairs (or "hop window") to compare with the next received packet. When a packet is received, it is marked in the hop window as such, so that a second packet with the same IP address pair will be discarded. If an out-of-sequence packet does not arrive within a predetermined timeout period, it can be requested for retransmission or simply discarded from the receive table, depending upon the protocol in use for that communications session, or possibly by convention.

[00100] When the router receives the client's packet, it compares the send and receive IP addresses of the packet with the next N predicted send and receive IP address pairs and rejects the packet if it is not a member of this set. Received packets that do not have the predicted source/destination IP addresses falling with the window are rejected, thus thwarting possible hackers. (With the number of possible combinations, even a fairly large window would be hard to fall into at random.) If it is a member of this set, the router accepts the packet and processes it further. This link-based IP-hopping strategy, referred to as "IHOP," is a network element that stands on its own and is not necessarily accompanied by elements of the boutique system described above. If the routing agility feature described in connection with the boutique embodiment is combined with this link-based IP-hopping strategy, the router's next step would be to decrypt the TARP header to determine the destination TARP router for the packet and determine what should be the next hop for the packet. The TARP router would then forward the packet to a random TARP router or the destination TARP router with which the source TARP router has a link-based IP hopping communication established.

[00101] Figure 8 shows how a client computer 801 and a TARP router 811 can establish a secure session. When client 801 seeks to establish an IHOP session with TARP router 811, the client 801 sends "secure synchronization" request ("SSYN") packet 821 to the TARP router 811. This SYN packet 821 contains the client's 801 authentication token, and may be sent to the router 811 in an encrypted format. The source and destination IP numbers on the packet 821 are the client's 801 current fixed IP address, and a "known" fixed IP address for the router 811. (For security purposes, it may be desirable to reject any packets from outside of the local network that are destined for the router's known fixed IP address.) Upon receipt and validation of the client's 801 SSYN packet 821, the router 811 responds by sending an encrypted "secure synchronization acknowledgment" ("SSYN ACK") 822 to the client 801. This SSYN ACK 822 will contain the transmit and receive hopblocks that the client 801 will use when communicating with the TARP router 811. The client 801 will acknowledge the TARP router's 811 response packet 822 by generating an encrypted SSYN ACK ACK packet 823 which will be sent from the client's 801 fixed IP address and to the TARP router's 811 known fixed IP address. The client 801 will simultaneously generate a SSYN ACK ACK packet; this SSYN ACK packet, referred to as the Secure Session Initiation (SSI) packet 824, will be sent with the first {sender, receiver} IP pair in the client's transmit table 921 (FIG. 9), as specified in the transmit hopblock provided by the TARP router 811 in the SSYN ACK packet 822. The TARP router 811 will respond to the SSI packet 824 with an SSI ACK packet 825, which will be sent with the first {sender, receiver} IP pair in the TARP router's transmit table 923. Once these packets have been successfully exchanged, the secure communications session is established, and all further secure communications between the client 801 and the TARP router 811 will be conducted via this secure session, as long as synchronization is maintained. If synchronization is lost, then the client 801 and TARP router 802 may re-establish the secure session by the procedure outlined in Figure 8 and described above.

[00102] While the secure session is active, both the client 901 and TARP router 911 (FIG. 9) will maintain their respective transmit tables 921, 923 and receive tables 922, 924, as provided by the TARP router during session synchronization 822. It is important that the sequence of IP pairs in the client's transmit table 921 be identical to those in the TARP router's receive table 924; similarly, the sequence of IP pairs in the client's receive table 922 must be identical to those in the router's transmit table 923. This is required for the session synchronization to be maintained. The client 901 need maintain only one transmit table 921 and one receive table 922 during the course of the secure session. Each sequential packet sent by the client 901 will employ the next {send, receive} IP address pair in the transmit table, regardless of TCP or UDP session. The TARP router 911 will expect each packet arriving from the client 901 to bear the next IP address pair shown in its receive table.

[00103] Since packets can arrive out of order, however, the router 911 can maintain a "look ahead" buffer in its receive table, and will mark previously-received IP pairs as invalid for future packets; any future packet containing an IP pair that is in the look-ahead buffer but is marked as previously received will be discarded. Communications from the TARP router 911 to the client 901 are maintained in an identical manner; in particular, the router 911 will select the next IP address pair from its transmit table 923 when constructing a packet to send to the client 901, and the client 901 will maintain a look-ahead buffer of expected IP pairs on packets that it is receiving. Each TARP router will maintain separate pairs of transmit and receive tables for each client that is currently engaged in a secure session with or through that TARP router.

[00104] While clients receive their hopblocks from the first server linking them to the Internet, routers exchange hopblocks. When a router establishes a link-based IP-hopping communication regime with another router, each router of the pair exchanges its transmit hopblock. The transmit hopblock of each router becomes the receive hopblock of the other router. The communication between routers is governed as described by the example of a client sending a packet to the first router.

[00105] While the above strategy works fine in the IP milieu, many local networks that are connected to the Internet are Ethernet systems. In Ethernet, the IP addresses of the destination devices must be translated into hardware addresses, and vice versa, using known processes ("address resolution protocol," and "reverse address resolution protocol"). However, if the link- based IP-hopping strategy is employed, the correlation process would become explosive and burdensome. An alternative to the link-based IP hopping strategy may be employed within an Ethernet network. The solution is to provide that the node linking the Internet to the Ethernet (call it the border node) use the link-based 1P-hopping communication regime to communicate with nodes outside the Ethernet LAN. Within the Ethernet LAN, each TARP node would have a single IP address which would be addressed in the conventional way. Instead of comparing the {sender, receiver} IP address pairs to authenticate a packet, the intra-LAN TARP node would use one of the IP header extension fields to do so. Thus, the border node uses an algorithm shared by the intra-LAN TARP node to generate a symbol that is stored in the free field in the IP header, and the intra-LAN TARP node generates a range of symbols based on its prediction of the next expected packet to be received from that particular source IP address. The packet is rejected if it does not fall into the set of predicted symbols (for example, numerical values) or is accepted if it does. Communications from the intra-LAN TARP node to the border node are accomplished in the same manner, though the algorithm will necessarily be different for security reasons. Thus, each of the communicating nodes will generate transmit and receive tables in a similar manner to that of Figure 9; the intra-LAN TARP nodes transmit table will be identical to the border node's receive table, and the intra-LAN TARP node's receive table will be identical to the border node's transmit table.

[00106] The algorithm used for IP address-hopping can be any desired algorithm. For example, the algorithm can be a given pseudo-random number generator that generates numbers of the range covering the allowed IP addresses with a given seed. Alternatively, the session participants can assume a certain type of algorithm and specify simply a parameter for applying the algorithm. For example the assumed algorithm could be a particular pseudo-random number generator and the session participants could simply exchange seed values.

[00107] Note that there is no permanent physical distinction between the originating and destination terminal nodes. Either device at either end point can initiate a synchronization of the pair. Note also that the authentication/synchronization-request (and acknowledgment) and hopblock-exchange may all be served by a single message so that separate message exchanges may not be required.

[00108] As another extension to the stated architecture, multiple physical paths can be used by a client, in order to provide link redundancy and further thwart attempts at denial of service and traffic monitoring. As shown in Figure 10, for example, client 1001 can establish three simultaneous sessions with each of three TARP routers provided by different ISPs 1011, 1012, 1013. As an example, the client 1001 can use three different telephone lines 1021, 1022, 1023 to connect to the ISPs, or two telephone lines and a cable modem, etc. In this scheme, transmitted packets will be sent in a random fashion among the different physical paths. This architecture provides a high degree of communications redundancy, with improved immunity from denial-of- service attacks and traffic monitoring.

2. FURTHER EXTENSIONS

[00109] The following describes various extensions to the techniques, systems, and methods described above. As described above, the security of communications occurring between computers in a computer network (such as the Internet, an Ethernet, or others) can be enhanced by using seemingly random source and destination Internet Protocol (IP) addresses for data packets transmitted over the network. This feature prevents eavesdroppers from determining which computers in the network are communicating with each other while permitting the two communicating computers to easily recognize whether a given received data packet is legitimate or not. In one embodiment of the above-described systems, an IP header extension field is used to authenticate incoming packets on an Ethernet.

[00110] Various extensions to the previously described techniques described herein include: (1) use of hopped hardware or "MAC" addresses in broadcast type network; (2) a self synchronization technique that permits a computer to automatically regain synchronization with a sender; (3) synchronization algorithms that allow transmitting and receiving computers to quickly re-establish synchronization in the event of lost packets or other events; and (4) a fast-packet rejection mechanism for rejecting invalid packets. Any or all of these extensions can be combined with the features described above in any of various ways.

A. Hardware Address Hopping

[00111] Internet protocol-based communications techniques on a LAN—or across any dedicated physical medium—typically embed the IP packets within lower-level packets, often referred to as "frames." As shown in FIG. 11, for example, a first Ethernet frame 1150 comprises a frame header 1101 and two embedded IP packets IP1 and IP2, while a second Ethernet frame 1160 comprises a different frame header 1104 and a single IP packet IP3. Each frame header generally includes a source hardware address 1101 A and a destination hardware address 1101 B; other well-known fields in frame headers are omitted from FIG. 11 for clarity. Two hardware nodes communicating over a physical communication channel insert appropriate source and destination hardware addresses to indicate which nodes on the channel or network should receive the frame.

[00112] It may be possible for a nefarious listener to acquire information about the contents of a frame and/or its communicants by examining frames on a local network rather than (or in addition to) the IP packets themselves. This is especially true in broadcast media, such as Ethernet, where it is necessary to insert into the frame header the hardware address of the machine that generated the frame and the hardware address of the machine to which frame is being sent. All nodes on the network can potentially "see" all packets transmitted across the network. This can be a problem for secure communications, especially in cases where the communicants do not want for any third party to be able to identify who is engaging in the information exchange. One way to address this problem is to push the address-hopping scheme down to the hardware layer. In accordance with various embodiments of the invention, hardware addresses are "hopped" in a manner similar to that used to change IP addresses, such that a listener cannot determine which hardware node generated a particular message nor which node is the intended recipient.

[00113] FIG. 12A shows a system in which Media Access Control ("MAC") hardware addresses are "hopped" in order to increase security over a network such as an Ethernet. While the description refers to the exemplary case of an Ethernet environment, the inventive principles are equally applicable to other types of communications media. In the Ethernet case, the MAC address of the sender and receiver are inserted into the Ethernet frame and can be observed by anyone on the LAN who is within the broadcast range for that frame. For secure communications, it becomes desirable to generate frames with MAC addresses that are not attributable to any specific sender or receiver.

[00114] As shown in FIG. 12A, two computer nodes 1201 and 1202 communicate over a communication channel such as an Ethernet. Each node executes one or more application programs 1203 and 1218 that communicate by transmitting packets through communication software 1204 and 1217, respectively. Examples of application programs include video conferencing, e-mail, word processing programs, telephony, and the like. Communication software 1204 and 1217 can comprise, for example, an OSI layered architecture or "stack" that standardizes various services provided at different levels of functionality.

[00115] The lowest levels of communication software 1204 and 1217 communicate with hardware components 1206 and 1214 respectively, each of which can include one or more registers 1207 and 1215 that allow the hardware to be reconfigured or controlled in accordance with various communication protocols. The hardware components (an Ethernet network interface card, for example) communicate with each other over the communication medium. Each hardware component is typically pre-assigned a fixed hardware address or MAC number that identifies the hardware component to other nodes on the network. One or more interface drivers control the operation of each card and can, for example, be configured to accept or reject packets from certain hardware addresses. As will be described in more detail below, various embodiments of the inventive principles provide for "hopping" different addresses using one or more algorithms and one or more moving windows that track a range of valid addresses to validate received packets. Packets transmitted according to one or more of the inventive principles will be generally referred to as "secure" packets or "secure communications" to differentiate them from ordinary data packets that are transmitted in the clear using ordinary, machine-correlated addresses.

[00116] One straightforward method of generating non-attributable MAC addresses is an extension of the IP hopping scheme. In this scenario, two machines on the same LAN that desire to communicate in a secure fashion exchange random-number generators and seeds, and create sequences of quasi-random MAC addresses for synchronized hopping. The implementation and synchronization issues are then similar to that of IP hopping.

[00117] This approach, however, runs the risk of using MAC addresses that are currently active on the LAN—which, in turn, could interrupt communications for those machines. Since an Ethernet MAC address is at present 48 bits in length, the chance of randomly misusing an active MAC address is actually quite small. However, if that figure is multiplied by a large number of nodes (as would be found on an extensive LAN), by a large number of frames (as might be the case with packet voice or streaming video), and by a large number of concurrent Virtual Private Networks (VPNs), then the chance that a non-secure machine's MAC address could be used in an address-hopped frame can become non-trivial. In short, any scheme that runs even a small risk of interrupting communications for other machines on the LAN is bound to receive resistance from prospective system administrators. Nevertheless, it is technically feasible, and can be implemented without risk on a LAN on which there is a small number of machines, or if all of the machines on the LAN are engaging in MAC-hopped communications.

[00118] Synchronized MAC address hopping may incur some overhead in the course of session establishment, especially if there are multiple sessions or multiple nodes involved in the communications. A simpler method of randomizing MAC addresses is to allow each node to receive and process every incident frame on the network. Typically, each network interface driver will check the destination MAC address in the header of every incident frame to see if it matches that machine's MAC address; if there is no match, then the frame is discarded. In one embodiment, however, these checks can be disabled, and every incident packet is passed to the TARP stack for processing. This will be referred to as "promiscuous" mode, since every incident frame is processed. Promiscuous mode allows the sender to use completely random, unsynchronized MAC addresses, since the destination machine is guaranteed to process the frame. The decision as to whether the packet was truly intended for that machine is handled by the TARP stack, which checks the source and destination IP addresses for a match in its IP synchronization tables. If no match is found, the packet is discarded; if there is a match, the packet is unwrapped, the inner header is evaluated, and if the inner header indicates that the packet is destined for that machine then the packet is forwarded to the IP stack—otherwise it is discarded.

[00119] One disadvantage of purely-random MAC address hopping is its impact on processing overhead; that is, since every incident frame must be processed, the machine's CPU is engaged considerably more often than if the network interface driver is discriminating and rejecting packets unilaterally. A compromise approach is to select either a single fixed MAC address or a small number of MAC addresses (e.g., one for each virtual private network on an Ethernet) to use for MAC-hopped communications, regardless of the actual recipient for which the message is intended. In this mode, the network interface driver can check each incident frame against one (or a few) pre-established MAC addresses, thereby freeing the CPU from the task of physical- layer packet discrimination. This scheme does not betray any useful information to an interloper on the LAN; in particular, every secure packet can already be identified by a unique packet type in the outer header. However, since all machines engaged in secure communications would either be using the same MAC address, or be selecting from a small pool of predetermined MAC addresses, the association between a specific machine and a specific MAC address is effectively broken.

[00120] In this scheme, the CPU will be engaged more often than it would be in non-secure communications (or in synchronized MAC address hopping), since the network interface driver cannot always unilaterally discriminate between secure packets that are destined for that machine, and secure packets from other VPNs. However, the non-secure traffic is easily eliminated at the network interface, thereby reducing the amount of processing required of the CPU. There are boundary conditions where these statements would not hold, of course—e.g., if *all* of the traffic on the LAN is secure traffic, then the CPU would be engaged to the same degree as it is in the purely-random address hopping case; alternatively, if each VPN on the LAN uses a different MAC address, then the network interface can perfectly discriminate secure frames destined for the local machine from those constituting other VPNs. These are engineering tradeoffs that might be best handled by providing administrative options for the users when installing the software and/or establishing VPNs.

[00121] Even in this scenario, however, there still remains a slight risk of selecting MAC addresses that are being used by one or more nodes on the LAN. One solution to this problem is to formally assign one address or a range of addresses for use in MAC-hopped communications. This is typically done via an assigned numbers registration authority; e.g., in the case of Ethernet, MAC address ranges are assigned to vendors by the Institute of Electrical and Electronics Engineers (IEEE). A formally-assigned range of addresses would ensure that secure frames do not conflict with any properly-configured and properly-functioning machines on the LAN.

[00122] Reference will now be made to FIGS. 12A and 12B in order to describe the many combinations and features that follow the inventive principles. As explained above, two computer nodes 1201 and 1202 are assumed to be communicating over a network or communication medium such as an Ethernet. A communication protocol in each node (1204 and 1217, respectively) contains a modified element 1205 and 1216 that performs certain functions that deviate from the standard communication protocols. In particular, computer node 1201 implements a first "hop" algorithm 1208X that selects seemingly random source and destination IP addresses (and, in one embodiment, seemingly random IP header discriminator fields) in order to transmit each packet to the other computer node. For example, node 1201 maintains a transmit table 1208 containing triplets of source (S), destination (D), and discriminator fields (DS) that are inserted into outgoing IP packet headers. The table is generated through the use of an appropriate algorithm (e.g., a random number generator that is seeded with an appropriate seed) that is known to the recipient node 1202. As each new IP packet is formed, the next sequential entry out of the sender's transmit table 1208 is used to populate the IP source, IP destination, and IP header extension field (e.g., discriminator field). It will be appreciated that the transmit table need not be created in advance but could instead be created on-the-fly by executing the algorithm when each packet is formed.

[00123] At the receiving node 1202, the same IP hop algorithm 1222X is maintained and used to generate a receive table 1222 that lists valid triplets of source IP address, destination IP address, and discriminator field. This is shown by virtue of the first five entries of transmit table 1208 matching the second five entries of receive table 1222. (The tables may be slightly offset at any particular time due to lost packets, misordered packets, or transmission delays). Additionally, node 1202 maintains a receive window W3 that represents a list of valid IP source, IP destination, and discriminator fields that will be accepted when received as part of an incoming IP packet. As packets are received, window W3 slides down the list of valid entries, such that the possible valid entries change over time. Two packets that arrive out of order but are nevertheless matched to entries within window W3 will be accepted; those falling outside of window W3 will be rejected as invalid. The length of window W3 can be adjusted as necessary to reflect network delays or other factors.

[00124] Node 1202 maintains a similar transmit table 1221 for creating IP packets and frames destined for node 1201 using a potentially different hopping algorithm 1221 X, and node 1201 maintains a matching receive table 1209 using the same algorithm 1209X. As node 1202 transmits packets to node 1201 using seemingly random IP source, IP destination, and/or discriminator fields, node 1201 matches the incoming packet values to those falling within window W1 maintained in its receive table. In effect, transmit table 1208 of node 1201 is synchronized (i.e., entries are selected in the same order) to receive table 1222 of receiving node 1202. Similarly, transmit table 1221 of node 1202 is synchronized to receive table 1209 of node 1201. It will be appreciated that although a common algorithm is shown for the source, destination and discriminator fields in FIG. 12A (using, e.g., a different seed for each of the three fields), an entirely different algorithm could in fact be used to establish values for each of these fields. It will also be appreciated that one or two of the fields can be "hopped" rather than all three as illustrated.

[00125] In accordance with another aspect of the invention, hardware or "MAC" addresses are hopped instead of or in addition to IP addresses and/or the discriminator field in order to improve security in a local area or broadcast-type network. To that end, node 1201 further maintains a transmit table 1210 using a transmit algorithm 121OX to generate source and destination hardware addresses that are inserted into frame headers (e.g., fields 1101A and 1101 B in FIG. 11) that are synchronized to a corresponding receive table 1224 at node 1202. Similarly, node 1202 maintains a different transmit table 1223 containing source and destination hardware addresses that is synchronized with a corresponding receive table 1211 at node 1201. In this manner, outgoing hardware frames appear to be originating from and going to completely random nodes on the network, even though each recipient can determine whether a given packet is intended for it or not. It will be appreciated that the hardware hopping feature can be implemented at a different level in the communications protocol than the IP hopping feature (e.g., in a card driver or in a hardware card itself to improve performance).

[00126] FIG. 12B shows three different embodiments or modes that can be employed using the aforementioned principles. In a first mode referred to as "promiscuous" mode, a common hardware address (e.g., a fixed address for source and another for destination) or else a completely random hardware address is used by all nodes on the network, such that a particular packet cannot be attributed to any one node. Each node must initially accept all packets containing the common (or random) hardware address and inspect the IP addresses or discriminator field to determine whether the packet is intended for that node. In this regard, either the IP addresses or the discriminator field or both can be varied in accordance with an algorithm as described above. As explained previously, this may increase each node's overhead since additional processing is involved to determine whether a given packet has valid source and destination hardware addresses.

[00127] In a second mode referred to as "promiscuous per VPN" mode, a small set of fixed hardware addresses are used, with a fixed source/destination hardware address used for all nodes communicating over a virtual private network. For example, if there are six nodes on an Ethernet, and the network is to be split up into two private virtual networks such that nodes on one VPN can communicate with only the other two nodes on its own VPN, then two sets of hardware addresses could be used: one set for the first VPN and a second set for the second VPN. This would reduce the amount of overhead involved in checking for valid frames since only packets arriving from the designated VPN would need to be checked. IP addresses and one or more discriminator fields could still be hopped as before for secure communication within the VPN. Of course, this solution compromises the anonymity of the VPNs (i.e., an outsider can easily tell what traffic belongs in which VPN, though he cannot correlate it to a specific machine/person). It also requires the use of a discriminator field to mitigate the vulnerability to certain types of DoS attacks, (For example, without the discriminator field, an attacker on the LAN could stream frames containing the MAC addresses being used by the VPN; rejecting those frames could lead to excessive processing overhead. The discriminator field would provide a low-overhead means of rejecting the false packets.)

[00128] In a third mode referred to as "hardware hopping" mode, hardware addresses are varied as illustrated in FIG. I 2A, such that hardware source and destination addresses are changed constantly in order to provide non-attributable addressing. Variations on these embodiments are of course possible, and the invention is not intended to be limited in any respect by these illustrative examples.

B. Extending the Address Space Address

[00129] Address hopping provides security and privacy. However, the level of protection is limited by the number of addresses in the blocks being hopped. A hopblock denotes a field or fields modulated on a packet-wise basis for the purpose of providing a VPN. For instance, if two nodes communicate with IP address hopping using hopblocks of 4 addresses (2 bits) each, there would be 16 possible address-pair combinations. A window of size 16 would result in most address pairs being accepted as valid most of the time. This limitation can be overcome by using a discriminator field in addition to or instead of the hopped address fields. The discriminator field would be hopped in exactly the same fashion as the address fields and it would be used to determine whether a packet should be processed by a receiver.

[00130] Suppose that two clients, each using four-bit hopblocks, would like the same level of protection afforded to clients communicating via IP hopping between two A blocks (24 address bits eligible for hopping). A discriminator field of 20 bits, used in conjunction with the 4 address bits eligible for hopping in the IP address field, provides this level of protection. A 24-bit discriminator field would provide a similar level of protection if the address fields were not hopped or ignored. Using a discriminator field offers the following advantages: (1) an arbitrarily high level of protection can be provided, and (2) address hopping is unnecessary to provide protection. This may be important in environments where address hopping would cause routing problems.

C. Synchronization Techniques

[00131] It is generally assumed that once a sending node and receiving node have exchanged algorithms and seeds (or similar information sufficient to generate quasi-random source and destination tables), subsequent communication between the two nodes will proceed smoothly. Realistically, however, two nodes may lose synchronization due to network delays or outages, or other problems. Consequently, it is desirable to provide means for re-establishing synchronization between nodes in a network that have lost synchronization.

[00132] One possible technique is to require that each node provide an acknowledgment upon successful receipt of each packet and, if no acknowledgment is received within a certain period of time, to re-send the unacknowledged packet. This approach, however, drives up overhead costs and may be prohibitive in high-throughput environments such as streaming video or audio, for example.

[00133] A different approach is to employ an automatic synchronizing technique that will be referred to herein as "self-synchronization." In this approach, synchronization information is embedded into each packet, thereby enabling the receiver to re-synchronize itself upon receipt of a single packet if it determines that is has lost synchronization with the sender. (If communications are already in progress, and the receiver determines that it is still in sync with the sender, then there is no need to re-synchronize.) A receiver could detect that it was out of synchronization by, for example, employing a "dead-man" timer that expires after a certain period of time, wherein the timer is reset with each valid packet. A time stamp could be hashed into the public sync field (see below) to preclude packet-retry attacks.

[00134] In one embodiment, a "sync field" is added to the header of each packet sent out by the sender. This sync field could appear in the clear or as part of an encrypted portion of the packet. Assuming that a sender and receiver have selected a random-number generator (RNG) and seed value, this combination of RNG and seed can be used to generate a random-number sequence (RNS). The RNS is then used to generate a sequence of source/destination IP pairs (and, if desired, discriminator fields and hardware source and destination addresses), as described above. It is not necessary, however, to generate the entire sequence (or the first N-1 values) in order to generate the Nth random number in the sequence; if the sequence index N is known, the random value corresponding to that index can be directly generated (see below). Different RNGs (and seeds) with different fundamental periods could be used to generate the source and destination IP sequences, but the basic concepts would still apply. For the sake of simplicity, the following discussion will assume that IP source and destination address pairs (only) are hopped using a single RNG sequencing mechanism.

[00135] In accordance with a "self-synchronization" feature, a sync field in each packet header provides an index (i.e., a sequence number) into the RNS that is being used to generate IP pairs. Plugging this index into the RNG that is being used to generate the RNS yields a specific random number value, which in turn yields a specific IP pair. That is, an IP pair can be generated directly from knowledge of the RNG, seed, and index number; it is not necessary, in this scheme, to generate the entire sequence of random numbers that precede the sequence value associated with the index number provided.

[00136] Since the communicants have presumably previously exchanged RNGs and seeds, the only new information that must be provided in order to generate an IP pair is the sequence number. If this number is provided by the sender in the packet header, then the receiver need only plug this number into the RNG in order to generate an IP pair — and thus verify that the IP pair appearing in the header of the packet is valid. In this scheme, if the sender and receiver lose synchronization, the receiver can immediately re-synchronize upon receipt of a single packet by simply comparing the IP pair in the packet header to the IP pair generated from the index number. Thus, synchronized communications can be resumed upon receipt of a single packet, making this scheme ideal for multicast communications. Taken to the extreme, it could obviate the need for synchronization tables entirely; that is, the sender and receiver could simply rely on the index number in the sync field to validate the IP pair on each packet, and thereby eliminate the tables entirely.

[00137] The aforementioned scheme may have some inherent security issues associated with it — namely, the placement of the sync field. If the field is placed in the outer header, then an interloper could observe the values of the field and their relationship to the IP stream. This could potentially compromise the algorithm that is being used to generate the IP-address sequence, which would compromise the security of the communications. If, however, the value is placed in the inner header, then the sender must decrypt the inner header before it can extract the sync value and validate the IP pair; this opens up the receiver to certain types of denial-of-service (DoS) attacks, such as packet replay. That is, if the receiver must decrypt a packet before it can validate the IP pair, then it could potentially be forced to expend a significant amount of processing on decryption if an attacker simply retransmits previously valid packets. Other attack methodologies are possible in this scenario.

[00138] A possible compromise between algorithm security and processing speed is to split up the sync value between an inner (encrypted) and outer (unencrypted) header. That is, if the sync value is sufficiently long, it could potentially be split into a rapidly-changing part that can be viewed in the clear, and a fixed (or very slowly changing) part that must be protected. The part that can be viewed in the clear will be called the "public sync" portion and the part that must be protected will be called the "private sync" portion.

[00139] Both the public sync and private sync portions are needed to generate the complete sync value. The private portion, however, can be selected such that it is fixed or will change only occasionally. Thus, the private sync value can be stored by the recipient, thereby obviating the need to decrypt the header in order to retrieve it. If the sender and receiver have previously agreed upon the frequency with which the private part of the sync will change, then the receiver can selectively decrypt a single header in order to extract the new private sync if the communications gap that has led to lost synchronization has exceeded the lifetime of the previous private sync. This should not represent a burdensome amount of decryption, and thus should not open up the receiver to denial-of-service attack simply based on the need to occasionally decrypt a single header.

[00140] One implementation of this is to use a hashing function with a one-to-one mapping to generate the private and public sync portions from the sync value. This implementation is shown in FIG. 13, where (for example) a first ISP 1302 is the sender and a second 1SP 1303 is the receiver. (Other alternatives are possible from FIG. 13.) A transmitted packet comprises a public or "outer" header 1305 that is not encrypted, and a private or "inner" header 1306 that is encrypted using for example a link key. Outer header 1305 includes a public sync portion while inner header 1306 contains the private sync portion. A receiving node decrypts the inner header using a decryption function 1307 in order to extract the private sync portion. This step is necessary only if the lifetime of the currently buffered private sync has expired. (If the currently-buffered private sync is still valid, then it is simply extracted from memory and "added" (which could be an inverse hash) to the public sync, as shown in step 1308.) The public and decrypted private sync portions are combined in function 1308 in order to generate the combined sync 1309. The combined sync (1309) is then fed into the RNG (1310) and compared to the IP address pair (1311) to validate or reject the packet.

[00141] An important consideration in this architecture is the concept of "future" and "past" where the public sync values are concerned. Though the sync values, themselves, should be random to prevent spoofing attacks, it may be important that the receiver be able to quickly identify a sync value that has already been sent — even if the packet containing that sync value was never actually received by the receiver. One solution is to hash a time stamp or sequence number into the public sync portion, which could be quickly extracted, checked, and discarded, thereby validating the public sync portion itself.

[00142] In one embodiment, packets can be checked by comparing the source/destination IP pair generated by the sync field with the pair appearing in the packet header. If (1) they match, (2) the time stamp is valid, and (3) the dead-man timer has expired, then re-synchronization occurs; otherwise, the packet is rejected. If enough processing power is available, the dead-man timer and synchronization tables can be avoided altogether, and the receiver would simply resynchronize (e.g., validate) on every packet.

[00143] The foregoing scheme may require large-integer (e.g., 160-bit) math, which may affect its implementation. Without such large-integer registers, processing throughput would be affected, thus potentially affecting security from a denial-of-service standpoint. Nevertheless, as large integer math processing features become more prevalent, the costs of implementing such a feature will be reduced.

D. Other Synchronization Schemes

[00144] As explained above, if W or more consecutive packets are lost between a transmitter and receiver in a VPN (where W is the window size), the receiver's window will not have been updated and the transmitter will be transmitting packets not in the receiver's window. The sender and receiver will not recover synchronization until perhaps the random pairs in the window are repeated by chance. Therefore, there is a need to keep a transmitter and receiver in synchronization whenever possible and to re-establish synchronization whenever it is lost.

[00145] A "checkpoint" scheme can be used to regain synchronization between a sender and a receiver that have fallen out of synchronization. In this scheme, a checkpoint message comprising a random IP address pair is used for communicating synchronization information. In one embodiment, two messages are used to communicate synchronization information between a sender and a recipient:

1. SYNC_REQ is a message used by the sender to indicate that it wants to synchronize; and
2. SYNC_ACK is a message used by the receiver to inform the transmitter that it has been synchronized.

[00146] According to one variation of this approach, both the transmitter and receiver maintain three checkpoints (see FIG. 14):

1. In the transmitter, ckpt_o ("checkpoint old") is the IP pair that was used to re-send the last SYNC_REQ packet to the receiver. In the receiver, ckpt_o ("checkpoint old") is the IP pair that receives repeated SYNC_REQ packets from the transmitter.
2. In the transmitter, ckpt_n ("checkpoint new") is the IP pair that will be used to send the next SYNC_REQ packet to the receiver. In the receiver, ckpt_n ("checkpoint new") is the IP pair that receives a new SYNC_REQ packet from the transmitter and which causes the receiver's window to be re-aligned, ckpt_o set to ckpt_n, a new ckpt_n to be generated and a new ckpt_r to be generated.

3. In the transmitter, ckpt_r is the IP pair that will be used to send the next SYNC_ACK packet to the receiver. In the receiver, ckpt_r is the IP pair that receives a new SYNC_ACK packet from the transmitter and which causes a new ckpt_n to be generated. Since SYNC_ACK is transmitted from the receiver ISP to the sender ISP, the transmitter ckpt_r refers to the ckpt_r of the receiver and the receiver ckpt_r refers to the ckpt_r of the transmitter (see FIG. 14).

When a transmitter initiates synchronization, the IP pair it will use to transmit the next data packet is set to a predetermined value and when a receiver first receives a SYNC_REQ, the receiver window is updated to be centered on the transmitter's next IP pair. This is the primary mechanism for checkpoint synchronization.

[00147] Synchronization can be initiated by a packet counter (e.g., after every N packets transmitted, initiate a synchronization) or by a timer (every S seconds, initiate a synchronization) or a combination of both. See FIG. 15. From the transmitter's perspective, this technique operates as follows: (1) Each transmitter periodically transmits a "sync request" message to the receiver to make sure that it is in sync. (2) If the receiver is still in sync, it sends back a "sync ack" message. (If this works, no further action is necessary). (3) If no "sync ack" has been received within a period of time, the transmitter retransmits the sync request again. If the transmitter reaches the next checkpoint without receiving a "sync ack" response, then synchronization is broken, and the transmitter should stop transmitting. The transmitter will continue to send syne_reqs until it receives a sync_ack, at which point transmission is reestablished.

[00148] From the receiver's perspective, the scheme operates as follows: (1) when it receives a "sync request" request from the transmitter, it advances its window to the next checkpoint position (even skipping pairs if necessary), and sends a "sync ack" message to the transmitter. If sync was never lost, then the "jump ahead" really just advances to the next available pair of addresses in the table (i.e., normal advancement).

[00149] If an interloper intercepts the "sync request" messages and tries to interfere with communication by sending new ones, it will he ignored if the synchronization has been established or it will actually help to re-establish synchronization.

[00150] A window is realigned whenever a re-synchronization occurs. This realignment entails updating the receiver's window to straddle the address pairs used by the packet transmitted immediately after the transmission of the SYNC_REQ packet. Normally, the transmitter and receiver are in synchronization with one another. However, when network events occur, the receiver's window may have to he advanced by many steps during resynchronization. In this case, it is desirable to move the window ahead without having to step through the intervening random numbers sequentially. (This feature is also desirable for the auto-sync approach discussed above).

E. Random Number Generator with a Jump-Ahead capability

[00151] An attractive method for generating randomly hopped addresses is to use identical random number generators in the transmitter and receiver and advance them as packets are transmitted and received. There are many random number generation algorithms that could be used. Each one has strengths and weaknesses for address hopping applications.

[00152] Linear congruential random number generators (LCRs) are fast, simple and well characterized random number generators that can be made to jump ahead *n* steps efficiently. An LCR generates random numbers X_1, X_2, X_3 ... Xk starting with seed X_0 using a recurrence

$$X_i=(a\ X_{i-1} + b) \bmod c, \qquad (1)$$

where a, b and c define a particular LCR. Another expression for X_i,

$$X_i=((a^i(X_0+b)-b)/(a-1)) \bmod c \qquad (2)$$

enables the jump-ahead capability. The factor a^i can grow very large even for modest i if left unfettered. Therefore some special properties of the modulo operation can be used to control the size and processing time required to compute (2). (2) can be rewritten as:

$$X_i=(a^i(X_0(a-1)+b)-b)/(a-1) \bmod c. \qquad (3)$$

It can be shown that:

$$(a^i(X_0(a-1)+b)-b)/(a-1) \bmod c =$$
$$((a^i \bmod((a-1)c)(X_0(a-1)+b) -b) /(a-1)) \bmod c \qquad (4).$$

[00153] $(X_0(a-1)+b)$ can be stored as $(X_0(a-1)+b) \bmod c$, b as b mod c and compute a^i mod((a-1)c) (this requires O(log(i)) steps).

[00154] A practical implementation of this algorithm would jump a fixed distance, n, between synchronizations; this is tantamount to synchronizing every *n* packets. The window would commence *n* IP pairs from the start of the previous window. Using X_j^w, the random number at the j^{th} checkpoint, as X_0 and *n* as *i*, a node can store a^n mod((a- 1)c) once per LCR and set

[00155] $X_{j+1}{}^{w}=X_{n(j+1)}=((a^n \bmod((a-1)c)\ (X_j^w\ (a-1)+b)-b)/(a-1)) \bmod c$, (5)

to generate the random number for the $j+1^{th}$ synchronization. Using this construction, a node could jump ahead an arbitrary (but fixed) distance between synchronizations in a constant amount of time (independent of n).

[00156] Pseudo-random number generators, in general, and LCRs, in particular, will eventually repeat their cycles. This repetition may present vulnerability in the IP hopping scheme. An adversary would simply have to wait for a repeat to predict future sequences. One way of coping with this vulnerability is to create a random number generator with a known long cycle. A random sequence can be replaced by a new random number generator before it repeats. LCRs can be constructed with known long cycles. This is not currently true of many random number generators.

[00157] Random number generators can be cryptographically insecure. An adversary can derive the RNG parameters by examining the output or part of the output. This is true of LCGs. This vulnerability can be mitigated by incorporating an encryptor, designed to scramble the output as part of the random number generator. The random number generator prevents an adversary from mounting an attack—e.g., a known plaintext attack—against the encryptor.

F. Random Number Generator Example

[00158] Consider a RNG where a=31,b=4 and c=15. For this case equation (1) becomes:

$X_i=(31\ X_{i-1} + 4) \bmod 15$. (6)

If one sets $X_0=1$, equation (6) will produce the sequence 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11, 0, 4, 8, 12. This sequence will repeat indefinitely. For a jump ahead of 3 numbers in this sequence $a^n= 31^3=29791$, $c^*(a-1)=15^*30=450$ and a^n mod((a-1)c) = 31^3mod(15*30)=29791mod(450)=91. Equation (5) becomes:

$((91\ (X_i30+4)-4)/30)\mathrm{mod}\ 15$ (7).

Table 1 shows the jump ahead calculations from (7) . The calculations start at 5 and jump ahead 3.

TABLE 1

I	X_i	(X_i30+4)	$91\ (X_i30+4)-4$	$((91\ (X_i30+4)-4)/30$	X_{i+3}
1	5	154	14010	467	2
4	2	64	5820	194	14
7	14	424	38580	1286	11
10	11	334	30390	1013	8
13	8	244	22200	740	5

G. Fast Packet Filter

[00159] Address hopping VPNs must rapidly determine whether a packet has a valid header and thus requires further processing, or has an invalid header (a hostile packet) and should be immediately rejected. Such rapid determinations will be referred to as "fast packet filtering." This capability protects the VPN from attacks by an adversary who streams hostile packets at the receiver at a high rate of speed in the hope of saturating the receiver's processor (a so-called "denial of service" attack). Fast packet filtering is an important feature for implementing VPNs on shared media such as Ethernet.

[00160] Assuming that all participants in a VPN share an unassigned "A" block of addresses, one possibility is to use an experimental "A" block that will never be assigned to any machine that is not address hopping on the shared medium. "A" blocks have a 24 bits of address that can be hopped as opposed to the 8 bits in "C" blocks. In this case a hopblock will be the "A" block. The use of the experimental "A" block is a likely option on an Ethernet because:

1. The addresses have no validity outside of the Ethernet and will not be routed out to a valid outside destination by a gateway.
2. There are 2^{24} (-16 million) addresses that can be hopped within each "A" block. This yields >280 trillion possible address pairs making it very unlikely that an adversary would guess a valid address. It also provides acceptably low probability of collision between separate VPNs (all VPNs on a shared medium independently generate random address pairs from the same "A" block).

3. The packets will not be received by someone on the Ethernet who is not on a VPN (unless the machine is in promiscuous mode) minimizing impact on non-VPN computers.

[00161] The Ethernet example will be used to describe one implementation of fast packet filtering. The ideal algorithm would quickly examine a packet header, determine whether the packet is hostile, and reject any hostile packets or determine which active IP pair the packet header matches. The problem is a classical associative memory problem. A variety of techniques have been developed to solve this problem (hashing, B—trees etc). Each of these approaches has its strengths and weaknesses. For instance, hash tables can be made to operate quite fast in a statistical sense, but can occasionally degenerate into a much slower algorithm. This slowness can persist for a period of time. Since there is a need to discard hostile packets quickly at all times, hashing would be unacceptable.

H. Presence Vector Algorithm

[00162] A presence vector is a bit vector of length 2^n that can be indexed by n-bit numbers (each ranging from 0 to 2^n -1). One can indicate the presence of k n-bit numbers (not necessarily unique), by setting the bits in the presence vector indexed by each number to 1. Otherwise, the bits in the presence vector are 0. An n-bit number, x, is one of the k numbers if and only if the x^{th} bit of the presence vector is 1. A fast packet filter can be implemented by indexing the presence vector and looking for a 1, which will be referred to as the "test."

[00163] For example, suppose one wanted to represent the number 135 using a presence vector. The 135th bit of the vector would be set. Consequently, one could very quickly determine whether an address of 135 was valid by checking only one bit: the 135th bit. The presence vectors could be created in advance corresponding to the table entries for the IP addresses. In effect, the incoming addresses can be used as indices into a long vector, making comparisons very fast. As each RNG generates a new address, the presence vector is updated to reflect the information. As the window moves, the presence vector is updated to zero out addresses that are no longer valid.

[00164] There is a trade-off between efficiency of the test and the amount of memory required for storing the presence vector(s). For instance, if one were to use the 48 bits of hopping addresses as an index, the presence vector would have to be 35 terabytes. Clearly, this is too large for practical purposes. Instead, the 48 bits can be divided into several smaller fields. For instance, one could subdivide the 48 bits into four 12-bit fields (see FIG. 16). This reduces the storage requirement to 2048 bytes at the expense of occasionally having to process a hostile packet. In effect, instead of one long presence vector, the decomposed address portions must match all four shorter presence vectors before further processing is allowed. (If the first part of the address portion doesn't match the first presence vector, there is no need to check the remaining three presence vectors).

[00165] A presence vector will have a 1 in the y^{th} bit if and only if one or more addresses with a corresponding field of y are active. An address is active only if each presence vector indexed by the appropriate sub-field of the address is 1.

[00166] Consider a window of 32 active addresses and 3 checkpoints. A hostile packet will be rejected by the indexing of one presence vector more than 99% of the time. A hostile packet will be rejected by the indexing of all 4 presence vectors more than 99.9999995% of the time. On average, hostile packets will be rejected in less than 1.02 presence vector index operations.

[00167] The small percentage of hostile packets that pass the fast packet filter will be rejected when matching pairs are not found in the active window or are active checkpoints. Hostile packets that serendipitously match a header will be rejected when the VPN software attempts to decrypt the header. However, these cases will be extremely rare. There are many other ways this method can be configured to arbitrate the space/speed tradeoffs.

<u>I. Further Synchronization Enhancenents</u>

[00168] A slightly modified form of the synchronization techniques described above can be employed. The basic principles of the previously described checkpoint synchronization scheme remain unchanged. The actions resulting from the reception of the checkpoints are, however, slightly different. In this variation, the receiver will maintain between OoO ("Out of Order") and 2×WINDOW_SIZE+OoO active addresses (I ≤OoO ≤WINDOW_SIZE and WINDOW_SIZE ≥1). OoO and WINDOW_SIZE are engineerable parameters, where OoO is the minimum number of addresses needed to accommodate lost packets due to events in the network or out of order arrivals and WINDOW_SIZE is the number of packets transmitted before a SYNC_REQ is issued. FIG. 17 depicts a storage array for a receiver's active addresses.