US007174018B1

(12) **United States Patent**
Patil et al.

(10) **Patent No.: US 7,174,018 B1**
(45) **Date of Patent: Feb. 6, 2007**

(54) **SECURITY FRAMEWORK FOR AN IP MOBILITY SYSTEM USING VARIABLE-BASED SECURITY ASSOCIATIONS AND BROKER REDIRECTION**

(75) Inventors: **Basavaraj B. Patil**, Plano, TX (US); **Raja P. Narayanan**, Irving, TX (US); **Haseeb Akhtar**, Garland, TX (US); **Emad A. Qaddoura**, Plano, TX (US)

(73) Assignee: **Nortel Networks Limited**, St. Laurent (CA)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 789 days.

(21) Appl. No.: **09/595,551**

(22) Filed: **Jun. 16, 2000**

Related U.S. Application Data

(60) Provisional application No. 60/140,704, filed on Jun. 24, 1999.

(51) **Int. Cl.**
H04K 1/00 (2006.01)
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **380/258**; 380/270; 713/153; 713/154

(58) **Field of Classification Search** 380/258, 380/270; 713/154, 153
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,539,824 A * 7/1996 Bjorklund et al. 380/249
5,793,762 A 8/1998 Penners et al.
5,883,890 A 3/1999 Okanoue et al.
5,905,719 A 5/1999 Arnold et al.
6,170,057 B1 * 1/2001 Inoue et al. 713/153
6,253,326 B1 * 6/2001 Lincke et al. 713/201
6,487,657 B1 * 11/2002 Brockmann 713/154
6,507,908 B1 * 1/2003 Caronni 713/153

OTHER PUBLICATIONS

Pat R. Calhoun, DIAMETER Mobile IP Extensions, Nov. 1998, Sun Laboratories, pp. 1-27.*
Pat R. Calhoun, Diameter Framework Document, Feb. 2001, Sun Laboratories, pp. 1-26.*

(Continued)

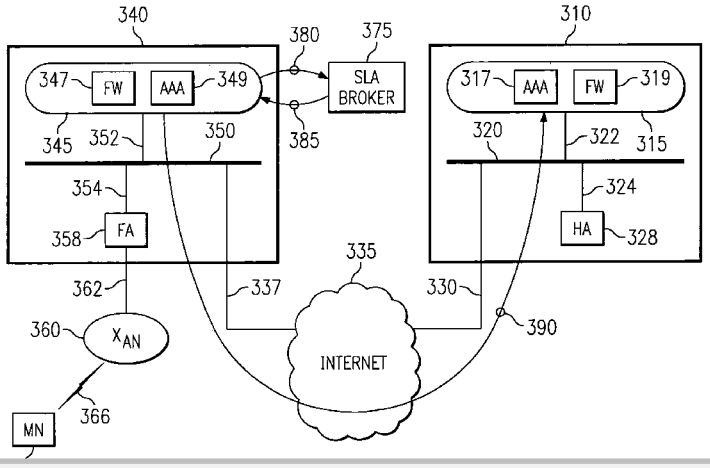
Primary Examiner—Kambiz Zand
Assistant Examiner—Benjamin E. Lanier
(74) *Attorney, Agent, or Firm*—Hemingway & Hansen, LLP; D. Scott Hemingway; Malcolm W. Pipes

(57) **ABSTRACT**

In an IP-based mobile communications system, the Mobile Node changes its point of attachment to the network while maintaining network connectivity. Security concerns arise in the mobile system because authorized users are subject to the following forms of attack: (1) session stealing where a hostile node hijacks session from mobile node by redirecting packets, (2) spoofing where the identity of an authorized user is utilized in an unauthorized manner to obtain access to the network, and (3) eavesdropping and stealing of data during session with authorized user. No separate secure network exists in the IP-based mobility communications system, and therefore, it is necessary to protect information transmitted in the mobile system from the above-identified security attacks.

The present invention improves the security of communications in a IP mobile communications system by creating variable-based Security Associations between various nodes on the system, a Virtual Private Network supported by an Service Level Agreement between various foreign networks and a home network, and an SLA Broker to promote large-scale roaming among different SLAs supported by the SLA Broker or agreements with other SLA Brokers.

37 Claims, 2 Drawing Sheets



OTHER PUBLICATIONS

Pat R. Calhoun, Diameter Base Protocol, Feb. 2001, Sun Laboratories, pp. 1-57.*
La Porta, Thomas F.; Salgarelli, Luca; Foster, Gerald T.; "Mobile IP and Wide Area Wireless Data;" 1998, IEEE.
Perkins, Charles E.; "Tutorial: Mobile Networking Through Mobile IP;" Jan. 1998; IEEE Internet Computing.
Perkins, CV; "RFC 2002: IP Mobility Support;" Oct. 1996, Network Working Group.

* cited by examiner

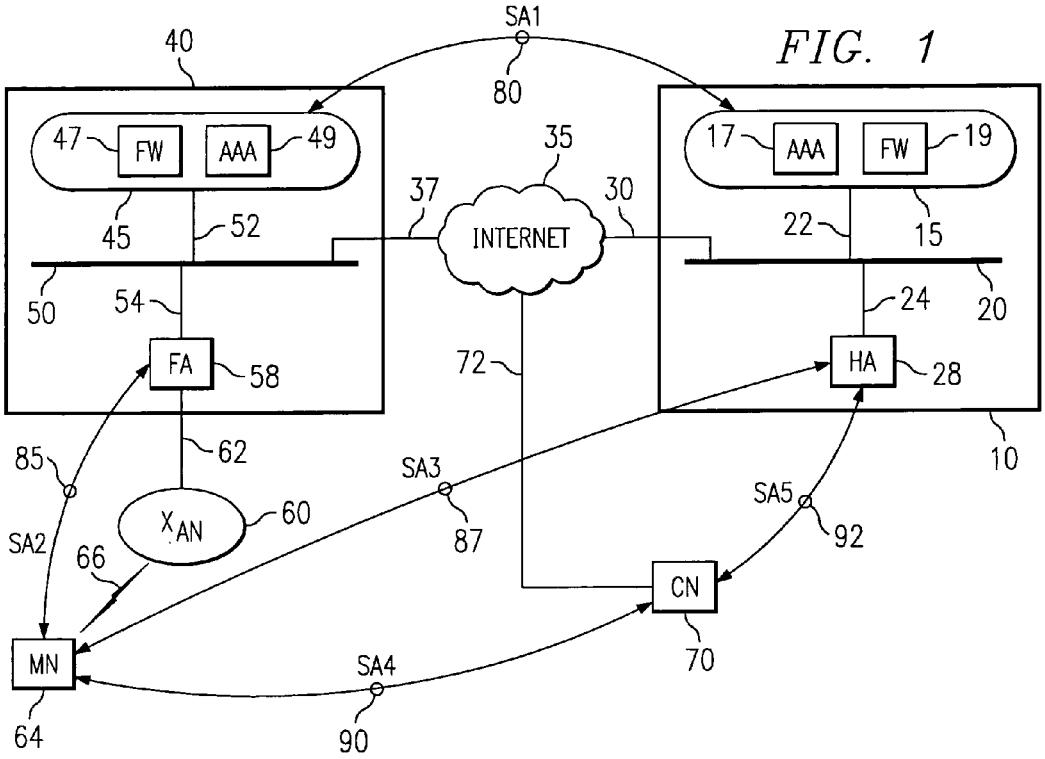


FIG. 1

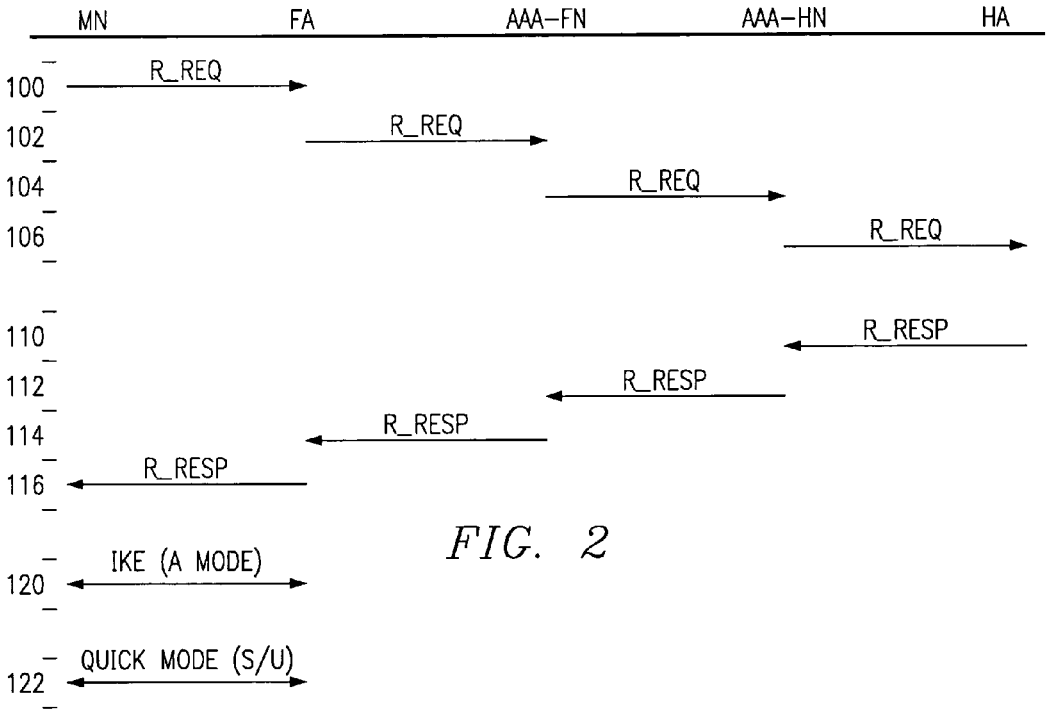


FIG. 2

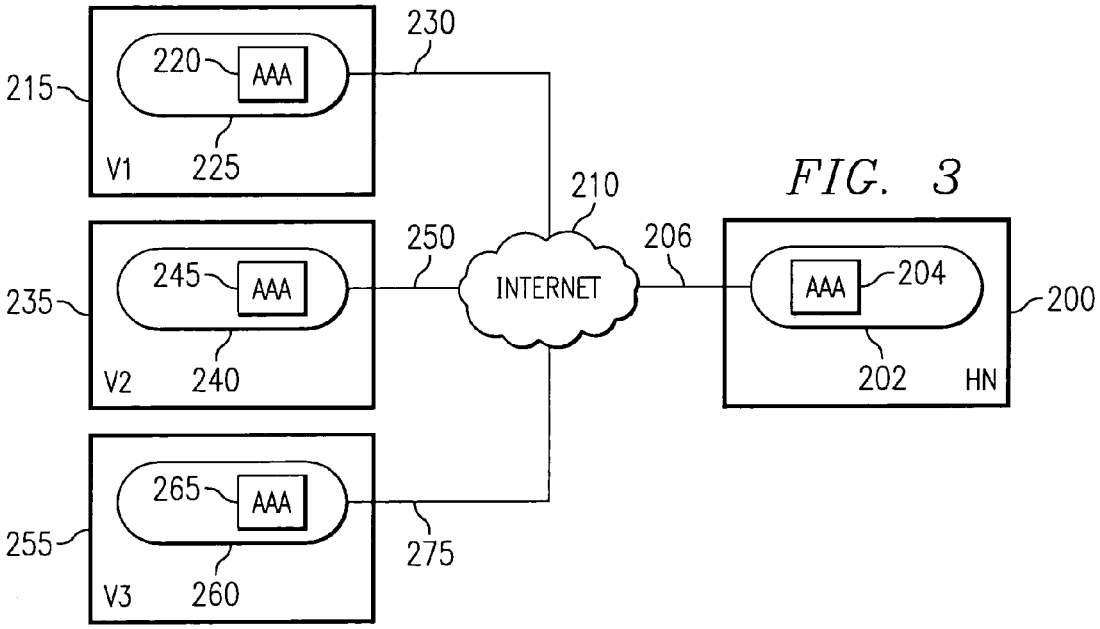


FIG. 3

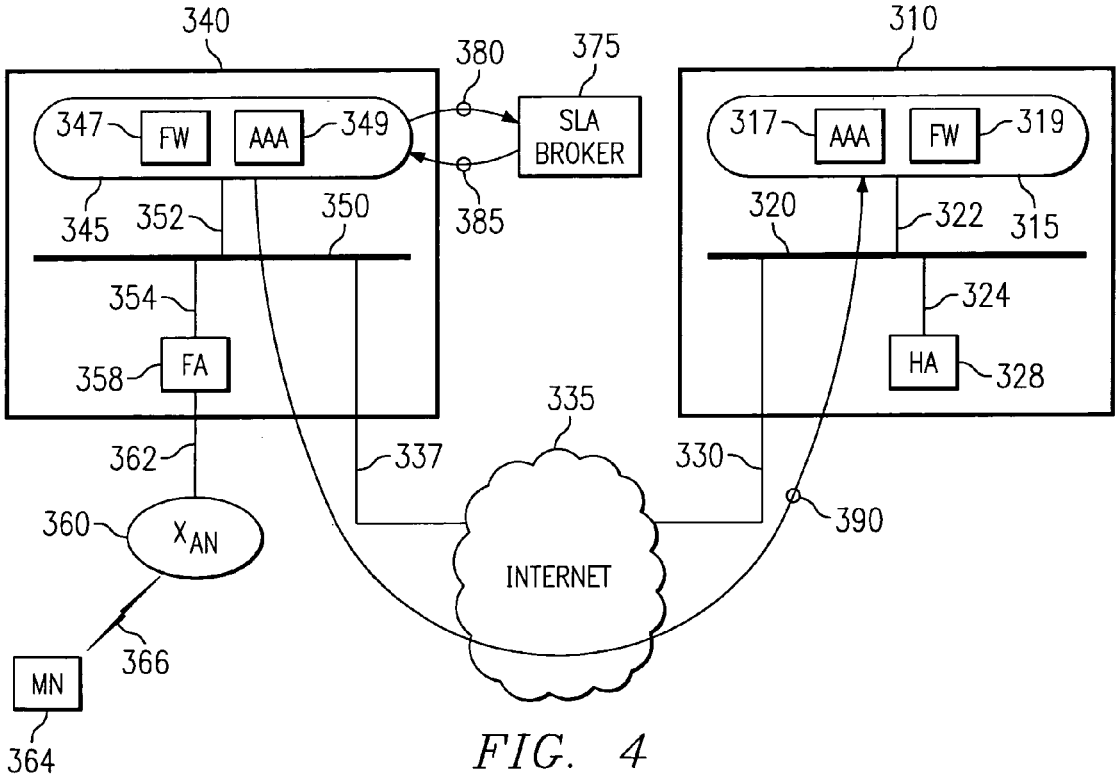


FIG. 4

SECURITY FRAMEWORK FOR AN IP MOBILITY SYSTEM USING VARIABLE-BASED SECURITY ASSOCIATIONS AND BROKER REDIRECTION

RELATED APPLICATION DATA

This application is the utility patent application related to provisional application Ser. No. 60/140,704 filed Jun. 24, 1999.

TECHNICAL FIELD OF THE INVENTION

A security framework for an IP-based mobile communication system having a home network, foreign network and a mobile node.

BACKGROUND OF THE INVENTION

Present-day Internet communications represent the synthesis of technical developments begun in the 1960s—the development of a system to support communications between different United States military computer networks, and the subsequent development of a system to support the communication between research computer networks at United States universities. These technological developments would subsequently revolutionize the world of computing.

The Internet, like so many other high tech developments, grew from research originally performed by the United States Department of Defense. In the 1960s, Defense Department officials began to notice that the military was accumulating a large collection of computers—-some of which were connected to large open computer networks and others that were connected to smaller closed computer networks. A network is a collection of computers or computer-like devices communicating across a common transmission medium. Computers on the Defense Department's open computer networks, however, could not communicate with the other military computers on the closed systems.

Defense Department officials requested that a system be built to permit communication between these different computer networks. The Defense Department recognized, however, that a single centralized system would be vulnerable to missile attacks or sabotage. Accordingly, the Defense Department mandated that the system to be used for communication between these military computer networks be decentralized and that no critical services be concentrated in a few, vulnerable failure points. In order to achieve these goals, the Defense Department established a decentralized standard protocol for communication between network computers.

A few years later, the National Science Foundation (NSF) wanted to connect network computers at various research institutions across the country. The NSF adopted the Defense Department's protocol for communication, and this combination of research computer networks would eventually evolve into the Internet.

Internet Protocols

The Defense Department's communication protocol governing data transmission between computers on different networks was called the Internet Protocol (IP) standard. The IP standard now supports communications between comput-

the mechanisms needed to support these services. The IP standard also describes the upper and lower system interfaces, defines the services to be provided on these interfaces, and outlines the execution environment for services needed in the system.

A transmission protocol, called the Transmission Control Protocol (TCP), was also developed to provide connection-oriented, end-to-end data transmission between packet-switched computer networks. The combination of TCP with IP (TCP/IP) forms a system or suite of protocols for data transfer and communication between computers on the Internet. The TCP/IP standard has become mandatory for use in all packet switching networks that connect or have the potential for utilizing connectivity across network or sub-network boundaries.

The TCP/IP Protocol

In a typical Internet-based communication scenario, data is transmitted from an applications program in a first computer, through the first computer's network hardware, and across the transmission medium to the intended destination on the Internet. After receipt at a destination computer network, the data is transmitted through the destination network to a second computer. The second computer then interprets the communication using the identical protocols on a similar application program. Because of the standard protocols used in Internet communications, the TCP/IP protocol on the second computer decodes the transmitted information into the original information transmitted by the first computer.

One of the rules in TCP/IP communications is that a computer user does not need to get involved with details of data communication. In order to accomplish this goal, the TCP/IP standard imposes a layered communications system structure. All the layers are located on each computer in the network, and each module or layer is a separate component that theoretically functions independent of the other layers.

TCP/IP and its related protocols form a standardized system for defining how data should be processed, transmitted and received on the Internet. TCP/IP defines the network communication process, and more importantly, defines how a unit of data should look and what information the message should contain so that the receiving computer can interpret the message correctly. Because the standardized layer design of TCP/IP, a consistent conversion of base data is ensured regardless of the version or vendor of the TCP/IP conversion software.

TCP/IP Addressing and Routing

A computer operating on a network is assigned a unique physical address. On a Local Area Network ("LAN"), the physical address of the computer is a number given to computer's network adapter card. Hardware LAN protocols use this physical address to deliver packets of data to computers on the LAN.

On the Internet, the TCP/IP protocol routes information packets using logical addressing. The network software in the Network Layer generates logical addresses. Specifically, a logical address in the TCP/IP network is translated into a corresponding physical address using the ARP (Address Resolution Protocol) and RARP (Reverse Address Resolution Protocol) protocols in the Network Layer.

The TCP/IP's logical address is also called an IP address. The IP address can include: (1) a network ID number identifying a network, (2) a sub-network ID number identifying a sub-network on the network, and, (3) a host ID

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.