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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 February 2012 (16.02.2012)

PCT

(10) International Publication Number
WO 2012/021284 A2

(51) International Patent Classification:
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)
H04L 9/06 (2006.01)

(21) International Application Number:
PCT/US2011/045196

(22) International Filing Date:
25 July 2011 (25.07.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/371,735 8 August 2010 (08.08.2010) US
13/174,324 30 June 2011 (30.06.2011) US

(71) Applicant *(for all designated States except US)*: **MOTOROLA SOLUTIONS, INC.** [US/US]; 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SENESE, Thomas, J.,** [US/US]; 618 Newbury Lane, Schaumburg, Illinois 60173 (US). **KRUEGEL, Chris, A.,** [US/US]; 12811 Scoter Court, Plainfield, Illinois 60585 (US). **LANGHAM, Timothy, M.,** [US/US]; 112 Parkwood Drive, Streamwood, Illinois 60107 (US). **LEIGH, Todd, A.** [US/US]; 1792 Walnut Heights Drive, East Lansing, Michigan 48823 (US). **WOODWARD, Timothy, G.,** [US/US]; 1125 E. Broadmor Drive, Tempe, Arizona 85282 (US).

(74) Agents: **KARPINIA, Randi, L.,** et al.; 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

(54) **Title**: METHODS FOR ESTABLISHING A SECURITY SESSION IN A COMMUNICATION SYSTEM

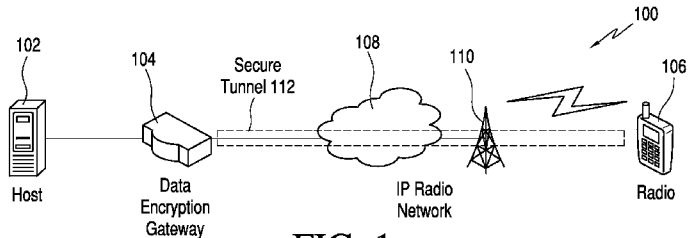

FIG. 1

(57) **Abstract**: A security gateway and an initiating device perform methods for establishing a security session. The methods includes the security gateway: receiving a first message from an initiating device, the first message including a first message authentication code; validating the first message using the message authentication code; and responsive to the validating, sending a second message to the initiating device, the second message including a timestamp and further including a second message authentication code for authenticating of the timestamp by the initiating device, wherein the first and second messages are used to establish the security session, and the authenticated timestamp is used for subsequent replay protection of messages between the security gateway and the initiating device. The method further includes the security gateway validating a dynamically assigned IP address for the initiating device to use in authorizing VPN traffic between the two devices.

WO 2012/021284 A2

METHODS FOR ESTABLISHING A SECURITY SESSION IN A COMMUNICATION SYSTEM

REFERENCE TO RELATED APPLICATIONS

The present application is related to the following U.S. applications commonly owned together with this application by Motorola, Inc.:

Serial no. 12/731,220, filed March 25, 2010, titled "Method and Apparatus for Secure Packet Transmission" by Larry Murrill (attorney docket no. CM12774), which claims the benefit of provisional application Serial No. 61/173,182 filed April 27, 2009;

Serial no. 61/370,943, filed August 5, 2010 titled "Method for Key Identification Using an Internet Security Association and Key Management Based Protocol" by Langham, et al. (attorney docket no. CM13837); and

Serial no.61/371,735 filed August 8, 2010 titled "Methods for Establishing a Security Session in a Communication System" by Senese, et al. (attorney docket no. CM13662), which is a provisional filing from which the present application claims the benefit of its priority date.

TECHNICAL FIELD

The technical field relates generally to secure session establishment or, more particularly, to methods for authenticated time synchronization and for network access control for communication devices using dynamically assigned Internet Protocol (IP) addresses.

BACKGROUND

In many instances today, when a source device sends information to a destination device, the information may travel through a network such as the Internet. Depending on the nature of the information, it may need to be secured in one or more ways. For example, the devices may implement one or more core security services, such as confidentiality, authentication, etc., wherein confidentiality (e.g., the use of encryption/decryption algorithms) provides information privacy and is applied to the information so that it is understandable only by the intended recipient, and

authentication is a process that evaluates the genuineness of the originator and recipient of the information.

A number of existing security protocols can be used to provide the core security services. One such suite of protocols is Internet Protocol Security (IPsec) defined in a number of standards documents (i.e., in a series of Requests for Comments (RFCs)) specified by the Internet Engineering Task Force (IETF). In systems making use of IPsec or other similar data security protocols, security session establishment protocols such as the Internet Key Exchange (IKE) defined in RFCs 2409 (IKEv1) and 4306 (IKEv2) are used to provide security session access control and exchange of data relevant to the security session, such as a basis for replay protection. For example, the IKE protocol first performs mutual authentication of both peers in the exchange before allowing IPsec security session establishment to continue. Furthermore, as an implicit part of creating an IPsec security session, sequence numbers used for replay protection are also synchronized.

IKE is widely used in peer-to-peer networks, often when the network connecting the two peers is a high bandwidth network. In this case, the overhead associated with the several messages transferred as part of an IKE session establishment is relatively small. However, in a low bandwidth network such as an APCO (Association of Public Safety Communications Officials International) Project 25 (P25) radio network or other wireless data network, the added overhead can add an unacceptable delay to security session establishment time. Solutions to this problem typically involve avoidance of IKE altogether and performing IPsec with fixed keys only. However, this solution is often not desirable because it does not allow the additional authentication step that is part of security session establishment and makes synchronizing sequence numbers for relay protection difficult or impossible. IKE is also not suitable for use in cases where messages are targeted to a large group of receivers, such as in sending multicast data.

Thus, there exists a need for a novel method for establishing a security session between devices, which at least supports authentication and replay protection.

BRIEF DESCRIPTION OF THE FIGURES

The accompanying figures, where like reference numerals refer to identical or functionally similar elements throughout the separate views, which together with the detailed description below are incorporated in and form part of the specification and serve to further illustrate various embodiments of concepts that include the claimed invention, and to explain various principles and advantages of those embodiments.

FIG. 1 is a system diagram of a communication system implementing embodiments of the present disclosure.

FIG. 2 is a message sequence chart illustrating a method for security session establishment in accordance with an embodiment.

FIG. 3 is a message sequence chart illustrating a method for security session establishment in accordance with another embodiment.

FIG. 4 is a table illustrating a format of a timestamp provided in the message exchange of the message sequence charts shown in FIG. 2 and FIG. 3.

FIG. 5 illustrates a format of a header used in the messages exchanged in the message sequence charts shown in FIG. 2 and FIG. 3.

Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been drawn to scale. For example, the dimensions of some of the elements in the figures may be exaggerated relative to other elements to help improve understanding of various embodiments. In addition, the description and drawings do not necessarily require the order illustrated. It will be further appreciated that certain actions and/or steps may be described or depicted in a particular order of occurrence while those skilled in the art will understand that such specificity with respect to sequence is not actually required. Apparatus and method components have been represented where appropriate by conventional symbols in the drawings, showing only those specific details that are pertinent to understanding the various embodiments so as not to obscure the disclosure with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein. Thus, it will be appreciated that for simplicity and clarity of illustration, common and well-understood elements that are useful or necessary in a commercially feasible embodiment may not be depicted in order to facilitate a less obstructed view of these various embodiments.

DETAILED DESCRIPTION

Generally speaking, pursuant to the various embodiments, a security gateway and an initiating device perform methods for establishing a security session. The methods includes the security gateway: receiving a first message from an initiating device, the first message including a first message authentication code; validating the first message using the message authentication code; and responsive to the validating, sending a second message to the initiating device, the second message including a timestamp and further including a second message authentication code for authenticating of the timestamp by the initiating device, wherein the first and second messages are used to establish the security session, and the authenticated timestamp is used for subsequent replay protection of messages between the security gateway and the initiating device. The method further includes the security gateway validating a dynamically assigned IP address for the initiating device to use in authorizing access of the initiating device to the security gateway.

Using the methods for security session establishment in accordance with the teachings herein (which is an alternative security session establishment procedure to that provided for by the IKE protocol) enables a number of illustrative advantages. For example, the security session establishment procedure in accordance with the present teachings, at a minimum, mutually authenticates both endpoint devices, provides an authorization mechanism for an initiating device to access a security gateway, and synchronizes an authenticated basis for replay protection, while using fewer and much smaller bandwidth messages than when using the IKE protocol. In addition, the prior art for access control to a security gateway by initiating devices provides a filter based only on static Internet Protocol (IP) addresses of the initiating devices; whereas, embodiments of the present disclosure provide a filter, for access control based on dynamically assigned IP addresses of the initiating devices. Those skilled in the art will realize that the above recognized advantages and other advantages described herein are merely illustrative and are not meant to be a complete rendering of all of the advantages of the various embodiments.

Referring now to the drawings, and in particular FIG. 1, a diagram of a communication system implementing embodiments of the present disclosure is shown

and indicated generally at 100. For example, system 100 may be a Project 25 compliant system (i.e., the system elements perform protocols as defined in Project 25 standards documents), or a TETRA compliant system, or another type low bandwidth system, where it is disadvantageous to use the IKE protocol for security session establishment. System 100 includes a Host 102 (such as a data application server in an enterprise network) and a host communication device 106 (illustrated as a radio but which can be any communication device that includes one or more applications and includes a security processing function), wherein each "host" may have running thereon applications that require secure communications.

To facilitate these secure communications, system 100 further includes a data encryption gateway (DEG) 104 and a DEG function (not shown) physically integrated within the radio 106 that communicate using a network 108, which in this case is an IP network (wherein IPv4 or IPv6 is implemented to enable endpoints to be reachable anywhere within system 100 using IP addresses). Accordingly, security processing by the DEGs is implemented in system 100 using IPsec. However, network 108 can be any type of suitable network, wherein security processing is performed using a correspondingly suitable security processing protocol.

Additionally, system 100 includes an infrastructure device 110 (such as a base site, base station, or the like) through which the radio 106 attaches to and communicates with wirelessly to operate over the network 108. Moreover, system 100 is shown as having two Host devices 102 and 106 and only two DEGs (only DEG 104 shown) for ease of illustration. However, in an actual system implementation, there may be hundreds and even thousands of host devices that use system 100 to facilitate communications with other host and infrastructure devices in system 100. Moreover, there may be additional DEGs in an actual system implementation, including DEGs that serve a number of host devices such as DEG 104.

DEG 104, in this illustrative implementation, provides data application services for multiple communication devices such as radio 106. In order for the radio 106 to access the data application services within host 102, radio 106 needs to authenticate to the DEG 104, which serves as a security gateway to a Virtual Private Network (VPN) that includes the host 102, wherein the DEG further serves to authorize VPN traffic, which is defined as traffic or messages communicated between

the security gateway (e.g., DEG) and authenticated communication devices. The authorized VPN traffic also undergoes security processing by the DEGs, using a data security protocol (which in this case is IPsec), as it travels through the network 108 to provide secure communications between the hosts 102 and 106.

Messages that have undergone security processing using a data security protocol are termed, herein, as "security processed messages." Accordingly, messages that have undergone IPsec processing are deemed security processed IPsec messages. As the term is used herein, a message is defined as a unit of communication sent between the devices, such as a packet, wherein the size and format of the communication unit depends on the particular protocol used to create the communication unit.

Prior to using IPsec for data encryption, a security session is established between the DEG 104 and the DEG in the radio 106. A "security session establishment procedure" is defined as an exchange of a sequence messages between the DEGs to provide, at a minimum, authentication of an initiating device (e.g., radio 106) and in many instances mutual authentication between the initiating device and the security gateway; an authorization mechanism for an initiating device to access the security gateway; and synchronization of an authenticated basis for replay protection. Accordingly, a security session is defined as the result of applying a security session establishment procedure; the security session and security processing of messages provide a secure "tunnel" 112 for messages traveling through the network 108. In the prior art, IKE served as the security session establishment procedure. However, IKE is not suitable for low bandwidth systems. Therefore, the present disclosure provides an alternative security session establishment procedure used to establish a security session using fewer and smaller messages than IKE. Examples of the security session establishment procedure in accordance with the present teachings are described by reference to Figures 2-5.

As illustrated by reference to FIG. 1, the data application function and security processing function can be housed within separate physical devices (e.g., Host 102 and DEG 104) or physically integrated within the same physical device (e.g., radio 106). When the host equipment includes both the application and the security processing functionality, the security processing can be integrated into the single

device using an integrated architecture implementation, wherein the security processing is natively in the layer-3 IP layer such as with IPv6; or using a bump in the stack (BITS) architecture that creates a protocol layer, e.g., an IPsec layer, that sits between the layer-3 IP layer and the layer-2 data link layer. The new layer intercepts packets sent down from the IP layer and adds security to them. When a gateway provides the security processing functionality, a bump in the wire (BITW) architecture is realized by a separate device that is placed within strategic points in the network to provide core security services to, for example, entire network segments.

In general, the Hosts 102 and 106 and the DEGs (104 shown) are each implemented using (although not shown) a memory, one or more network interfaces, and a processing device that are operatively coupled, and which when programmed form the means for these system elements to implement their desired functionality, for example as illustrated by reference to the MSCs shown in FIG. 2 and FIG. 3. The network interfaces are used for passing signaling, also referred to herein as messaging, (e.g., messages, packets, datagrams, frames, superframes, and the like) between the elements of the system 100. The implementation of the network interface in any particular element depends on the particular type of network, i.e., wired and/or wireless, to which the element is connected.

For example, where the network supports wired communications, the interfaces may comprise a serial port interface (e.g., compliant to the RS-232 standard), a parallel port interface, an Ethernet interface, a USB interface, and/or a FireWire interface, and the like. Where the network supports wireless communications, the interfaces comprise elements including processing, modulating, and transceiver elements that are operable in accordance with any one or more standard or proprietary wireless interfaces, wherein some of the functionality of the processing, modulating, and transceiver elements may be performed by means of the processing device through programmed logic such as software applications or firmware stored on the memory device of the system element or through hardware.

The processing device utilized by these elements may be partially implemented in hardware and thereby programmed with software or firmware logic or code for performing functionality described by reference to FIG. 2 and FIG. 3; and/or the processing device may be completely implemented in hardware, for example, as a

state machine or ASIC (application specific integrated circuit). The memory implemented by these system elements can include short-term and/or long-term storage of various information needed for the functioning of the respective elements. The memory may further store software or firmware for programming the processing device with the logic or code needed to perform its functionality.

Turning now to FIG. 2, shown therein is a security session establishment procedure, in accordance with an embodiment of the present disclosure, comprising a sequence of messages 206 and 208 of a message sequence chart (MSC) 200. Messages 206 and 208 are exchanged between a radio 202 (the initiating device, which normally sends the initial message that starts the security session establishment procedure) and a DEG 204 (the security gateway). In one example, message 206 is an IPsec Session Initiation Request, and message 208 is an IPsec Session Initiation Response. Message 206 comprises a header (HDR), an identifier for radio 202 (Radio ID), a nonce (Ni), and a parameter AUTH. Message 208 comprises a header (HDR), a timestamp (TIME), a nonce (Nr), and a parameter AUTH. The headers and parameters of message 206 and 208 are next described.

In this illustrative implementation, AUTH is a Message Authentication Code (MAC), e.g., an 8-byte MAC. As used herein, a MAC is defined as a short piece of information used to authenticate a message. A MAC algorithm, sometimes called a keyed (cryptographic) hash function, accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a tag). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content. In one example implementation, AUTH = function {HDR, TIME, Nr, Ni, auth_key}. For instance, the secret key (auth_key) can be provisioned in both the radio 202 and DEG 204 using over the air rekeying (OTAR) or Key Fill. The same or a different secret key may also be provisioned in both devices using OTAR and used for encrypting the messages 206 and 208. HDR, TIME, Nr, and Ni are next described.

In this illustrative implementation, all headers (HDR) shown in FIG. 2 and FIG. 3 have the format of an IKE header, and more particularly, an IKEv2 header.

FIG. 5 shows an example IKE header 500 with fields 502, 504, 506, 508, 510. The following Table 1 defines the fields contained in message 500:

Field	Definition of use in P25 Packet Data Security
IKE_SA Initiator's/Responder's SPI (502 and 504)	In one embodiment the SPI (security parameter index) is defined, for instance, as a concatenation of algorithm ID (ALGID), key ID (KID), and manufacturer's ID (MFID) fields. This SPI is similarly constructed based on a key used to protect session establishment messages. This is an extension of RFC 4306.
Next Payload (506)	Same use as defined in RFC 4306, wherein it indicates the type of payload that immediately follows the header.
Major Version (506)	Same use as defined in RFC 4306, wherein it indicates the major version of the protocol in use.
Minor Version (506)	Same use as defined in RFC 4306, wherein it indicates the minor version of the protocol in use.
Exchange Type (506)	Indicates the type of exchange being used, such as P25_AUTH exchange, for indicating the message exchange in accordance with the present teachings. This is an extension of RFC 4306.
Flags (506)	I (initiator) and R (responder) flags are used as defined below. This is an extension of RFC 4306.
Message ID (508)	Same use as defined in RFC 4306, wherein it used to control retransmission of lost packets and matching of requests and responses.
Length (508)	Same use as defined in RFC 4306, wherein it indicates a length of total message (header + payloads) in octets.

Table 1

Nonce (N) is a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks. As used herein random or pseudo-random means non-order or non-coherence in a sequence of symbols or steps, such that there is no intelligible pattern or combination, and such numbers can be generated using any suitable random (or pseudo-random) number generator function. Ni signifies the nonce sent by the initiating device, and Nr signifies the nonce sent by the responder, e.g., the security gateway. Moreover, a replay attack is defined as a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. A technique that protects against or guards against a replay attack is deemed to provide "replay protection". For IPsec, for instance, replay protection is provided for in the prior art using sequence numbers

that are initiated using IKE. However, the present disclosure provides for a novel replay protection technique for use with IPsec, as further described below.

TIME is a timestamp, which is defined as a sequence of characters denoting the date and/or time at which a certain event occurred, such as a recorded time at which a message was sent. In one illustrative implementation, TIME is a 32-bit value. An illustrative timestamp format with 32 bits is contained in a table shown in FIG. 4, wherein a first column 402 indicates a timestamp sub-field, and a second column 404 indicates a length of the corresponding sub-field. As illustrated, the timestamp includes the following sub-fields: Month (4 bits), Day (5 bits), Hour (5 bits), Minute (6 bits), Microslot (2 bits).

Turning again to MSC 200, in the normal case for session establishment shown in FIG. 2, the radio initiates the handshake (message sequence). The first message (206) is authenticated or validated with a MAC, where the initiator's nonce (Ni) is used to add freshness to the message digest. The security gateway 204 responds to message 206 by sending, in the message 208, its current time (TIME), thereby, providing a timestamp that has the format shown in FIG. 4, for example. The radio 202 unit verifies that the responder is not sending a replayed message by validating the MAC, whose message digest uses the original initiator's nonce. In the exception case where the security gateway 204 cannot authenticate the message sent by the radio 202, the security gateway sends a rejection notification to the radio in place of the second message 208 that is shown in FIG. 2.

As explained above, the AUTH function for generating the MAC uses both Ni and Nr. Nr is sent in message 208 and Ni is "implied" in that the radio 202 should know its nonce. The radio 202 uses the implied Ni, as well as the explicit Nr, to calculate the AUTH value, and then compares the calculated AUTH value to the AUTH value that it received in message 208; although, in an alternative implementation, Ni could also be sent in message 208 (and 308 of FIG. 3). The radio 202 does not transact with the security gateway 204 if it fails to complete AUTH validation process. However, upon completing the AUTH validation process using the MAC, the timestamp provided by the gateway device 204 is authenticated.

It should be noted that all of the messages shown in FIG. 2 and FIG. 3 can be less than 100 bytes, which includes a 20-byte IPv4 and UDP overhead. Conversely,

for the IKEv2 message exchange, in order to establish a security session, 6 messages having a size less than 100 bytes and another 12 messages having a size equal to 512 bytes are exchanged. Thus, there is a significant savings in the number and size of the messages exchanged to establish a security session.

Also, FIG. 2 illustrated a two-message sequence for completing the establishment of a security session between a radio and a security gateway device in accordance with the present teachings. FIG. 3 illustrates a three-message sequence for completing the establishment of a security session between a radio and a security gateway device in accordance with the present teachings. A MSC 300 includes messages 306, 308, and 310 exchanged between a radio 302 (the initiating device) and a DEG 304 (the responding device and security gateway). Messages 306 and 308 are the same are messages 206 and 208 of FIG. 2, and the description of these messages is not repeated here for the sake of brevity. MSC 300 includes the third message 310 as a means of further strengthening the security session establishment process by providing another opportunity for reply protection of the message. Namely, message 310 includes a HDR, Nr, and AUTH, wherein the Nr is the same Nr provided in message 308, which serves as replay protection and enables the DEG 304 to validate message 310 by validating the AUTH value (MAC).

As mentioned earlier, the authenticated timestamp is used in providing replay protection. More particularly, the authenticated timestamp is used for replay protection of security processed messages sent between the radio and DEG after the security session is established. The session establishment synchronizes authentic time between the radio and the security gateway. The time is used to construct a number that can only be used once. The purpose of this number is to provide uniqueness to a message that is being authenticated through the MAC, and thus prevent replay of the message. Both security endpoints need to have the synchronized timestamp in order to implement the time-based authentication validation.

In this illustrative embodiment, the authenticated timestamp is used for replay protection of IPsec security processed messages sent between the radio and DEG after the security session is established. More particularly, with regards to replay protection, the radio needs to keep its time synchronized with the time of the security gateway. This can be done initially through the session-establishment exchange,

where the timestamp is authenticated by the MAC. The radio can also readjust its authenticated time to account for drift by checking the unauthenticated time using any suitable means such as on a trunking control channel or by checking time broadcasts on a conventional traffic channel.

If the radio sees the broadcasted control channel time change abruptly, and determines that the unauthenticated control channel time differs significantly (e.g., is outside of a defined threshold) with the authenticated timestamp that was initialized by the security gateway, then the radio does not resynchronize its authenticated time to the new control channel time. The radio instead requests to receive an authenticated time stamp from the security gateway by initiating a new session-establishment exchange. In order to prevent flooding of the system, in one example implementation, the radio only reinitiates the session-establishment exchange when it either receives or needs to transmit a new security processed message that includes or needs to have included therein an authenticated time stamp.

To facilitate the replay protection using the authenticated timestamp, the radio or security gateway inserts, into a security processed message (such as an IPsec message), a current timestamp that is derived from the authenticated timestamp; or in other words, the current timestamp uses the authenticated timestamp as a synchronized time basis. In one example implementation, the current timestamp is inserted into a sequence number field of an Encapsulating Security Payload (ESP) header or into a sequence number field of an Authentication Header (AH) protocol header within the IPsec message. Furthermore, the current timestamp may be inserted into an unencrypted portion of a payload in the IPsec message. Correspondingly, the radio or the security gateway receives an IPsec having a timestamp included in a sequence number field of an ESP or AH header of the IPsec message; and verifies the timestamp in the sequence number field against the authenticated timestamp to evaluate the IPsec message for replay attack.

Insertion of the timestamp into the ESP header is described herein, but the description is equally applicable to insertion of the timestamp into the AH header. The ESP header's Sequence Number field is 32 bits in length, and is populated with the ESP transmitter's current time stamp. The subfields that are inserted into the Sequence Number field include: Month, Day, Hour, Minute, and Microslot (12 bits),

as shown in FIG. 4. Using 12 bits for the Microslot field provides time granularity of 15 Ms. A crypto period on the security equipment may be changed at least once per year in order to prevent roll-over of the time stamp. As mentioned above, the current time can also be inserted into the unencrypted portion of the payload. The receiving ESP device compares the timestamp in the received ESP packet to its own current time as part of the procedure to qualify (verify) the packet. A packet that is deemed to be too old, or one with a time stamp that has previously been sent from the same source, is discarded. An advantage of using time instead of sequence number (as in the prior art) is that time can be used to prevent replay of group messaging.

An ESP device should also be capable of handling conditions where packets are received out of chronological order. For example, the ESP device has a configurable Anti-Replay Window (ARW) parameter. The ARW defines the interval of time where the ESP device will accept a packet whose time stamp is older than the previously received packet from the same source. Otherwise, received packets whose time stamps are older than the previously received packet from the same source are discarded. A smaller ARW value provides tighter protection against replay attack. A larger value loosens the security, but will allow for more flexible network operation. A typical default value of the ARW parameter is on the order of a couple of seconds.

In some networks, instead of having static IP addresses (meaning IP addresses that do not change over time), the radios have dynamically assigned IP addresses (meaning IP addresses that change over time), which are usually assigned through context activation. However, access control methods for a radio to access the gateway device, and hence the application service of the enterprise network) do not address access control when IP addresses are dynamically assigned. However, an embodiment of the present disclosure provides access control for radios having dynamically assigned IP addresses.

The radio is authorized to use a VPN based upon the settings of the security gateway's access control list. The security gateway's access control list contains the radio IDs of all authorized radios and may also contains a unique MAC key for each radio through OTAR provisioning or Key Fill. Accordingly, the security gateway verifies the received radio ID (e.g., from message 206 or 306) to the stored radio IDs. If there's a match and upon successful security session completion, the radio is

authorized to use the VPN via the security gateway, and the dynamically assigned IP address (which is now an authorized IP address) is stored for that radio and associated with (or mapped to) the radio's stored ID. Since a radio ID is not present in later IPsec messages, the security gateway allows or authorizes VPN traffic to and from radios that have authorized IP addresses. The filtering can be performed based on IP addresses since each message contains the radio's IP address.

In the foregoing specification, specific embodiments have been described. However, one of ordinary skill in the art appreciates that various modifications and changes can be made without departing from the scope of the invention as set forth in the claims below. Accordingly, the specification and figures are to be regarded in an illustrative rather than a restrictive sense, and all such modifications are intended to be included within the scope of present teachings. The benefits, advantages, solutions to problems, and any element(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as a critical, required, or essential features or elements of any or all the claims. The invention is defined solely by the appended claims including any amendments made during the pendency of this application and all equivalents of those claims as issued.

Moreover in this document, relational terms such as first and second, top and bottom, and the like may be used solely to distinguish one entity or action from another entity or action without necessarily requiring or implying any actual such relationship or order between such entities or actions. The terms "comprises," "comprising," "has", "having," "includes", "including," "contains", "containing" or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that comprises, has, includes, contains a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. An element proceeded by "comprises ...a", "has ...a", "includes ...a", "contains ...a" does not, without more constraints, preclude the existence of additional identical elements in the process, method, article, or apparatus that comprises, has, includes, contains the element. The terms "a" and "an" are defined as one or more unless explicitly stated otherwise herein. The terms "substantially", "essentially", "approximately", "about" or any other version thereof, are defined as being close to as understood by one of

ordinary skill in the art, and in one non-limiting embodiment the term is defined to be within 10%, in another embodiment within 5%, in another embodiment within 1% and in another embodiment within 0.5%. The term "coupled" as used herein is defined as connected, although not necessarily directly and not necessarily mechanically. A device or structure that is "configured" in a certain way is configured in at least that way, but may also be configured in ways that are not listed.

It will be appreciated that some embodiments may be comprised of one or more generic or specialized processors (or "processing devices") such as microprocessors, digital signal processors, customized processors and field programmable gate arrays (FPGAs) and unique stored program instructions (including both software and firmware) that control the one or more processors to implement, in conjunction with certain non-processor circuits, some, most, or all of the functions of the method and apparatus for secure packet transmission described herein. The non-processor circuits may include, but are not limited to, a radio receiver, a radio transmitter, signal drivers, clock circuits, power source circuits, and user input devices. As such, these functions may be interpreted as steps of a method to perform the secure packet transmission described herein. Alternatively, some or all functions could be implemented by a state machine that has no stored program instructions, or in one or more application specific integrated circuits (ASICs), in which each function or some combinations of certain of the functions are implemented as custom logic. Of course, a combination of the two approaches could be used. Both the state machine and ASIC are considered herein as a "processing device" for purposes of the foregoing discussion and claim language.

Moreover, an embodiment can be implemented as a computer-readable storage element or medium having computer readable code stored thereon for programming a computer (e.g., comprising a processing device) to perform a method as described and claimed herein. Examples of such computer-readable storage elements include, but are not limited to, a hard disk, a CD-ROM, an optical storage device, a magnetic storage device, a ROM (Read Only Memory), a PROM (Programmable Read Only Memory), an EPROM (Erasable Programmable Read Only Memory), an EEPROM (Electrically Erasable Programmable Read Only Memory) and a Flash memory. Further, it is expected that one of ordinary skill, notwithstanding possibly significant

effort and many design choices motivated by, for example, available time, current technology, and economic considerations, when guided by the concepts and principles disclosed herein will be readily capable of generating such software instructions and programs and ICs with minimal experimentation.

The Abstract of the Disclosure is provided to allow the reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, it can be seen that various features are grouped together in various embodiments for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separately claimed subject matter.

CLAIMS

We claim:

1. A method for establishing a security session in a communication system, the method comprising:

a security gateway performing:

receiving a first message from an initiating device, the first message including a first message authentication code;

validating the first message using the message authentication code;

responsive to the validating, sending a second message to the initiating device, the second message including a timestamp and further including a second message authentication code for authenticating of the timestamp by the initiating device.

2. The method of claim 1, wherein the second message further includes a random or pseudo-random number, the method further comprising receiving a third message from the initiating device, the third message including the same random or pseudo-random number as in the second message, and the third message further including a third message authentication code for validating of the third message by the security gateway.

3. The method of claim 2, wherein the third message completes an establishment of a security session between the security gateway and the initiating device.

4. The method of claim 1, wherein the second message completes an establishment of a security session between the security gateway and the initiating device.

5. The method of claim 1, wherein the first and second messages each include a header having a format of an Internet Key Exchange header.

6. The method of claim 1, wherein the timestamp is for replay protection of messages sent between the initiating device and security gateway after the second message.

7. The method of claim 6, wherein the timestamp is for replay protection of Internet Protocol Security (IPsec) messages sent between the initiating device and security gateway after the second message.

8. The method of claim 1, wherein the first message further includes a first identifier for the initiating device and an Internet Protocol (IP) address for the initiating device, the method further comprising:

verifying that the first identifier matches a second stored identifier for the initiating device;

upon establishing a security session between the initiating device and the security gateway using the first and second messages, associating the IP address with the second identifier, and storing the IP address.

9 The method of claim 8, wherein the IP address is a dynamically assigned IP address.

10. The method of claim 8, wherein the IP address authorizes Virtual Private Network traffic between the initiating device and the security gateway.

11. A method for establishing a security session in a communication system, the method comprising:

an initiating device performing:

sending a first message to a security gateway, the first message including a first message authentication code for validating of the first message by the security gateway;

after the validating, receiving a second message from the security gateway, the second message including a timestamp and a second message authentication code;

authenticating the timestamp using the second message authentication code, wherein the authenticated timestamp is for replay protection of messages sent between the initiating device and the security gateway.

12. The method of claim 11, wherein the second message further includes a random or pseudo-random number, the method further comprising sending a third message to the security gateway, the third message comprising the same random or pseudo-random number as in the second message, and the third message further including a third message authentication code for validating of the third message by the security gateway.

13. The method of claim 12, wherein the third message completes an establishment of a security session between the security gateway and the initiating device.

14. The method of claim 12, wherein the first, second, and third messages each include a header having a format of an Internet Key Exchange header.

15. The method of claim 11, wherein the second message completes an establishment of a security session between the security gateway and the initiating device.

16. The method of claim 11, wherein the first and second messages each include a header having a format of an Internet Key Exchange header.

17. The method of claim 11 further comprising inserting, into a security processed message, a current timestamp that is derived from the authenticated timestamp.

18. The method of claim 17, wherein the security processed message comprises an Internet Protocol Security (IPsec) message, and the current timestamp is inserted into a sequence number field of an Encapsulating Security Payload header or into a sequence number field of an Authentication Header protocol header within the IPsec message.

19. The method of claim 18 further comprising inserting the current timestamp into an unencrypted portion of a payload in the IPsec message.

20. The method of claim 11 further comprising:

receiving an Internet Protocol Security (IPsec) message from the security gateway, the IPsec message having a timestamp included in a sequence number field of an Encapsulating Security Payload header or in an Authentication Header protocol header of the IPsec message;

verifying the timestamp in the sequence number field against the authenticated timestamp to evaluate the IPsec message for replay attack.

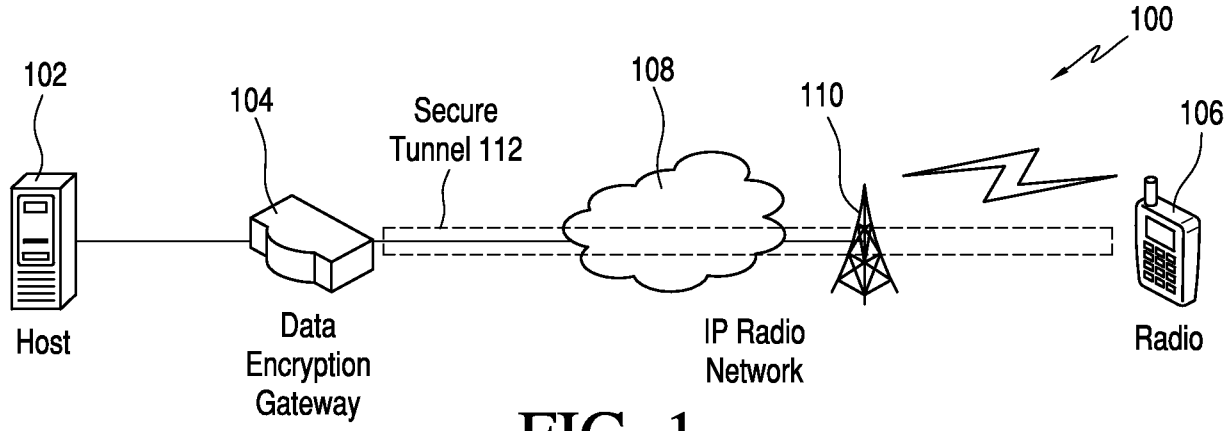

FIG. 1

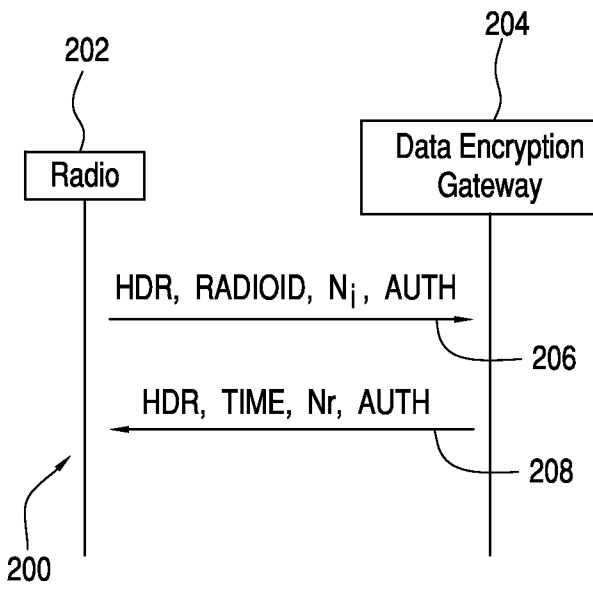

FIG. 2

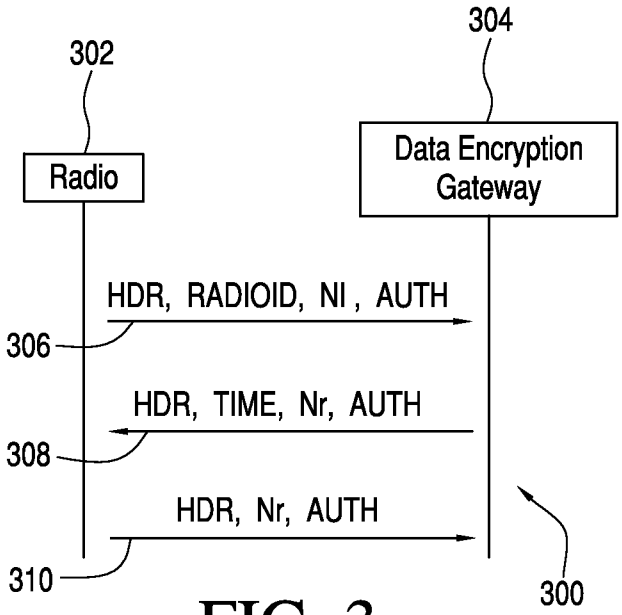

FIG. 3

402 Sub-field	404 Length (bits)
Month	4
Day	5
Hour	5
Minute	6
Microslot	12

FIG. 4

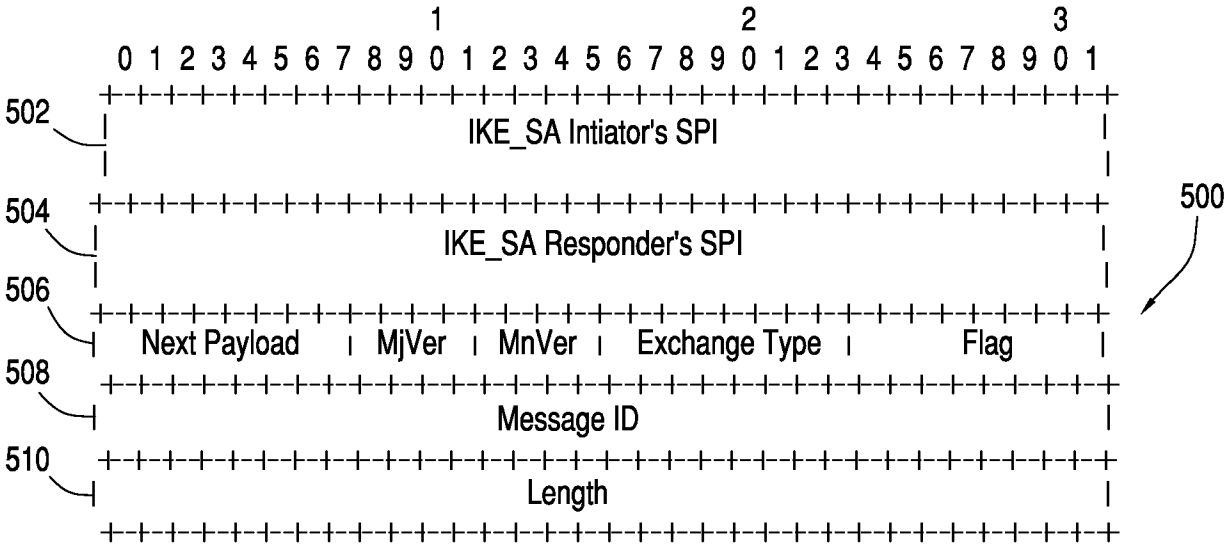
1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
502
IKE_SA Intiator's SPI
504
IKE_SA Responder's SPI
500
506
Next Payload
MjVer
MnVer
Exchange Type
Flag
508
Message ID
510
Length

FIG. 5