

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

(19) World Intellectual Property Organization

International Bureau



(10) International Publication Number

WO 2013/106163 A1

(43) International Publication Date

18 July 2013 (18.07.2013)

WIPO | PCT

(51) International Patent Classification:

H04W 12/02 (2009.01) H04L 29/06 (2006.01)

(21) International Application Number:

PCT/US2012/069588

(22) International Filing Date:

13 December 2012 (13.12.2012)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

13/349,543 12 January 2012 (12.01.2012) US

(71) Applicant (for all designated States except US): THE BOEING COMPANY [US/US]; 100 North Riverside Plaza, Chicago, Illinois 60606-2016 (US).

(72) Inventors; and

(71) Applicants : ANDREWS, Eric, J. [US/US]; 5301 Bolsa Ave, M/C: H011-C190, Huntington Beach, California 92647 (US). EIGLE, Ted [US/US]; 5301 Bolsa Ave, M/C: H011-B152, Huntington Beach, California 92647 (US). HOFFMAN, Ceilidh [US/US]; 5301 Bolsa Ave, M/C: H011-B156, Huntington Beach, California 92647 (US).

(74) Agents: SATERMO, Eric, K et al.; The Boeing Company, PO Box 2515, MC 110-SD54, Seal Beach, California 90740-1515 (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, BN, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, 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:

— with international search report (Art. 21(3))

(54) Title: A SYSTEM AND METHOD FOR SECURE COMMUNICATION

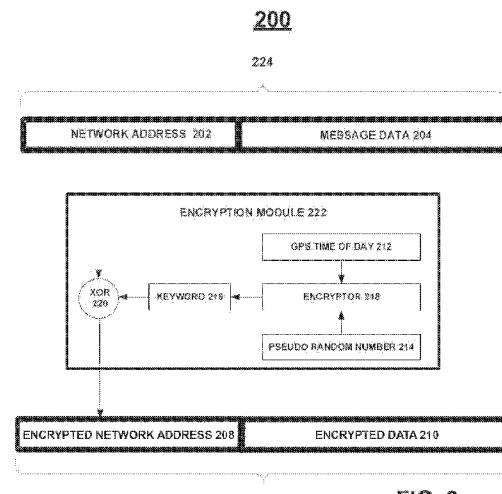


FIG. 2

(57) Abstract: A system and methods for secure communication are disclosed. A network packet (224) comprising encrypted network address (208) comprising an unencrypted network address (202) encrypted by a first GPS time (212) and a first pseudo random number (214) is received. The encrypted network address (208) is decrypted using the first GPS time (212) and the first pseudo random number (214) to provide the unencrypted network address (404). The network packet (224) is transmitted based on the unencrypted network address(406).

WO 2013/106163 A1

A SYSTEM AND METHOD FOR SECURE COMMUNICATION

FIELD

Embodiments of the present disclosure relate generally to communication systems. More particularly, embodiments of the present disclosure relate to encrypted communication systems 5 for secure communication.

BACKGROUND

In general commercial wireless networks do not encrypt and protect user information data that is transmitted over the air. Data security and integrity are expected to be handled by an end-user application. Most end-user applications that traverse via the Internet Protocol (IP) network rely 10 on public key encryption methods for both end-user authentication and data security.

With ubiquity of wireless local area networks in public spaces, commercial wireless industry standards bodies have implemented an additional layer of security that serves as gatekeeping to grant access to only authorized users; i.e., users who have a correct network encryption-decryption key. An over-the-air transmitted radio frequency (RF) signal, however, is not 15 protected from eavesdroppers. In contrast, most military wireless networks support both end-user data security as well as protection of over-the-air transmitted RF signal. However, such networks are closed and proprietary and generally cannot interoperate with commercially available wireless devices such as cellular phones, personal computers and tablets.

SUMMARY

20 A system and methods for secure communication using modified commercial equipment are disclosed. A network packet comprising an encrypted network address for transmission security comprising an unencrypted network address encrypted by a first Global Positioning System (GPS) time and a first pseudo random number is received. The encrypted network address is

decrypted using the first GPS time and the first pseudo random number to provide the unencrypted network address. The network packet is transmitted based on the unencrypted network address. In this manner, embodiments of the disclosure make use of low cost high bandwidth commercial-off-the-shelf (COTS) networks to transmit classified data.

- 5 In an embodiment, a method for secure communication receives a network packet comprising an encrypted network address comprising an unencrypted network address encrypted by a first GPS time and a first pseudo random number. The method further decrypts the encrypted network address using the first GPS time and the first pseudo random number to provide the unencrypted network address. The method further transmits the network packet based on the unencrypted network address. Advantageously the method further includes transmitting the network packet through a closed commercial network. The closed commercial network includes one or more of: an internet protocol network, a circuit-switched network, a packet-switched network, or a wireless communication network. Advantageously, the network packet may further include encrypted data.
- 10 In another embodiment, a system for secure communication comprises a receiver module, a decryption module, and a transmitter module. The receiver module is operable to receive a network packet comprising an encrypted network address comprising an unencrypted network address encrypted by a first GPS time and a first pseudo random number. The decryption module is operable to decrypt the encrypted network address to provide an unencrypted network address. The transmitter module is operable to transmit the network packet based on the unencrypted network address. Advantageously the system comprises a mobile communication device. Advantageously, the transmitter module is further operable to transmit the network packet through a closed commercial network. The closed commercial network includes one or more of: an internet protocol network, a circuit-switched network, a packet-switched network, or a wireless communication network.
- 15
- 20
- 25

In a further embodiment, a computer readable storage medium comprises computer-executable instructions for performing a method for secure communication. The method executed by the computer-executable instructions receives a network packet comprising an encrypted network address comprising an unencrypted network address encrypted by a first GPS time and a first 5 pseudo random number. The method further decrypts the encrypted network address using the first GPS time and the first pseudo random number to provide the unencrypted network address. The method further transmits the network packet based on the unencrypted network address. Advantageously the method executed by the computer-executable instructions further includes transmitting the network packet through a closed commercial network. The closed commercial 10 network includes one or more of: an internet protocol network, a circuit-switched network, a packet-switched network, or a wireless communication network.

15

This summary is provided to introduce a selection of concepts in a simplified form that are further described below in the detailed description. This summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid 15 in determining the scope of the claimed subject matter.

BRIEF DESCRIPTION OF DRAWINGS

A more complete understanding of embodiments of the present disclosure may be derived by referring to the detailed description and claims when considered in conjunction with the following figures, wherein like reference numbers refer to similar elements throughout the 20 figures. The figures are provided to facilitate understanding of the disclosure without limiting the breadth, scope, scale, or applicability of the disclosure. The drawings are not necessarily made to scale.

Figure 1 is an illustration of an exemplary wireless communication environment for transmitting and receiving secure information according to an embodiment of the disclosure.

Figure 2 is an illustration of an exemplary encryption process of a network packet encrypted according to an embodiment of the disclosure.

Figure 3 is an illustration of an exemplary schematic functional block diagram of an encrypted routing system according to an embodiment of the disclosure.

5 Figure 4 is an illustration of an exemplary flowchart showing a process for secure communication according to an embodiment of the disclosure.

DETAILED DESCRIPTION

The following detailed description is exemplary in nature and is not intended to limit the disclosure or the application and uses of the embodiments of the disclosure. Descriptions of 10 specific devices, techniques, and applications are provided only as examples. Modifications to the examples described herein will be readily apparent to those of ordinary skill in the art, and the general principles defined herein may be applied to other examples and applications without departing from the spirit and scope of the disclosure. Furthermore, there is no intention to be bound by any expressed or implied theory presented in the preceding field, background, 15 summary or the following detailed description. The present disclosure should be accorded scope consistent with the claims, and not limited to the examples described and shown herein.

Embodiments of the disclosure may be described herein in terms of functional and/or logical block components and various processing steps. It should be appreciated that such block components may be realized by any number of hardware, software, and/or firmware components 20 configured to perform the specified functions. For the sake of brevity, conventional techniques and components related to standard communication systems, military communication systems, network protocols, and other functional aspects of the systems (and the individual operating components of the systems) may not be described in detail herein.

Embodiments of the disclosure are described herein in the context of a practical non-limiting 25 application, namely, a secure communication for a mobile phone application. Embodiments of

the disclosure, however, are not limited to such mobile phone applications, and the techniques described herein may also be utilized in other applications. For example, embodiments may be applicable to a desktop computer, a laptop or notebook computer, a DroidTM phone, an iPhoneTM, a mainframe, a server, a client, or any other type of special or general purpose internally or externally GPS enabled computing device as may be desirable or appropriate for a given application or environment.

As would be apparent to one of ordinary skill in the art after reading this description, the following are examples and embodiments of the disclosure and are not limited to operating in accordance with these examples. Other embodiments may be utilized and changes may be made without departing from the scope of the exemplary embodiments of the present disclosure.

With proliferation of inexpensive commercial-off-the-shelf (COTS) wireless devices (due to economies of scale) and rapid technology advancements in commercial wireless standards, it is desirable to modify both COTS wireless devices and their associated network design such that in tandem military-grade security is offered for both end-user data as well as over-the-air RF signals.

Embodiments of disclosure allow any closed commercial network to be used for secure and classified high bandwidth communication, linking commercial networks with any isolated network such as network for communicating with: drones, aircraft, ground force hand held radios, or other secure network.

Figure 1 is an illustration of an exemplary wireless communication environment 100 for transmitting and receiving secure information according to an embodiment of the disclosure.

The wireless communication environment 100 comprises an isolated network 102, an ad-hoc network 104, and an infrastructure network 106, a plurality of mobile communication devices 108 each comprising an encryption system 300 for secure communication within the wireless communication environment 100. Each of the isolated network 102, the ad-hoc network 104, and the infrastructure network 106, may comprise, for example but without limitation, an internet

protocol network, a circuit-switched network, a packet-switched network, and a wireless communication network.

The mobile communication devices 108 each comprise the encryption system 300 as explained in more detail below in context of discussion of Figure 3. The encryption system 300 (system 5 300) comprises a high grade transmission security (TRANSEC) that allows the mobile communication device 108 to communicate with the isolated network 102 at high bandwidth (e.g., 50 Mbps) for data (e.g., maps, voice, video) communication. The encryption system 300 allows any closed commercial network such as the ad-hoc network 104, and the infrastructure network 106, to be used for secure and classified high bandwidth communication via a 10 communication link 114. In this manner, these closed commercial networks can be linked with any isolated network such as the isolated network 102.

The mobile communication devices 108, can communicate:

- peer-to-peer in the ad-hoc network 104 via a communication channel 110;
- base-to-user in the infrastructure network 106 via a communication channel 112 to a base 15 station 116;
- bridge the ad-hoc network 104 that interconnects with an isolated communication network;
- bridge the infrastructure network 106 that interconnects with the isolated network 102;
- bridge the ad-hoc network 104 that connects with another peer-to-peer or infrastructure mobile network via the isolated network 102 used as a backbone transit network; and
- 20 - bridge the infrastructure network 106 that connects with another peer-to-peer or infrastructure mobile network via an isolated communication network used as a backbone transit network, or other communication channel.

The mobile communication devices 108 may comprise, for example but without limitation, a desktop computer, a laptop or notebook computer, a DroidTM phone, an iPhoneTM, a mainframe, 25 a server, a client, or any other type of special or general purpose internally or externally GPS

enabled computing device as may be desirable or appropriate for a given application or environment.

The isolated network 102 may comprise communication channels configured to support, for example but without limitation, Wideband Networking Waveform (WNW), Enhanced Position

5 Location Reporting System (EPLRS), Soldier Radio Waveform (SRW), Satellite Communications 165 (SATCOM 165), Demand Assigned Multiple Access (DAMA), Mobile User Objective System (MUOS), Single Channel Ground and Airborne Radio System (SINCGARS), or other secure network. The isolated network 102 can be used for communication with, for example but without limitation, drones, aircraft, ground force hand held
10 radios, or other secure device.

The ad-hoc network 104 and the infrastructure network 106 may comprise a closed commercial network comprising communication channels 110/112 configured to support industry standards communication protocols such as, but without limitation, the Third Generation Partnership

15 Project Long Term Evolution (3GPP LTE)TM, Third Generation Partnership Project 2 Ultra Mobile Broadband (3Gpp2 UMB)TM, Time Division-Synchronous Code Division Multiple Access (TD-SCDMA)TM, and Wireless Interoperability for Microwave Access (WiMAX)TM, and other usually used communication protocols. The communication channels 110/112 may also be configured to support alternate, or additional, wireless data communication protocols, including Wi-FiTM, BluetoothTM, and so on.

20 Figure 2 is an illustration of an encryption process 200 of a network packet 224 according to an embodiment of the disclosure. The network packet 224 comprises a network address 202 (unencrypted network address 202) and a message data 204. The network address 202 may be encrypted via a Transmission Security (TRANSEC) using a GPS time of day 212 (GPS time 212) and a pseudo random number 214 encryption to provide an encrypted network address 208.

25 The message data 204 may be encrypted via a communication security (COMSEC) encryption to provide an encrypted data 210.

An encryption module 222 receives the GPS time 212, and the pseudo random number 214 at an encryptor 218 therein. The encryptor 218 utilizes the GPS time 212, and the pseudo random number 214 to provide an encryption keyword 216 (keyword 216). The keyword 216 may be exclusive-or'ed by an XOR module 220 with the network address 202 to provide the encrypted 5 network address 208.

The TRANSEC is a component of communications security (COMSEC) that results from application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. Goals of transmission security comprise low probability of interception (LPI), low probability of detection (LPD), Antijam — resistance to jamming, or 10 other characteristic. Embodiments of the disclosure can be used for LPI through use of TRANSEC cover using, for example, a GPS time of day such as the GPS time 212 and a pseudo random number such as the pseudo random number 214 for encryption of the network address 202 for transmission through a closed commercial network such as the ad-hoc network 104, and the infrastructure network 106.

15 Encryption is a method of converting plaintext into an unreadable and unintelligible format called ciphertext. The process of converting ciphertext back to a recognizable and readable format is called decryption. Using the process of encryption, a user can store or send sensitive information over public networks (e.g., using existing U.S. SIPRNet protocols) in a more secure manner than just sending or storing data in plaintext. When intended viewers of the data wish to access the 20 encrypted data, they use the process of decryption to convert the ciphertext back to a readable format.

Cryptography can be generally defined as the science of using mathematics to encrypt and 25 decrypt data enabling the storage and transmission of sensitive data in a secure manner. A cryptosystem comprises a cryptographic algorithm, or cipher, which is a mathematical function to encrypt and decrypt data and all of the possible keys and protocols that make it work. Using a key, the cryptographic cipher can be used to convert plaintext to and from ciphertext.

Figure 3 is an illustration of a schematic functional block diagram of an encrypted routing system 300 (system 300, encryption system 300 in Figure 1) according to an embodiment of the disclosure. The various illustrative blocks, modules, processing logic, and circuits described in connection with the system 300 may be implemented or performed with a general purpose processor, a content addressable memory, a digital signal processor, an application specific integrated circuit, a field programmable gate array, any suitable programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof, designed to perform the functions described herein. The embodiment shown in Figure 3 may have functions, material, and structures that are similar to the embodiments shown in Figures 1-2. Therefore common features, functions, and elements may not be redundantly described here. The system 300 may comprise an encryption module 302 (222 in Figure 2), a decryption module 304, a receiver module 306, a transmitter module 308, a network communication module 310, a processor module 312, and a memory module 314. The system 300 generally comprises a physical housing (not shown).

The illustrated system 300 depicts a simple embodiment for ease of description. These and other elements of the system 300 are interconnected together, allowing communication between the various elements of the system 300. In one embodiment, these and other elements of the system 300 may be interconnected together via a data communication bus 316. The system 300 may be implemented in the mobile communication device 108 as explained above.

The system 300 receives the network packet 224 (Figure 2) comprising the encrypted network address 208 and the encrypted data 210, decrypts the encrypted network address 208 to provide unencrypted network address, and transmit the network packet 224 based on the unencrypted network address.

The encryption module 302 (222 in Figure 2) is operable to encrypt the network packet 224 as explained above. Additionally, the encryption module 302 also calculates next stage network address for the network packet through the closed commercial network such as the ad-hoc

network 104, and the infrastructure network 106, and encrypts the next stage network address using a second GPS time and a second pseudo random number to provide the encrypted network address 208. In an embodiment, the second GPS time may be the first GPS time and the second pseudo random number may be the first pseudo random number. In other embodiments, the 5 second GPS time may be different from the first GPS time, and the second pseudo random number may be different from the first pseudo random number.

The decryption module 304 is operable to decrypt the encrypted network address 208 (Figure 2) to provide the unencrypted network address 202. The decryption module 304 receives the 10 network packet 224 from the receiver module 306. The network packet 224 comprises the encrypted network address 208 comprising the unencrypted network address 202 encrypted by the GPS time 212 (Figure 2) and the pseudo random number 214 (Figure 2). The decryption module 304 decrypts the encrypted network address 208 using the GPS time 212 and the pseudo random number 214 to provide the unencrypted network address 202. The network packet 224 can then be transmitted based on the unencrypted network address 202 by the transmitter module 15 308.

The receiver module 306 is operable to receive the network packet 224 via an antenna 318. The network packet 224 comprises the encrypted network address 208 comprising an unencrypted network address encrypted by a first GPS time such as the GPS time 212 and a first pseudo random number such as the pseudo random number 214. The network packet 224 may also 20 comprise an encrypted data such as the encrypted data 210.

The transmitter module 308 is operable to transmit the network packet 224 based on the unencrypted network address 202.

The network communication module 310 is operable to enable the communication channels 110/112/114 for communication between, the ad-hoc network 104, the infrastructure network 25 106, the isolated network 102, or any other internet protocol network circuit-switched network, and packet-switched network.

The receiver module 306 and the transmitter module 308 are coupled to their respective antenna 318/320. Although in a simple system 300 only one antenna 318 for receiving information and only one antenna 320 for transmitting information may be required, a more sophisticated system 300 may be provided with multiple and/or more complex antenna configurations. Additionally, 5 although not shown in this Figure 3, those skilled in the art will recognize that a transmitter may transmit to more than one receiver, and that multiple transmitters may transmit to the same receiver.

Processor module 312 may be implemented, or realized, with a general purpose processor, a content addressable memory, a digital signal processor, an application specific integrated circuit, 10 a field programmable gate array, any suitable programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof, designed to perform the functions described herein. In this manner, a processor may be realized as a microprocessor, a controller, a microcontroller, a state machine, or the like.

A processor may also be implemented as a combination of computing devices, e.g., a 15 combination of a digital signal processor and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a digital signal processor core, or any other such configuration. In practice, processor modules 312 comprise processing logic that is configured to carry out the functions, techniques, and processing tasks associated with the operation of the system 300.

20 In particular, the processing logic is configured to support the secure communication method of the system 300. For example, the processor module 312 may be suitably configured to direct the system 300 to encrypt the unencrypted network address 202 by the first GPS time 212 and the first pseudo random number 214 to provide the encrypted network address 208, and transmit the network packet 224 based on the unencrypted network address 202. For another example, the 25 processor module 312 may be suitably configured to direct the system 300 to decrypt the encrypted network address 208 by the first GPS time 212 and the first pseudo random number

214 to provide the unencrypted network address 202, and transmit the network packet 224 based on the unencrypted network address 202.

Furthermore, the steps of a method or algorithm described in connection with the embodiments disclosed herein may be embodied directly in hardware, in firmware, in a software module 5 executed by processor module 312, or in any practical combination thereof.

The memory module 314, may be realized as a non-volatile storage device (non-volatile semiconductor memory, hard disk device, optical disk device, and the like), a random access storage device (for example, SRAM, DRAM), or any other form of storage medium known in the art. The memory module 314 may be coupled to the processor module 312 respectively such 10 that the processor module 312 can read information from and write information to memory module 314.

As an example, the processor module 312 and memory module 314, may reside in their respective ASICs. The memory module 314 may also be integrated into the processor modules 312 respectively. In an embodiment, the memory module 314 may include a cache memory for 15 storing temporary variables or other intermediate information during execution of instructions to be executed by processor module 312. The memory module 314 may also include non-volatile memory for storing instructions to be executed by the processor module 312.

The memory module 314 may include a database (not shown) for storing the network packet 224 in accordance with an embodiment of the disclosure. The database may be configured to store, 20 maintain, and provide data as needed to support the functionality of the system 300 in the manner described below. Moreover, the database may be a local database coupled to the processor module 312, or may be a remote database, for example, a central network database, and the like. The database may include a lookup table for purposes of storing the encryption information. The memory module 314 may also store, a computer program that is executed by 25 the processor module 312, an operating system, an application program, tentative data used in executing a program processing, or other application.

Those skilled in the art will understand that the various illustrative blocks, modules, circuits, and processing logic described in connection with the embodiments disclosed herein may be implemented in hardware, computer-readable software, firmware, or any practical combination thereof. To clearly illustrate this interchangeability and compatibility of hardware, firmware, and software, various illustrative components, blocks, modules, circuits, and steps are described generally in terms of their functionality.

5 Whether such functionality is implemented as hardware, firmware, or software depends upon the particular application and design constraints imposed on the overall system. Those familiar with the concepts described herein may implement such functionality in a suitable manner for each 10 particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.

15 Figure 4 is an illustration of an exemplary flowchart showing a process 400 for secure communication according to an embodiment of the disclosure. The various tasks performed in connection with the process 400 may be performed by software, hardware, firmware, a computer-readable medium having computer executable instructions for performing the process method, or any combination thereof. The process 400 may be recorded in a computer-readable medium such as a semiconductor memory, a magnetic disk, an optical disk, and the like, and can be accessed and executed, for example, by a computer CPU such as the processor module 312 in which the computer-readable medium is stored.

20 It should be appreciated that process 400 may include any number of additional or alternative tasks, the tasks shown in Figure 4 need not be performed in the illustrated order, and process 400 may be incorporated into a more comprehensive procedure or process having additional functionality not described in detail herein. In practical embodiments, portions of the process 400 may be performed by different elements of the environment 100, the network packet 224, 25 and the system 300 such as: the mobile communication device 108, the encryption module 302, the decryption module 304, the receiver module 306, the transmitter module 308, the network

communication module 310, the processor module 312, the memory module 314, etc. Process 400 may have functions, material, and structures that are similar to the embodiments shown in Figures 1-3. Therefore common features, functions, and elements may not be redundantly described here.

- 5 Process 400 may begin by receiving a network packet such as the network packet 224 comprising an encrypted network address such as the encrypted network address 208 comprising an unencrypted network address such as the unencrypted network address 202 encrypted by a first GPS time and a first pseudo random number such as the first GPS time 212 and the first pseudo random number 214 respectively (task 402).
- 10 Process 400 may continue by decrypting the encrypted network address 208 using the first GPS time 212 and the first pseudo random number 214 to provide the unencrypted network address 202 (task 404).

Process 400 may continue by transmitting the network packet 224 based on the unencrypted network address 202 (task 406).

- 15 Process 400 may continue by calculating a next stage network address for the network packet through a closed commercial network such as the ad-hoc network 104 and the infrastructure network 106 (task 408).

Process 400 may continue by encrypting the next stage network address using a second GPS time and a second pseudo random number to provide the encrypted network address 208 (task

- 20 410). As mentioned above, in an embodiment, the second GPS time may be the first GPS time 212 and the second pseudo random number may be the first pseudo random number 214. In other embodiments, the second GPS time may be different from the first GPS time 212, and the second pseudo random number may be different from the first pseudo random number 214.

Process 400 may continue by transmitting the network packet 224 through the closed

- 25 commercial network (task 412).

While at least one example embodiment has been presented in the foregoing detailed description, it should be appreciated that a vast number of variations exist. It should also be appreciated that the example embodiment or embodiments described herein are not intended to limit the scope, applicability, or configuration of the subject matter in any way. Rather, the foregoing detailed description will provide those skilled in the art with a convenient road map for implementing the described embodiment or embodiments. It should be understood that various changes can be made in the function and arrangement of elements without departing from the scope defined by the claims, which includes known equivalents and foreseeable equivalents at the time of filing this patent application.

10 In this document, the term "module" as used herein, refers to software, firmware, hardware, and any combination of these elements for performing the associated functions described herein. Additionally, for purpose of discussion, the various modules are described as discrete modules; however, as would be apparent one of skilled in the art, two or more modules may be combined to form a single module that performs the associated functions according the embodiments of the
15 present disclosure.

In this document, the terms "computer program product", "computer-readable medium", and the like may be used generally to refer to media such as, for example, memory, storage devices, or storage unit. These and other forms of computer-readable media may be involved in storing one or more instructions for use by the processor modules 312 to cause the processor modules 312 to
20 perform specified operations. Such instructions, generally referred to as "computer program code" or "program code" (which may be grouped in the form of computer programs or other groupings), when executed, enable a method of using a system.

The above description refers to elements or nodes or features being "connected" or "coupled" together. As used herein, unless expressly stated otherwise, "connected" means that one
25 element/node/feature is directly joined to (or directly communicates with) another element/node/feature, and not necessarily mechanically. Likewise, unless expressly stated

otherwise, "coupled" means that one element/node/feature is directly or indirectly joined to (or directly or indirectly communicates with) another element/node/feature, and not necessarily mechanically. Thus, although Figures 1-3 depict example arrangements of elements, additional intervening elements, devices, features, or components may be present in an embodiment of the disclosure.

5 Terms and phrases used in this document, and variations thereof, unless otherwise expressly stated, should be construed as open ended as opposed to limiting. As examples of the foregoing: the term "including" should be read as mean "including, without limitation" or the like; the term "example" is used to provide exemplary instances of the item in discussion, not an exhaustive or 10 limiting list thereof; and adjectives such as "conventional," "traditional," "normal," "standard," "known" and terms of similar meaning should not be construed as limiting the item described to a given time period or to an item available as of a given time, but instead should be read to encompass conventional, traditional, normal, or standard technologies that may be available or known now or at any time in the future.

15 Likewise, a group of items linked with the conjunction "and" should not be read as requiring that each and every one of those items be present in the grouping, but rather should be read as "and/or" unless expressly stated otherwise. Similarly, a group of items linked with the conjunction "or" should not be read as requiring mutual exclusivity among that group, but rather should also be read as "and/or" unless expressly stated otherwise.

20 Furthermore, although items, elements or components of the disclosure may be described or claimed in the singular, the plural is contemplated to be within the scope thereof unless limitation to the singular is explicitly stated. The presence of broadening words and phrases such as "one or more," "at least," "but not limited to" or other like phrases in some instances shall not be read to mean that the narrower case is intended or required in instances where such broadening 25 phrases may be absent. The term "about" when referring to a numerical value or range is

intended to encompass values resulting from experimental error that can occur when taking measurements.

As used herein, unless expressly stated otherwise, "operable" means able to be used, fit or ready for use or service, usable for a specific purpose, and capable of performing a recited or desired

5 function described herein. In relation to systems and devices, the term "operable" means the system and/or the device is fully functional and calibrated, comprises elements for, and meets applicable operability requirements to perform a recited function when activated. In relation to systems and circuits, the term "operable" means the system and/or the circuit is fully functional and calibrated, comprises logic for, and meets applicable operability requirements to perform a

10 recited function when activated.

15

20

25

CLAIMS

1. A method for secure communication, the method comprising:
 - receiving a network packet comprising an encrypted network address comprising an unencrypted network address encrypted by a first GPS time and a first pseudo random number;
 - 5 decrypting the encrypted network address using the first GPS time and the first pseudo random number to provide the unencrypted network address; and
 - transmitting the network packet based on the unencrypted network address.
2. The method of claim 1, further comprising transmitting the network packet through a closed commercial network.
- 10 3. The method of claim 1, further comprising:
 - calculating a next stage network address for the network packet through a closed commercial network; and
 - encrypting the next stage network address using a second GPS time and a second pseudo random number to provide the encrypted network address.
- 15 4. The method of claim 3, wherein the second GPS time is the first GPS time, and the second pseudo random number is the first pseudo random number.
5. The method of claim 3, wherein the second GPS time is different from the first GPS time, and the second pseudo random number is different from the first pseudo random number.
6. A system for secure communication, the system comprising:
 - 20 a receiver module operable to receive a network packet comprising an encrypted network address comprising an unencrypted network address encrypted by a first GPS time and a first pseudo random number;

a decryption module operable to decrypt the encrypted network address using the first GPS time and the first pseudo random number to provide the unencrypted network address; and

a transmitter module operable to transmit the network packet based on the unencrypted network address.

5 7. The system of claim 6, wherein the transmitter module is further operable to transmit the network packet through a closed commercial network.

8. The system of claim 6, further comprising an encryption module operable to:

calculate a next stage network address for the network packet through a closed commercial network; and

10 encrypt the next stage network address using a second GPS time and a second pseudo random number to provide the encrypted network address.

9. The system of claim 8, wherein the second GPS time is the first GPS time, and the second pseudo random number is the first pseudo random number.

10. The system of claim 8, wherein the second GPS time is different from the first GPS time, 15 and the second pseudo random number is different from the first pseudo random number.

11. A computer readable storage medium comprising computer-executable instructions for performing a method for secure communication, the method executed by the computer-executable instructions comprising:

20 receiving a network packet comprising an encrypted network address comprising an unencrypted network address encrypted by a first GPS time and a first pseudo random number;

decrypting the encrypted network address using the first GPS time and the first pseudo random number to provide the unencrypted network address; and

transmitting the network packet based on the unencrypted network address.

12. The computer readable storage medium of claim 11, the method executed by the computer-executable instructions further comprising transmitting the network packet through a closed commercial network.

13. The computer readable storage medium of claim 11, the method executed by the
5 computer-executable instructions further comprising:

calculating a next stage network address for the network packet through a closed commercial network; and

encrypting the next stage network address using a second GPS time and a second pseudo random number to provide the encrypted network address.

10 14. The computer readable storage medium of claim 13, wherein the second GPS time is the first GPS time, and the second pseudo random number is the first pseudo random number.

15. The computer readable storage medium of claim 13, wherein the second GPS time is different from the first GPS time, and the second pseudo random number is different from the first pseudo random number.

15

20

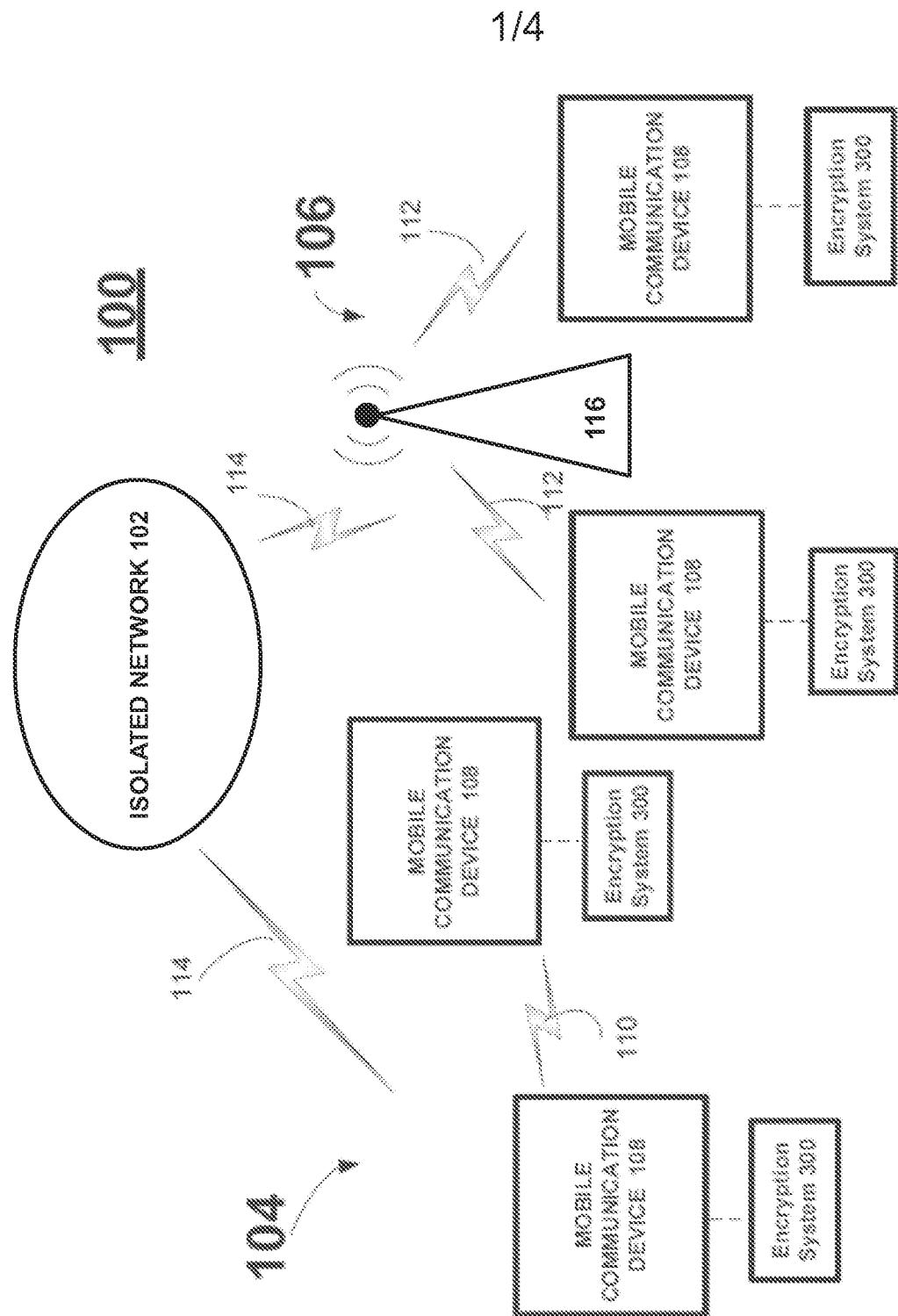


FIG. 1

2/4

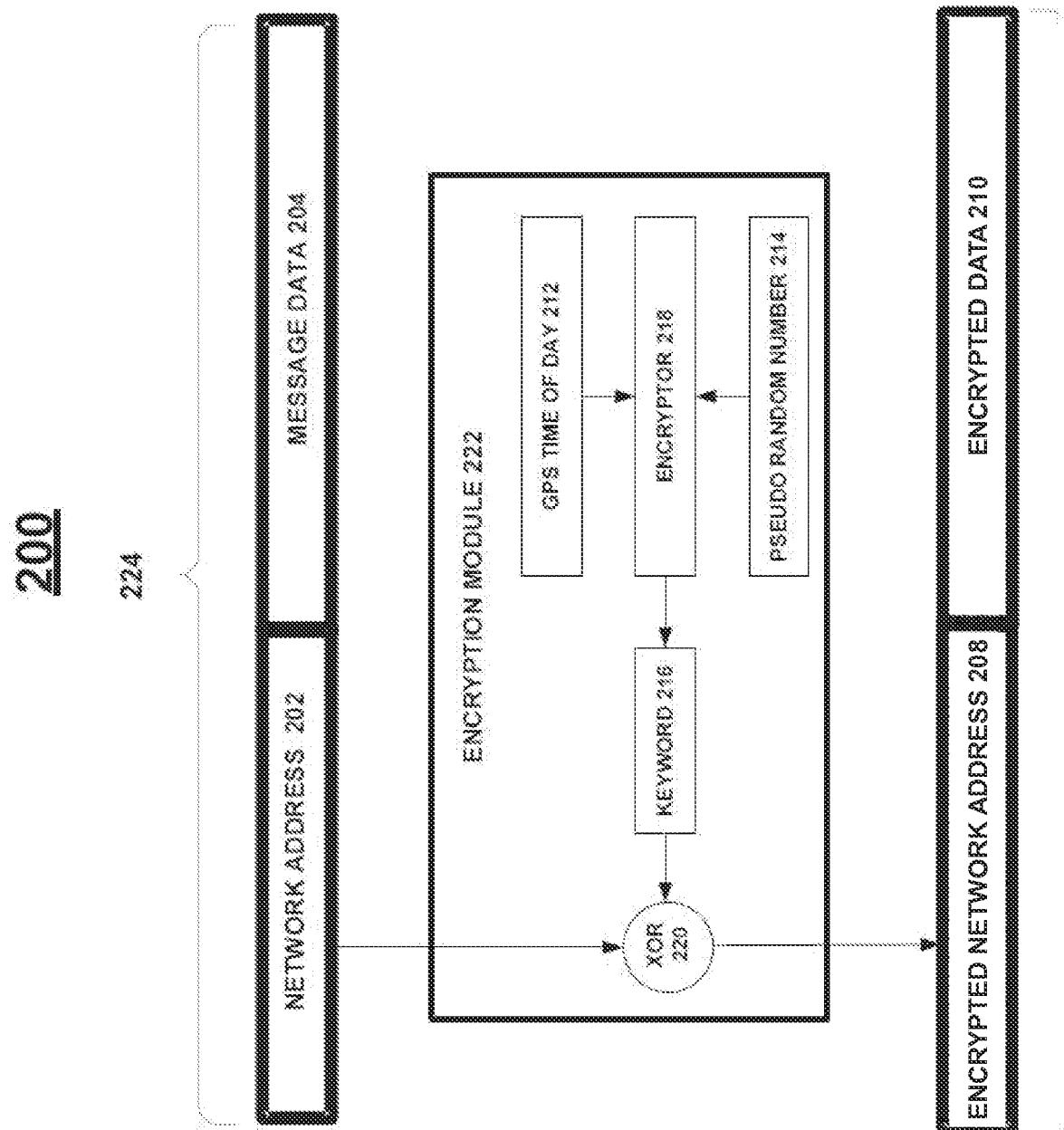


FIG. 2

224

3/4

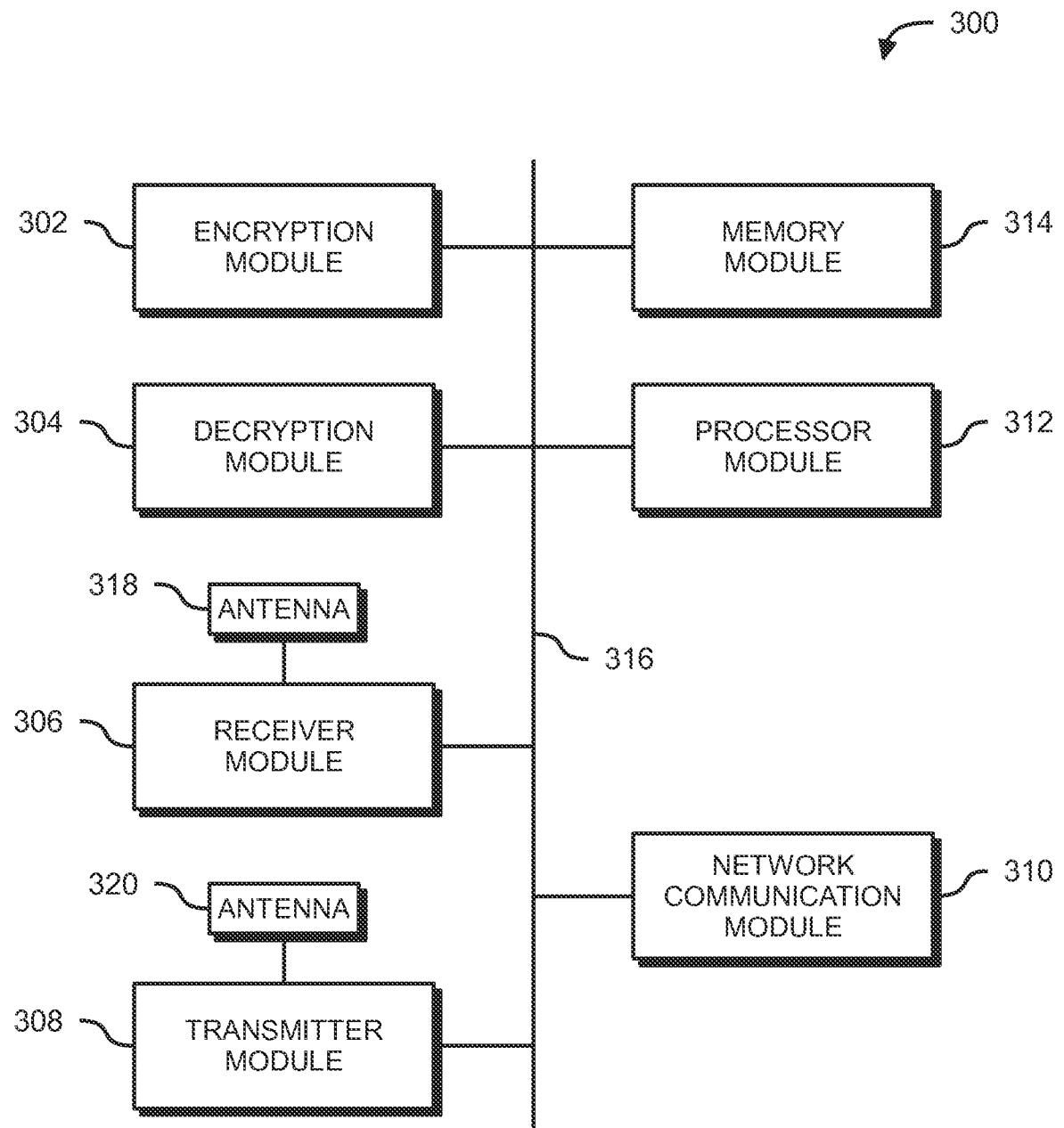


FIG. 3

4/4

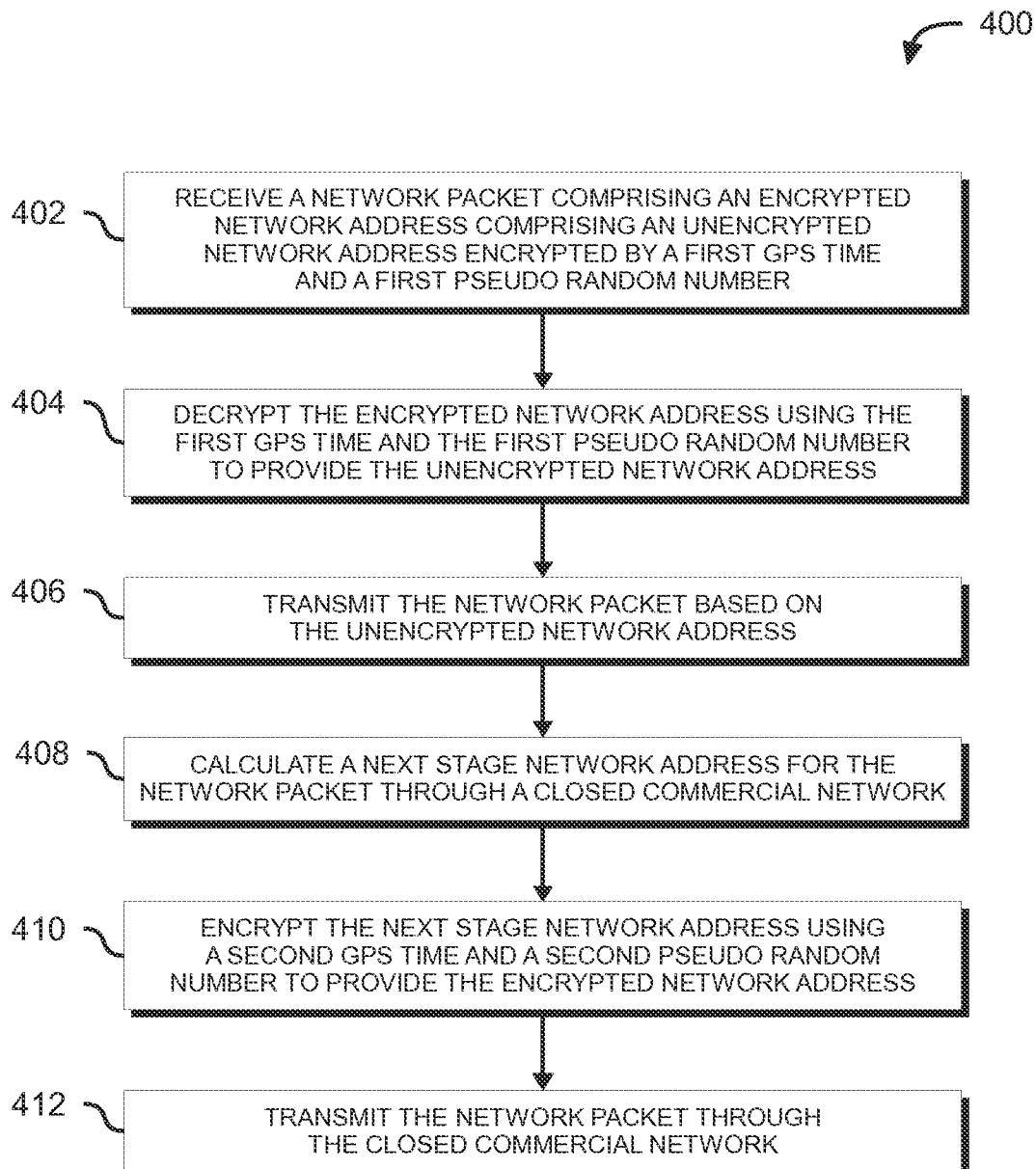


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/069588

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/02 H04L29/06
ADD.

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)
H04W H04L

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)

EPO-Internal, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	<p>Hsien-Chou Liao, Yun-Hsiang Chao, Chia-Yi Hsu: "A Novel Approach for Data Encrypting Depending on User Location", The Tenth Pacific Asia Conference on Information Systems (PACIS 2006)</p> <p>, 22 July 2006 (2006-07-22), pages 470-481, XP002694121, Retrieved from the Internet: URL:http://www.pacis-net.org/file/2006/1117.pdf [retrieved on 2013-03-18]</p> <p>abstract page 470, line 4 page 472, line 4 - line 35 figure 1 page 479, line 26 - line 27</p> <p>-----</p> <p style="text-align: center;">-/-</p>	1-15

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 application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"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

Date of mailing of the international search report

20 March 2013

04/04/2013

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Kufer, Léna

INTERNATIONAL SEARCH REPORT

International application No PCT/US2012/069588

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/098249 A1 (SHIN JUN-BUM [KR] ET AL) 22 April 2010 (2010-04-22) abstract figures 6,7 paragraphs [0008], [0009], [0013] paragraphs [0018], [0019], [0031] paragraphs [0043], [0058], [0063] paragraph [0072] -----	1-15
A	US 2010/088511 A1 (TAVERNIER CEDRIC [FR] ET AL) 8 April 2010 (2010-04-08) paragraphs [0004], [0007], [0012] paragraphs [0022], [0035], [0036] paragraphs [0044], [0058] -----	1-15
A	US 2004/068647 A1 (HARIHARAN RAJARAMAN [US] ET AL HARIHARAN RAJARAMAN [IN] ET AL) 8 April 2004 (2004-04-08) paragraphs [0041] - [0043], [0046] -----	1-15
A	ELMASRY G F ET AL: "Partitioned QOS Solution for Tactical Networks - Addressing the Existence of Encryption", MILITARY COMMUNICATIONS CONFERENCE, 2005. MILCOM 2005. IEEE ATLANTIC CITY, NJ, USA 17-20 OCT. 2005, PISCATAWAY, NJ, USA, IEEE, PISCATAWAY, NJ, USA, 17 October 2005 (2005-10-17), pages 1-6, XP010901239, DOI: 10.1109/MILCOM.2005.1605653 ISBN: 978-0-7803-9393-6 Introduction page 2, lines 1-10 -----	1-15
A	CN 101 466 144 A (UNIV SHANDONG [CN]) 24 June 2009 (2009-06-24) abstract -----	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2012/069588

Patent document cited in search report	Publication date	Patent family member(s)			Publication date
US 2010098249	A1 22-04-2010	KR 20100042457 A	US 2010098249 A1		26-04-2010 22-04-2010
US 2010088511	A1 08-04-2010	EP 2119096 A1	FR 2912020 A1	US 2010088511 A1	18-11-2009 01-08-2008 08-04-2010
				WO 2008095788 A1	14-08-2008
US 2004068647	A1 08-04-2004	US 2004068647 A1	US 2007113274 A1		08-04-2004 17-05-2007
CN 101466144	A 24-06-2009	NONE			