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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 January 2008 (10.01.2008)

PCT

(10) International Publication Number
WO 2008/005162 A2

(51) International Patent Classification:
H04Q 7/38 (2006.01)

(21) International Application Number:
PCT/US2007/013914

(22) International Filing Date: 14 June 2007 (14.06.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/815,245 19 June 2006 (19.06.2006) US
60/832,632 21 July 2006 (21.07.2006) US

(71) Applicant *(for all designated States except US)*: **INTERDIGITAL TECHNOLOGY CORPORATION** [US/US]; 3411 Silverside Road, Concord Plaza, Suite 105, Hagley Building, Wilmington, Delaware 19810 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **WANG, Peter, S.** [US/US]; 412 Pond Path, E. Setauket, New York 11733 (US). **GUCCIONE, Louis, J.** [US/US]; 211 Lincoln Drive, East Chester, NY 10709 (US). **TERRY, Stephen, E.** [US/US]; 15 Summit Avenue, Northport, New York 11768 (US).

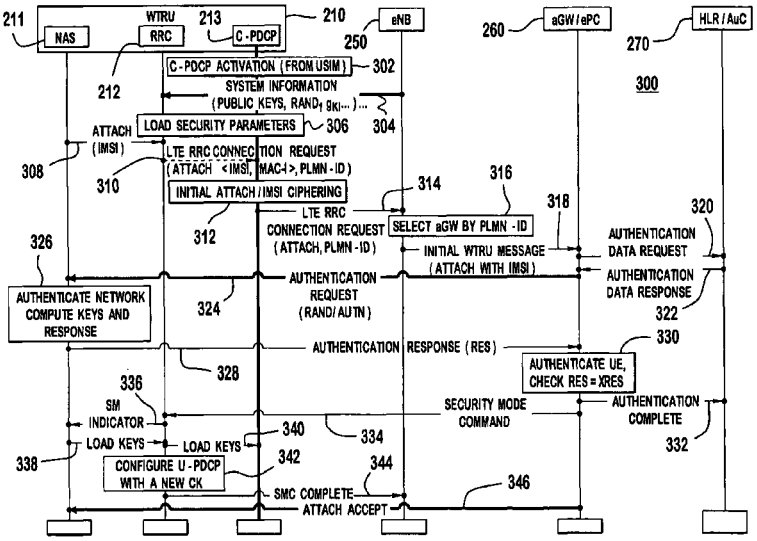
(74) Agent: **BALLARINI, Robert, J.**; Volpe And Koenig, P.C., United Plaza, Suite 1600, 30 S. 17th Street, Philadelphia, Pennsylvania 19103 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR SECURITY PROTECTION OF AN ORIGINAL USER IDENTITY IN AN INITIAL SIGNALING MESSAGE



(57) Abstract: A wireless transmit/receive unit (WTRU) includes a control plane (C-plane) packet data convergence protocol (C-PDCP) layer which performs ciphering of a signaling message. The C-PDCP layer is activated upon power up of the WTRU and initial security parameters are loaded to the C-PDCP layer. An initial connection signaling message and a user identity are ciphered using the initial security parameters even before the WTRU is authenticated. The initial security parameters including a ciphering key (CK) may be generated from system information broadcast from the network. The CK may be a public key for asymmetric encryption, and may be selected from a public key set broadcast by or derived from the network system information. An index of the selected public key may be separately encoded. Alternatively, the index may be communicated by using a Diffie-Hellman key exchange method.

WO 2008/005162 A2

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Express Mail Label No. EV748353363US

[0001] METHOD AND APPARATUS FOR SECURITY PROTECTION OF AN ORIGINAL USER IDENTITY IN AN INITIAL SIGNALING MESSAGE

[0002] FIELD OF INVENTION

[0003] The present invention is related to wireless communication systems. More particularly, the present invention is related to a method and apparatus for security protection of an original user identity (ID) in an initial access signaling message in a wireless communication system including third generation (3G) long term evolution (LTE).

[0004] BACKGROUND

[0005] In a third generation (3G) universal mobile telecommunication system (UMTS), during an initial connection for attachment and authentication procedure, a wireless transmit/receive unit (WTRU) identity, (i.e., international mobile subscriber identity (IMSI)), is transmitted via a radio interface to a core network for authentication purposes. However, the IMSI and some messages exchanged during the initial connection for attachment and authentication procedure are not protected, but transmitted in an open environment unprotected.

[0006] Figure 1 shows an initial attachment and authentication procedure in a 3G UMTS network 10. Upon power up of a WTRU 12, a non-access stratum (NAS) layer 14 of the WTRU 12 sends a signal (ATTACH) to a radio resource control (RRC) layer 16 of the WTRU 12 to trigger an RRC connection (step 102). The RRC layer 16 sends an RRC connection request to a universal terrestrial radio access network (UTRAN) 18 with a WTRU initial identity, (i.e., IMSI), to establish an RRC connection (step 104). The UTRAN 18 responds with an RRC setup request message (step 106). The RRC layer 16 sends an RRC setup complete message to the UTRAN 18 (step 108). The RRC layer 16 then sends a layer 3 message (INITIAL DIRECT TRANSFER) to the UTRAN 18 (step 110).

Petitioner Samsung Ex-1006, 0003

The UTRAN 18 then sends an INITIAL UE MESSAGE with the IMSI to a visitor location register (VLR) 20, (or serving general packet radio services (GPRS) support node (SGSN)) (step 112). A user is identified with the use of the IMSI. Under certain conditions, (e.g., if the user has not been authenticated), the VLR/SGSN 20 requires an authentication and key agreement (AKA) and sends an authentication data request to a home location register (HLR) 22, (or authentication center (AuC)), (step 114). Upon receipt of the authentication data request, the HLR/AuC 22 sends a set of authentication vectors (AVs) to the VLR/SGSN 20 (step 116).

[0007] Each AV contains a quintet of numbers that includes a random number (RAND), an expected response (XRES) which is used to authenticate the user, a cipher key (CK) for establishing confidentiality, an integrity key (IK), and an authentication token (AUTN). The AUTN comprises a sequence number (SQN) hidden by an anonymity key (AK), an authentication management field (AMF) which specifies certain authentication components, (such as algorithms to be used, key lifetime, etc.), and a message authentication code (MAC) which is functionally dependent on the SQN, the AMF, and the RAND.

[0008] The VLR/SGSN 20 sends the RAND and the AUTN from the AV that it has selected to the NAS layer 14 via the UTRAN 18 (steps 118, 120). The NAS layer 14 then authenticates the network by calculating an expected MAC (XMAC) and determining whether the XMAC matches the MAC (step 122). The NAS layer 14 also computes session security keys to the WTRU 12, (i.e., the CK and IK in the AV) at step 122. The key generation is performed using predefined UMTS algorithms which take RAND as input and apply the shared secret key K.

[0009] The NAS layer 14 computes a response (RES) and sends the RES to the VLR/SGSN 20 via the UTRAN 18 (steps 124, 126). The VLR/SGSN 20 determines if the RES matches the XRES to authenticate the WTRU 12 (step 128). An authentication failure occurs if either of these authentication attempts fails at steps 122 and 128. Once mutual authentication has succeeded, the VLR/SGSN 20 sends an authentication complete message to the HLR/AuC 22 (step 130) and a local security activation procedure starts.

Petitioner Samsung Ex-1006, 0004

[0010] The VLR/SGSN 20 sends a security mode command to the UTRAN 18 including the negotiated UMTS encryption algorithms (UEAs) and UMTS integrity algorithms (UIAs), and the current session keys, CK and IK (step 132). As secure communication can now begin the UTRAN 18 sends a security mode command to the RRC layer 16 with a message authentication code for integrity (MAC-I) (step 134). The MAC-I value protects the integrity of the security mode command message. The MAC-I is a type of hash computed by a UIA on the message's contents using the session key IK.

[0011] The RRC layer 16 sends a security mode indicator to the NAS layer 14 (step 136) and the NAS layer 14 loads security session keys IK and CK to the RRC layer 16 (step 138). The RRC integrity protection entity verifies the integrity of the received message by calculating a MAC-I in a similar manner, using the UIA with the IK on the security mode command message's contents, and comparing it to the received MAC-I. The RRC layer 16 also loads the CK to an RLC ciphering entity to start ciphering (step 140). If the authentication codes match, the RRC layer 16 sends a security mode complete message to the UTRAN 18 (step 142). The VLR/SGSN 20 sends an attach accept message to the NAS layer 12 (step 144).

[0012] For the process illustrated in Figure 1, the RRC connection request message with the IMSI, the RRC setup request message, the RRC setup complete message, the initial direct transfer message with an optional IMSI, the authentication request message and the authentication response message are not protected, but transmitted in an open environment unprotected. The fact that the important WTRU identity, (i.e., IMSI), is sent over the air unprotected provokes an "IMSI catching threat." The caught IMSI could be used by a malignant denial of service (DoS) attack or other possible attacks to the network and users.

[0013] Therefore, it would be desirable to provide a method and system for protecting initial control signaling messages and especially the WTRU identity, (i.e., IMSI), during the initial connection for attachment and authentication procedure

Petitioner Samsung Ex-1006, 0005

[0014] SUMMARY

[0015] The present invention is related to a method and apparatus for security protection of an original user identity in an initial access signaling message in a wireless communication system including third generation (3G) LTE. A WTRU includes a control plane (C-plane) packet data convergence protocol (C-PDCP) layer which performs ciphering and integrity protection of a signaling message. The C-PDCP layer is activated upon power up of the WTRU and initial security parameters are loaded to the C-PDCP layer. An initial connection signaling message for network attachment, and a user ID, (e.g., an IMSI), are ciphered using the initial security parameters even before the WTRU is authenticated. The initial security parameters are loaded from a universal subscriber identity module (USIM) and generated from system information broadcast from the network. The system information includes a public key set with at least one public key for asymmetric encryption of the IMSI or information from which the public key(s) can be derived. The initial security parameters for ciphering include a CK. The CK may be a public key or may be selected from the public key set broadcast by or derived from the network system information. An index of the selected public key may be separately encoded. Alternatively, the index may be communicated by using a Diffie-Hellman key exchange method.

[0016] BRIEF DESCRIPTION OF THE DRAWINGS

[0017] A more detailed understanding of the invention may be had from the following description of a preferred embodiment, given by way of example and to be understood in conjunction with the accompanying drawings wherein:

[0018] Figure 1 shows an initial attachment and authentication procedure in a 3G UMTS network;

[0019] Figure 2 shows a wireless communication system in accordance with the present invention;

[0020] Figure 3 is a signaling diagram of a process for attachment and authentication in accordance with the present invention;

Petitioner Samsung Ex-1006, 0006

[0021] Figure 4 shows a ciphering process including conventional f8 ciphering and ciphering parameters;

[0022] Figure 5 shows conventional f9 integrity protection process and parameters;

[0023] Figure 6 shows generation of the IK using f4 algorithm with a random number (RAND) and a shared secret key (K) in accordance with the present invention; and

[0024] Figure 7 shows an example of generation of the FRESH value with the RAND and the shared secret key K.

[0025] DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0026] When referred to hereafter, the terminology "WTRU" includes but is not limited to a user equipment (UE), a mobile station, a fixed or mobile subscriber unit, a pager, a cellular telephone, a personal digital assistant (PDA), a computer, or any other type of user device capable of operating in a wireless environment. When referred to hereafter, the terminology "eNode-B" includes but is not limited to a base station, a site controller, an access point (AP), or any other type of interfacing device capable of operating in a wireless environment.

[0027] Figure 2 shows a wireless communication system 200 in accordance with the present invention. The system 200 includes a WTRU 210 and an LTE network 230. The WTRU 210 includes a non-access stratum (NAS) layer 211, an RRC layer 212, a C-PDCP layer 213, a U-plane PDCP (U-PDCP) layer 214, and lower layers including an RLC layer 215, a medium access control layer 216 and a physical layer 217. The RRC layer 212 includes an integrity protection entity 218. The C-PDCP layer 213 includes a C-plane cipher entity 219 and the U-PDCP layer 214 includes a U-plane cipher entity 220. The LTE network 230 includes an NAS layer 231, an RRC layer 232, a C-PDCP layer 233, and a U-PDCP layer 234. The RRC layer 232 includes an integrity protection entity 235. The C-PDCP layer 233 includes a C-plane cipher entity 236 and the U-PDCP layer 234 includes a U-plane cipher entity 237. In a C-plane, the RRC layers 212 and 232 are responsible for integrity protection, and the C-PDCP layers 213 and

Petitioner Samsung Ex-1006, 0007

233 are responsible for ciphering of the NAS/RRC control signaling messages, while in a U-plane the U-PDCP layers 214 and 234 are responsible for Internet protocol (IP) header compression and ciphering.

[0028] In accordance with the present invention, the C-PDCP layers 213 and 233 perform ciphering of the previously unprotected initial NAS signaling messages and WTRU IMSI transmission. Otherwise, it is transparent to control signaling messages. The present invention provides methods for initial loading and generation of security parameters, encryption key arrangements between the WTRU 210 and a network, IMSI encryption, and WTRU signaling adjustment for the IMSI encryption for the initial NAS signaling messages, which will be explained in detail hereinafter.

[0029] Figure 3 is a signaling diagram of a process 300 for attachment and authentication in accordance with the present invention. Upon WTRU power up, the C-PDCP layer 213 of the WTRU 210 is activated (step 302). The RRC layer 212 receives system information broadcast by an eNode-B 250 and forwards it to the C-PDCP layer 213 (step 304). The system information includes information for the initial security parameters including, but not limited to, a public key(s) or key derivation information, a random number(s) (RAND(s) and/or a key seed g_{KI}.

[0030] Initial security parameters are loaded into the C-PDCP layer 213 at step 306, which will be explained in detail hereinafter. The C-PDCP initial security parameter loading is mainly from a universal subscriber identity module (USIM) of the WTRU 210 where consistent security parameters and runtime values for the WTRU 210 are updated and stored. The C-PDCP initial security parameter may additionally be from the system information broadcast from the eNode-B 250, which may include the public key information. The initial security parameters for ciphering include a CK and an IK. The CK may be a public key or may be selected from the public key set broadcast by or derived from the network system information. The C-PDCP layer 213 is ready to operate, (i.e., ready to perform cipher/decipher when a first NAS/RRC signaling message, (e.g., an ATTACH or those messages triggered by it), is to be transmitted even before the WTRU 210 is authenticated.

Petitioner Samsung Ex-1006, 0008

[0031] The NAS layer 211 triggers an RRC connection by sending an attach message along with an IMSI to the RRC layer 212 (step 308). The RRC layer 212 sends an LTE RRC connection request to the C-PDCP layer 213 including the attach message and MAC-I and preferably a public land mobile network (PLMN) identity (ID) (step 310). The C-PDCP layer 213 then performs ciphering on the attach message and the IMSI with the initial CK (from USIM or system information broadcast), and sends an LTE RRC connection request message including ciphered attach message and IMSI along with the MAC-I from the RRC layer 212 (steps 312, 314). Unlike the conventional attachment procedure, the attach message and the IMSI are protected with initial CK and IK.

[0032] The LTE RRC connection request message may also include a second seed, g_{FRESH}, for Diffie-Hellman key exchange, which will be explained in detail hereinafter. The eNode-B 250 selects an appropriate aGW 260 based on the PLMN ID included in the connection request message (step 316). The eNode-B 250 forwards the attach message with the IMSI to the selected aGW 260 (step 318).

[0033] If the user has not been authenticated, the aGW 260 sends an authentication data request to an HLR 270, (or AuC) (step 320). Upon receipt of the authentication data request, the HLR/AuC 270 sends an authentication data response including a set of authentication vectors (AVs) to the aGW 260 (step 322).

[0034] The aGW 260 sends an authentication request message to the NAS layer 211 of the WTRU 210 including the RAND and the AUTN from the first AV (step 324). The connection response message does not have to be ciphered or integrity protected. Alternatively, the connection response message may be ciphered at the eNode-B 250 with a public key with an index from the HLR/AuC 270 with the conventional symmetric ciphering algorithm. The NAS layer 211 then authenticates the network by calculating an expected MAC (XMAC) and determining whether the XMAC matches the MAC (step 326). The NAS layer 211 also computes new session keys, (i.e., CK and IK in the AV) at step 326. The key generation is performed using predefined algorithms which take RAND as

Petitioner Samsung Ex-1006, 0009

input and apply the shared secret key K.

[0035] The NAS layer 211 computes a response (RES) and sends an authentication response message including the RES to the aGW 260 (step 328). The authentication response message may optionally be protected with the initial CK and/or IK. The aGW 260 determines if the RES matches the XRES to authenticate the WTRU 210 (step 330). An authentication failure occurs if either of these authentication attempts fails at steps 326 and 330. Once mutual authentication has succeeded, the aGW 260 sends an authentication complete message to the HLR/AuC 270 (step 332).

[0036] The aGW 260 sends a security mode command message to the RRC layer 212 of the WTRU 210 (step 334). The RRC layer 212 sends a security mode indicator to the NAS layer 211 (step 336). The NAS layer 211 loads session keys to the RRC layer 212 (step 338) and to the C-PDCP layer 213 (step 340). The RRC layer 212 then configures a U-PDCP layer (not shown in Figure 3) with a new CK for U-plane ciphering (step 342). The RRC layer 212 verifies the integrity of the received security mode command message by calculating a MAC-I using the IK on the security mode command message's contents, and comparing the calculated MAC-I to the received MAC-I. If they match, the RRC layer 212 sends a security mode complete message to the eNode-B 250 (step 344). The aGW 260 sends an attach accept message to the NAS layer 211 (step 346) and secure communication, (ciphering, deciphering, and integrity protection), begins.

[0037] Initial loading of ciphering parameters at step 306 is explained hereinafter. Ciphering algorithm to be used is one of the parameters to be selected. An initial ciphering algorithm may be an asymmetric encryption algorithm and a default ciphering algorithm later may be a symmetric algorithm such as the f8 algorithm. However, any other ciphering algorithm may be used. Hereinafter, the present invention will be explained with reference to f8 algorithm parameters for illustration purpose.

[0038] Figure 4 shows a ciphering process including conventional f8 ciphering and ciphering parameters. The ciphering algorithm may be a conventional symmetric ciphering algorithm such as f8 or an asymmetric

Petitioner Samsung Ex-1006, 0010

encryption algorithm used for the ciphering with public and private keys. The ciphering parameters necessary for the f8 algorithm include CK 402, COUNT-C value 404, Bearer ID 406, Direction value 408, and Length value 410. The WTRU 210 generates a keystream block 412 using the f8 algorithm and adds the keystream block 412 to an unciphered plain text input data block 414 to generate a ciphered data block 416, which is transmitted to the network 230. The network 230 also generates a keystream block 418 using the same f8 algorithm and same parameters and adds the generated keystream block 418 to the received ciphered data block 416 to recover the plain text data block 420. The ciphering parameters for the asymmetric encryption algorithm may have at least the CK 402 for the public/private key pair and may have other parameters.

[0039] The CK 402 may be a public/private key-pair in an asymmetric encryption system. The WTRU 210 uses the public key for ciphering the whole or a part of the uplink NAS message and/or the whole or a part of the RRC initial access message including the IMSI, and the network 230 deciphers the ciphered NAS message with a corresponding private key. The CK 402 may be a pre-arranged public/private key between the WTRU 210 and the network 230. Alternatively, the public key may be broadcast via the system information. The network 230 may broadcast only one public key, or a set of n public keys, ($k_1, \ldots, k_n$) or information for key derivation.

[0040] If a set of public keys are broadcast, the WTRU 210 selects one from the public key set. In selecting the public key, the WTRU 210 may use the FRESH value to compute an index into the public key set, (e.g., the index a = FRESH % n) to select the initial CK 402. Alternatively, the WTRU 210 may use its IMSI value for the key index, (i.e., the index $a = IMSI \% n$) to select the initial CK 402. With this scheme, the randomness of the key usage is increased and it becomes more difficult for security attackers.

[0041] Since the network 230 does not know the FRESH value before the IMSI has been correctly decoded and, as a result, cannot independently calculate the index of the selected public key, information about the selected public key should be communicated between the WTRU 210 and the network 230. The

Petitioner Samsung Ex-1006, 0011

WTRU 210 may include the index of the selected public key in the NAS message. For example, the WTRU 210 encodes the index a of the selected public key with a pre-agreed public key, (say k_I), and the rest of the NAS or RRC message including the IMSI with the selected public key k_a. The network 230 first decodes the index a, and then decodes the whole message with the selected public key k_a including the IMSI.

[0042] Alternatively, the public key may be selected using a Diffie-Hellman key exchange method. The LTE network 230 and the WTRU 210 agree on two values, (a very large prime number p and a generator g of the multiplicative group F_p^* of the field F_p), that are publicly known. The LTE network 230 broadcasts via system information a set of public keys with a first seed, g_{KI} (where a randomly selected KI is such that $1 \le KI \le p-2$ and $g_{KI} \equiv g^{KI} \bmod p$). The set of public keys may be from a larger group of encryption keys with random periodicity and order. The WTRU 210 randomly selects a value $KIn2$, ($1 \le KIn2 \le p-2$), to compute a second seed, $g_{KIn2} \equiv g^{KIn2} \bmod p$. The WTRU 210 then computes $k' \equiv (g_{KI})^{KIn2} \bmod p$. The public key index $a = k' \, mod \, n$, where n is the current number of public keys broadcast from the system information with the first seed, g_{KI}. The computed a is an index to the public key set for the chosen public key k_a. The WTRU 210 ciphers the NAS or the RRC message including the IMSI with the selected public k_a and includes the second seed, g_{KIn2}, in the NAS or RRC message to the LTE network 230. The second seed is not encrypted. The LTE network 230 first takes the unencrypted second seed, g_{KIn2}, and computes $k \equiv (g_{KIn2})^{KI} \bmod p$. The index a is then obtained by $a \equiv k \bmod n$ for the private key index a. The LTE network 230 then decodes the whole message with the private key corresponding to public key k_a.

[0043] The COUNT-C value 404 may be a pre-arranged value known only to the WTRU 210 and the LTE network 230 at the initial stage. Alternatively, the COUNT-C value 404 may be the START value (or an equivalent) stored in the USIM and its network counterpart combined with other values known only

Petitioner Samsung Ex-1006, 0012

between the WTRU 210 and the LTE network 230, (e.g., NAS message sequence number). Alternatively, the COUNT-C value 404 may be a computed value by the WTRU 210 and the LTE network 230 as in the case of FRESH value derivation.

[0044] The Bearer ID 406 may be the configured radio bearer ID value of the channel such as '3' for signaling radio bearer 3 (SRB-3). Alternatively, the Bearer ID 406 may be some pre-arranged value. The Direction value 408 is set to '0' for uplink. The Length value 410 is the NAS or RRC message (including the IMSI) length in unit of a bit.

[0045] Initial loading of integrity protection parameters at step 306 is explained hereinafter. The initial integrity protection can help combat the denial of service attack. Integrity protection algorithm to be used is one of the parameters to be selected. A default integrity protection algorithm may be f9 algorithm. However, any other integrity protection algorithm may be used. Hereinafter, the present invention will be explained with reference to f9 algorithm for illustration purpose.

[0046] Figure 5 shows conventional f9 integrity protection process and parameters. The parameters necessary for the f9 algorithm include IK 502, COUNT-I value 504, Message 506, Direction value 508, and FRESH value 510. The WTRU 210 uses the initial IK 502 to generate an MAC-I 512 for the first NAS/RRC message and sends the generated MAC-I 512 to the network 230 along with the NAS/RRC message. The LTE network 230 generates an expected MAC-I (XMAC-I) 514 with the same parameters 502-510 and compares the received MAC-I 512 and the XMAC-I 514 to verify the message integrity after it has decoded the IMSI for the WTRU 210.

[0047] The IK 502 may be generated by the WTRU 210 (and the network 230) at the initial C-PDCP activation and configuration using a RAND value received from the system information. For example, the IK 502 may be generated by using f4 algorithm with a random number (RAND) 602 and a shared secret key (K) 604 as shown in Figure 6. Given the secret key K 604, which is shared between the WTRU 210 and the network 230 via IMSI, the

Petitioner Samsung Ex-1006, 0013

generated IK 502 bears affinity to the unique association between the WTRU 210 and the network 230. It, in turn, enables the MAC-I generated by the integrity protection algorithm f9 bearing the signature of a particular WTRU.

[0048] The COUNT-I value 504 may be a pre-arranged value known only to the WTRU 210 and the network 230 at the initial stage. Alternatively, the COUNT-I value 504 may be set to the START value (or an equivalent) stored in the USIM and its network counterpart combined with other values known only between the WTRU 210 and the network 230, (e.g., the NAS message sequence number). Alternatively, the COUNT-I value 504 may be a computed value by the WTRU 210 and the network 230 as in the case of FRESH value derivation.

[0049] The Message parameter 506 may be the NAS/RRC message itself with the radio bearer identity appended in front of the message. The Direction value 508 is set to a certain value, (e.g., '0'), for uplink. The FRESH value 510 may be selected from a set of pre-arranged FRESH values ($FRESH_0$, $FRESH_1$, ..., $FRESH_{n-1}$) between the WTRU 210 and the network 230, using the IK to compute the index m, (e.g., m = IK % n). Alternatively, the FRESH value 510 may be generated by using a FRESH value generation algorithm with the RAND 602 and the shared secret key 604 as input, as shown in Figure 7.

[0050] Initial loading of these security parameters enables the C-PDCP layer 212 to enter an operational state when the first NAS signal message is to be transmitted from the WTRU 210. This also enables the C-PDCP layer 212 to decipher subsequent incoming and outgoing NAS signaling messages, if necessary. The C-PDCP layer 212 may switch to the security parameters generated from the normal AKA procedure when it is successfully performed.

[0051] The present invention is also applicable to the downlink NAS message encryption in the initial stage before AKA completion. In order to have the downlink encryption work before AKA, the LTE network 230 needs to encrypt the NAS/RRC message using the same "public key" (given the network has all the public/private keys and also knowing the key-index) that the WTRU 210 has used for the first uplink message/IMSI and the encryption algorithm needs to be a symmetric algorithm such as f8.

Petitioner Samsung Ex-1006, 0014

[0052] Embodiments.

[0053] 1. A method for security protection of a user ID in an initial connection signaling message in a wireless communication system including a WTRU, the WTRU including a C-PDCP layer for performing ciphering and integrity protection of an initial connection signaling message.

[0054] 2. The method of embodiment 1 comprising activating the C-PDCP layer upon power up of the WTRU.

[0055] 3. The method of embodiment 2 comprising loading initial security parameters to the C-PDCP layer.

[0056] 4. The method of embodiment 3 comprising ciphering the initial connection signaling message including the user ID using the initial security parameters.

[0057] 5. The method of embodiment 4 comprising sending the ciphered initial connection signaling message and the user ID to a network.

[0058] 6. The method as in any one of embodiments 3-5, wherein the initial security parameters are loaded from a USIM.

[0059] 7. The method as in any one of embodiments 3-6, wherein the initial security parameters are generated from system information broadcast from the network.

[0060] 8. The method of embodiment 7, wherein the system information includes at least one public key or information for deriving a public key.

[0061] 9. The method as in any one of embodiments 1-8, wherein the initial connection signaling message includes a PLMN identity.

[0062] 10. The method as in any one of embodiments 5-9, further comprising the network sending an authentication request message to the WTRU including a random number and an authentication token.

[0063] 11. The method of embodiment 10 comprising the WTRU authenticating the network based on the random number and the authentication token.

Petitioner Samsung Ex-1006, 0015

[0064] 12. The method of embodiment 11 comprising the WTRU computing session keys and an RES.

[0065] 13. The method of embodiment 12 comprising the WTRU sending an authentication response message including the RES to the network.

[0066] 14. The method of embodiment 13 comprising the network authenticating the WTRU using the RES.

[0067] 15. The method of embodiment 14 comprising the network sending a security mode command message to the WTRU.

[0068] 16. The method as in any one of embodiments 13-15, wherein the authentication response message is protected by using the initial security parameters.

[0069] 17. The method as in any one of embodiments 15-16, wherein the network ciphers a downlink control message including the security mode command message with a key used for ciphering the initial connection signaling message using a symmetric encryption algorithm.

[0070] 18. The method as in any one of embodiments 15-17, further comprising configuring a U-plane PDCP layer with a new session key for U-plane data ciphering.

[0071] 19. The method as in any one of embodiments 3-18, wherein a ciphering algorithm to be used is one of the initial security parameters.

[0072] 20. The method of embodiment 19, wherein the ciphering algorithm is f8 algorithm and the initial security parameters include a CK, a COUNT-C value, a bearer ID, a direction value, and a length value.

[0073] 21. The method of embodiment 20, wherein the COUNT-C value is a pre-arranged value known only to the WTRU and the network.

[0074] 22. The method of embodiment 20, wherein the COUNT-C value is a START value stored in a USIM combined with a pre-agreed value known between the WTRU and the network.

[0075] 23. The method of embodiment 22, wherein the pre-agreed value is an NAS layer sequence number.

Petitioner Samsung Ex-1006, 0016

[0076] 24. The method of embodiment 20, wherein the COUNT-C value is a computed value by the WTRU and the network.

[0077] 25. The method as in any one of embodiments 20-24, wherein the bearer ID is a signaling radio bearer ID number.

[0078] 26. The method as in any one of embodiments 20-24, wherein the bearer ID is a pre-arranged value between the WTRU and the network.

[0079] 27. The method as in any one of embodiments 20-26, wherein the direction value is set to '0' for uplink.

[0080] 28. The method as in any one of embodiments 4-19, wherein a ciphering algorithm is an asymmetric encryption algorithm.

[0081] 29. The method of embodiment 28, wherein the ciphering algorithm uses a CK which is a pre-arranged public/private key-pair between the WTRU and the network.

[0082] 30. The method of embodiment 29, wherein the public key is broadcast via system information by the network.

[0083] 31. The method of embodiment 30, wherein the WTRU selects a public key from a public key set comprising a plurality of public keys.

[0084] 32. The method of embodiment 31, wherein the WTRU uses its IMSI value to select an index into the public key set to select a public key.

[0085] 33. The method of embodiment 31, wherein the WTRU uses a FRESH value to select an index into the public key set to select a public key.

[0086] 34. The method of embodiment 33, wherein the WTRU encrypts the index with a pre-agreed public key and includes the encrypted index in the connection request message.

[0087] 35. The method as in any one of embodiments 30-34, wherein the system information includes a first key index seed and the connection request message includes a second key index seed, and the public key is selected using a Diffie-Hellman key exchange method.

[0088] 36. The method as in any one of embodiments 1-35, wherein an integrity protection algorithm to be used is one of the initial security parameters.

Petitioner Samsung Ex-1006, 0017

[0089] 37. The method of embodiment 36, wherein the integrity protection algorithm is f9 algorithm, and the initial security parameters include an IK, a COUNT-I value, a message, a direction value, and a FRESH value.

[0090] 38. The method of embodiment 37, wherein the IK is generated by the WTRU using a random number received from the network via system information and a shared secret key K.

[0091] 39. The method of embodiment 37, wherein the IK is generated by using f4 algorithm.

[0092] 40. The method as in any one of embodiments 37-39, wherein the COUNT-I value is a pre-arranged value known to the WTRU and the network.

[0093] 41. The method as in any one of embodiments 37-40, wherein the COUNT-I value is set to a START value stored in a USIM combined with a pre-agree value known between the WTRU and the network.

[0094] 42. The method of embodiment 41, wherein the pre-agreed value is an NAS layer sequence number.

[0095] 43. The method as in any one of embodiments 37-42, wherein the COUNT-I value is a computed value by the WTRU and the network.

[0096] 44. The method as in any one of embodiments 37-43, wherein the direction value is set to '0' for uplink.

[0097] 45. The method as in any one of embodiments 37-44, wherein the message is a radio bearer ID plus a first NAS message.

[0098] 46. The method as in any one of embodiments 37-45, wherein the FRESH value is selected from a set of pre-arranged FRESH values between the WTRU and the network.

[0099] 47. The method of embodiment 46, wherein the IK is used to compute an index for the FRESH value.

[00100] 48. The method as in any one of embodiments 37-45, wherein the FRESH value is generated by using a FRESH value generation algorithm with a random number broadcast via system information and a shared secret key K.

[00101] 49. The method as in any one of embodiments 1-48, wherein the wireless communication system is a 3G LTE.

Petitioner Samsung Ex-1006, 0018

[00102] 50. A WTRU for security protection of a user ID in an initial connection signaling message in a wireless communication system.

[00103] 51. The WTRU of embodiment 50, comprising an NAS layer configured to generate a first control signaling message and trigger a connection to a network.

[00104] 52. The WTRU as in any one of embodiments 50-51, comprising an RRC layer configured to generate a second control signaling message and perform integrity protection of the first and second control signaling messages.

[00105] 53. The WTRU as in any one of embodiments 51-52, comprising a C-PDCP layer configured to perform ciphering of at least one of the first and second control signaling messages including an initial connection signaling message and the user ID using initial security parameters that are loaded to the C-PDCP layer upon power up of the C-PDCP layer and send the ciphered initial connection signaling message and the user ID to a network.

[00106] 54. The WTRU of embodiment 53, wherein the initial security parameters are loaded from a USIM.

[00107] 55. The WTRU of embodiment 53, wherein the initial security parameters are generated from system information broadcast from the network.

[00108] 56. The WTRU of embodiment 55, wherein the system information includes at least one public key or information for deriving a public key.

[00109] 57. The WTRU as in any one of embodiments 53-56, wherein the initial connection signaling message includes a PLMN identity.

[00110] 58. The WTRU as in any one of embodiments 51-57, wherein the NAS layer is configured to authenticate the network based on a random number and an authentication token included in an authentication request message from the network, and compute session keys and send an authentication response message including an RES to the network so that the network authenticates the WTRU using the RES.

[00111] 59. The WTRU of embodiment 58, wherein the authentication response message is protected by using the initial security parameters.

Petitioner Samsung Ex-1006, 0019

[00112] 60. The WTRU as in any one of embodiments 52-59, further comprising a U-plane PDCP layer for processing U-plane data, the RRC layer loads a new session key to the U-plane PDCP layer for U-plane ciphering.

[00113] 61. The WTRU as in any one of embodiments 53-60, wherein a ciphering algorithm to be used is one of the initial security parameters.

[00114] 62. The WTRU of embodiment 61, wherein the ciphering algorithm is an f8 algorithm, wherein the initial security parameters include at least one of a CK, a COUNT-C value, a bearer ID, a direction value, and a length value.

[00115] 63. The WTRU of embodiment 62, wherein the COUNT-C value is a pre-arranged value known only to the WTRU and the network.

[00116] 64. The WTRU of embodiment 62, wherein the COUNT-C value is a START value stored in a USIM combined with a pre-agreed value known between the WTRU and the network.

[00117] 65. The WTRU of embodiment 64, wherein the pre-agreed value is an NAS layer sequence number.

[00118] 66. The WTRU of embodiment 62, wherein the COUNT-C value is a computed value by the WTRU and the network.

[00119] 67. The WTRU as in any one of embodiments 62-66, wherein the bearer ID is a signaling radio bearer ID number.

[00120] 68. The WTRU as in any one of embodiments 62-66, wherein the bearer ID is a pre-arranged value between the WTRU and the network.

[00121] 69. The WTRU as in any one of embodiments 62-68, wherein the direction value is set to '0' for uplink.

[00122] 70. The WTRU as in any one of embodiments 53-69, wherein a ciphering algorithm is an asymmetric encryption algorithm.

[00123] 71. The WTRU of embodiment 70, wherein the ciphering algorithm uses a CK which is a pre-arranged public/private key-pair between the WTRU and the network.

[00124] 72. The WTRU of embodiment 71, wherein the public key is broadcast via system information.

Petitioner Samsung Ex-1006, 0020

[00125] 73. The WTRU of embodiment 72, wherein the C-PDCP layer selects a public key from a public key set comprising a plurality of public keys.

[00126] 74. The WTRU of embodiment 73, wherein the C-PDCP layer uses the user ID to select an index into the public key set.

[00127] 75. The WTRU of embodiment 73, wherein the C-PDCP layer uses a FRESH value to select an index into the public key set.

[00128] 76. The WTRU as in any one of embodiments 74-75, wherein the C-PDCP layer encrypts the index with a pre-agreed public key and includes the encrypted index in the connection request message.

[00129] 77. The WTRU as in any one of embodiments 74-76, wherein the system information includes a first key index seed and the connection request message includes a second key index seed, wherein the public key is selected using a Diffie-Hellman key exchange method.

[00130] 78. The WTRU as in any one of embodiments 53-77, wherein an integrity protection algorithm to be used is one of the initial security parameters.

[00131] 79. The WTRU of embodiment 78, wherein the integrity protection algorithm is an f9 algorithm, and parameters include an IK, a COUNT-I value, a message, a direction value, and a FRESH value.

[00132] 80. The WTRU of embodiment 79, wherein the IK is generated by the WTRU using a random number received via system information and a shared secret key K.

[00133] 81. The WTRU of embodiment 79, wherein the IK is generated by using an f4 algorithm.

[00134] 82. The WTRU as in any one of embodiments 79-81, wherein the COUNT-I value is a pre-arranged value known to the WTRU and the network.

[00135] 83. The WTRU as in any one of embodiments 79-81, wherein the COUNT-I value is set to a START value stored in a USIM combined with a pre-agree value known between the WTRU and the network.

[00136] 84. The WTRU of embodiment 83, wherein the pre-agreed value is an NAS layer sequence number.

Petitioner Samsung Ex-1006, 0021

[00137] 85. The WTRU as in any one of embodiments 79-81, wherein the COUNT-I value is a computed value by the WTRU and the network.

[00138] 86. The WTRU as in any one of embodiments 79-85, wherein the direction value is set to '0' for uplink.

[00139] 87. The WTRU as in any one of embodiments 79-86, wherein the message is a radio bearer ID plus a first NAS message.

[00140] 88. The WTRU as in any one of embodiments 79-87, wherein the FRESH value is selected from a set of pre-arranged FRESH values between the WTRU and the network.

[00141] 89. The WTRU of embodiment 88, wherein the IK is used to compute an index for the FRESH value.

[00142] 90. The WTRU of embodiment 88, wherein the FRESH value is generated by using a FRESH value generation algorithm with a random number broadcast via system information and a shared secret key K.

[00143] 91. The WTRU as in any one of embodiments 50-90, wherein the wireless communication system is a 3G LTE.

[00144] 92. The WTRU as in any one of embodiments 50-91, wherein the network ciphers a downlink control message with a key used for ciphering the initial connection signaling message using a symmetric encryption algorithm.

[00145] Although the features and elements of the present invention are described in the preferred embodiments in particular combinations, each feature or element can be used alone without the other features and elements of the preferred embodiments or in various combinations with or without other features and elements of the present invention. The methods or flow charts provided in the present invention may be implemented in a computer program, software, or firmware tangibly embodied in a computer-readable storage medium for execution by a general purpose computer or a processor. Examples of computer-readable storage mediums include a read only memory (ROM), a random access memory (RAM), a register, cache memory, semiconductor memory devices, magnetic media such as internal hard disks and removable disks, magneto-

Petitioner Samsung Ex-1006, 0022

optical media, and optical media such as CD-ROM disks, and digital versatile disks (DVDs).

[00146] Suitable processors include, by way of example, a general purpose processor, a special purpose processor, a conventional processor, a digital signal processor (DSP), a plurality of microprocessors, one or more microprocessors in association with a DSP core, a controller, a microcontroller, Application Specific Integrated Circuits (ASICs), Field Programmable Gate Arrays (FPGAs) circuits, any other type of integrated circuit (IC), and/or a state machine.

[00147] A processor in association with software may be used to implement a radio frequency transceiver for use in a wireless transmit receive unit (WTRU), user equipment (UE), terminal, base station, radio network controller (RNC), or any host computer. The WTRU may be used in conjunction with modules, implemented in hardware and/or software, such as a camera, a video camera module, a videophone, a speakerphone, a vibration device, a speaker, a microphone, a television transceiver, a hands free headset, a keyboard, a Bluetooth® module, a frequency modulated (FM) radio unit, a liquid crystal display (LCD) display unit, an organic light-emitting diode (OLED) display unit, a digital music player, a media player, a video game player module, an Internet browser, and/or any wireless local area network (WLAN) module.

* * *

Petitioner Samsung Ex-1006, 0023

CLAIMS

What is claimed is:

1. In a wireless communication system including a wireless transmit/receive unit (WTRU), the WTRU including a control plane (C-plane) packet data convergence protocol (C-PDCP) layer for performing ciphering and integrity protection of an initial connection signaling message, a method for security protection of a user identity (ID) in an initial connection signaling message, the method comprising:

activating the C-PDCP layer upon power up of the WTRU;

loading initial security parameters to the C-PDCP layer;

ciphering the initial connection signaling message including the user ID using the initial security parameters; and

sending the ciphered initial connection signaling message and the user ID to a network.

2. The method of claim 1 wherein the initial security parameters are loaded from a universal subscriber identity module (USIM).

3. The method of claim 1 wherein the initial security parameters are generated from system information broadcast from the network.

4. The method of claim 3 wherein the system information includes at least one public key or information for deriving a public key.

5. The method of claim 1 wherein the initial connection signaling message includes a public land mobile network (PLMN) identity.

6. The method of claim 1 further comprising:

the network sending an authentication request message to the WTRU including a random number and an authentication token;

Petitioner Samsung Ex-1006, 0024

the WTRU authenticating the network based on the random number and the authentication token;

the WTRU computing session keys and a response (RES);

the WTRU sending an authentication response message including the RES to the network;

the network authenticating the WTRU using the RES; and

the network sending a security mode command message to the WTRU.

7. The method of claim 6 wherein the authentication response message is protected by using the initial security parameters.

8. The method of claim 6 wherein the network ciphers a downlink control message including the security mode command message with a key used for ciphering the initial connection signaling message using a symmetric encryption algorithm.

9. The method of claim 6 further comprising:

configuring a user plane (U-plane) PDCP layer with a new session key for U-plane data ciphering.

10. The method of claim 1 wherein a ciphering algorithm to be used is one of the initial security parameters.

11. The method of claim 10 wherein the ciphering algorithm is f8 algorithm and the initial security parameters include a ciphering key (CK), a COUNT-C value, a bearer ID, a direction value, and a length value.

12. The method of claim 11 wherein the COUNT-C value is a pre-arranged value known only to the WTRU and the network.

Petitioner Samsung Ex-1006, 0025

13. The method of claim 11 wherein the COUNT-C value is a START value stored in a universal subscriber identity module (USIM) combined with a pre-agreed value known between the WTRU and the network.

14. The method of claim 13 wherein the pre-agreed value is a non-access stratum (NAS) layer sequence number.

15. The method of claim 11 wherein the COUNT-C value is a computed value by the WTRU and the network.

16. The method of claim 11 wherein the bearer ID is a signaling radio bearer ID number.

17. The method of claim 11 wherein the bearer ID is a pre-arranged value between the WTRU and the network.

18. The method of claim 11 wherein the direction value is set to '0' for uplink.

19. The method of claim 10 wherein the ciphering algorithm is an asymmetric encryption algorithm.

20. The method of claim 19 wherein the ciphering algorithm uses a ciphering key (CK) which is a pre-arranged public/private key-pair between the WTRU and the network.

21. The method of claim 20 wherein the public key is broadcast via system information by the network.

22. The method of claim 21 wherein the WTRU selects a public key from a public key set comprising a plurality of public keys.

Petitioner Samsung Ex-1006, 0026

23. The method of claim 22 wherein the WTRU uses its IMSI value to select an index into the public key set to select a public key.

24. The method of claim 22 wherein the WTRU uses a FRESH value to select an index into the public key set to select a public key.

25. The method of claim 24 wherein the WTRU encrypts the index with a pre-agreed public key and includes the encrypted index in the connection request message.

26. The method of claim 22 wherein the system information includes a first key index seed and the connection request message includes a second key index seed, and the public key is selected using a Diffie-Hellman key exchange method.

27. The method of claim 1 wherein an integrity protection algorithm to be used is one of the initial security parameters.

28. The method of claim 27 wherein the integrity protection algorithm is f9 algorithm, and the initial security parameters include an integrity key (IK), a COUNT-I value, a message, a direction value, and a FRESH value.

29. The method of claim 28 wherein the IK is generated by the WTRU using a random number received from the network via system information and a shared secret key K.

30. The method of claim 29 wherein the IK is generated by using f4 algorithm.

Petitioner Samsung Ex-1006, 0027

31. The method of claim 28 wherein the COUNT-I value is a pre-arranged value known to the WTRU and the network.

32. The method of claim 28 wherein the COUNT-I value is set to a START value stored in a universal subscriber identity module (USIM) combined with a pre-agree value known between the WTRU and the network.

33. The method of claim 32 wherein the pre-agreed value is a non-access stratum (NAS) layer sequence number.

34. The method of claim 28 wherein the COUNT-I value is a computed value by the WTRU and the network.

35. The method of claim 28 wherein the direction value is set to '0' for uplink.

36. The method of claim 28 wherein the message is a radio bearer ID plus a first non-access stratum (NAS) message.

37. The method of claim 28 wherein the FRESH value is selected from a set of pre-arranged FRESH values between the WTRU and the network.

38. The method of claim 37 wherein the IK is used to compute an index for the FRESH value.

39. The method of claim 28 wherein the FRESH value is generated by using a FRESH value generation algorithm with a random number broadcast via system information and a shared secret key K.

40. The method of claim 1 wherein the wireless communication system is a third generation (3G) long term evolution (LTE).

Petitioner Samsung Ex-1006, 0028

41. A wireless transmit/receive unit (WTRU) for security protection of a user identity (ID) in an initial connection signaling message in a wireless communication system, the WTRU comprising:

a non-access stratum (NAS) layer configured to generate a first control signaling message and trigger a connection to a network;

a radio resource control (RRC) layer configured to generate a second control signaling message and perform integrity protection of the first and second control signaling messages; and

a control plane (C-plane) packet data convergence protocol (C-PDCP) layer configured to perform ciphering of at least one of the first and second control signaling messages including an initial connection signaling message and the user ID using initial security parameters that are loaded to the C-PDCP layer upon power up of the C-PDCP layer and send the ciphered initial connection signaling message and the user ID to a network.

42. The WTRU of claim 41 wherein the initial security parameters are loaded from a universal subscriber identity module (USIM).

43. The WTRU of claim 41 wherein the initial security parameters are generated from system information broadcast from the network.

44. The WTRU of claim 43 wherein the system information includes at least one public key or information for deriving a public key.

45. The WTRU of claim 41 wherein the initial connection signaling message includes a public land mobile network (PLMN) identity.

46. The WTRU of claim 41 wherein the NAS layer is configured to authenticate the network based on a random number and an authentication token included in an authentication request message from the network, and

Petitioner Samsung Ex-1006, 0029

compute session keys and send an authentication response message including a response (RES) to the network so that the network authenticates the WTRU using the RES.

47. The WTRU of claim 46 wherein the authentication response message is protected by using the initial security parameters.

48. The WTRU of claim 46 further comprising:

a user plane (U-plane) PDCP layer for processing U-plane data, the RRC layer loads a new session key to the U-plane PDCP layer for U-plane ciphering.

49. The WTRU of claim 41 wherein a ciphering algorithm to be used is one of the initial security parameters.

50. The WTRU of claim 49 wherein the ciphering algorithm is an f8 algorithm, wherein the initial security parameters include at least one of a ciphering key (CK), a COUNT-C value, a bearer ID, a direction value, and a length value.

51. The WTRU of claim 50 wherein the COUNT-C value is a pre-arranged value known only to the WTRU and the network.

52. The WTRU of claim 50 wherein the COUNT-C value is a START value stored in a universal subscriber identity module (USIM) combined with a pre-agreed value known between the WTRU and the network.

53. The WTRU of claim 52 wherein the pre-agreed value is a non-access stratum (NAS) layer sequence number.

54. The WTRU of claim 50 wherein the COUNT-C value is a computed value by the WTRU and the network.

Petitioner Samsung Ex-1006, 0030

55. The WTRU of claim 50 wherein the bearer ID is a signaling radio bearer ID number.

56. The WTRU of claim 50 wherein the bearer ID is a pre-arranged value between the WTRU and the network.

57. The WTRU of claim 50 wherein the direction value is set to '0' for uplink.

58. The WTRU of claim 49 wherein the ciphering algorithm is an asymmetric encryption algorithm.

59. The WTRU of claim 58 wherein the ciphering algorithm uses a ciphering key (CK) which is a pre-arranged public/private key-pair between the WTRU and the network.

60. The WTRU of claim 59 wherein the public key is broadcast via system information.

61. The WTRU of claim 60 wherein the C-PDCP layer selects a public key from a public key set comprising a plurality of public keys.

62. The WTRU of claim 60 wherein the C-PDCP layer uses the user ID to select an index into the public key set.

63. The WTRU of claim 60 wherein the C-PDCP layer uses a FRESH value to select an index into the public key set.

Petitioner Samsung Ex-1006, 0031

64. The WTRU of claim 63 wherein the C-PDCP layer encrypts the index with a pre-agreed public key and includes the encrypted index in the connection request message.

65. The WTRU of claim 61 wherein the system information includes a first key index seed and the connection request message includes a second key index seed, wherein the public key is selected using a Diffie-Hellman key exchange method.

66. The WTRU of claim 41 wherein an integrity protection algorithm to be used is one of the initial security parameters.

67. The WTRU of claim 66 wherein the integrity protection algorithm is an f9 algorithm, and parameters include an integrity key (IK), a COUNT-I value, a message, a direction value, and a FRESH value.

68. The WTRU of claim 67 wherein the IK is generated by the WTRU using a random number received via system information and a shared secret key K.

69. The WTRU of claim 68 wherein the IK is generated by using an f4 algorithm.

70. The WTRU of claim 67 wherein the COUNT-I value is a pre-arranged value known to the WTRU and the network.

71. The WTRU of claim 67 wherein the COUNT-I value is set to a START value stored in a universal subscriber identity module (USIM) combined with a pre-agree value known between the WTRU and the network.

Petitioner Samsung Ex-1006, 0032

72. The WTRU of claim 71 wherein the pre-agreed value is a non-access stratum (NAS) layer sequence number.

73. The WTRU of claim 67 wherein the COUNT-I value is a computed value by the WTRU and the network.

74. The WTRU of claim 67 wherein the direction value is set to '0' for uplink.

75. The WTRU of claim 67 wherein the message is a radio bearer ID plus a first non-access stratum (NAS) message.

76. The WTRU of claim 67 wherein the FRESH value is selected from a set of pre-arranged FRESH values between the WTRU and the network.

77. The WTRU of claim 76 wherein the IK is used to compute an index for the FRESH value.

78. The WTRU of claim 67 wherein the FRESH value is generated by using a FRESH value generation algorithm with a random number broadcast via system information and a shared secret key K.

79. The WTRU of claim 41 wherein the wireless communication system is a third generation (3G) long term evolution (LTE).

80. The WTRU of claim 41 wherein the network ciphers a downlink control message with a key used for ciphering the initial connection signaling message using a symmetric encryption algorithm.

Petitioner Samsung Ex-1006, 0033

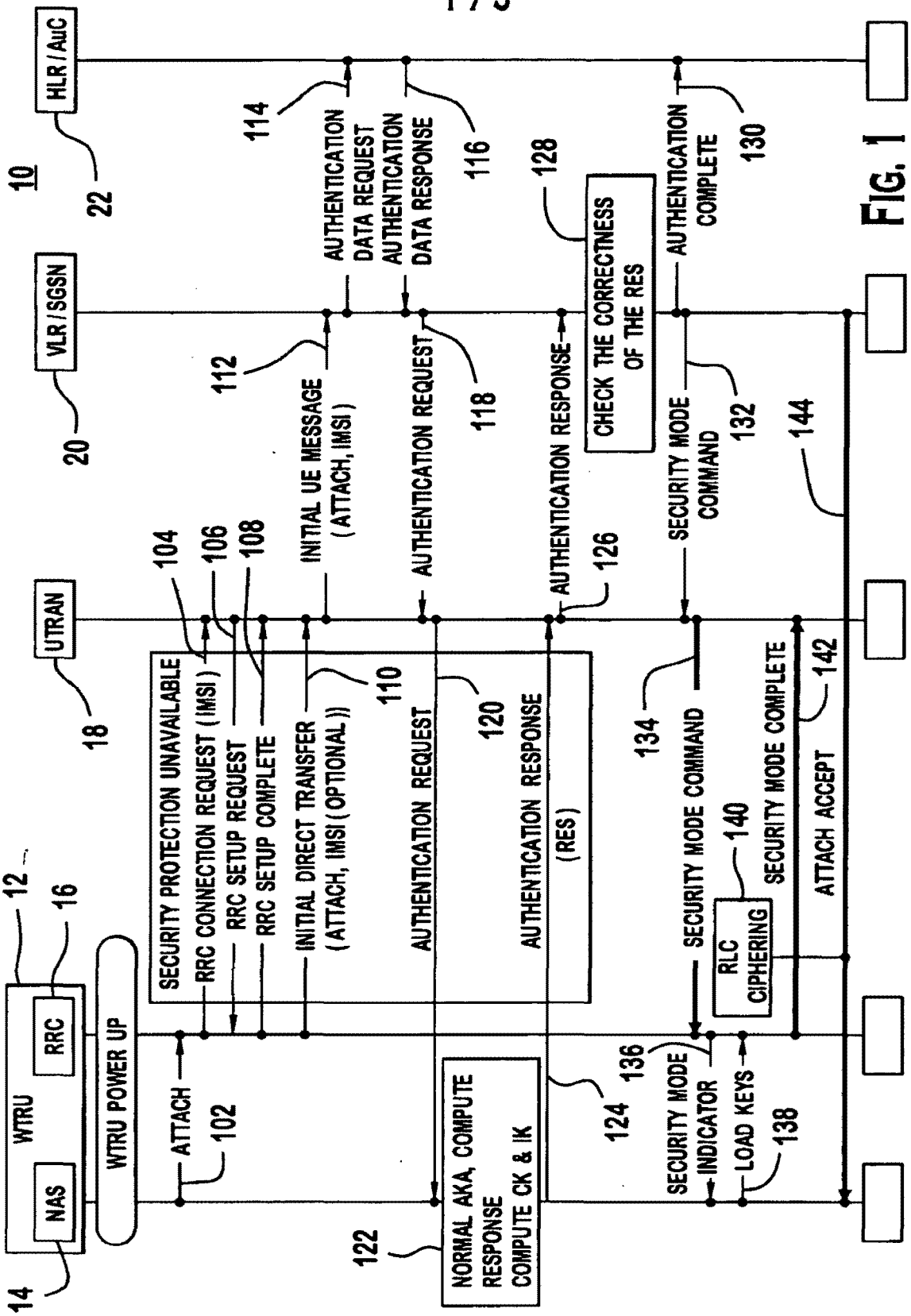


FIG. 1
PRIOR ART

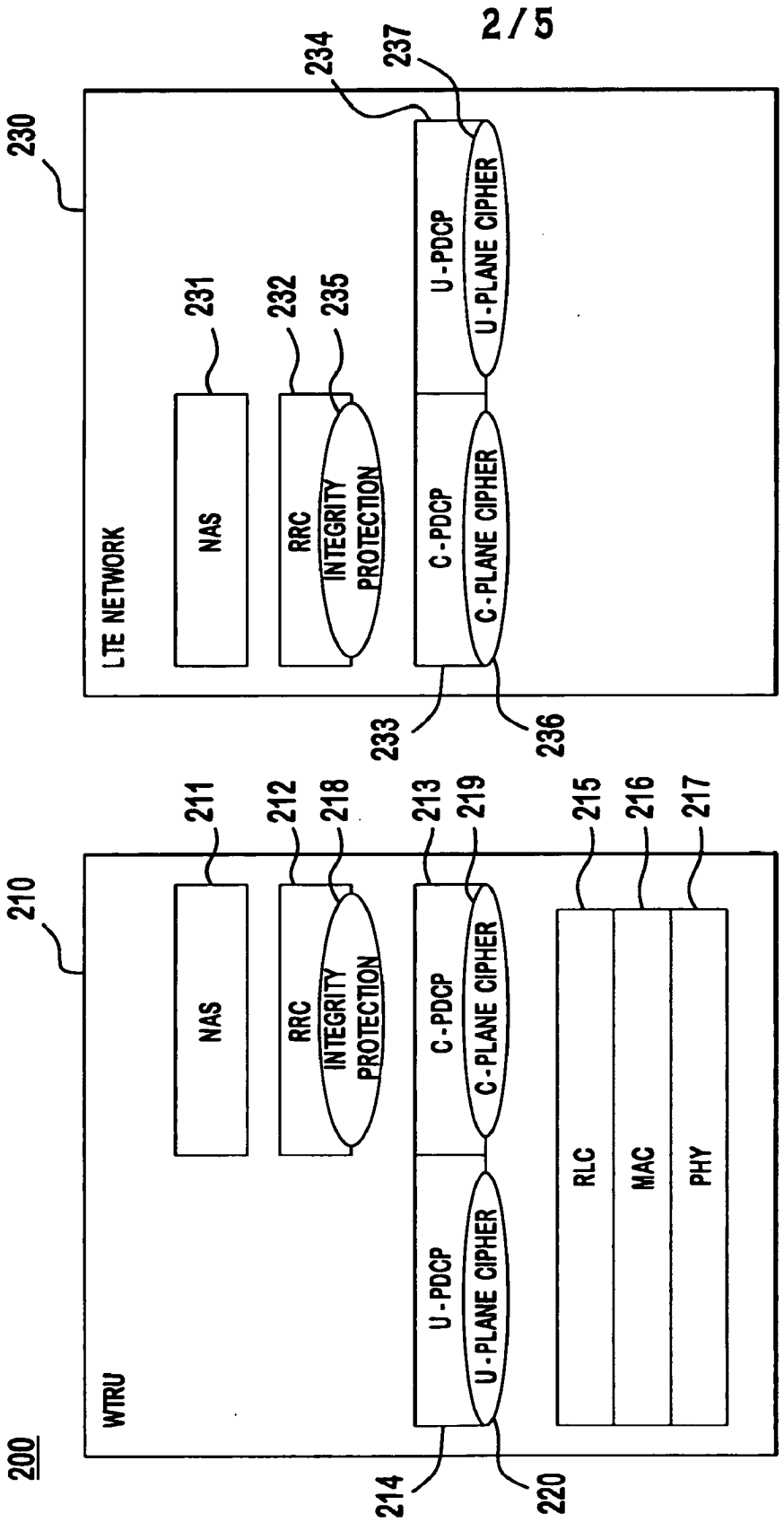

200
WTRU
210
NAS
211
RRC
212
INTEGRITY PROTECTION
218
C-PDCP
213
C-PLANE CIPHER
219
U-PDCP
214
U-PLANE CIPHER
220
RLC
215
MAC
216
PHY
217
LTE NETWORK
230
NAS
231
RRC
232
INTEGRITY PROTECTION
235
C-PDCP
233
C-PLANE CIPHER
236
U-PDCP
234
U-PLANE CIPHER
237

FIG. 2

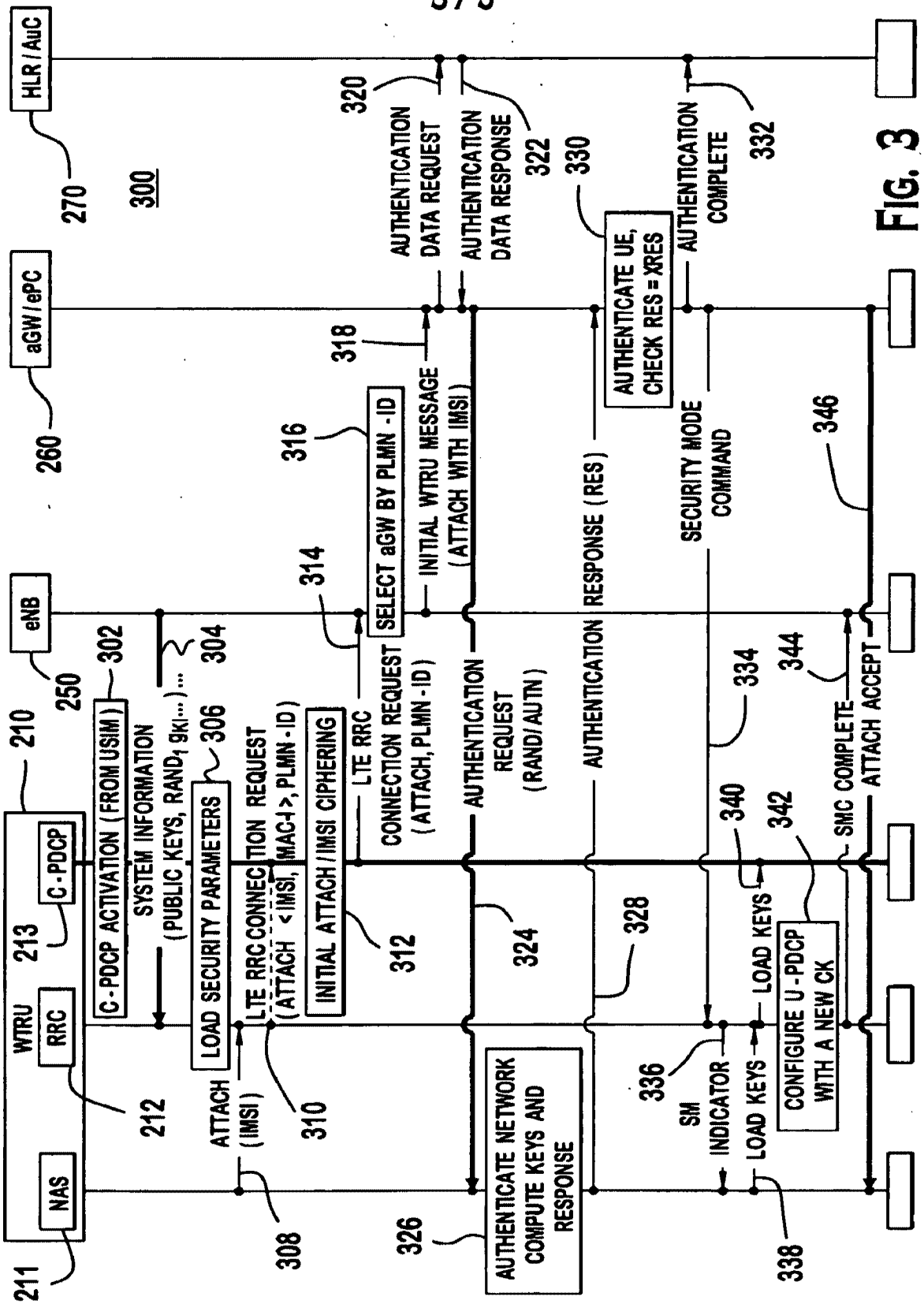

HLR / AuC
aGW / ePC
eNB
WTRU
RRC
NAS
C - PDCP
C - PDCP ACTIVATION (FROM USIM)
SYSTEM INFORMATION
(PUBLIC KEYS, RAND1 9KI...)...
LOAD SECURITY PARAMETERS
ATTACH (IMSI)
LTE RRC CONNECTION REQUEST
(ATTACH <IMSI, MAC-I>, PLMN - ID)
INITIAL ATTACH / IMSI CIPHERING
LTE RRC CONNECTION REQUEST (ATTACH, PLMN - ID)
SELECT aGW BY PLMN - ID
INITIAL WTRU MESSAGE (ATTACH WITH IMSI)
AUTHENTICATION DATA REQUEST
AUTHENTICATION DATA RESPONSE
AUTHENTICATION REQUEST (RAND/AUTN)
AUTHENTICATE NETWORK COMPUTE KEYS AND RESPONSE
AUTHENTICATE UE, CHECK RES = XRES
AUTHENTICATION RESPONSE (RES)
AUTHENTICATION COMPLETE
SECURITY MODE COMMAND
SM INDICATOR
LOAD KEYS
LOAD KEYS
CONFIGURE U - PDCP WITH A NEW CK
SMC COMPLETE
ATTACH ACCEPT
300
210
211
212
213
250
260
270
302
304
306
308
310
312
314
316
318
320
322
324
326
328
330
332
334
336
338
340
342
344
346

FIG. 3

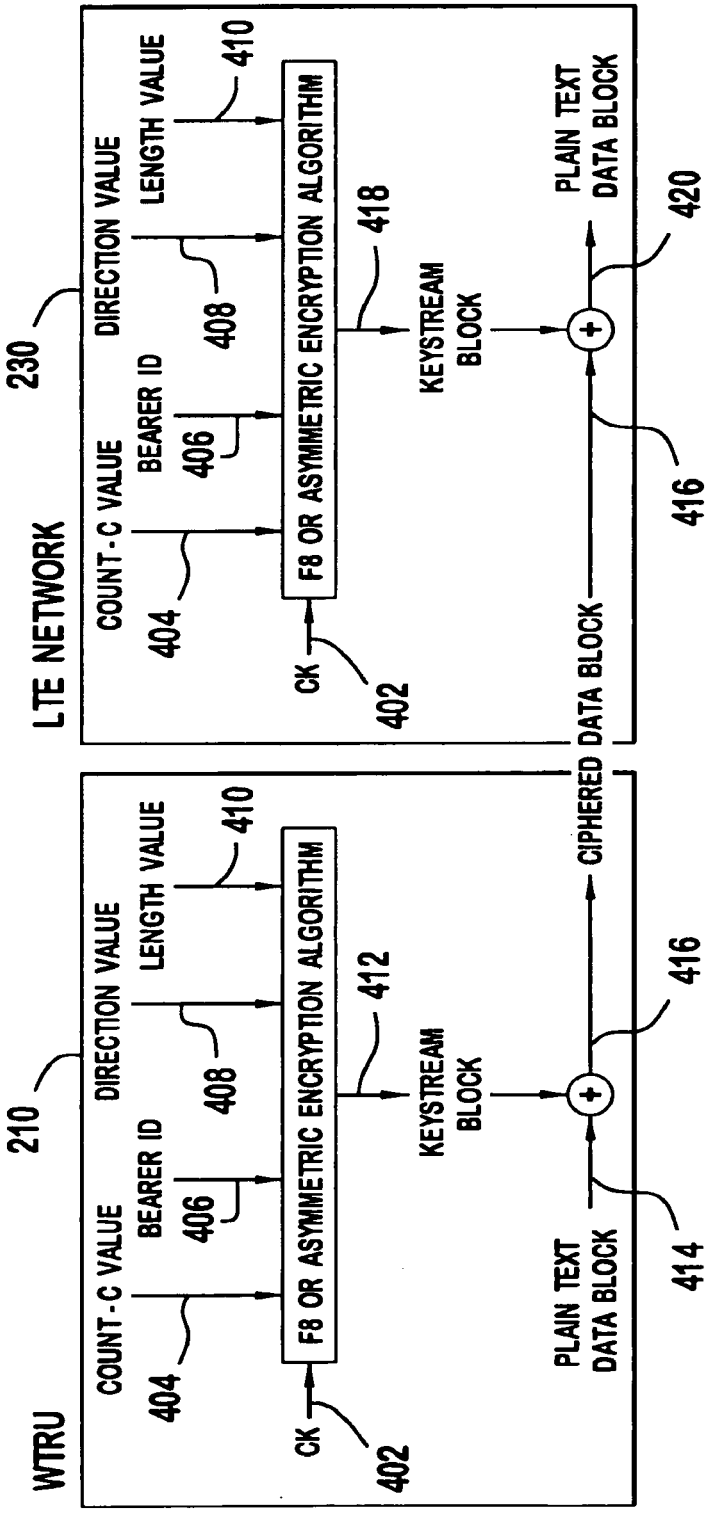
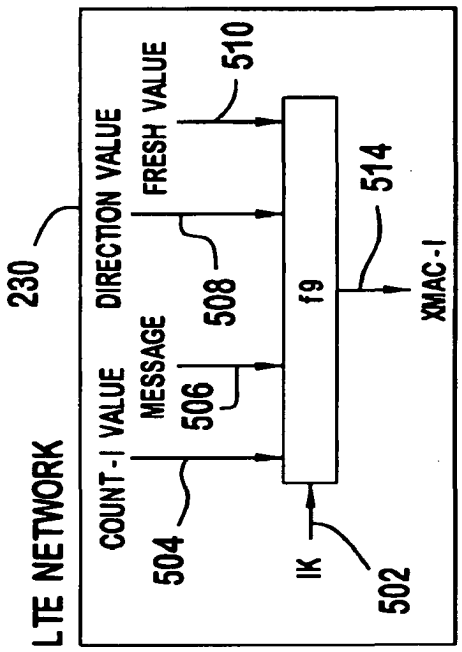

LTE NETWORK
230
COUNT-C VALUE
BEARER ID
DIRECTION VALUE
LENGTH VALUE
404
406
408
410
CK
402
F8 OR ASYMMETRIC ENCRYPTION ALGORITHM
418
KEYSTREAM BLOCK
PLAIN TEXT DATA BLOCK
416
420
CIPHERED DATA BLOCK
WTRU
210
COUNT-C VALUE
BEARER ID
DIRECTION VALUE
LENGTH VALUE
404
406
408
410
CK
402
F8 OR ASYMMETRIC ENCRYPTION ALGORITHM
412
KEYSTREAM BLOCK
PLAIN TEXT DATA BLOCK
414
416

FIG. 4



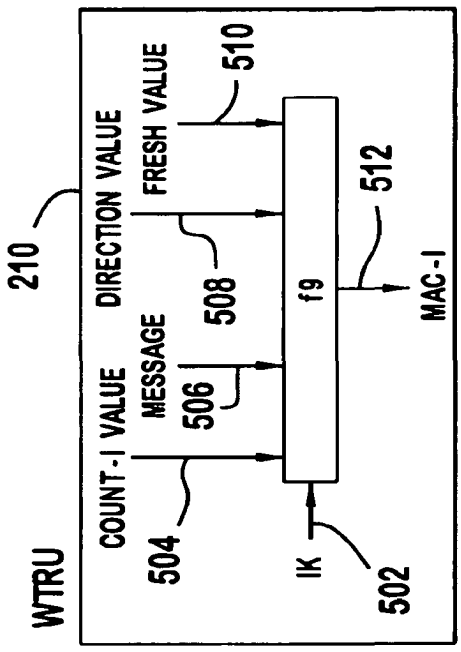


FIG. 5

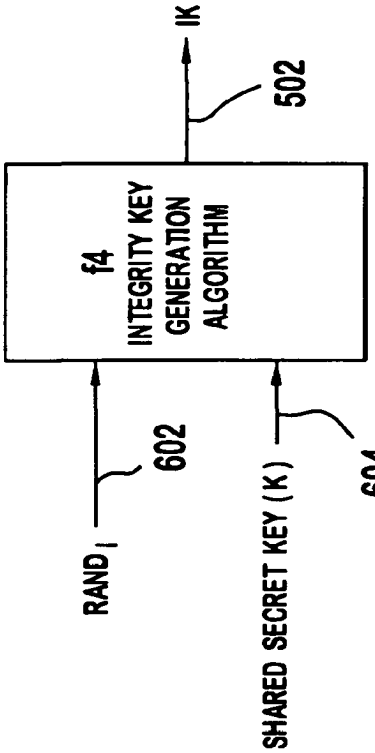


FIG. 6

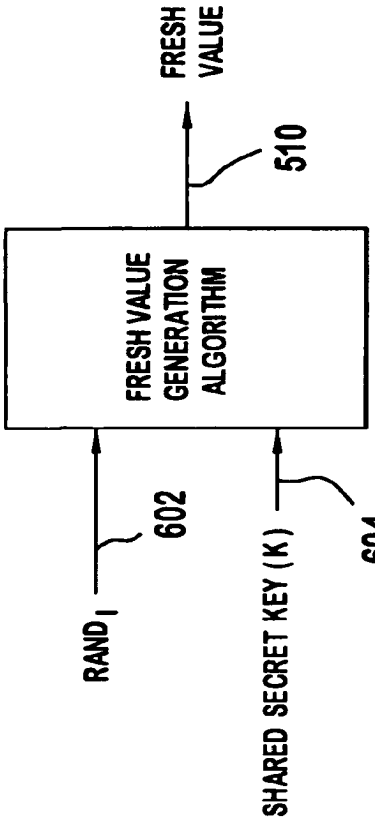


FIG. 7