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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 February 2017 (02.02.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/016450 A1

(51) International Patent Classification:
H04W 12/02 (2009.01)

(21) International Application Number:
PCT/CN2016/091053

(22) International Filing Date:
22 July 2016 (22.07.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/196,667 24 July 2015 (24.07.2015) US
15/213,266 18 July 2016 (18.07.2016) US

(71) Applicant: **HUAWEI TECHNOLOGIES CO., LTD.** [CN/CN]; Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129 (CN).

(72) Inventors: **MUHANNA, Ahmad Shawky**; 3904 Compton Dr., Richardson, Texas 75082 (US). **WANG, Zhibi**; 8100 Middlebury Ave, Woodridge, Illinois 60517 (US). **WANG, Jiangsheng**; Jingao Road # 1058, Shanghai 201208 (CN).

(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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, 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, SA, 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, ST, 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, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

(54) Title: ULTRA DENSE NETWORK SECURITY ARCHITECTURE AND METHOD

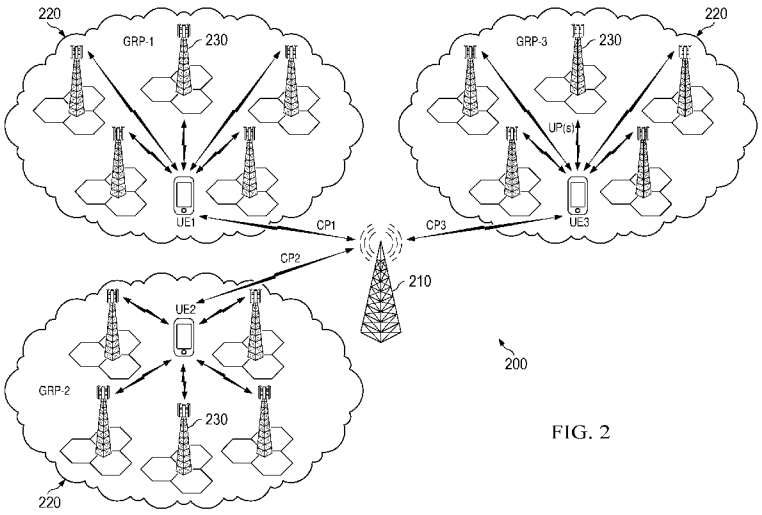

FIG. 2

(57) Abstract: A method for establishing a trust relationship in an ultra dense network is provided. The method comprises receiving, by a user equipment (UE), a reconfiguration request from a macrocell; deriving, by the UE, a user plane encryption key according to information in the reconfiguration request; transmitting, by the UE, a first user plane signaling message to a first microcell in a group of microcells when the UE is attached to the first microcell; and transmitting, by the UE, a second user plane signaling message to a second microcell in the group of microcells when the UE is attached to the second microcell, wherein the first user plane signaling message and the second user plane signaling message are both encrypted according to the user plane encryption key.

WO 2017/016450 A1

Ultra Dense Network Security Architecture and Method

[0001] This patent application claims priority to U.S. Provisional Application No. 62/196,667, filed on July 24, 2015 entitled "Ultra Dense Network Security Architecture and Method," and U.S. Application No. 15/213,266, filed on July 18, 2016 entitled "Ultra Dense Network Security Architecture and Method," which are hereby incorporated by reference herein as if reproduced in its entirety.

TECHNICAL FIELD

[0002] The present invention relates to a network security architecture and method, and, in particular embodiments, to an ultra dense network security architecture and method.

BACKGROUND

[0003] The use of Ultra Dense Networks (UDNs) is anticipated to be one of the 5G architectural solutions for providing high speed services with high quality of service (QoS) and quality of experience (QoE) in highly populated areas. In a UDN, a plurality of small cells or microcells may be deployed within the coverage area of a large cell or macrocell. Because the coverage of a microcell is limited compared with that of a macrocell, it is possible for a user equipment (UE) to move from one microcell to another very frequently, which may increase the number of microcells with which the UE needs to have a security trust relationship.

SUMMARY

[0004] An embodiment method for establishing a trust relationship in an ultra dense network includes receiving, by a user equipment (UE), a reconfiguration request from a macrocell; deriving, by the UE, a user plane encryption key according to information in the reconfiguration request; transmitting, by the UE, a first user plane signaling message to a first microcell in a group of microcells when the UE is attached to the first microcell; and transmitting, by the UE, a second user plane signaling message to a second microcell in the group of microcells when the UE is attached to the second microcell, wherein the first user plane signaling

message and the second user plane signaling message are both encrypted according to the user plane encryption key.

[0005] An embodiment UE includes a processor and a non-transitory computer readable storage medium storing programming for execution by the processor. The programming includes instructions for receiving, by the UE, a reconfiguration request from a macrocell; deriving, by the UE, a user plane encryption key according to information in the reconfiguration request; transmitting, by the UE, a first user plane signaling message to a first microcell in a group of microcells when the UE is attached to the first microcell; and transmitting, by the UE, a second user plane signaling message to a second microcell in the group of microcells when the UE is attached to the second microcell, wherein the first user plane signaling message and the second user plane signaling message are both encrypted according to the user plane encryption key.

[0006] An embodiment computer program product includes a non-transitory computer readable storage medium storing programming. The programming includes instructions to receive a reconfiguration request from a macrocell; derive a user plane encryption key according to information in the reconfiguration request; transmit a first user plane signaling message to a first microcell in a group of microcells when a UE is attached to the first microcell; and transmit a second user plane signaling message to a second microcell in the group of microcells when the UE is attached to the second microcell, wherein the first user plane signaling message and the second user plane signaling message are both encrypted according to the user plane encryption key.

[0007] An embodiment secure macrocell group includes a first microcell and a second microcell. The first microcell is configured to receive a secure microcells group key and further configured to transmit user plane signaling to a UE when the UE is attached to the first microcell, wherein the signaling is encrypted according to a user plane encryption key derived by the first microcell according to the secure microcells group key. The second microcell is configured to receive the secure microcells group key and further configured to transmit user plane signaling to the UE when the UE is attached to the second microcell, wherein the signaling is encrypted according to the user plane encryption key derived by the second microcell according to the secure microcells group key.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] For a more complete understanding of the present invention, and the advantages thereof, reference is now made to the following descriptions taken in conjunction with the accompanying drawing, in which:

[0009] Figure 1 illustrates an embodiment of a network for communicating data;

[0010] Figure 2 illustrates an embodiment of a UDN security architecture;

[0011] Figure 3 illustrates signaling used to establish a security trust relationship between a UE, a master eNB and a secondary eNB according to the prior art;

[0012] Figure 4 illustrates an embodiment of signaling used to establish a security trust relationship between a UE, a master eNB and a plurality of secondary eNBs;

[0013] Figure 5 illustrates a flowchart of an embodiment method for establishing a trust relationship in an ultra dense network;

[0014] Figure 6 illustrates an embodiment of a UDN architecture that allows an MME to communicate with microcells;

[0015] Figure 7 illustrates an embodiment of a UDN architecture that allows an eNB to communicate with microcells;

[0016] Figure 8 illustrates a block diagram of an embodiment of a processing system for performing methods described herein; and

[0017] Figure 9 illustrates a block diagram of a transceiver adapted to transmit and receive signaling over a telecommunications network.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

[0018] The structure, manufacture and use of the presently preferred embodiments are discussed in detail below. It should be appreciated, however, that the present invention provides many applicable inventive concepts that can be embodied in a wide variety of specific contexts. The specific embodiments discussed are merely illustrative of specific ways to make and use the invention, and do not limit the scope of the invention.

[0019] In the current 4G Long Term Evolution (LTE) architecture, both the control plane (CP) signaling and the user plane (UP) signaling are anchored at a macrocell, e.g., an enhanced node B (eNB). Thus, any UE attached to an Evolved Packet System (EPS) is usually anchored at a single eNB with both CP and UP associated with the same eNB. When a UE is anchored over a microcell and both the control plane and the user plane are anchored at that microcell, the procedures for the UE to attach to the microcell are similar to those where the UE attaches to a macrocell.

[0020] The vast majority of the eNB activities while serving a specific UE involve handling the UE user plane traffic. In densely populated areas, e.g., shopping malls, stadiums, etc., the user plane traffic may be offloaded to multiple small microcells through the use of a 5G Ultra Dense Network (UDN) architecture. UDNs generally anchor the control plane air interface signaling at a macrocell, e.g., an eNB in 4G, and anchor user plane traffic on a microcell or small cell. The same UE/user may have multiple user plane flows that are anchored at different microcells while the control plane is anchored at the macrocell. It is also possible that a small amount of control signaling may be needed between the UE and the microcell for maintaining the user plane session that is being anchored.

[0021] FIG. 1 illustrates a network 100 for communicating data. The network 100 comprises a base station 110 having a coverage area 101, a plurality of mobile devices 120, and a backhaul network 130. As shown, the base station 110 establishes uplink (dashed line) and/or downlink (dotted line) connections with the mobile devices 120, which serve to carry data from the mobile devices 120 to the base station 110 and vice-versa. Data carried over the uplink/downlink connections may include data communicated between the mobile devices 120, as well as data communicated to/from a remote-end (not shown) by way of the backhaul network 130. As used herein, the term "base station" refers to any component (or collection of components) configured to provide wireless access to a network, such as an enhanced base station (eNB), a macrocell, a femtocell, a Wi-Fi access point (AP), or other wirelessly enabled devices. Base stations may provide wireless access in accordance with one or more wireless communication protocols, e.g., LTE, LTE advanced (LTE-A), High Speed Packet Access (HSPA), Wi-Fi 802.11a/b/g/n/ac, etc. As used herein, the term "mobile device" refers to any component (or collection of components) capable of establishing a wireless connection with a base station, such as a user equipment (UE),

a mobile station (STA), and other wirelessly enabled devices. In some embodiments, the network 100 may comprise various other wireless devices, such as relays, low power nodes, etc.

[0022] While specific embodiments described herein primarily utilize the terms "macrocell" and "microcell" for the communications controllers, embodiments are generally applicable to access points (APs) as communications controllers. Thus, the term "access point" may be used for the macrocells and microcells described herein. Furthermore, in some embodiments, the control plane may be anchored by a microcell or an access point in general, and the user plane may be anchored by a macrocell or an access point in general.

[0023] Figure 2 illustrates an embodiment of a UDN architecture 200. In this architecture, control plane signaling is anchored at a macrocell 210, which in 4G is referred to as an eNB. User plane traffic is anchored at a plurality of microcells groups 220, each of which includes a plurality of microcells, such as microcells 230.

[0024] In such an architecture, a UE may have a single trust relationship with the eNB, which may cover both the control plane and the user plane at the same time. That is, all user plane traffic may be protected by a single security trust relationship between the UE and the eNB. Thus, if that trust relationship is compromised, then all the UE user plane traffic and flows may be compromised at once.

[0025] In 5G, the control plane continues to be protected with the security trust relationship between the UE and the eNB. For user plane traffic, a different trust relationship may be established between the UE and each of a plurality of microcells associated with the eNB. Maintaining multiple simultaneous user plane trust relationships in such a manner may not be efficient. A 5G architecture that handles densely populated areas with a UDN may call for the use of an optimized security architecture that reduces the burden on the UE in order to avoid maintaining a large number of security trust relationships when the UE user plane traffic is anchored at different microcells.

[0026] An embodiment provides a security architecture that maintains the same security trust relationship for all microcells within a group of microcells. That is, a new trust model is provided, wherein the trust relationship between a UE and a microcell within a specific group of microcells is the same as the trust relationship between the UE and any other microcell within that specific group of microcells. When the UE has multiple user plane flows, each anchored at a

different microcell, the UE may have a single security trust relationship, i.e., security association, for all of the user plane flows. Thus, when a UE attaches to a 5G architecture where the UDN architecture is present, the UE maintains a single security trust relationship with each microcell in a group of microcells, instead of a different security trust relationship with each microcell in the group. When a user plane flow moves from a source microcell to a target microcell in the same group as the source microcell, the UE continues to have the same security trust relationship with the target microcell as the UE had with the source microcell. Also, if the UE maintains a user plane flow with a first microcell in a group and then attaches an additional user plane flow to a second microcell in the same group, the UE has the same security trust relationship with the second microcell as with the first. In general, once a UE has derived a key for secure communication with a microcell in a group of microcells, the UE may use the same key for secure communication with any other microcell in the group of microcells.

[0027] As used herein, terms such as "group" and "group of microcells" may refer to a set of microcells that have been defined as a group for reasons other than security considerations or may refer to a set of microcells that have been defined as a group specifically due to security considerations. A microcell may belong to a single group of microcells or to multiple groups of microcells. When multiple microcell groups are associated with a macrocell, the macrocell may be aware of which microcells belong to which groups. A UE may determine the group to which a microcell belongs based on information transmitted by that microcell or by the macrocell associated with that microcell or based on information the UE receives in some other manner.

[0028] In an embodiment, all microcells in a group of microcells may have the same security capabilities and criteria at all times. A group of microcells may be located within the same geographical area. The number of microcells within a given microcell group may be less than a defined maximum. In addition, all microcells in a microcell group may belong to the same operator.

[0029] In an embodiment, a group of microcells may be assigned a globally unique identifier (ID). A group of microcells that share a globally unique ID and the same security criteria and characteristics may be referred to as a secure microcells group (SMG). When a UE has a trust relationship or security association with a specific SMG, then the same trust relationship and security association may be valid with all microcells that are part of the SMG. In

an embodiment, a UE may have a single security relationship with an SMG. In another embodiment, the UE may have more than one security association with the same SMG. Each SMG may have a single trust relationship with any visiting UE without introducing any security weaknesses or vulnerabilities relative to 4G architecture.

[0030] Figure 3 illustrates a protocol diagram of a conventional communications sequence 300 for establishing a security trust relationship between a UE 301, a master eNB (MeNB) 302, and a first secondary eNB (SeNB1) 303. The communications sequence 300 begins when a Radio Resource Control (RRC) connection 310 is established between the UE 301 and the MeNB 302. Next, the MeNB 302 sends an SeNB Addition Request 320 to SeNB1 303. The SeNB Addition Request 320 may include K-SeNB, which is a master key for a specific pair of a UE and an SeNB. The SeNB Addition Request 320 may also include the UE's EPS security capabilities. Upon receiving the SeNB Addition Request 320, SeNB1 303 performs a capability negotiation and an algorithm selection 325. Thereafter, SeNB1 303 sends an SeNB Addition Request Acknowledgement 330 to the MeNB 302. The MeNB 302 then sends an RRC Connection Reconfigure Request 340 to the UE 301. The RRC Connection Reconfigure Request 340 may include a counter, an algorithm, and other information needed for the UE 301 to generate a key. The UE 301 then sends an RRC Connection Reconfigure Response 350 to the MeNB 302. The MeNB 302 then sends an SeNB Reconfiguration Complete message 360 to SeNB1 303. The UE 301 and SeNB1 303 then perform activation encryption and decryption, at blocks 363 and 366 respectively, using the generated key. The UE 301 and SeNB1 303 then perform a random access procedure 370. That is, the UE 301 and SeNB1 303 acquire the air interface resources needed for communication with one another and communicate securely using the encryption and decryption based on the generated key.

[0031] Figure 4 illustrates a protocol diagram of an embodiment of a communications sequence 400 for establishing a security trust relationship between a UE 301, a master eNB 302, a first secondary eNB 303, and a second secondary eNB 304 according to the procedures disclosed herein. A Radio Resource Control (RRC) connection 402 is established between the UE 301 and the MeNB 302, and the MeNB 302 sends an SeNB Addition Request 404 to SeNB1 303 as described above. The MeNB 302 also sends an SeNB Addition Request 406 to at least one additional SeNB, here labeled SeNB2 304. Like the SeNB Addition Request 404 sent to SeNB1 303, the SeNB Addition Request 406 sent to SeNB2 304 may include K-SeNB and the

UE's EPS security capabilities. SeNB1 303 and SeNB2 304 then perform a capability negotiation and an algorithm selection 407. Based on the information in the SeNB Addition Request 404 and the SeNB Addition Request 406 and on the results of the capability negotiation and algorithm selection 407, SeNB1 303 and SeNB2 304 may derive a user plane encryption key for secure communication with the UE 301. SeNB1 303 and SeNB2 304 then send SeNB Addition Request Acknowledgements 408 and 410 to the MeNB 302. The MeNB 302 then sends an RRC Connection Reconfigure Request 412 to the UE 301. The RRC Connection Reconfigure Request 412 may include a counter, an algorithm, and other information needed for the UE 301 to generate the same user plane encryption key derived by SeNB1 303 and SeNB2 304. The other information may include an ID for the SMG to which SeNB1 303 and SeNB2 304 belong. The UE 301 may then derive the user plane encryption key according to the information in the RRC Connection Reconfigure Request 412. The UE 301 then sends an RRC Connection Reconfigure Response 414 to the MeNB 302. The MeNB 302 then sends SeNB Reconfiguration Complete messages 416 and 418 to SeNB1 303 and SeNB2 304, respectively. The UE 301, SeNB1 303, and SeNB2 304 then perform activation encryption and decryption, at blocks 430, 440, and 450 respectively, all using the same user plane encryption key. The UE 301 and SeNB1 303 then perform a random access procedure 420. The UE 301 and SeNB2 304 may also perform a random access procedure 422. The random access procedures 420 and 422 may include the UE 301 sending user plane messages encrypted according to the user plane encryption key to SeNB1 303 and SeNB2 304.

[0032] Figure 5 illustrates a flowchart of an embodiment method 500 for establishing a trust relationship in an ultra dense network, as may be performed by a UE. At step 510, the UE receives a reconfiguration request from a macrocell. At step 520, the UE derives a user plane encryption key according to information in the reconfiguration request. At step 530, the UE transmits a first user plane signaling message to a first microcell in a group of microcells when the UE is attached to the first microcell. At step 540, the UE transmits a second user plane signaling message to a second microcell in the group of microcells when the UE is attached to the second microcell. In an embodiment, the first user plane signaling message and the second user plane signaling message are both encrypted according to the user plane encryption key.

[0033] In an embodiment, the procedures for deriving a key for the microcells in an SMG may be an enhancement of the 4G key derivation procedure. In the 4G key derivation procedure,

a mobility management entity (MME) receives a key known as K_{asme} from a home subscriber server (HSS) for a specific UE. K_{asme} is the master key for a specific pair of a UE and an MME that is acting as an Access Security Management Entity (ASME). The MME typically derives a key known as K_{eNB} based on K_{asme}. K_{eNB} is the master key for the communication between an eNB and a specific UE.

[0034] In an embodiment, the MME derives an additional key for all microcells in an SMG. This key, which may be referred to as K_{smg} or the key for an SMG, is a master key between a UE and a group of microcells or secondary eNBs in an SMG. In some cases, K_{smg} may reflect the identity of an SMG.

[0035] The techniques the MME uses to generate K_{smg} and cause K_{smg} to be transmitted to the microcells in an SMG may depend on the 5G architecture for handling the UDN architecture and approach. The techniques may not change the current security architecture when the UE control plane and user plane are anchored at the same macrocell.

[0036] In some circumstances, the MME may be aware of all SMGs that belong to a specific eNB, the members of each SMG, and the ID of each SMG. In such circumstances, the MME may be capable of communicating directly with each of the microcells in each SMG associated with the eNB. In an embodiment, when such circumstances exist, the MME may generate a different K_{smg} key for each SMG based on K_{asme}. The MME may then communicate the respective K_{smg} keys directly to every microcell in the corresponding SMG. Alternatively, K_{smg} may be communicated to a leader microcell in an SMG and/or to the leader's backup, and one or both of those microcells may communicate K_{smg} to the rest of the microcells in the SMG. After receiving K_{smg} in either of the above manners, each microcell in an SMG may use K_{smg} to protect user plane traffic for a specific UE, e.g., for purposes of encryption/decryption, authentication, verification, and/or other security procedures between the UE and each microcell in the SMG.

[0037] Figure 6 is a diagram of an embodiment scheme for deriving K_{smg} when the MME is capable of communicating directly with the microcells. At block 610, a master key (K) is generated and may reside in an HSS and in a UE's Universal Subscriber Identity Module (USIM). At block 620, the UE and the HSS generate a ciphering key (CK) and an integrity protection key (IK) based on K. At block 630, the UE and the HSS generate K_{asme} based on CK

and IK. The HSS may then send K_{asme} to an MME. At block 640, a key for non-access stratum (NAS) signaling encryption (K_{NASenc}) is generated for a pair of the UE and the MME based on K_{asme}. At block 650, a key for NAS signaling integrity protection (K_{NASint}) is generated for the pair of the UE and the MME based on K_{asme}. At block 660, the MME generates K_{eNB} for the UE and an eNB associated with the UE based on K_{asme}. At block 670, K_{eNB} is used to generate the keys needed for secure communication between the UE and the eNB. In an embodiment, at block 680, the UE and the MME independently generate K_{smg} based on K_{asme}. In the manner described above, the MME then provides K_{smg} to the microcells in the SMG for which K_{smg} was generated. In an embodiment, at block 690, the UE and the microcells in the SMG use the independently derived versions of K_{smg} to generate the keys needed for secure user plane communication between the UE and the microcells. In particular, the UE and the microcells may generate a user plane encryption key based on K_{smg}.

[0038] In some circumstances, the MME communicates directly only with the macrocell. That is, the MME communicates with an eNB but does not communicate directly with the microcells in each SMG associated with the eNB. In an embodiment, when such circumstances exist, the MME may generate a general SMG key for all the SMGs that belong to the eNB. The general SMG key may be similar to K_{eNB} and may be based on K_{asme} and on a common identifier for all the SMGs. The MME may then transmit the general SMG key to the eNB. The eNB may then generate an individualized K_{smg} for each SMG based on the general SMG key and on the ID for each SMG. Each individualized K_{smg} may be associated with a specific group of microcells. The eNB may then communicate each individualized K_{smg} to its respective SMG. The eNB may send an individualized K_{smg} to each microcell in an SMG or to a leader and/or backup microcell in the SMG, and either or both of those microcells may then send the individualized K_{smg} to the other microcells in the SMG. Each microcell may then use K_{smg} to protect user plane traffic for a specific UE, e.g., for purposes of encryption/decryption, authentication, verification, and/or other security procedures between the UE and each microcell in the SMG.

[0039] Figure 7 is a diagram of an embodiment scheme for deriving K_{smg} when the MME communicates with an eNB but does not communicate directly with the microcells. K 610, CK/ IK 620, K_{asme} 630, K_{NASenc} 640, K_{NASint} 650, and K_{eNB} 660 are generated and used as described with regard to Figure 6. In this embodiment, the MME and the UE do not separately generate a specific K_{smg} for each SMG associated with the eNB, as in block 680 of Figure 6. Instead, the

MME and the UE, at block 710, separately generate a general K_{smg} for all SMGs associated with a particular eNB based on K_{asme} and on a common ID for all the SMGs. At block 720, the eNB generates a different individualized K_{smg} for each SMG associated with the eNB based on the general K_{smg} and on the respective ID for each SMG. The eNB then sends the individualized K_{smg} keys to the associated SMGs. At block 730, the UE also generates the individualized K_{smg} key corresponding to the individualized K_{smg} key received by the SMG associated with the UE. The UE and the microcells in the SMG then use the independently derived versions of K_{smg} to generate the keys needed for secure user plane communication between the UE and the microcells. In particular, the UE and the microcells may generate a user plane encryption key based on K_{smg}.

[0040] The procedures depicted in Figure 4 have been depicted separately from the procedures depicted in Figures 6 and 7, but the steps depicted in the three figures may be components in an overall method for establishing a trust relationship in an ultra dense network. An example of such an overall method will now be described, but it should be understood that the steps do not necessarily occur in the order described below. In this example, it will be assumed for the sake of simplicity that only one SMG is present.

[0041] The method may be considered to begin when a UE establishes a connection, such as an RRC connection, with an MeNB. A master key, K, for the UE is then generated and stored in the UE and an HSS. The UE and the HSS each separately generate a ciphering key, CK, and an integrity protection key, IK, based on K. Based on CK and IK, the UE and the HSS each separately generate a master key, K_{asme}, for the pair of the UE and an MME associated with the UE and the HSS. The HSS then sends K_{asme} to the MME. Based on K_{asme}, the MME generates K_{eNB}, which is a key for communication between the UE and the MeNB. In an embodiment, the MME also generates, also based on K_{asme}, a key for communication between the UE and the SeNBs in an SMG, and this key may be referred to as K_{smg}. In some cases, K_{smg} may reflect the identity of an SMG.

[0042] The MME causes K_{smg} to be transmitted to the SeNBs in one of several ways. If the MME is capable of communicating directly with the SeNBs, the MME may send K_{smg} to all of the SeNBs in the SMG. Alternatively, the MME may send K_{smg} to only one of the SeNBs, which then sends K_{smg} to the other SeNBs in the SMG. If the MME is capable of communicating with

the MeNB but is not capable of communicating directly with the SeNBs, the MME generates a generic version of K_{smg} and sends the generic version of K_{smg} to the MeNB. The MeNB then generates an individualized version of K_{smg} for the SMG based on the generic version of K_{smg} and on the ID of the SMG. The MeNB then sends the individualized version to the SeNBs. If other SMGs were present, the MeNB would generate a different individualized version of K_{smg} for each of the SMGs.

[0043] The MeNB also informs the SeNBs of the UE's security capabilities. In the case where the MeNB sends K_{smg} to the SeNBs, the MeNB may send the security capabilities information to the SeNBs in the same message in which the MeNB sends K_{smg} to the SeNBs. In the case where the MME sends K_{smg} to the SeNBs, the MeNB may send the security capabilities information to the SeNBs in some other manner.

[0044] Based on K_{smg} and the UE's security capabilities, the SeNBs select an algorithm to be used to derive a key for secure communication between the SeNBs and the UE. The algorithm may be a Key Derivation Function (KDF) or a similar algorithm. The SeNBs also select a unique counter to be used as input into the algorithm. Alternatively, a group ID for the SMG could be used instead of a counter. At this point, all SeNBs in the SMG have the same K_{smg}, counter, and ID for the algorithm.

[0045] The SeNBs then send the algorithm ID and the counter to the MeNB, and the MeNB sends the algorithm ID and the counter to the UE. The MeNB may transmit that information in a Reconfiguration Request message in RRC signaling.

[0046] At some point, the UE generates K_{smg} based on K_{asme}, which the UE had previously generated as described above. Since the UE uses the same inputs and same procedures used by the HSS in generating K_{asme}, the version of K_{asme} generated by the UE is the same as the version of K_{asme} that the HSS sent to the MME. Thus, the version of K_{smg} that the UE generates based on K_{asme} is the same as the version of K_{smg} that the MME generates and causes to be transmitted to the SeNBs. Therefore, at this point, the UE has same K_{smg}, counter, and algorithm ID as the SeNBs.

[0047] The UE and each of the SeNBs separately provide the same K_{smg} and the same counter as input into the same algorithm, such as a KDF, and thus generate the same user plane

encryption key (KUP_{enc}) as output. The same KUP_{enc} may then be used for secure communication of user plane signaling between the UE and each of the SeNBs.

[0048] In some cases, the UE and the MME may generate other keys based on KUP_{enc}, K_{asme}, and/or other parameters. For example, the key for NAS signaling encryption, K_{NASenc}, and the key for NAS signaling integrity protection, K_{NASint}, may be generated for the UE and the MME based on K_{asme}. In addition, a key for RRC encryption ($KRRC_{enc}$) and a key for RRC integrity protection ($KRRC_{int}$) may be generated. $KRRC_{enc}$ and $KRRC_{int}$ may be derived from information provided to the UE that reflects the identity and protocol of RRC communication. A new counter that is dedicated for RRC communication may be used to guarantee the freshness of these keys and to ensure that the keys are different from KUP_{enc}, for example.

[0049] If needed for integrity protection, a user plane integrity protection key (KUP_{int}) may also be generated using the counter used for KUP_{enc} plus an identifier to indicate that KUP_{int} is for integrity protection.

[0050] In general, an identifier for an RRC protocol specific for encryption and a separate identifier specific for integrity protection may be added as input to the key derivation function. The use of an identifier that reflects the nature of the generated key may differentiate between an encryption key and an integrity protection key that are derived from the same master key.

[0051] Under the above procedures, the MeNB may still communicate the $S\text{-}K_{eNB}$ over the X2-C plane to all members of the small cell group. The SeNBs may then derive the user plane encryption key for the UE. The MeNB may then communicate an S-eNB group special counter to the UE once, and the UE may then derive the $S\text{-}K_{eNB}$ and user plane encryption keys to share with all members of the group. That is, under existing procedures, each time the UE moves from one microcell in an SMG to another or adds a microcell in the SMG for user plane traffic, the MeNB sends the UE information from which the UE may derive a new user plane encryption key for use with the new microcell. Under the embodiments disclosed herein, on the other hand, the MeNB sends such information to the UE only once as long as the UE remains in the same SMG. The UE then uses the information to derive a single user plane encryption key that may be used with all the microcells in the SMG. Thus, under the procedures disclosed herein, the amount of signaling from the MeNB to the UE may be reduced compared to the amount of signaling previously used. In particular, the RRC Connection Reconfigure Request message shown at

event 550 in the prior art Figure 5 may be sent from the MeNB to the UE multiple times, once for each time the UE moves from one microcell in an SMG to another or attaches to an additional microcell. By contrast, the RRC Connection Reconfigure Request message shown at event 614 in the embodiment of Figure 6 may be sent from the MeNB to the UE only once, namely when the UE enters the SMG.

[0052] In 5G, it is expected that the MeNB may have more than one group of SeNBs. In such a case, the small cell group ID may be used in addition to a special counter to derive the S-K_{eNB}. This assumes that the small cell group ID can be communicated to the UE in a timely enough manner for the UE to make use of the small cell group ID. If communicating the small cell group ID to UE is not possible, the MeNB may ensure that the special counter is unique for a group of small cells that are associated with the MeNB. When the MeNB communicates K-S_{eNB} to a group of small cells, the MeNB may inform some members of the group to keep K-S_{eNB} until the UE starts the random access procedure, which may not occur immediately.

[0053] When the UE hands over from a first microcell that belongs to a first SMG to a second microcell that belongs to a second SMG, the UE automatically uses the key that belongs to the second SMG for securing user plane communication with the second microcell.

[0054] As part of the UDN architecture, it is possible for a UE to have some limited control signaling with a microcell. In this case, it is possible to use a different key to protect the control plane signaling between the UE and the microcells within each SMG. For example, there may be one control plane key per SMG, or the same user plane key may be reused.

[0055] The concept of security keys has been used herein as an example for the purposes of illustration and explanation. Other similar concepts, such as certificates, can be used and can follow the same general approach, such that each microcell in a microcell group uses the same certificate or other security component.

[0056] Various embodiments provide a security architecture solution that is based on the existing 4G LTE security architecture, but is optimized to handle UDN security architecture. Embodiments may be used for the 5G UDN security architecture. 3GPP TS 33.401 V12.5.1 (Oct. 2012) provides further details regarding message flows/sequences utilized by the various procedures described herein.

[0057] Figure 8 illustrates a block diagram of an embodiment processing system 800 for performing methods described herein, which may be installed in a host device. As shown, the processing system 800 includes a processor 804, a memory 806, and interfaces 810-814, which may (or may not) be arranged as shown the figure. The processor 804 may be any component or collection of components adapted to perform computations and/or other processing related tasks, and the memory 806 may be any component or collection of components adapted to store programming and/or instructions for execution by the processor 804. In an embodiment, the memory 806 includes a non-transitory computer readable medium. The interfaces 810, 812, 814 may be any component or collection of components that allow the processing system 800 to communicate with other devices/components and/or a user. For example, one or more of the interfaces 810, 812, 814 may be adapted to communicate data, control, or management messages from the processor 804 to applications installed on the host device and/or a remote device. As another example, one or more of the interfaces 810, 812, 814 may be adapted to allow a user or user device (e.g., personal computer (PC), etc.) to interact/communicate with the processing system 800. The processing system 800 may include additional components not depicted in the figure, such as long term storage (e.g., non-volatile memory, etc.).

[0058] In some embodiments, the processing system 800 is included in a network device that is accessing, or part otherwise of, a telecommunications network. In one example, the processing system 800 is in a network-side device in a wireless or wireline telecommunications network, such as a base station, a relay station, a scheduler, a controller, a gateway, a router, an applications server, or any other device in the telecommunications network. In other embodiments, the processing system 800 is in a user-side device accessing a wireless or wireline telecommunications network, such as a mobile station, a user equipment (UE), a personal computer (PC), a tablet, a wearable communications device (e.g., a smartwatch, etc.), or any other device adapted to access a telecommunications network.

[0059] In some embodiments, one or more of the interfaces 810, 812, 814 connects the processing system 800 to a transceiver adapted to transmit and receive signaling over the telecommunications network. Figure 9 illustrates a block diagram of a transceiver 900 adapted to transmit and receive signaling over a telecommunications network. The transceiver 900 may be installed in a host device. As shown, the transceiver 900 comprises a network-side interface 902, a coupler 904, a transmitter 906, a receiver 908, a signal processor 910, and a device-side

interface 912. The network-side interface 902 may include any component or collection of components adapted to transmit or receive signaling over a wireless or wireline telecommunications network. The coupler 904 may include any component or collection of components adapted to facilitate bi-directional communication over the network-side interface 902. The transmitter 906 may include any component or collection of components (e.g., up-converter, power amplifier, etc.) adapted to convert a baseband signal into a modulated carrier signal suitable for transmission over the network-side interface 902. The receiver 908 may include any component or collection of components (e.g., down-converter, low noise amplifier, etc.) adapted to convert a carrier signal received over the network-side interface 902 into a baseband signal. The signal processor 910 may include any component or collection of components adapted to convert a baseband signal into a data signal suitable for communication over the device-side interface(s) 912, or vice-versa. The device-side interface(s) 912 may include any component or collection of components adapted to communicate data-signals between the signal processor 910 and components within the host device (e.g., the processing system 800, local area network (LAN) ports, etc.).

[0060] The transceiver 900 may transmit and receive signaling over any type of communications medium. In some embodiments, the transceiver 900 transmits and receives signaling over a wireless medium. For example, the transceiver 900 may be a wireless transceiver adapted to communicate in accordance with a wireless telecommunications protocol, such as a cellular protocol (e.g., long-term evolution (LTE), etc.), a wireless local area network (WLAN) protocol (e.g., Wi-Fi, etc.), or any other type of wireless protocol (e.g., Bluetooth, near field communication (NFC), etc.). In such embodiments, the network-side interface 902 comprises one or more antenna/radiating elements. For example, the network-side interface 902 may include a single antenna, multiple separate antennas, or a multi-antenna array configured for multi-layer communication, e.g., single input multiple output (SIMO), multiple input single output (MISO), multiple input multiple output (MIMO), etc. In other embodiments, the transceiver 900 transmits and receives signaling over a wireline medium, e.g., twisted-pair cable, coaxial cable, optical fiber, etc. Specific processing systems and/or transceivers may utilize all of the components shown, or only a subset of the components, and levels of integration may vary from device to device.

[0061] It should be appreciated that one or more steps of the embodiment methods provided herein may be performed by corresponding units or modules. For example, a signal may be transmitted by a transmitting unit or a transmitting module. A signal may be received by a receiving unit or a receiving module. A signal may be processed by a processing unit or a processing module. Other steps may be performed by a deriving unit/module and/or a verifying unit/module. The respective units/modules may be hardware, software, or a combination thereof. For instance, one or more of the units/modules may be an integrated circuit, such as field programmable gate arrays (FPGAs) or application-specific integrated circuits (ASICs).

[0062] It is contemplated that there are various embodiments the present disclosure enables. For example, in one embodiment a user equipment (UE) is disclosed that includes a processor means and a non-transitory computer readable storage medium means for storing programming for execution by the processor. The programming includes instructions to receive a reconfiguration request from a macrocell, derive a user plane encryption key according to information in the reconfiguration request, transmit a first user plane signaling message to a first microcell in a group of microcells when the UE is attached to the first microcell and transmit a second user plane signaling message to a second microcell in the group of microcells when the UE is attached to the second microcell, wherein the first user plane signaling message and the second user plane signaling message are both encrypted according to the user plane encryption key.

[0063] In some embodiments, the information in the reconfiguration request identifies an algorithm to be used by the UE for deriving the user plane encryption key and includes a unique counter to be used as an input into the algorithm. The programming of the UE may further includes instructions to derive a radio resource control (RRC) encryption key (KRRCenc) according to the user plane encryption key and transmit an RRC message to the first microcell, wherein signaling in the RRC message is encrypted according to KRRCenc. The programming of the UE may also include instructions to derive a radio resource control (RRC) integrity key (KRRCint) according to the user plane encryption key, receive an RRC message from the first microcell, and verify the integrity of the RRC message according to KRRCint. It is understood that the UE may receive an identity of the group of microcells from the first microcell, the second microcell, or a macrocell associated with the first microcell and the second microcell.

[0064] The following references are related to subject matter of the present application. Each of these references is incorporated herein by reference in its entirety:

• 3GPP TS 33.401 V12.5.1, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Release 12) (Oct. 2012).

[0065] While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications and combinations of the illustrative embodiments, as well as other embodiments of the invention, will be apparent to persons skilled in the art upon reference to the description. It is therefore intended that the appended claims encompass any such modifications or embodiments.

WHAT IS CLAIMED IS:

1. A method for establishing a trust relationship in an ultra dense network, the method comprising:

receiving, by a user equipment (UE), a reconfiguration request from a macrocell;

deriving, by the UE, a user plane encryption key according to information in the reconfiguration request;

transmitting, by the UE, a first user plane signaling message to a first microcell in a group of microcells when the UE is attached to the first microcell; and

transmitting, by the UE, a second user plane signaling message to a second microcell in the group of microcells when the UE is attached to the second microcell, wherein the first user plane signaling message and the second user plane signaling message are both encrypted according to the user plane encryption key.

2. The method of claim 1, wherein the information in the reconfiguration request identifies an algorithm to be used by the UE for deriving the user plane encryption key and includes a unique counter to be used as an input into the algorithm.

3. The method of claim 1 or claim 2, further comprising:

deriving a radio resource control (RRC) encryption key (KRRCenc) according to the user plane encryption key; and

transmitting an RRC message to the first microcell, wherein signaling in the RRC message is encrypted according to KRRCenc.

4. The method of claim 1 or claim 2, further comprising:

deriving a radio resource control (RRC) integrity key (KRRCint) according to the user plane encryption key;

receiving an RRC message from the first microcell; and

verifying the integrity of the RRC message according to KRRCint.

5. The method of any of claims 1-4, wherein the UE receives an identity of the group of microcells from at least one of:

the first microcell;

the second microcell; and

a macrocell associated with the first microcell and the second microcell.

6. A user equipment (UE) comprising:

a processor; and

a non-transitory computer readable storage medium storing programming for execution by the processor, the programming including instructions to:

receive a reconfiguration request from a macrocell;

derive a user plane encryption key according to information in the reconfiguration request;

transmit a first user plane signaling message to a first microcell in a group of microcells when the UE is attached to the first microcell; and

transmit a second user plane signaling message to a second microcell in the group of microcells when the UE is attached to the second microcell, wherein the first user plane signaling message and the second user plane signaling message are both encrypted according to the user plane encryption key.

7. The UE of claim 6, wherein the information in the reconfiguration request identifies an algorithm to be used by the UE for deriving the user plane encryption key and includes a unique counter to be used as an input into the algorithm.

8. The UE of claim 6 or claim 7, wherein the programming further includes instructions to:

derive a radio resource control (RRC) encryption key (KRRCenc) according to the user plane encryption key; and

transmit an RRC message to the first microcell, wherein signaling in the RRC message is encrypted according to KRRCenc.

9. The UE of claim 6 or claim 7, wherein the programming further includes instructions to:

derive a radio resource control (RRC) integrity key (KRRCint) according to the user plane encryption key;

receive an RRC message from the first microcell; and

verify the integrity of the RRC message according to KRRCint.

10. The UE of any of claims 6-9, wherein the UE receives an identity of the group of microcells from at least one of:

the first microcell;

the second microcell; and

a macrocell associated with the first microcell and the second microcell.

11. A computer program product comprising a non-transitory computer readable storage medium storing programming, the programming including instructions to:

receive a reconfiguration request from a macrocell;

derive a user plane encryption key according to information in the reconfiguration request;

transmit a first user plane signaling message to a first microcell in a group of microcells when a user equipment (UE) is attached to the first microcell; and

transmit a second user plane signaling message to a second microcell in the group of microcells when the UE is attached to the second microcell, wherein the first user plane signaling message and the second user plane signaling message are both encrypted according to the user plane encryption key.

12. The computer program product of claim 11, wherein the information in the reconfiguration request identifies an algorithm to be used by the UE for deriving the user plane encryption key and a unique counter to be used as an input into the algorithm.

13. The computer program product of claim 11 or claim 12, wherein the programming further includes instructions to:

derive a radio resource control (RRC) encryption key (KRRCenc) according to the user plane encryption key; and

transmit an RRC message to the first microcell, wherein signaling in the RRC message is encrypted according to KRRCenc.

14. The computer program product of claim 11 or claim 12, wherein the programming further includes instructions to:

derive a radio resource control (RRC) integrity key (KRRCint) according to the user plane encryption key;

receive an RRC message from the first microcell; and

verify the integrity of the RRC message according to KRRCint.

15. The computer program product of any of claims 11-14, wherein the UE receives an identity of the group of microcells from at least one of:

the first microcell;

the second microcell; and

a macrocell associated with the first microcell and the second microcell.

16. A secure microcells group comprising:

a first microcell configured to receive a secure microcells group key and further configured to transmit user plane signaling to a user equipment (UE) when the UE is attached to the first microcell, wherein the signaling is encrypted according to a user plane encryption key derived by the first microcell according to the secure microcells group key; and

a second microcell configured to receive the secure microcells group key and further configured to transmit user plane signaling to the UE when the UE is attached to the second microcell, wherein the signaling is encrypted according to the user plane encryption key derived by the second microcell according to the secure microcells group key.

17. The secure microcells group of claim 16, wherein a single security association is established for the first microcell and the second microcell based on at least one of:

the first microcell and the second microcell supporting the same security capabilities;

the first microcell and the second microcell belonging to the same operator;

the first microcell and the second microcell being located in a limited geographical area; and

the number of microcells being less than a defined maximum.

18. The secure microcells group of claim 16 or claim 17, wherein, when a mobility management entity is capable of communicating directly with the first microcell and the second microcell, the mobility management entity sends the secure microcells group key to one of:

both the first microcell and the second microcell; and

the first microcell, which sends the secure microcells group key to the second microcell.

19. The secure microcells group of claim 16 or claim 17, wherein, when a mobility management entity is capable of communicating with an access point associated with the first microcell and the second microcell but is not capable of communicating directly with the first microcell and the second microcell, the mobility management entity generates a general secure microcells group key from which the access point can generate an individualized secure microcells group key for the first microcell and the second microcell and sends the general secure microcells group key to the access point.

20. The secure microcells group of any of claims 16-19, wherein at least one of the first microcell and the second microcell transmits to the UE an identity of a group of microcells to which the first microcell and the second microcell belong.

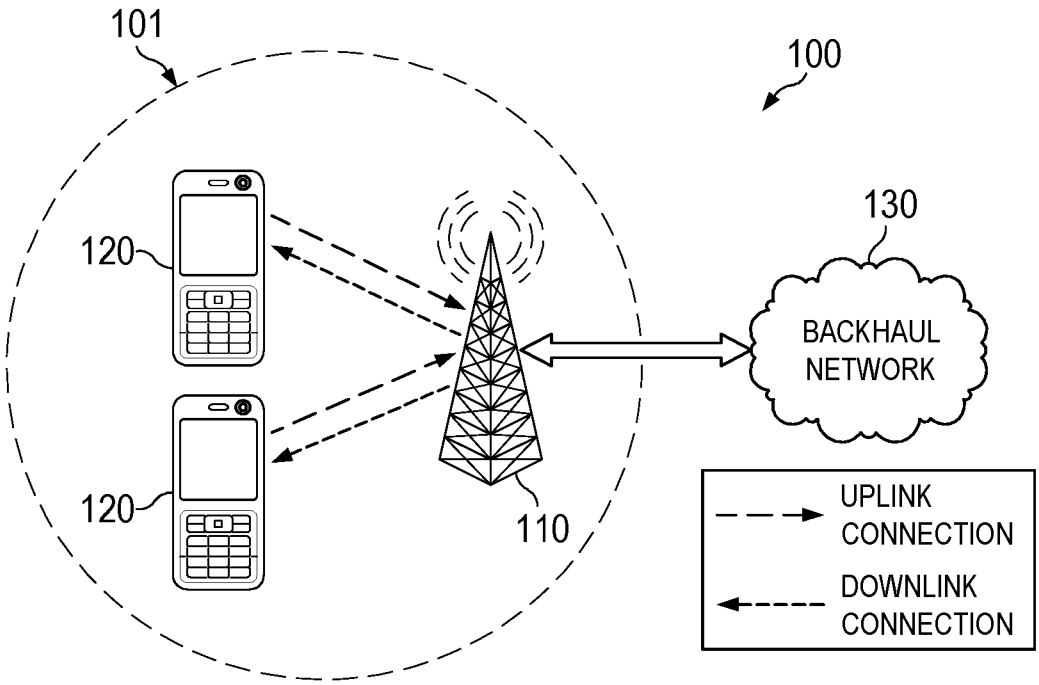
101
100
130
120
120
BACKHAUL NETWORK
110
UPLINK CONNECTION
DOWNLINK CONNECTION

FIG. 1

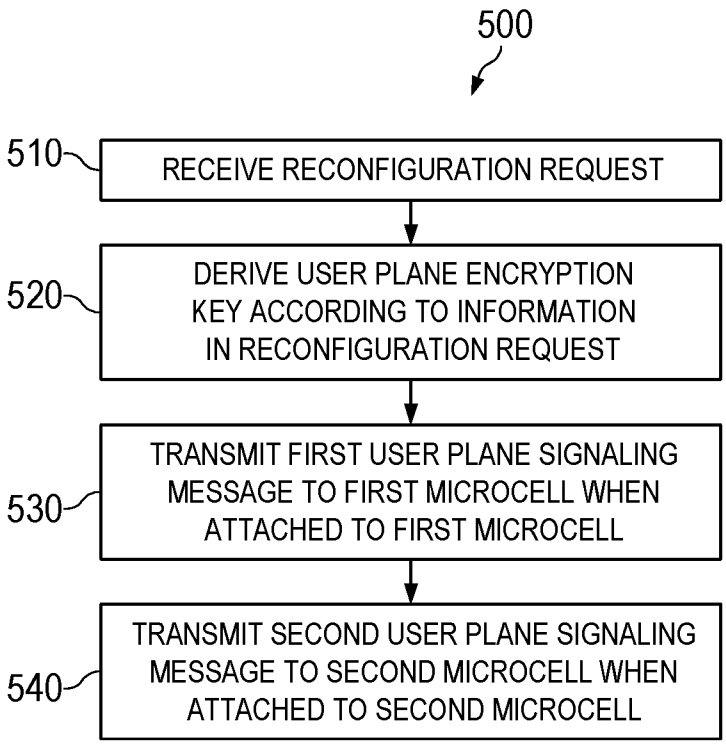
500
510
RECEIVE RECONFIGURATION REQUEST
520
DERIVE USER PLANE ENCRYPTION KEY ACCORDING TO INFORMATION IN RECONFIGURATION REQUEST
530
TRANSMIT FIRST USER PLANE SIGNALING MESSAGE TO FIRST MICROCELL WHEN ATTACHED TO FIRST MICROCELL
540
TRANSMIT SECOND USER PLANE SIGNALING MESSAGE TO SECOND MICROCELL WHEN ATTACHED TO SECOND MICROCELL

FIG. 5

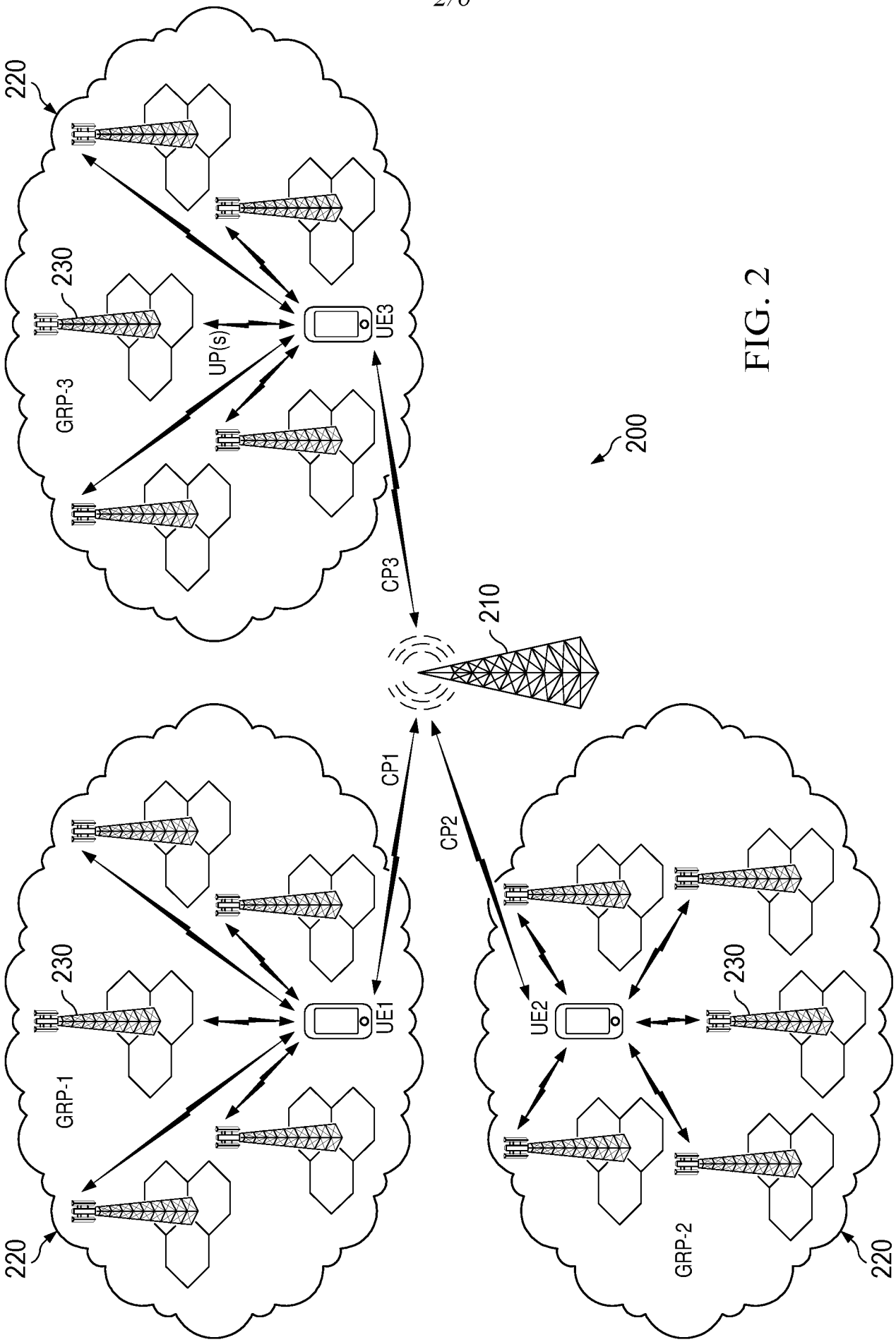
220
230
GRP-3
UP(s)
UE3
CP3
210
200
CP1
CP2
UE1
UE2
GRP-1
GRP-2
220
230
230
220

FIG. 2

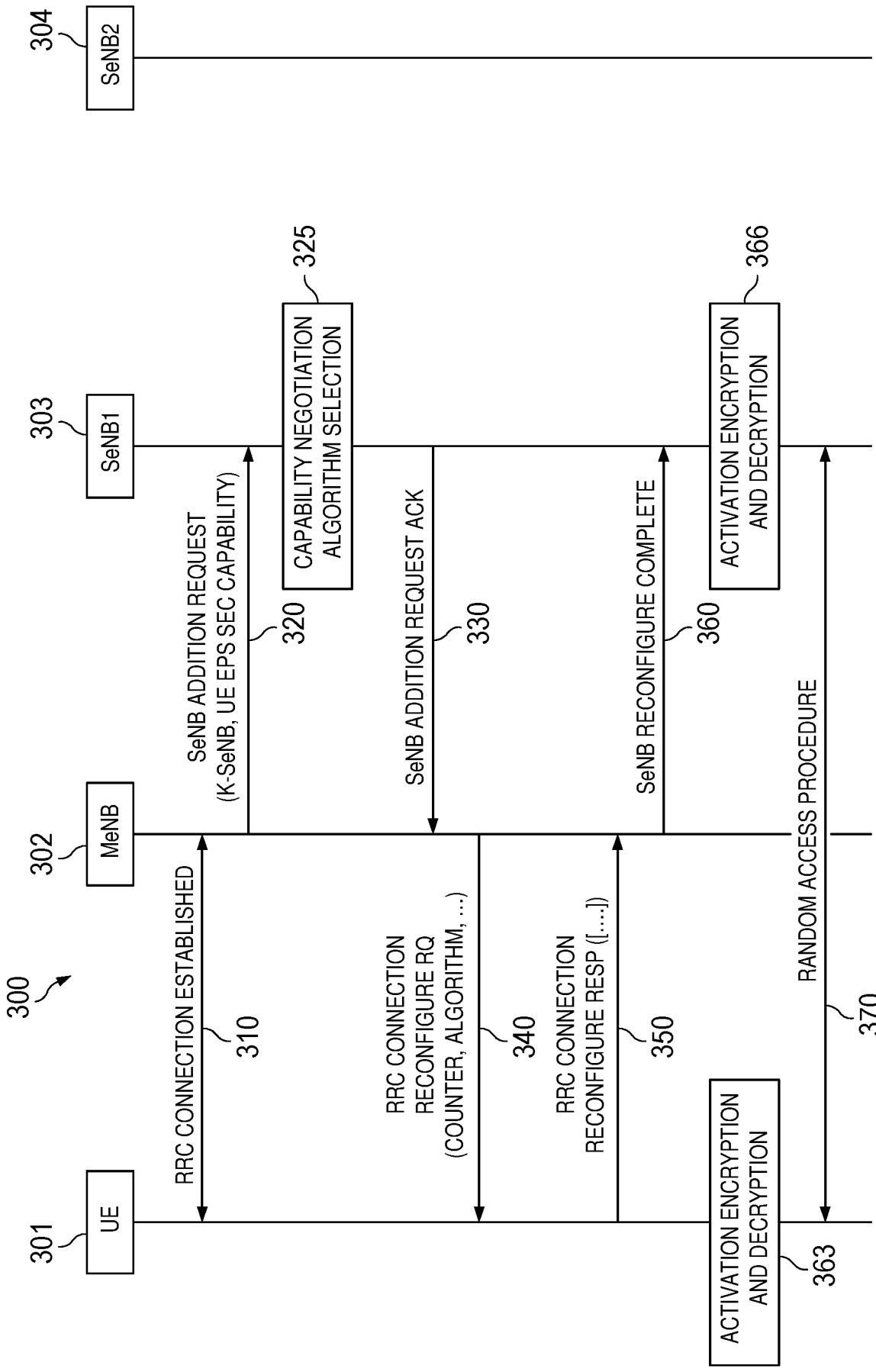
300
301
UE
302
MeNB
303
SeNB1
304
SeNB2
RRC CONNECTION ESTABLISHED
310
SeNB ADDITION REQUEST
(K-SeNB, UE EPS SEC CAPABILITY)
320
CAPABILITY NEGOTIATION
ALGORITHM SELECTION
325
SeNB ADDITION REQUEST ACK
330
RRC CONNECTION
RECONFIGURE RQ
(COUNTER, ALGORITHM, ...)
340
RRC CONNECTION
RECONFIGURE RESP ([....])
350
SeNB RECONFIGURE COMPLETE
360
ACTIVATION ENCRYPTION
AND DECRYPTION
366
ACTIVATION ENCRYPTION
AND DECRYPTION
363
RANDOM ACCESS PROCEDURE
370

FIG. 3

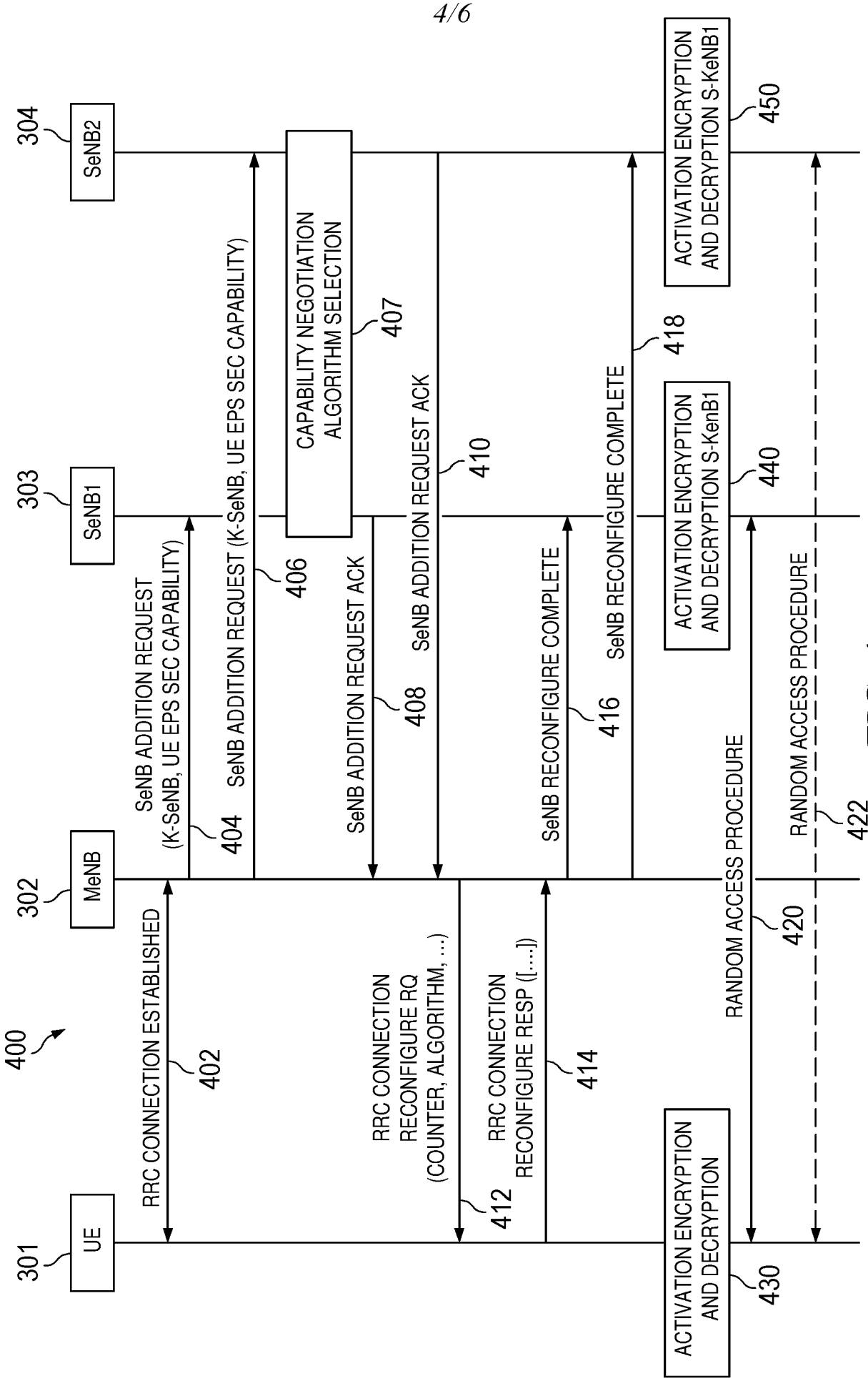
400
301
UE
302
MeNB
303
SeNB1
304
SeNB2
RRC CONNECTION ESTABLISHED
402
SeNB ADDITION REQUEST
(K-SeNB, UE EPS SEC CAPABILITY)
404
SeNB ADDITION REQUEST (K-SeNB, UE EPS SEC CAPABILITY)
406
CAPABILITY NEGOTIATION
ALGORITHM SELECTION
407
SeNB ADDITION REQUEST ACK
408
SeNB ADDITION REQUEST ACK
410
RRC CONNECTION
RECONFIGURE RQ
(COUNTER, ALGORITHM, ...)
412
RRC CONNECTION
RECONFIGURE RESP ([....])
414
SeNB RECONFIGURE COMPLETE
416
SeNB RECONFIGURE COMPLETE
418
RANDOM ACCESS PROCEDURE
420
RANDOM ACCESS PROCEDURE
422
ACTIVATION ENCRYPTION
AND DECRYPTION
430
ACTIVATION ENCRYPTION
AND DECRYPTION S-KenB1
440
ACTIVATION ENCRYPTION
AND DECRYPTION S-KeNB1
450

FIG. 4

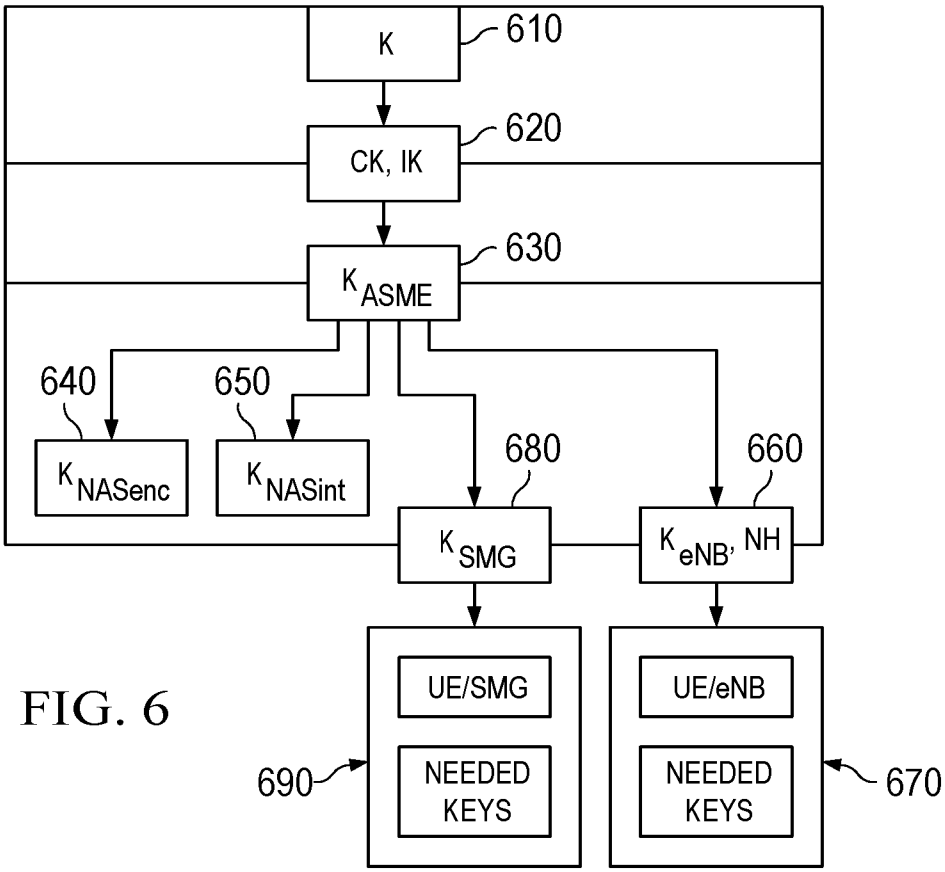
K
610
CK, IK
620
K ASME
630
640
650
K NASenc
K NASint
680
660
K SMG
K eNB, NH
UE/SMG
UE/eNB
NEEDED KEYS
NEEDED KEYS
690
670

FIG. 6

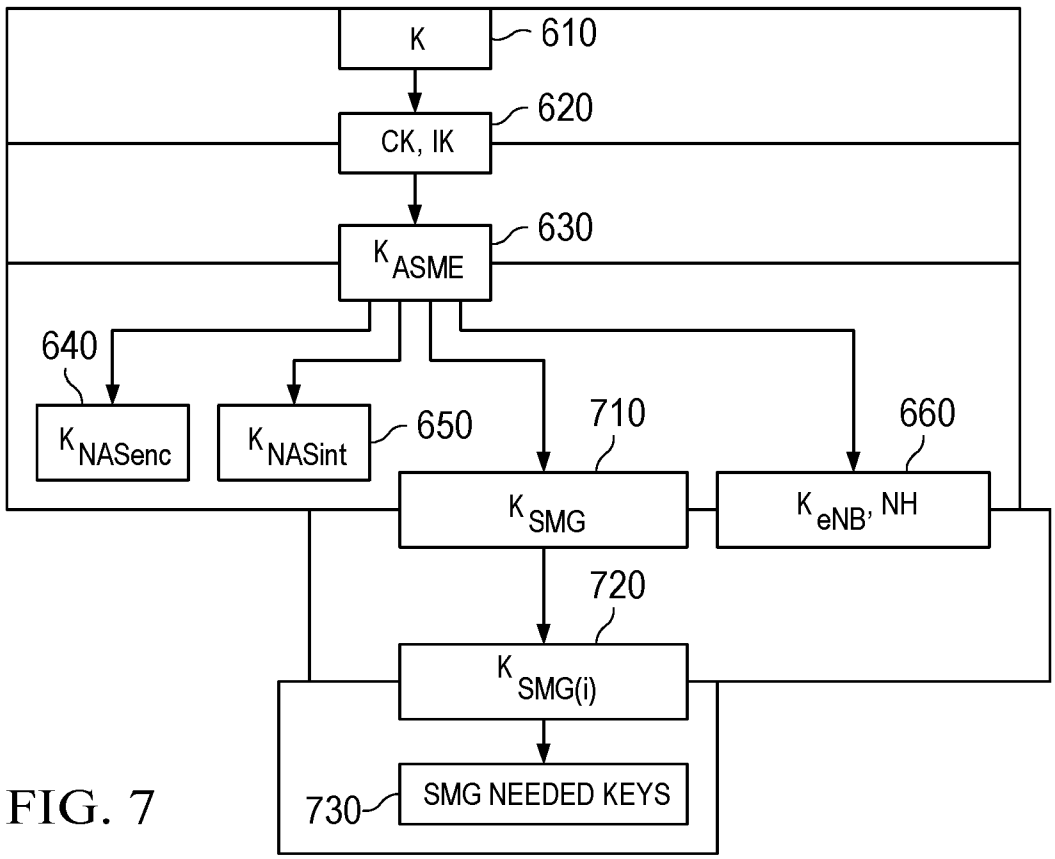
K
610
CK, IK
620
K ASME
630
640
K NASenc
K NASint
650
710
660
K SMG
K eNB, NH
720
K SMG(i)
730
SMG NEEDED KEYS

FIG. 7

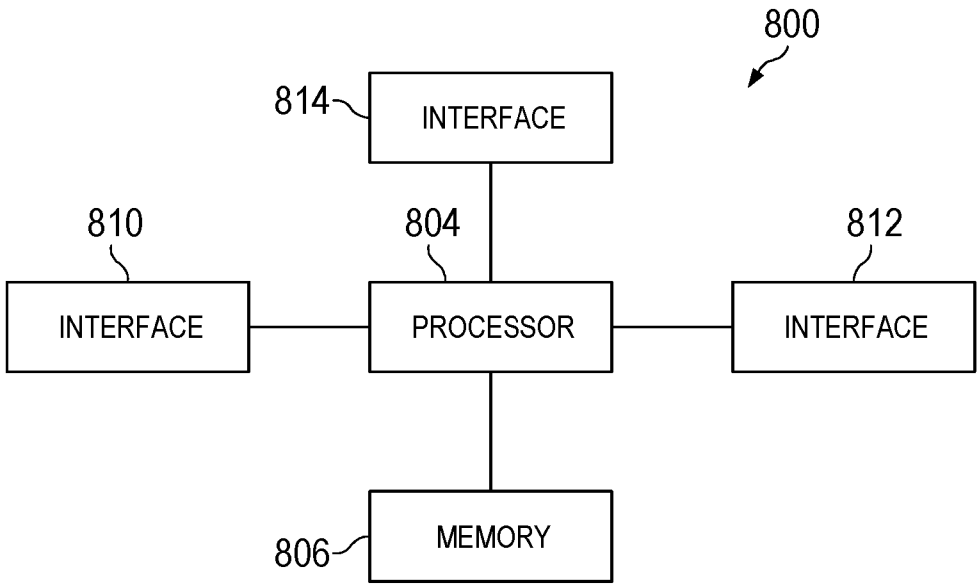
800
814
INTERFACE
810
804
812
INTERFACE
PROCESSOR
INTERFACE
806
MEMORY

FIG. 8

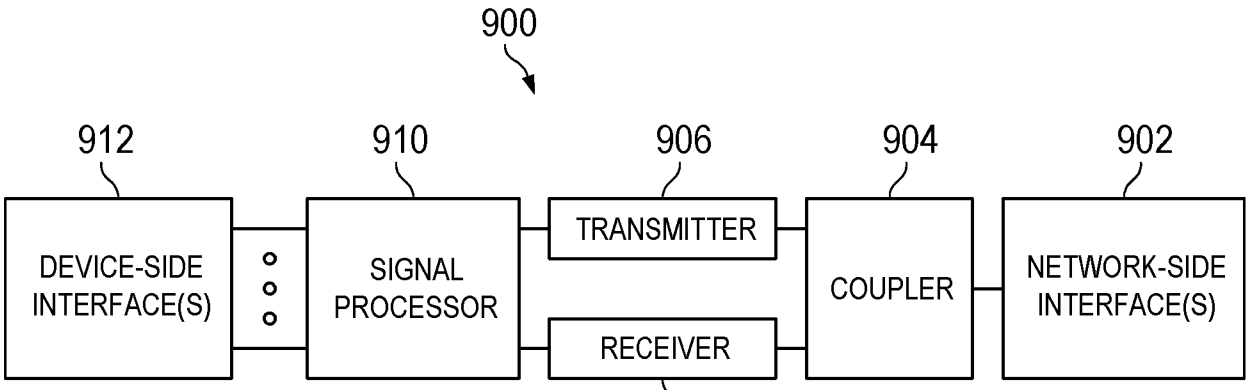
900
912
910
906
904
902
DEVICE-SIDE INTERFACE(S)
SIGNAL PROCESSOR
TRANSMITTER
RECEIVER
COUPLER
NETWORK-SIDE INTERFACE(S)
908

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/091053

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/02(2009.01)i

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)

WPI, EPODOC, CNPAT, CNKI, GOOGLE：key, encrypt, macro, micro, cell, small 2w cell, SeNB, MeNB, control, node, eNB, dual, connection, group, cluster, user 2w plane, UE, configure, hand 2w off, hand 2w over, switch, reselect

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103959829 A (HUAWEI TECHNOLOGIES CO.，LTD.) 30 July 2014 (2014-07-30) abstract，description，paragraphs [0003]-[0034]	1-20
A	CN 104349312 A (ALCATEL LUCENT ET AL.) 11 February 2015 (2015-02-11) the whole document	1-20
A	CN 102740289 A (CHINA ACADEMY OF TELECOMMUNICATIONS TECHNOLOGY) 17 October 2012 (2012-10-17) the whole document	1-20
A	WO 2014120077 A1 (TELEFONAKTIEBOLAGET L M ERICSSONPUBL) 07 August 2014 (2014-08-07) the whole document	1-20

☐ 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
11 October 2016	**26 October 2016**

Name and mailing address of the ISA/CN	Authorized officer
STATE INTELLECTUAL PROPERTY OFFICE OF THE P.R.CHINA **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088** **China**	**XU,Quan**
Facsimile No. **(86-10)62019451**	Telephone No. **(86-10)62413354**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/091053

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	103959829	A	30 July 2014	WO	2015062097	A1	07 May 2015
				US	2016249210	A1	25 August 2016
				EP	3057349	A1	17 August 2016
CN	104349312	A	11 February 2015	WO	2015015300	A2	05 February 2015
CN	102740289	A	17 October 2012	US	2015126154	A1	07 May 2015
				EP	2863668	A1	22 April 2015
				WO	2013185579	A1	19 December 2013
				KR	20150028991	A	17 March 2015
WO	2014120077	A1	07 August 2014	EP	3018850	A1	11 May 2016
				KR	20150114978	A	13 October 2015
				JP	2016509804	A	31 March 2016
				HK	1210881	A1	06 May 2016
				AU	2014213034	A1	06 August 2015
				EP	2951975	A1	09 December 2015
				CA	2899721	A1	07 August 2014
				MA	38355	A1	29 January 2016
				US	2016174070	A1	16 June 2016
				US	2015092942	A1	02 April 2015
				MX	2015009101	A	05 October 2015
				CN	104956644	A	30 September 2015