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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 August 2009 (27.08.2009)

PCT

(10) International Publication Number
WO 2009/105155 A2

(51) International Patent Classification:
H04W 36/00 (2009.01)

(21) International Application Number:
PCT/US2009/000705

(22) International Filing Date:
4 February 2009 (04.02.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/071,098 15 February 2008 (15.02.2008) US

(71) Applicant *(for all designated States except US)*: **ALCATEL-LUCENT USA INC.** [US/US]; 600-700 Mountain Avenue, Murray Hill, NJ 07974-0636 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BRUSILOVSKY, Alec** [US/US]; 3844 Caine Court, Naperville, IL 60564 (US). **GODARD, Tania** [FR/FR]; 1. Avenue Pierre Grenier, F-92100 Boulogne-Billancourt (FR). **PATEL, Sarvar** [US/US]; 34 Millers Lane, Montville, NJ 07045 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, ST, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

(54) **Title**: SYSTEM AND METHOD FOR PERFORMING HANDOVERS, OR KEY MANAGEMENT WHILE PERFORMING HANDOVERS IN A WIRELESS COMMUNICATION SYSTEM

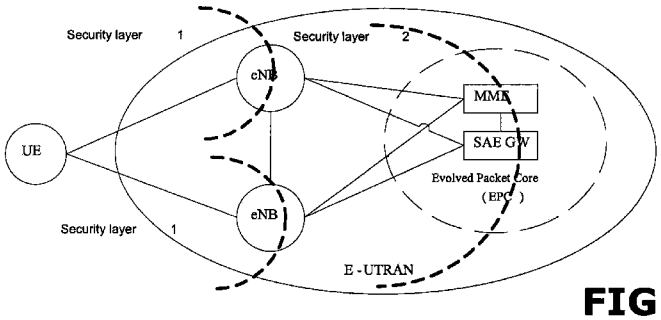

FIG. 1

(57) **Abstract**: Example embodiments provide a method for performing handovers and key management while performing handovers. The method includes communicating a random handover seed key protected by a secure protocol from a core component of a network to a user equipment. The secure protocol prevents the random handover seed key from being learned by base stations supported by the core component of the network. The secure protocol may be non-access stratum signaling of an evolved packet system environment for wireless communications.

WO 2009/105155 A2

SYSTEM AND METHOD FOR PERFORMING HANDOVERS, OR KEY MANAGEMENT WHILE PERFORMING HANDOVERS IN A WIRELESS COMMUNICATION SYSTEM

BACKGROUND

Field of the Invention

Example embodiments of the present application relate to a system and method for telecommunications. More particularly, example embodiments relate to a method of providing secure wireless communication between a network and user equipment using secure keys.

Background Information

Security methods and processes relating to wireless communications are evolving. For example, the 3rd Generation Partnership Project (3GPP), which is a collaboration between various groups of telecommunications associations, is currently working on developing security protocols applicable to wireless communications within an enhanced packet system (EPS).

FIG. 1 illustrates an example of an EPS environment for wireless communications. The EPS of FIG. 1 illustrates a user equipment (UE), evolved NodeBs (eNBs) and a mobility management entity (MME). FIG. 1 also illustrates that the eNBs and the MMEs are part of the evolved UMTS terrestrial radio access network (eUTRAN) indicated by the solid-line oval, while the UE is outside of the eUTRAN. Further, the MME is included in the evolved packet core (EPC) of the EPS environment shown in FIG. 1. The EPC is identified by the thin dashed-line oval.

Generally, an EPS has two layers of protection instead of one layer perimeter security as is used in universal mobile telecommunications system (UMTS). The first security layer is the evolved UMTS Terrestrial Radio Access Network (eUTRAN), and the second security layer is evolved Packet Core (EPC) network security. Evolved Packet Core security involves the use of non-access stratum (NAS) signaling security.

A conventional example of security of an EPS environment is now discussed with respect to the signaling diagram illustrated in FIG. 2.

The signaling diagram of FIG. 2 illustrates messages communicated between and operations of a user equipment (UE), first evolved NodeB (source eNB), second evolved NodeB (target eNB), and an evolved packet core (EPC). The EPC includes a Mobility Management Entity (MME) and system architecture evolution gateway (SAE GW). Specifically, the conventional signaling diagram of FIG. 2 illustrates communication between these various components during an intra-MME handover. An intra-MME handover refers to a handover of a UE from a source eNB to a target eNB, in which both the source eNB and target eNB are supported by the same MME.

Referring to FIG. 2, the UE sends a measurement report to the source eNB in message 1. The contents of the measurement report are well-known in the art and thus, are not discussed herein for the sake of brevity.

In response to receiving the measurement report, the source eNB determines which target eNB to conduct the handover procedure with. To begin this conventional handover, the source eNB derives a second key KeNB* from a first key KeNB that is known at the source eNB as shown by operation 1A. Once the second key KeNB* is derived by the source eNB, the source eNB sends a handover request to the target eNB along with the second key KeNB* in message 2.

In response to receiving the handover request, the target eNB provides a handover response to the source eNB along with a Cell Radio Temporary Identity (C-RNTI) in message 3. Conventionally, this C-RNTI is a 16 bit or 32 bit number. Further, this C-RNTI may simply be an identifier related to the target eNB. In the conventional signal diagram of FIG. 2, the second key KeNB* and C-RNTI are being relied on for security. As shown by operation 3A, the target eNB also derives a third key KeNB** from the KeNB* and the C-RNTI. Further, Radio Resource Control and User Plane (RRC/UP) keys are derived from the third key keNB** by the target eNB in operation 3B as is well known in the art.

Still referring to FIG. 2, the source eNB in response to receiving the handover response in message 3, transmits a handover command to the UE. The handover command instructs the UE to perform a handover with the target eNB as shown by Message 4.

Once the UE receive the handover command of message 4, the UE derives a third key KeNB** from the KeNB* and the C-RNTI in operation 4A, which is the same as the key derived in operation 3A by the target eNB. From the third key KeNB**, the UE derives RRC/UP keys as is well-known in the art as shown by operation 4B. As such, both the UE and target eNB have the RRC/UP keys. The UE then sends a handover confirm message to the target eNB as indicated by message 5.

In response to receiving the handover confirm message from the UE, the target eNB sends a handover complete message to the source eNB indicating the intra-MME handover is complete in message 6. Lastly, as indicated by message 7, the target eNB, which is now the source eNB sends a UE location update message to the EPC.

SUMMARY

Example embodiments provide a method of providing secure wireless communication between a network and user equipment using secure keys. In particular, example embodiments provide a method for performing handovers and key management while providing increased security.

An example embodiment provides a method performed by user equipment. The method includes receiving a random handover seed key protected by a secure protocol from a core component of a network such as a MME. The secure protocol prevents the random handover seed key from being learned by base stations (e.g., eNBs) supported by the core component of the network. The method also includes receiving a handover command from a source base station. The handover command includes a target base station identifier identifying a target base station. The target base station is a base station targeted to provide services to a user equipment that is supported by the source base station. The method also includes deriving encryption keys using the received random handover seed key and the target base station identifier, and communicating with the target base station based on the derived encryption keys and the target base station identifier.

According to an example embodiment, the method performed by the user equipment further includes sending a confirmation message to the target base station to confirm handover from the source base station to the target base station is acceptable.

According to an example embodiment, the method performed by the user equipment further includes sending a measurement report to the source base station. Further, the receiving step may receive the handover command from the source base station in response to the sent measurement report.

According to an example embodiment, in the method performed by the user equipment, the deriving step may input the random handover seed key and the target base station identifier as inputs to a key derivation function to derive the encryption keys.

According to an example embodiment, the secure protocol is a non-access stratum (NAS) protocol.

Another example embodiment provides a method performed by a core component (e.g., MME) of the network. The method includes sending a random handover seed key from the core component of a network to a user equipment using a secure protocol that prevents the random handover seed key from being learned by base stations supported by the core network component.

According to the example embodiment, the method performed by the core component of the network further includes assigning a first random key at the core component of a network to each base station supported by the core component, and providing the first random key to each of the respective base stations. The first random key is different for each base station and is provided prior to sending the random handover seed key to the user equipment.

According to the example embodiment of the method performed by the core component of the network, the providing step may provide the first random key to each of the respective base stations prior to a handover procedure involving the respective base stations.

According to the example embodiment, the method performed by the core component further includes receiving a list of potential handover target base stations for the user equipment from a source base station currently supporting the user equipment, selecting the random handover seed key, deriving a second random key specific for

each target base station listed in the list of potential handover target base stations by using the random handover seed key and respective target base station identifiers as inputs to a key derivation function (e.g., AES). Still further, the method includes encrypting each second random key with the corresponding first random key to obtain an encrypted second random key for each target base station listed in the list of potential handover target base stations, and sending a list of the encrypted second random keys to the source base station.

Another example embodiment provides a method performed by base station. The method performed by a base station includes sending a list identifying potential handover target base stations for a user equipment to a core component to request information for each of the potential handover target base stations included in the list, and receiving a list of encrypted first random keys. Each of the encrypted first random keys is specific to one of the potential handover target base stations.

According to the example embodiment, a random handover seed key protected by a secure protocol is sent from a core component of a network to the user equipment. The secure protocol prevents the random handover seed key from being learned by a source base station currently supporting the user equipment and the potential handover target base stations supported by the core component of the network.

According to the example embodiment, the method performed by a base station further includes receiving a measurement report from the user equipment, selecting one of the potential handover target base stations as a target base station to support the user equipment following a successful handover, and forwarding a handover request to the target base station. The handover request includes the encrypted first random key corresponding to the selected target. Still further, the method includes sending a handover command to the user equipment, receiving a handover complete signal from

the target base station, and handing over support of the user equipment to the target base station in response to receiving the handover complete signal.

Still another example embodiment provides a method performed by a base station. The method includes receiving a first random key from a core component of a network including a plurality of base stations one of which is a source base station supporting a user equipment and another of which is a target base station for supporting the user equipment after handover. The method also includes receiving a handover request including an encrypted first random key at the target base station, decrypting the handover request using the first random key to recover a second random key, deriving encryption keys from the second random key at the target base station, and communicating with the user equipment based on the derived encryption keys.

According to the example embodiment, the first random key is received prior to a handover procedure started by receiving the handover request.

According to the example embodiment, a random handover seed key protected by a secure protocol is sent from the core component of the network to the user equipment. The secure protocol prevents the random handover seed key from being learned by the source base station currently supporting the user equipment and the target base station supported by the core component of the network.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other features and advantages of example embodiments will become more apparent by reviewing the following detailed description of example embodiments of this disclosure with reference to the attached drawings in which:

FIG. 1 illustrates a EPS environment for wireless communications; illustrates a signal flow diagram of message and operations performed in a conventional Intra-MME handover procedure;

FIG. 2 illustrates a signal flow diagram of message and operations performed in a conventional intra-MME handover procedure; and

FIG. 3 illustrates a signal flow diagram illustrating messages and operations of a Intra-MME handover procedure according to an example embodiment.

DETAILED DESCRIPTION OF EXAMPLE EMBODIMENTS

In the following description, for purposes of explanation and not limitation, specific details are set forth such as particular architectures, interfaces, techniques, etc., in order to provide a thorough understanding of example embodiments. However, it will be apparent to those skilled in the art that example embodiments may be practiced in other illustrative embodiments that depart from these specific details. In some instances, detailed descriptions of well-known devices, circuits, and methods are omitted so as not to obscure the description of example embodiments with unnecessary detail. All principles, aspects, and embodiments, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future.

Example embodiments are discussed herein as being implemented in a suitable computing environment. Although not required, example embodiments will be described in the general context of computer-executable instructions, such as program modules or functional processes, being executed by one or more computer processors or CPUs. Generally, program modules or functional processes include routines,

programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. The program modules and functional processes discussed herein may be implemented using existing hardware in existing communication networks. For example, program modules and functional processes discussed herein may be implemented using existing hardware at existing radio network control nodes.

In the following description, illustrative embodiments will be described with reference to acts and symbolic representations of operations (e.g., in the form of signaling diagrams) that are performed by one or more processors, unless indicated otherwise. As such, it will be understood that such acts and operations, which are at times referred to as being computer-executed, include the manipulation by the processor of electrical signals representing data in a structured form. This manipulation transforms the data or maintains it at locations in the memory system of the computer, user equipment and/or access network, which reconfigures or otherwise alters the operation of the computer, user equipment and/or access network in a manner well understood by those skilled in the art.

An example embodiment of a method for performing handovers as well as key management in a wireless communication system is explained below with respect to the signal flow diagram illustrated in FIG. 3. One skilled in the art will appreciate that the method explained below may be implemented in an EPS environment for wireless communication such as that shown in FIG. 1. In particular, the example embodiments described below leverage use of NAS signaling security of an EPS. The NAS security essentially provides a tunnel between the UE and the MME, which is transparent to the eNBs. In particular, the NAS security tunnel cannot be read and/or decoded by the eNBs according to example embodiments.

FIG. 3 illustrates an example embodiment of an MME-assisted key refresh procedure for intra-MME handovers. In particular, the signaling diagram of FIG. 3 shows message exchanges between and operations performed by a UE, a source eNB, a target eNB and the MME of the EPS previously described with respect to FIG. 1. The signaling diagram of FIG. 3 also identifies three different groupings of the messages and operations including the initial security association (SA) establishment messages and operations, messages and operations performed prior to handover, and handover messages and operations.

Referring to FIG. 3, the MME generates an eNB random key MME-eNB_key[eNB_ID] for each of the eNBs of the EPS in operation 1. The number of bits of this random key may vary. According to examples described herein, each eNB random key MME-eNB_key[eNB_ID] is 128 or 256 bits long, matches the length of the serving system keys (128 or 256 bits), and is specific to a corresponding eNB. In the initial security establishment phase, the eNB and MME have a security association established, only afterwards do they try to agree on a MME-eNB_Key. This happens to each eNB, perhaps after it has booted up and established a security association. It is noted that there is no waiting for an eNB to become a source or target eNB in a handover. The MME-eNB key is established independent of handovers. Further, the MME-eNB key may be refreshed after some period.

As indicated by message 2, the MME sends a different eNB random key MME-eNB_key[eNB_ID] to each of the target eNBs connected to the MME via a S1 interface. The source eNB is the eNB currently providing wireless communication services to the UE. Prior to handover, a UE location update message is sent from the source eNB to the MME as indicated by message 3. The UE location update message includes a list of eNBs to which wireless communication services for the UE may be

handed over from the source eNB. Stated differently, the location update message includes a list of neighbor eNBs that is transmitted from the source eNB to the MME. Still referring to FIG. 3, the MME selects and/or creates a random handover seed key H_key as indicated by operation 3A. According to example embodiments, the random handover seed key H_key is unknown to the eNBs of the EPS. In operation 3B, the MME uses an identifier eNB ID individually identifying each of the eNBs of the system as an input to a key derivation function along with the random handover seed key H_key to create a first key $KeNB_{eNB\_ID}$ for each target eNB in the received neighbor list. For example, the key derivation function is an AES and thus, the first key for an eNB is represented as follows: $KeNB_{eNB\_ID} = AES_{H\_key}(eNB\_ID)$. Further, the MME then encrypts the calculated first key $KeNB_{eNB\_ID}$ with the respective eNB random keys MME-eNB_key[eNB_ID_{Target}] of the target eNBs in operation 3C to obtain an encrypted first key $\{KeNB_{eNB\_ID}\}_{MME\text{-}eNB\_key[eNB\_ID]}$. The notation $\{X\}_Y$ designates the encryption of X using the key Y. The encryption of the key should be semantically secure encryption. For example a 128 bit key could be encrypted by using it as input to a 128 bit AES block cipher and using MME-eNB_key as the AES key. Another option is to use any form of encryption, but supplement with a message integrity tag. An encrypted first key $\{KeNB_{eNB\_ID}\}_{MME\text{-}eNB\_key[eNB\_ID]}$ is obtained for each of the potential target eNBs identified in the UE location update message sent from the source eNB to the MME in message 3.

Once the MME obtains the encrypted first keys $\{KeNB_{eNB\_ID}\}_{MME\text{-}eNB\_key[eNB\_ID]}$ for each of the potential target eNBs, the encrypted first keys $\{KeNB_{eNB\_ID}\}_{MME\text{-}eNB\_key[eNB\_ID]}$ are provided to the source eNB as indicated by message 4. Stated differently, the MME sends an array or list of obtained encrypted first keys $\{KeNB_{eNB\_ID}\}_{MME\text{-}eNB\_key[eNB\_ID]}$ for the potential target eNBs. Each element of that

array corresponds to a potential target eNB and is indexed by the identifier eNB_ID. Thus, according to example embodiments, the keys provided to the source eNB in response to receiving the UE location update message are encrypted, specific to the different potential target eNBs, and generated based on the random handover seed key H_key.

Referring to FIG. 3, the MME forwards the random handover seed key H_key selected in operation 3A to the UE in message 5. According to example embodiments, the forwarding of the H_key is protected by a NAS security. It is noted that at any initial and/or subsequent authentication using Authentication Key Agreement (AKA), the UE and MME create security contexts, including NAS encryption and NAS integrity keys. When messages pass through one or more eNBs over the air interface to the UE, eNBs cannot see the content of the NAS messages since neither the MME nor the UE share NAS keys with eNBs. As such, the random handover seed key H_key cannot be eavesdropped by either the source eNB or target eNB during the transmission of message 5. Stated differently, the random handover seed key H_key is protected by NAS security to prevent the eNBs supported by the MME from learning the random handover seed key H_key. Accordingly, even if an attacker has control over the source eNB, the attacker is inhibited and/or prevented from obtaining the random handover seed key H_key.

Once the message exchanges 1-5 and operations 1 and 3A-3B described above are completed, an example embodiment of a handover procedure for handing over the UE from the source eNB to a target eNB is performed as detailed below.

Still referring to FIG. 3, the UE sends a measurement report to the source eNB as indicated by message 6. As described in the background section with respect to FIG. 1, the measurement report is well-known in the art and thus, is not described herein

for the sake of brevity. In response to receiving the measurement report, the source eNB makes a handover decision for the UE as indicated in operation 6a. As such, the source eNB determines which target eNB will provide communication services to the UE following the handover procedure. Once the handover decision is made by the source eNB, the source eNB sends a handover request to the target eNB. The handover request includes the encrypted first key $\{KeNB_{Target\ eNB\_ID}\}_{MME\text{-}eNB\_key[Target\ eNB\_ID]}$ corresponding to the target eNB as shown by message 7.

As previously described with respect to message 4, the MME sends an array or list of obtained encrypted first keys $\{KeNB_{eNB\_ID}\}_{MME\text{-}eNB\_key[eNB\_ID]}$ for the potential target eNBs. Each element of that array corresponds to a potential target eNB and is indexed by the identifier eNB_ID. As such, when the source eNB knows the target eNB identifier Target eNB_ID, the source eNB forwards the encrypted KeNB for the identified target eNB to the target eNB. The encrypted first key $\{KeNB_{Target\ eNB\_ID}\}_{MME\text{-}eNB\_key[Target\ eNB\_ID]}$ is sent to the target eNB according to example embodiment, as compared with merely sending a handover request including the second key KeNB* derived with a one-way function from the first KeNB as described in the conventional method of FIG. 2.

Referring to operation 7A of FIG. 3, the target eNB recovers first key $KeNB_{eNB\_ID}$ for the target eNB by decrypting the encrypted first key value $\{KeNB_{Target\ eNB\_ID}\}_{MME\text{-}eNB\_key[Target\ eNB\_ID]}$ using the key MME-eNB_key[Target eNB_ID_{Target}] previously sent to the target eNB from the MME in message 2. The target eNB sends a handover response to the source eNB in message 8. Further, the target eNB derives RRC/UP keys from the decrypted first key value $KeNB_{Target\ eNB\_ID}$ in operation 8A.

As indicated by message 9, the source eNB sends a handover command to the UE. The handover command of message 9 makes the target eNB known to the UE by

including an identifier Target eNB_ID of the target eNB. As previously discussed, the UE has already received the random handover seed key H_Key. Accordingly, the UE derives the first key for the target eNB $KeNB_{Target\ eNB\_ID}$ in operation 9A. An equation for deriving the first key for the target eNB is as follows: $KeNB_{Target\ eNB\_ID} = AES_{H\_key}$(Target eNB_ID). From the obtained first key for the target eNB $KeNB_{Target\ eNB\_ID}$, the UE derives RRC/UP keys in operation 9B. Derivation of the RRC/UP keys are well-known in the art and thus, are not discussed herein for the sake of brevity.

Still referring to FIG. 3, the UE sends a handover confirm message to the target eNB as shown by message 10. The target eNB receives the handover confirm message from the UE and notifies the source eNB that the handover is complete. The target eNB notifies the source eNB by transmitting a handover complete signal in message 10.

Once the handover procedure is complete, the target eNB, which is now the second source eNB for the UE, sends a UE location update message with a list of potential targets, i.e., neighbor eNBs, to the MME in order to prepare for a possible second handover in message 12. As such, message 12 is similar to message 3, which was sent from the first source eNB to the MME prior to the handover from the first source eNB to the target eNB. Message 13 is similar to previously described message 4 for the same reasons. In particular, the MME again obtains encrypted first keys $\{KeNB_{eNB\_ID}\}_{MME\text{-}eNB\_key[eNB\_ID]}$ for each of the potential target eNBs, and the encrypted first keys $\{KeNB_{eNB\_ID}\}_{MME\text{-}eNB\_key[eNB\_ID]}$ are provided to the source eNB in message 13

Example embodiments being thus described, it will be obvious that the same may be varied in many ways. Such variations are not to be regarded as a departure from the

example embodiments, and all such modifications are intended to be included within the scope.

WE CLAIM:

1. A method for secure wireless communication, the method comprising:

receiving, at a user equipment (UE), a random handover seed key (H_Key) protected by a secure protocol (NAS security) from a core component of a network, the secure protocol preventing the random handover seed key from being learned by base stations supported by the core component of the network;

receiving, at the user equipment, a handover command from a source base station, the handover command including a target base station identifier (Target eNB_ID) identifying a target base station, the target base station being a base station targeted to provide services to the user equipment that is supported by the source base station;

deriving encryption keys (RRC/UP key) using the received random handover seed key and the target base station identifier; and

communication with the target base station based on the derived encryption keys and the target base station.

2. The method of claim 1, wherein the deriving step inputs the random handover seed key and the target base station identifier as inputs to a key derivation function (AES) to derive the encryption keys.

3. The method of claim 1, wherein the secure protocol is a non-access stratum (NAS) protocol.

4. A method for secure wireless communication, the method comprising:

sending a random handover seed key (H_Key) from a core component (MME) of a network to a user equipment (UE) using a secure protocol that prevents the random handover seed key from being learned by base stations supported by the core network component.

5. The method of claim 4, further comprising:

assigning a first random key (MME-eNB-key[eNB_ID]) at the core component of a network to each base station supported by the core component; and

providing the first random key to each of the respective base stations, the first random key being different for each base station and being provided prior to sending the random handover seed key to the user equipment.

6. The method of claim 5, further comprising:

receiving, at the core component of the network, a list of potential handover target base stations for the user equipment (UE location update) from a source base station currently supporting the user equipment;

selecting the random handover seed key;

deriving a second random key ($KeNB_{eNB\_ID}$) specific for each target base station listed in the list of potential handover target base stations by using the random handover seed key and respective target base station identifiers as inputs to a key derivation function (AES);

encrypting each second random key with the corresponding first random key to obtain an encrypted second random key ($\{KeNBeNB\_ID\}_{MME\text{-}eNB\_key[eNB\_ID]}$) for each target base station listed in the list of potential handover target base stations; and

sending a list of the encrypted second random keys to the source base station.

7. A method for secure wireless communication, the method comprising:

sending a list identifying potential handover target base stations (UE location update) from a source base station to a core component (MME) of a network to request information for each of the potential handover target base stations included in the list;

receiving a list of encrypted first random keys from the core component of the network, each of the encrypted first random keys being specific to one of the potential handover target base stations.

8. The method of claim 7, wherein a random handover seed key (H_Key) protected by a secure protocol is sent from the core component of a network to a user equipment (UE), the secure protocol preventing the random handover seed key from being learned by a source base station currently supporting the user equipment and the potential handover target base stations supported by the core component of the network.

9. The method of claim 7, further comprising:

receiving, at the source base station, a measurement report from the user equipment;

selecting one of the potential handover target base stations as a target base station to support the user equipment following a successful handover;

forwarding a handover request to the target base station, the handover request including the encrypted first random key corresponding the selected target base station;

sending a handover command to the user equipment, the handover command identifies the selected target base station;

receiving a handover complete signal from the target base station; and

handing over support of the user equipment to the target base station in response to receiving the handover complete signal.

10. A method for wireless communication, the method comprising:

receiving a first random key (MME-eNB_key[eNB_ID]) from a core component (MME) of a network, the network including a plurality of base stations one of which is a source base station supporting a user equipment (UE) and another of which is a target base station for supporting the user equipment after handover;

receiving a handover request at the target base station, the handover request (HO request) including an encrypted key for the target base station;

decrypting the encrypted key using the first random key to recover the key for the target base station;

deriving additional encryption keys (RRC/UP) from the key for the target base station; and

communicating with the user equipment using the derived additional encryption keys.

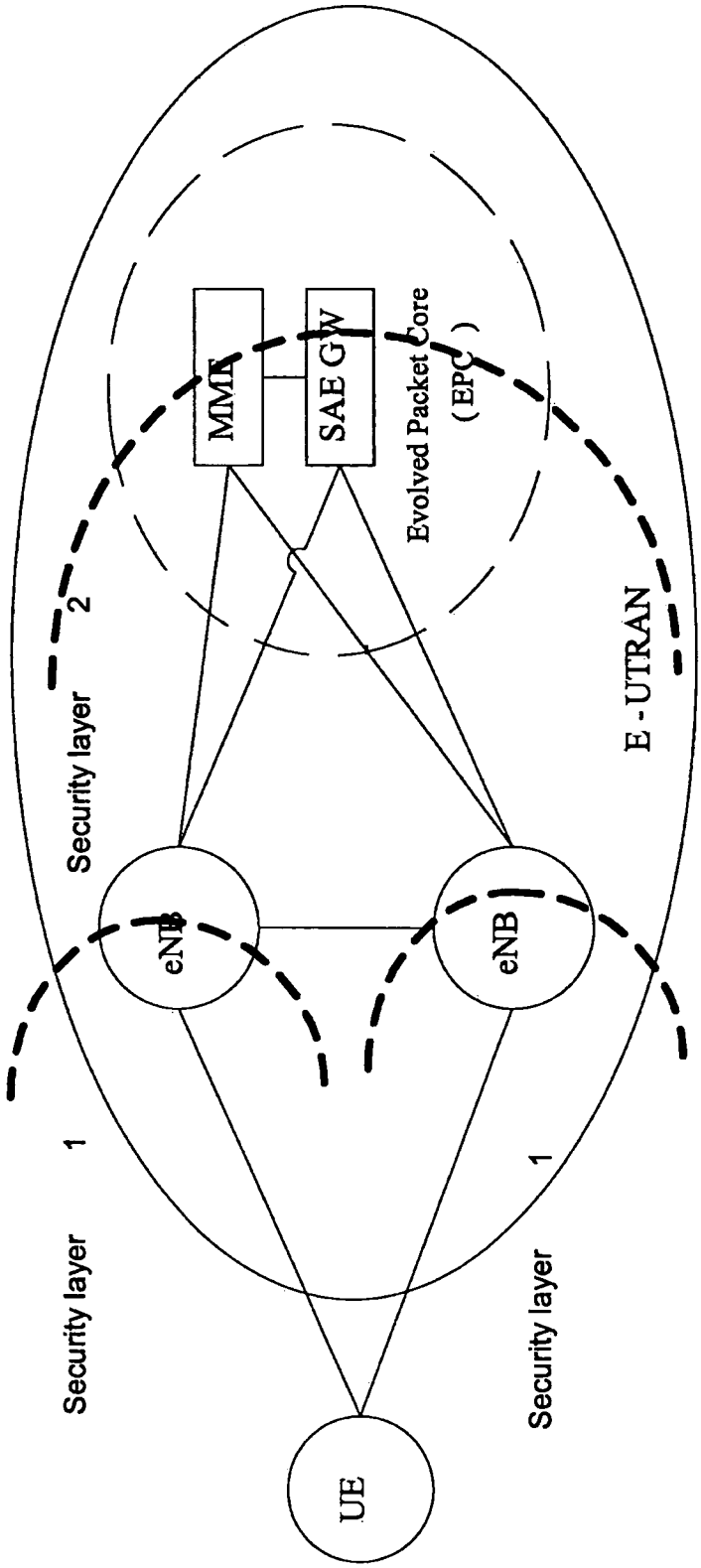
MME
SAE GW
Evolved Packet Core
(EPC)
E-UTRAN
Security layer 2
Security layer 1
Security layer 1
eNB
eNB
UE

FIG. 1

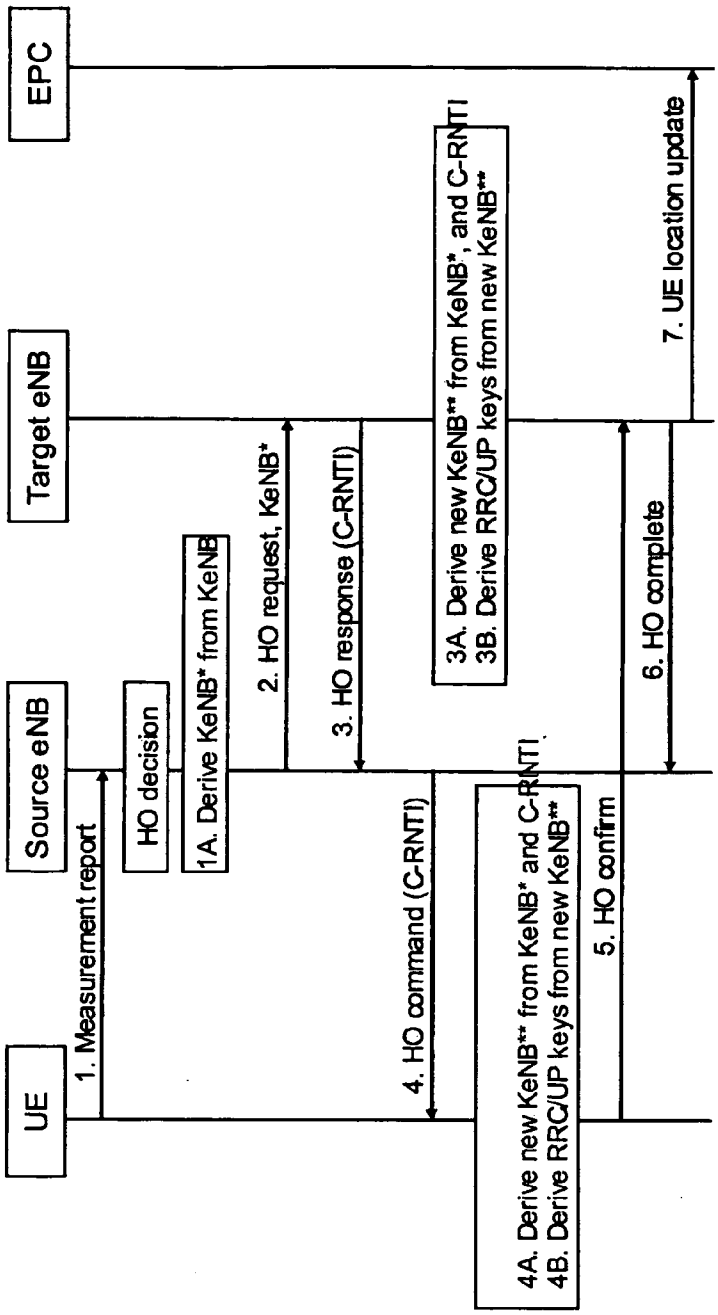
EPC
Target eNB
Source eNB
UE
1. Measurement report
HO decision
1A. Derive KeNB* from KeNB
2. HO request, KeNB*
3. HO response (C-RNTI)
3A. Derive new KeNB** from KeNB*, and C-RNTI
3B. Derive RRC/UP keys from new KeNB**
7. UE location update
6. HO complete
4. HO command (C-RNTI)
4A. Derive new KeNB** from KeNB* and C-RNTI
4B. Derive RRC/UP keys from new KeNB**
5. HO confirm

FIG. 2

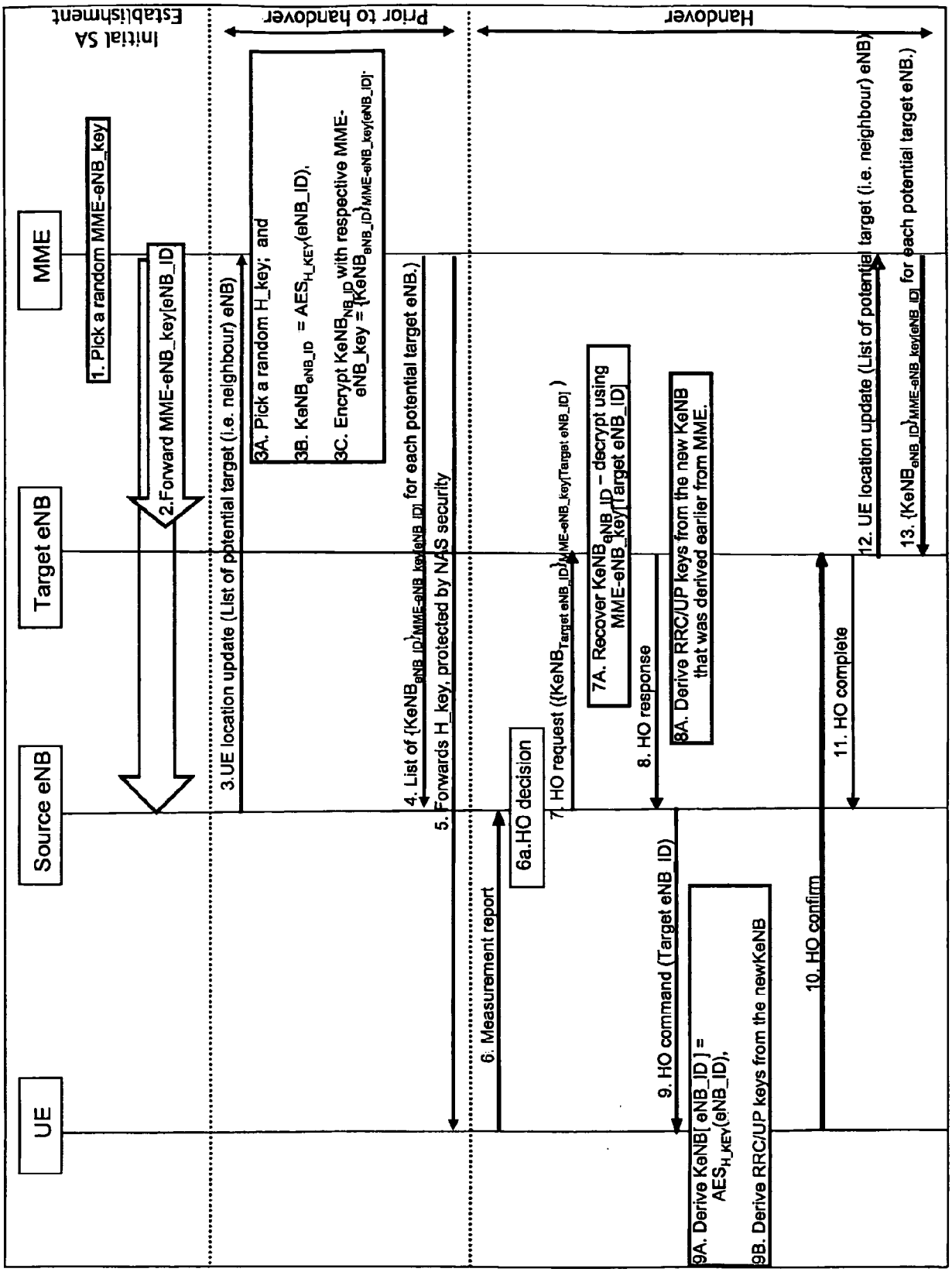
Initial SA Establishment
Prior to handover
Handover
UE
Source eNB
Target eNB
MME
1. Pick a random MME-eNB_key
2.Forward MME-eNB_key[eNB_ID]
3.UE location update (List of potential target (i.e. neighbour) eNB)
3A. Pick a random H_key; and
3B. KeNB_eNB_ID = AES_H_KEY(eNB_ID),
3C. Encrypt KeNB_NB_ID with respective MME-eNB_key = {KeNB_eNB_ID}MME-eNB_key[eNB_ID].
4. List of {KeNB_eNB_ID}MME-eNB key[eNB_ID] for each potential target eNB.)
5. Forwards H_key, protected by NAS security
6. Measurement report
6a.HO decision
7. HO request ({KeNB_Target eNB_ID}MME-eNB_key[Target eNB_ID])
7A. Recover KeNB_eNB_ID – decrypt using MME-eNB_key[Target eNB_ID]
8. HO response
8A. Derive RRC/UP keys from the new KeNB that was derived earlier from MME.
9. HO command (Target eNB_ID)
9A. Derive KeNB[eNB_ID] = AES_H_KEY(eNB_ID),
9B. Derive RRC/UP keys from the newKeNB
10. HO confirm
11. HO complete
12. UE location update (List of potential target (i.e. neighbour) eNB)
13. {KeNB_eNB_ID}MME-eNB_key[eNB_ID] for each potential target eNB.)

FIG. 3