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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 March 2017 (23.03.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/048434 A1

(51) International Patent Classification:
H04W 12/02 (2009.01) *H04W 12/04* (2009.01)

(21) International Application Number:
PCT/US2016/047101

(22) International Filing Date:
15 August 2016 (15.08.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/218,863 15 September 2015 (15.09.2015) US
15/089,396 1 April 2016 (01.04.2016) US

(71) Applicant: **QUALCOMM INCORPORATED** [US/US]; Attn: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121-1714 (US).

(72) Inventors: **LEE, Soo Bum**; 5775 Morehouse Drivel, San Diego, California 92121-1714 (US). **ESCOTT, Adrian Edward**; 5775 Morehouse Drive, San Diego, California 92121-1714 (US). **HORN, Gavin Bernard**; 5775 Morehouse Drive, San Diego, California 92121-1714 (US). **PALANIGOUNDER, Anand**; 5775 Morehouse Drive, San Diego, California 92121-1714 (US).

(74) Agent: **LOZA, Julio**; Loza & Loza, LLP, 305 North Second Avenue #127, Upland, California 91786 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, 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,

[Continued on next page]

(54) Title: APPARATUS AND METHOD FOR MOBILITY PROCEDURE INVOLVING MOBILITY MANAGEMENT ENTITY RELOCATION

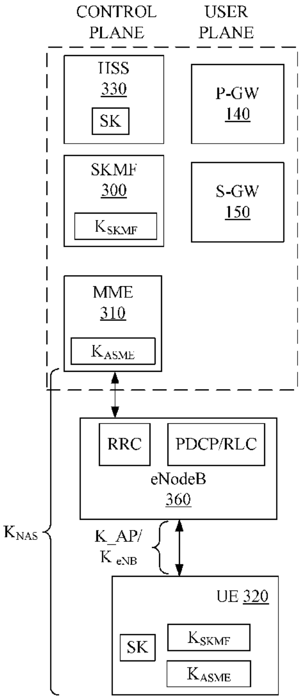

FIG. 3

(57) Abstract: A device that identifies entry into a new service area, transmits a service area update request to a network device associated with a network, receives a control plane message from the network indicating control plane device relocation or a key refresh due to a service area change in response to transmitting the service area update request, and derives a first key based in part on data included in the control plane message and a second key shared between the device and a key management device. Another device that receives a handover command from a network device associated with a network, the handover command indicating a new service area, derives a first key based on data included in the handover command and on a second key shared between the device and a key management device, and sends a handover confirmation message that is secured based on the first key.

WO 2017/048434 A1

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))*

APPARATUS AND METHOD FOR MOBILITY PROCEDURE INVOLVING MOBILITY MANAGEMENT ENTITY RELOCATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to and the benefit of Provisional Application No. 62/218,863 filed in the U.S. Patent and Trademark Office on September 15, 2015, and Non-Provisional Application No. 15/089,396 filed in the U.S. Patent and Trademark Office on April 1, 2016, the entire contents of which are incorporated herein by reference.

BACKGROUND

Field

[0002] The present disclosure relates generally to apparatuses and methods for improved mobility procedures involving mobility management entity (MME) relocation.

Background

[0003] A current cellular network architecture, shown in FIG. 1, uses a mobility management entity (MME) 110 to implement procedures for controlling access to the cellular network by a user equipment (UE) 120. Typically, the MME is owned and operated by a network service provider (system operator) as a core network element, and is located in a secure location controlled by the network service provider. The core network 100 has a control plane including a Home Subscriber Server (HSS) 130 and the MME, and a user plane including a Packet Data Network (PDN) Gateway (PGW) 140 and a Serving Gateway (SGW) 150. The MME is connected to an evolved Node B (eNodeB) 160. The eNodeB provides radio interfaces, RRC 180 and PDCP/RLC 190, with the UE.

[0004] In future cellular network architectures it is envisioned that the MMEs 110 or network components that perform many of the functions of the MMEs 110 will be pushed out towards the network edge where they are less secure either because they are physically more accessible and/or are not isolated from other network operators. As network functions are moved to, for example, the cloud (e.g., internet), it may not be assumed that they are secure because they may have a lower level of physical isolation, or no physical isolation. Further, network equipment may not be owned by a single network service provider. As an example, multiple MME instances may be hosted with a single physical hardware device. As a result, the keys sent to the MMEs may need refreshing more frequently and hence it may not be advisable to forward the authentication vectors (AVs) to the MMEs.

[0005] There is a need for improved apparatuses and methods that provide additional security for the cellular network architectures of the future where MME functions are performed close to the network edge.

SUMMARY

[0006] One feature provides a device (e.g., user device) that comprises a wireless communication interface adapted to transmit and receive data wirelessly to and from a network, and a processing circuit communicatively coupled to the wireless communication interface. The processing circuit may be adapted to identify entry into a new service area, transmit a service area update request to a network device associated with the network, receive a control plane message from the network indicating control plane device relocation or a key refresh due to a service area change in response to transmitting the service area update request, and derive a first key based in part on data included in the control plane message received and a second key shared between the device and a key management device, the key management device associated with the network. According to one aspect, the control plane message is received from a target control plane device due to the service area change, the target control plane device being a different control plane device from one currently serving the device. According to another aspect, the data included in the control plane message includes a control plane device identifier that identifies a control plane device that is and/or will be serving the device.

[0007] According to one aspect, deriving the first key is further based in part on a counter value Key Count maintained at the key management device and included in the control plane message. According to another aspect, the processing circuit is further adapted to derive at least one of an evolved node B (eNB) key K_{eNB}, a non-access stratum key K_{NAS}, and/or a next hop (NH) key based on the first key to secure communications between the device and the network. According to yet another aspect, the new service area is at least one of a new tracking area and/or a new routing area, and the service area update request is associated with at least one of a tracking area update and/or a routing area update.

[0008] According to one aspect, the control plane message is a security mode command, the target control plane device is a target mobility management entity (MME), the key management device is a session key management function (SKMF) device, and the second key is a session root key for an authentication session. According to another aspect, a control plane device maintains a mobility management context and a session management context for the device, and the key management device maintains the second key.

[0009] Another feature provides a device comprising a wireless communication interface adapted to transmit and receive data wirelessly to a network, and a processing circuit communicatively coupled to the wireless communication interface. The processing circuit is adapted to receive a handover command from a network device associated with the network, the handover command indicating a new service area, derive a first key based on data included in the handover command and on a second key shared between the device and a key management device, the key management device associated with the network, and send a handover confirmation message that is secured based on the first key. According to one aspect, the handover command includes a target control plane device identifier associated with a target control plane device serving a target radio access node that is and/or will be serving the device. According to another aspect, deriving the first key is based in part on the target control plane device identifier.

[0010] According to one aspect, the target control plane device is a target mobility management entity (MME), the key management device is a session key management function (SKMF) device, and the target control plane device identifier is an MME identifier associated with the target MME. According to another aspect, deriving the first key is further based in part on a counter value Key Count maintained at the key management device. According to yet another aspect, the second key is a session root key for an authentication session.

[0011] Another feature provides a network device associated with a network, the network device comprising a communication interface adapted to transmit and receive information, and a processing circuit communicatively coupled to the communication interface. The processing circuit is adapted to receive a service area update request from a device for which the network device does not have a device context or the device has changed service areas, transmit a request for a first key to a key management device, receive the first key from the key management device, the first key based in part on a second key shared between the key management device and the device, and transmit a control plane message to the device that includes data allowing the device to derive the first key. According to one aspect, the network device is a mobility management entity (MME) and the first key is further based on an MME identifier that identifies the MME. According to another aspect, the processing circuit is further adapted to transmit a device context request to a prior control plane device that previously served the device if the network device does not have the device context, and receive the device context from the prior control plane device in response to transmitting the device context request.

[0012] According to one aspect, the data includes a control plane device identifier that identifies the network device. According to another aspect, the processing circuit is further adapted to receive a counter value Key Count from the key management device along with the first key, and include the counter value Key Count in the data transmitted to the device. According to yet another aspect, the processing circuit is further adapted to transmit a service area update to the device after receiving notification from the device that the control plane message was successfully received.

[0013] According to one aspect, the service area update request is associated with at least one of a tracking area update and/or a routing area update and changing service areas includes at least one of changing tracking areas and/or changing routing areas. According to another aspect, the control plane message is a non-access stratum security mode command, the key management device is a session key management function (SKMF) device, the device is a user equipment, the device context is a user equipment context associated with the user equipment, and the second key is a session root key for an authentication session.

[0014] Another feature provides a network device associated with a network, the network device comprising a communication interface adapted to transmit and receive information, and a processing circuit communicatively coupled to the communication interface. The processing circuit adapted to receive a forward relocation request at the network device from a source control plane device, transmit a request for a first key to a key management device, receive the first key from the key management device, the first key based in part on a second key shared between the key management device and a device, and transmit a handover request to a target radio access node (RAN) with a RAN session key derived from the first key. According to one aspect, the processing circuit is further adapted to receive a handover request acknowledgement message from the target RAN indicating the target RAN will serve the device. According to another aspect, the processing circuit is further adapted to transmit an acknowledgement message to the key management device indicating receipt of the first key only after receiving the handover request acknowledgement message from the target RAN.

[0015] According to one aspect, the processing circuit is further adapted to transmit a forward relocation response to the source control plane device that includes data utilized by the device to derive the first key. According to another aspect, the network device is a target control plane device that will serve the device and the data includes a target control plane device identifier that identifies the target control plane device. According to yet another aspect, the target control plane device is a target mobility management entity (MME), the source control plane device is a source MME, the target control plane device identifier is a globally unique MME identifier (GUMMEI), the key management device is a session key management function (SKMF) device, and the device is a user equipment.

[0016] According to one aspect, the data includes a counter value Key Count maintained at the key management device. According to another aspect, the processing circuit adapted to receive the first key from the key management device is further adapted to receive a counter value Key Count along with the first key.

[0017] Another feature provides a method operational at a device for performing tracking area updates involving mobility management entity (MME) relocation or a change of tracking area, the method comprising identifying entry into a new tracking area, transmitting a tracking area update (TAU) request to a network device associated with a wireless communication network, receiving a security mode command from the network device indicating MME relocation or a key refresh due to a change of tracking area in response to transmitting the TAU request, and deriving a first key K_{ASME} based in part on data included in the security mode command received. According to one aspect, the security mode command is sent by an MME to refresh the first key K_{ASME}. According to another aspect, the security mode command is sent by a target MME due to tracking area change.

[0018] According to one aspect, the data included in the security mode command includes an MME identifier. According to another aspect, the MME identifier is a globally unique MME identifier (GUMMEI). According to yet another aspect, deriving the first key K_{ASME} is based in part on the GUMMEI.

[0019] According to one aspect, deriving the first key K_{ASME} is further based in part on a second key K_{SKMF} shared between the device and a session key management function (SKMF) device. According to another aspect, deriving the first key K_{ASME} is further based in part on a counter value Key Count maintained at the SKMF device. According to yet another aspect, the data included in the security mode command further includes the counter value Key Count.

[0020] According to one aspect, the method further comprises receiving a tracking area update message from the network device. According to another aspect, the method further comprises decrypting the tracking area update message using one or more keys derived from the first key K_{ASME}. According to yet another aspect, the tracking area update message includes a new globally unique temporary identifier (GUTI).

[0021] Another feature provides a device comprising a wireless communication interface adapted to transmit and receive data wirelessly with a network device associated with a wireless communication network, and a processing circuit communicatively coupled to the wireless communication interface, the processing circuit adapted to identify entry into a new tracking area, transmit a tracking area update (TAU) request to the network device associated with the wireless communication network, receive a security mode command from the network device indicating mobility management entity (MME) relocation or a key refresh due to a change of tracking area in response to transmitting the TAU request, and derive a first key K_{ASME} based in part on data included in the security mode command received.

[0022] Another feature provides a device comprising means for identifying entry into a new tracking area, means for transmitting a tracking area update (TAU) request to a network device associated with a wireless communication network, means for receiving a security mode command from the network device indicating mobility management entity (MME) relocation or a key refresh due to a change of tracking area in response to transmitting the TAU request, and means for deriving a first key K_{ASME} based in part on data included in the security mode command received.

[0023] Another feature provides a non-transitory computer-readable storage medium having instructions for performing tracking area updates involving mobility management entity (MME) relocation or a change of tracking area stored thereon, the instructions when executed by at least one processor causes the processor to identify entry into a new tracking area, transmit a tracking area update (TAU) request to a network device associated with a wireless communication network, receive a security mode command from the network device indicating MME relocation or a key refresh due to a change of tracking area in response to transmitting the TAU request, and derive a first key K_{ASME} based in part on data included in the security mode command received.

[0024] Another feature provides a method operational at a device for performing handover involving mobility management entity (MME) relocation or a change of tracking area, the method comprising receiving a handover command from a network device indicating a new tracking area, deriving a first key K_{ASME} based on data included in the handover command, and sending a handover confirmation message secured based on the first key K_{ASME}. According to one aspect, the method further comprises verifying the handover command before deriving the first key K_{ASME}. According to another aspect, the handover command includes a target MME identifier associated with a target MME serving the network device.

[0025] According to one aspect, deriving the first key K_{ASME} is based in part on the target MME identifier. According to another aspect, the target MME identifier is a globally unique MME identifier (GUMMEI) associated with the target MME serving the network device. According to yet another aspect, deriving the first key K_{ASME} is further based in part on a second key K_{SKMF} shared between the device and a session key management function (SKMF) device serving the target MME.

[0026] According to one aspect, deriving the first key K_{ASME} is further based in part on a counter value Key Count maintained at the SKMF device. According to another aspect, the data included in the handover command further includes the counter value Key Count.

[0027] Another feature provides a device comprising a wireless communication interface adapted to transmit and receive data wirelessly with a network device associated with a wireless communication network, and a processing circuit communicatively coupled to the wireless communication interface, the processing circuit adapted to receive a handover command from the network device indicating a new tracking area, derive a first key K_{ASME} based on data included in the handover command, and send a handover confirmation message secured based on the first key K_{ASME}.

[0028] Another feature provides a device comprising means for receiving a handover command from a network device indicating a new tracking area, means for deriving a first key K_{ASME} based on data included in the handover command, and means for sending a handover confirmation message secured based on the first key K_{ASME}.

[0029] Another feature provides a non-transitory computer-readable storage medium having instructions for performing handover involving mobility management entity (MME) relocation or a change of tracking area stored thereon, the instruction when executed by at least one processor causes the processor to receive a handover command from a network device indicating a new tracking area, derive a first key K_{ASME} based on data included in the handover command, and send a handover confirmation message secured based on the first key K_{ASME}.

[0030] Another feature provides a method for performing a tracking area update involving mobility management entity (MME) relocation or a change of tracking area at the MME, the method comprising receiving a tracking area update (TAU) request from a user equipment (UE) for which the MME does not have a UE context associated with the UE or for which the UE has changed tracking areas, transmitting a request for a first key K_{ASME} to a session key management function (SKMF) device, receiving the first key K_{ASME} from the SKMF device, and transmitting a non-access stratum (NAS) security mode command (SMC) to the UE that includes data allowing the UE to derive the first key K_{ASME}. According to one aspect, the method further comprises transmitting a UE context request to a source MME that previously served the UE if the MME does not have the UE context. According to another aspect, the method further comprises receiving the UE context from the source MME in response to transmitting the UE context request. According to yet another aspect, the method further comprises transmitting a key acknowledgment to the SKMF device after receiving the first key K_{ASME}.

[0031] According to one aspect, the data includes an MME identifier that identifies the MME. According to another aspect, the MME identifier is a globally unique MME identifier (GUMMEI). According to yet another aspect, the data includes a counter value Key Count maintained at the SKMF device.

[0032] According to one aspect, receiving the first key K_{ASME} from the SKMF device further includes receiving a counter value Key Count from the SKMF device. According to another aspect, the method further comprises transmitting a tracking area update to the UE after receiving notification from the UE that NAS SMC is successfully completed. According to yet another aspect, the method further comprises transmitting an encrypted tracking area update to the UE concurrently with the NAS SMC. According to another aspect, transmitting the request for the first key K_{ASME} includes transmitting a UE location update.

[0033] Another feature provides a network device associated with a wireless communication network, the network device comprising a communication interface adapted to transmit and receive information, and a processing circuit communicatively coupled to the communication interface, the processing circuit adapted to receive a tracking area update (TAU) request from a user equipment (UE) for which the network device does not have a UE context associated with the UE or for which the UE has changed tracking areas, transmit a request for a first key K_{ASME} to a session key management function (SKMF) device, receive the first key K_{ASME} from the SKMF device, and transmit a non-access stratum (NAS) security mode command (SMC) to the UE that includes data allowing the UE to derive the first key K_{ASME}.

[0034] Another feature provides a network device associated with a wireless communication network, the network device comprising means for receiving a tracking area update (TAU) request from a user equipment (UE) for which the network device does not have a UE context associated with the UE or for which the UE has changed tracking areas, means for transmitting a request for a first key K_{ASME} to a session key management function (SKMF) device, means for receiving the first key K_{ASME} from the SKMF device, and means for transmitting a non-access stratum (NAS) security mode command (SMC) to the UE that includes data allowing the UE to derive the first key K_{ASME}.

[0035] Another feature provides a non-transitory computer-readable storage medium having instructions for performing a tracking area update involving mobility management entity (MME) relocation or a change of tracking area at the MME stored thereon, the instructions when executed by at least one processor causes the processor to receive a tracking area update (TAU) request from a user equipment (UE) for which the MME does not have a UE context associated with the UE or for which the UE has changed tracking areas, transmit a request for a first key K_{ASME} to a session key management function (SKMF) device, receive the first key K_{ASME} from the SKMF device, and transmit a non-access stratum (NAS) security mode command (SMC) to the UE that includes data allowing the UE to derive the first key K_{ASME}.

[0036] Another feature provides a method for performing handover involving mobility management entity (MME) relocation or a change of tracking area at the MME, the method comprising receiving a forward relocation request at a target MME from a source MME, transmitting a request for a first key K_{ASME} to a session key management function (SKMF) device, receiving the first key K_{ASME} from the SKMF device, and transmitting a handover request to a target radio access node (RAN) with a key K_{eNB} derived from the first key K_{ASME}. According to one aspect, the method further comprises receiving a handover request acknowledgement message from the target RAN indicating the target RAN will serve a user equipment (UE). According to another aspect, the method further comprises transmitting an acknowledgement message to the SKMF indicating receipt of the first key K_{ASME} only after receiving the handover request acknowledgement message from the target RAN.

[0037] According to one aspect, the method further comprises transmitting a forward relocation response to the source MME that includes data utilized by a UE to derive the first key K_{ASME}. According to another aspect, the data includes an MME identifier that identifies the target MME. According to yet another aspect, the MME identifier is a globally unique MME identifier (GUMMEI).

[0038] According to one aspect, the data includes a counter value Key Count maintained at the SKMF device. According to another aspect, receiving the first key K_{ASME} from the SKMF device further includes receiving a counter value Key Count from the SKMF device.

[0039] Another feature provides a network device comprising a communication interface adapted to transmit and receive information, and a processing circuit communicatively coupled to the communication interface, the processing circuit adapted to receive a forward relocation request at the network device from a source mobility management entity (MME), transmit a request for a first key K_{ASME} to a session key management function (SKMF) device, receive the first key K_{ASME} from the SKMF device, and transmit a handover request to a target radio access node (RAN) with a key K_{eNB} derived from the first key K_{ASME}.

[0040] Another feature provides a network device associated with a wireless communication network, the network device comprising means for receiving a forward relocation request at the network device from a source mobility management entity (MME), means for transmitting a requesting for a first key K_{ASME} to a session key management function (SKMF) device, means for receiving the first key K_{ASME} from the SKMF device, and means for transmitting a handover request to a target radio access node (RAN) with a key K_{eNB} derived from the first key K_{ASME}.

[0041] Another feature provides a non-transitory computer-readable storage medium having instructions for performing handover involving mobility management entity (MME) relocation or a change of tracking area at the MME stored thereon, the instructions when executed by at least one processor causes the processor to receive a forward relocation request at the network device from a source MME, transmit a requesting for a first key K_{ASME} to a session key management function (SKMF) device, receive the first key K-$_{ASME}$ from the SKMF device, and transmit a handover request to a target radio access node (RAN) with a key K_{eNB} derived from the first key K_{ASME}.

BRIEF DESCRIPTION OF THE DRAWINGS

[0042] FIG. 1 is a block diagram of an example of a wireless communication system found in the prior art.

[0043] FIG. 2 is flow chart of a method for deriving digital keys for a cellular network security.

[0044] FIG. 3 is a block diagram of a first embodiment of a wireless communication system having an improved network key hierarchy.

[0045] FIG. 4 is a block diagram of a second embodiment of a wireless communication system having an improved network key hierarchy.

[0046] FIG. 5 is a block diagram of a third embodiment of a wireless communication system having an improved network key hierarchy.

[0047] FIG. 6 is a schematic diagram of an improved key hierarchy for a cellular network.

[0048] FIG. 7 illustrates a flow diagram of an attach procedure and initial data transfer for a UE connecting to a wireless communication network (e.g., wireless cellular network).

[0049] FIG. 8 illustrates a flow diagram of an S1-handover procedure.

[0050] FIG. 9 illustrates a flow diagram of a tracking area update procedure after a UE moves to a new location requiring an MME relocation.

[0051] FIG. 10 illustrates a first exemplary schematic block diagram of a device such as a user device/equipment.

[0052] FIG. 11 illustrates a first exemplary method operational at a device for performing service area updates involving control plane device relocation or a change of service area.

[0053] FIG. 12 illustrates a second exemplary method operational at a device for performing handover involving control plane device relocation or a change of service area.

[0054] FIG. 13 illustrates a first exemplary schematic block diagram of a network device such as an MME.

[0055] FIG. 14 illustrates a first exemplary method operational at a network device for performing a service area update involving control plane device relocation or a change of service area at the control plane device.

[0056] FIG. 15 illustrates a second exemplary method operational at a network device for performing handover involving control plane device relocation or a change of service area at the control plane device.

[0057] FIG. 16 illustrates a second exemplary schematic block diagram of a device such as a user device/equipment.

[0058] FIG. 17 illustrates a third exemplary schematic block diagram of a device such as a user device/equipment.

[0059] FIG. 18 illustrates a second exemplary schematic block diagram of a network device such as an MME.

[0060] FIG. 19 illustrates a third exemplary schematic block diagram of a network device such as an MME.

DETAILED DESCRIPTION

[0061] The word “exemplary” is used herein to mean “serving as an example, instance, or illustration.” Any embodiment described herein as “exemplary” is not necessarily to be construed as preferred or advantageous over other embodiments.

[0062] With reference to FIGS. 2 and 3, an aspect of the present disclosure may reside in a method 200 for deriving digital keys for cellular network security. In the method, a user equipment (UE) 320 mutually authenticates with a session key management function device 300 (hereinafter “SKMF”). The user equipment derives a first session key (e.g,, K_{SKMF}) shared with the SKMF 300 using a secret key (SK) shared with a home subscriber server (HSS) 330. The user equipment then derives a second session key (e.g,, K_{ASME}) shared with a mobility management entity (MME) 310 using the first session key.

[0063] In more detailed aspects of the disclosure, the SKMF (authenticator) may be a trust anchor (or key anchor) located deep inside the telecommunications network that derives a key (e.g., K_{ASME}) for each MME. Thus, as MMEs and/or network devices that perform their functions are pushed to the network’s edge, the SKMF stays deep inside the network and is very secure. The first session key may be derived using a first key derivation function having the secret key and a serving network identity (SN_id) as inputs. The first key derivation function may be based on, e.g., HMAC-256. The mutual authentication may be performed using an extensible authentication protocol (EAP), or specific NAS signaling. The second session key may be derived during an authentication and key agreement (AKA) procedure (for the currently attached MME with the UE), or during a handover involving an MME relocation. The session may be defined for the currently attached MME by the AAA server. The MME relocation may be performed within a group of MMEs sharing an MME group identity (MMEGI).

Alternatively, the MME relocation may be performed with another MME having a different MMEGI.

[0064] In other more detailed aspects of the disclosure, the second session key may be derived using a second key derivation function having the first session key and a unique globally unique MME identifier (GUMMEI) as inputs. The GUMMEI may be based on a combination of an MMEGI and an MME code. The second key derivation function may be based on HMAC-256. Alternatively, the second session key may be derived using a second key derivation function having the first session key and an MMEGI as inputs.

[0065] Another aspect of the disclosure may reside in a method for deriving a key for a user equipment 320. In the method, a network entity receives a session key (e.g,, K_{ASME}), for the user equipment, from the SKMF 300. A communication channel for receiving the session key may be security protected. The network entity may be an eNB 360, MME, GW, etc. Alternatively, an aspect of the disclosure may reside in a method wherein the network entity may receive the session key, for the user equipment, from another network entity in a same group. In a more detailed aspect of the disclosure, a network entity may request a session key (e.g,, K_{ASME}) from the SKMF when a source MME requests a handover without transferring a session key.

[0066] Another aspect of the disclosure, the SKMF 300 may mutually authenticate with a user equipment 320. The SKMF 300 may derive a session key (e.g,, K_{ASME}) for use in communicating with a UE 320 connected to an MME 310. The SKMF 300 may send the session key, for the UE 320, to the MME 10. Mutually authenticating with the UE 320 may include the SKMF 300 forwarding a request to an HSS 330 for authentication information for the UE 320. The authentication information may include authentication vectors (AVs) for the UE 320. Mutually authenticating with the UE 320 may further include the SKMF 300 receiving an authentication response from the UE 320. An authentication vector may include an expected response (XRES), an authentication value (AUTN), a random number (RAND), and the first session key (e.g., K_{SKMF}). The AUTN may be based on a sequence number and a secret key (SK) which the UE 320 shares with the HSS 330.

[0067] The present disclosure allows network functions (e.g., the MME 310) to be moved to an edge of the network away from a network core. The SKMF 300 may be placed between the MME 310 and the HSS 330. The SKMF 300 may act a local key anchor.

Accordingly, the trust required by the MME 310 may be reduced. As a result, an MME 310 for a UE 320 would not be transferred during MME relocation.

[0068] The UE may perform Authentication Key Agreement (AKA) with the SKMF. The HHS may send an AV to the SKMF. The AV may include XRES, AUTN, RAND, and K_{SKMF}. K_{SKMF} may be derived from a shared secret key SK between the UE and the HSS. Thus, mutual authentication may be performed between the UE and the SKMF. This architecture may be used in a fifth generation (5G) cellular network.

[0069] If the AKA is successful, the SKMF sends an MME key (e.g., K_{ASME}) to the MME. The MME key (and other keys derived from it) may be derived according to the details provided further below.

[0070] In a roaming scenario (i.e., the UE is in a visited network), the SKMF in the visited network may become the local key anchor. Similarly, the AKA may be performed through the SKMF. As shown in FIGS. 4 and 5, an SKMF 300, which is in the visited network, and not in the home network 406, is the local key anchor. During an MME relocation (e.g., handover or tracking area update) within the local network, the SKMF derives a new K_{ASME} and provides it to the target/new MME. The radio access node (RAN) session key (e.g., K_{eNB}) may be derived from the new K_{ASME}.

[0071] FIG. 6 illustrates a schematic diagram of an improved key hierarchy for a cellular network. The UE's universal subscriber identity module (USIM) and the network's authentication center (AuC) store the shared secret key (SK). From the SK the integrity key (IK) and cipher key (CK) are derived and provided to the HSS. The HSS may in turn generate the first session key (K_{SKMF}) and provide it to the SKMF. The first session key K_{SKMF} is valid during the entire authentication session. The SKMF may utilize the K_{SKMF} to generate the second session key (K_{ASME}) and provide that key to the MME. The K_{ASME} may be valid for only a specific MME. The MME may in turn generate other keys (K_{NASenc}, K_{NASint}, K_{eNB}/NH, etc.) based on the K_{ASME}.

Exemplary Attach, Handover, and Tracking Area Update (TAU) Processes

[0072] Aspects of the disclosure are descried in some parts below with respect to 4G Long Term Evolution system components. This is merely exemplary. The disclosure is not limited by any one specific network system such as 4G LTE and instead may be applied to other types of communication systems including but not limited to 5G systems.

[0073] During an initial attach to a network, a UE performs an authentication and key agreement (AKA) procedure with a session key management function (SKMF) device. Once authentication is successful, SKMF derives a key (e.g., K_{ASME}) for the MME to which the UE is attached and provides the key to the MME.

[0074] When a tracking area update (TAU) involving MME relocation is requested by a UE, the new MME (e.g., target MME) that receives the TAU request receives a new key K_{ASME} from the SKMF and establishes a security association with the UE by performing a non-access stratum (NAS) security mode command (SMC) procedure. Similarly, when a handover involving MME relocation happens, the target MME also gets a new key K_{ASME} from the SKMF and establishes a security association with the UE.

[0075] An MME that supports two tracking areas may initiate a change of K_{ASME} when the UE moves between tracking areas. This hides the network configuration from UE. For example, the UEs only see tracking areas not MMEs. This may happen both in response to a TAU and a handover that changes tracking areas.

[0076] FIG. 7 illustrates a flow diagram of an attach procedure and initial data transfer for a UE connecting to a wireless communication network (e.g., wireless cellular network) according to one aspect of the disclosure. First, the UE transmits an attach request 702 to an eNB, which in turn transmits an initial UE message 704 to the MME. Next, the UE and the SKMF perform an authentication and key agreement (AKA) 706. To perform the AKA, the SKMF transmits an authentication information request 707 to the HSS and in response it receives an authentication vector 708 from the HSS that may include an expected response (XRES), an authentication value (AUTN), a random number (RAND), and an MME specific key K_{SKMF}. The AUTN may be based on a sequence number and a secret key (SK) which the UE shares with the HSS.

[0077] Once AKA is successful, the SKMF may derive a session key K_{ASME} (e.g., “first key”) based on K_{SKMF} (e.g., “second key”), an MME identifier (e.g., GUMMEI), and/or a counter value (e.g., Key Count). Thus, K_{ASME} may equal KDF(K_{SKMF}, GUMMEI | Key Count) where KDF is a key derivation function. The counter value Key Count is a counter value that may be incremented by the SKMF to enable the SKMF to derive a fresh K_{ASME} key for the same MME whenever handover back to the MME occurs. According to one aspect, a number used once (nonce) may be used instead of the counter value. According to another aspect, the GUMMEI may be omitted if it’s not used to authorize a particular MME identity. For example, if SKMF is always in the same network as the MMEs it provides K_{ASME} for, then including GUMMEI in the key derivation may be unnecessary. Thus, according to another example, K_{ASME} may equal KDF(K_{SKMF}, nonce). The MME specific key K_{ASME} is then sent to the MME 710. The MME may then use the key K_{ASME} to perform a non-access stratum (NAS) security mode command (SMC) procedure 712 with the UE. During the NAS SMC procedure 712, the MME may provide its GUMMEI and/or the Key Count to the UE so the UE can also derive K_{ASME}. The remaining 714 – 728 shown in FIG. 7 are similar to those found in 4G LTE cellular communication protocols.

[0078] FIG. 8 illustrates a flow diagram of an S1-handover procedure according to one aspect of the disclosure. First, the source eNB (i.e., the current eNB) transmits a handover (HO) required message 802 to the source MME (i.e., the current MME). Next, the source MME transmits/forwards a relocation request 804 to the target MME (i.e., the new MME). The target MME may create and transmit a session request 806 to a target serving gateway (S-GW) and receive a session response 808 from the target S-GW. The target MME may also transmit a key request 810 for an MME specific key K_{ASME} to the SKMF. In so doing, the target MME may provide the SKMF with its GUMMEI. The SKMF may in turn generate the K_{ASME} using the MME's GUMMEI, the K_{SKMF} key it previously received from the HSS (described above), and the Key Count. According to one aspect, a number used once (nonce) may be used instead of the Key Count. According to another aspect, the GUMMEI may be omitted if it is not desired to authorize a particular MME identity. The SKMF transmits the K_{ASME} 812 to the target MME. According to one aspect, the target MME may transmit the session request 806 to the target S-GW and transmit the key request 810 at about the same time. Thus, steps 806 and 810 may be carried out concurrently with steps 808 and 812.

[0079] The target MME may then transmit a handover request 814 to the target eNB (i.e., the potential new eNB) and in response the target eNB sends back a handover response 816. The handover request 814 may include the key K_{eNB} derived by the target MME using K_{ASME}. The handover response 816 indicates whether the target eNB agrees to accept the handover. If the target eNB does agree to accept the handover then the target MME sends a key (i.e., K_{ASME}) acknowledgement message 818 to the SKMF. Upon receiving the key acknowledgement message, the SKMF may then increment the Key Count counter value. The step of sending the key acknowledgement message 818 is delayed until the handover request acknowledgement 816 is received because the handover request may be rejected by the target eNB. In such case, a new K_{ASME} doesn't need to be derived by the UE, and SKMF may not need to increase the Key Count. After the target MME sends the source MME the relocation response 820, the source MME sends a handover command 822 to the source eNB which is forwarded 824 to the UE. The handover command 822, 824 may include the GUMMEI of the target MME and the Key Count so that the UE can derive the new K_{ASME} and the new K_{eNB} for the target eNB. The UE responds with a handover confirmation message 826 to the target eNB. The handover confirmation message 826 is integrity protected and ciphered.

[0080] FIG. 9 illustrates a flow diagram of a tracking area update procedure after a UE moves to a new location requiring an MME relocation according to one aspect of the disclosure. First, the UE generates and transmits a tracking area update request 902 to the eNB. The eNB in turn forwards the tracking area update request 904 to a target MME that will be associated with the UE. The eNB determines which new/target MME to send the tracking area update request to based on various criteria including the location of the UE. The tracking area update request may include a globally unique temporary identifier (GUTI) which in turn includes the GUMMEI of the source MME (i.e., MME currently associated with the UE). The target MME may then use the GUMMEI in the tracking area update request it receives to transmit a UE context request message 906 to the source MME. The source MME then responds with the UE context information in a UE context response message 908. An acknowledgment 910 may be sent from the target MME to the source MME once this response is received.

[0081] The target MME may then send a location update and a key request (i.e., K_{ASME} key request) to the SKMF 912. The location update is forwarded to the HSS which then sends a location cancelation message 914 to the old MME (old MME may transmit a location cancelation acknowledgement message 916 back to the HSS). The SKMF 912 may generate a new K_{ASME} for the target MME based on the GUMMEI of the target MME and/or the Key Count counter value as previously described. According to one aspect, a number used once (nonce) may be used instead of the Key Count. According to another aspect, the GUMMEI may be omitted if it is not desired to authorize a particular MME identity. The new K_{ASME} 918 is transmitted to the target MME along with a location update acknowledgment. Upon receiving K_{ASME} from the SKMF, the target MME may reply with a key acknowledgement message 920 to the SKMF. According to one aspect, the target MME may transmit the UE context request message

906 to the source MME at about the same time it transmits the location update and key request 912 to the SKMF. Thus, steps 906, 908, and 910 may be performed concurrently with steps 914, 916, 918, 920.

[0082] Once the target MME has received the K_{ASME} from the SKMF, the target MME may then perform a non-access stratum security mode command procedure 922, 924 with the UE. During the security mode command procedure the UE derives the key K_{ASME} used by the target MME since the target MME provides the UE with its GUMMEI. Once the UE also has the same K_{ASME} as the target MME, the UE and the target MME may engage in secure communications based on the K_{ASME} key. For example, the target MME may engage in a tracking area update exchange 926, 928 with the UE whose communications are encrypted by K_{ASME} or other keys (e.g., NAS encryption and integrity protection keys) derived from K_{ASME}. This exchange may include a message sent from the target MME to the UE that includes the new GUTI based on the target MME's GUMMEI. Such a message is again encrypted by K_{ASME} or another key derived from K_{ASME}.

[0083] As shown in FIG. 9 and described above, the NAS SMC 922, 924 is followed by the tracking area update process 926, 928. In some aspects of the disclosure, the NAS SMC 922, 924 and the tracking area update process 926, 928 may be combined. For example, the NAS SMC message 922 sent from the target MME to the UE may be combined with the tracking area update message 926. In so doing, only part of the combined message (e.g., the part associated with the tracking area update) may be encrypted, while the portion of the message that helps the UE derive K_{ASME} is left unencrypted. A new temporary mobile subscriber identity (TMSI), which is part of GUTI, allocated by the MME may be encrypted.

Key Derivation

[0084] As discussed above, AKA is run between the UE and the SKMF. The key K_{SKMF} is derived by the HSS and sent to the SKMF. From the HSS' perspective, authentication vectors are constructed in the same manner as 4G LTE and sent to the SKMF instead of the MME. Thus, HSS may be connected to SKMF without any modification.

[0085] SKMF derives an MME specific key K_{ASME} for a given MME and thus the MME's GUMMEI may be used in the K_{ASME} key derivation process. A NAS Count value may be initialized to zero (0) for a new K_{ASME}. In one example, the old NAS Count values are not discarded if tracking area update(s) doesn't complete. For the freshness of the key K_{ASME} the UE and the SKMF may maintain a Key Count counter value and use it for K_{ASME} derivation. This may be done to avoid deriving the same K_{ASME} in cases where the UE moves back to an old MME (e.g., source MME). The Key Count counter value may be initialized to zero (0) or some other pre-determined value when the initial AKA is performed successfully. In some aspect, a nonce may be used instead of the Key Count counter value. In another aspect, the GUMMEI may be omitted from the key derivation.

[0086] The key derivation function (KDF) used to generate the keys K_{SKMF}, K_{ASME}, K_{eNB}, next hop (NH), etc. may utilize HMAC-SHA-256, HMAC-SHA-3, etc. The input string S may be constructed from $n + 1$ input parameters. For example, S = [FC || P_0 || L_0 || P_1 || L_1 || P_2 || L_2 || ... || P_N || L_N]. The field code FC may be a single octet used to distinguish between different instances of the algorithm and may use a value in the range 0x50 – 0x5F. The input parameters P_0 through P_N are the $n + 1$ input parameter encodings. P_0 may be a static ASCII-encoded string. The values L_0 through L_N are two octet representations of the length of the corresponding input parameters P_0 through P_N.

[0087] K_{SKMF} Derivation.

[0088] K_{SKMF} = KDF($K_{CK/IK}$, S). The input S may be equal to [FC || P_0 || L_0 || P_1 || L_1] where FC = 0x50, P_0 = SN id, L_0 = length of SN id (i.e., L_0 = 0x00 0x03), P_1 = SQN XOR AK, and L_1 = length of P_1 (i.e., L_1 = 0x00 0x06). SQN is the sequence number and AK is anonymity key, and XOR is the exclusive OR operation. The value SQN XOR AK is sent to the UE as part of the authentication token (AUTN). If AK is not used then AK may be treated in accordance with TS 33.102 (i.e., 000...0). The input key $K_{CK/IK}$ is the concatenation of the cipher key (CK) and the integrity key (IK), i.e., $K_{CK/IK}$ = CK || IK.

[0089] K_{ASME} Derivation.

[0090] K_{ASME} = KDF(K_{SKMF}, S). The input S may be equal to [FC || P_0 || L_0 || P_1 || L_1] where FC = 0x51, P_0 = GUMMEI, L_0 = length of 48 bit GUMMEI (i.e., L_0 = 0x00 0x06), P_1 = Key Count, and L_1 may equal the length of P_1 (e.g., L_1 = 0x00 0x08). This is merely one example of how K_{ASME} may be derived. In another aspects, the GUMMEI may be omitted and rand number used once (e.g., nonce) may be used instead of the Key Count counter value.

[0091] NH Derivation.

[0092] NH = KDF(K_{ASME}, S). The input S may be equal to [FC || P_0 || L_0] where FC = 0x52, P_0 = Sync-Input, L_0 = length of Sync-Input (i.e., L_0 = 0x00 0x20). The Sync-Input parameter may be newly derived K_{eNB} for the initial NH derivation, and the previous NH for all subsequent derivations. This results in an NH chain, where the next NH is always fresh and derived from the previous NH.

[0093] K_{eNB} Derivation.

[0094] K'_{eNB} = KDF(K_X, S). When deriving K'_{eNB} from the current K_{eNB} or from a fresh NH and the target physical cell identifier in the UE and the eNB as specified in clause 7.2.8 for handover purposes, the input S may be equal to [FC || P_0 || L_0 || P_1 || L_1] where FC = 0x53, P_0 = target physical cell identifier (PCI), L_0 = length of PCI (e.g., L_0 = 0x00 0x02), P_1 = EARFCN-DL (target physical cell downlink frequency), and L_1 = length of P_1 (e.g., L_1 = 0x00 0x02). The input key K_X may be the 256 bit next hop (NH) key when the index in the handover increases otherwise the current 256 bit K_{eNB} is used.

[0095] FIGS. 7 – 9 shown and described above assume that the MMEs change from source to target MME. However, the same process flow diagrams may be used when a single MME assumes the role of two MMEs (source MME and target MME) and there is no actual interface between the two MMEs.

[0096] In the above description with regards to FIGS. 7 – 9 and key derivation, specific non-exclusive, non-limiting examples of network components and related terminology was used to demonstrate aspects of the disclosure of the present application. For example, the “user equipment” may be just one example of a device. The MMEs may be just one example of control plane devices. The SMKF may be just one example of a key management device. The MME identifier (e.g., GUMMEI) may be just one example of a control plane device identifier. The tracking area may be just one example of a service area, and similarly, the tracking area update may be just one example a service area update. The SMC and NAS SMC may be just some examples of control plane messages. The eNB may be just one example of a radio access node.

[0097] FIG. 10 illustrates a schematic block diagram of a device 1000 (e.g., “user device”, “user equipment”, “wireless device”, etc.) according to one aspect of the disclosure. The user device 1000 may be any wireless communication device such as, but not limited to, a mobile phone, a smartphone, a laptop, a personal digital assistant (PDA), a tablet, a computer, a smartwatch, and a head-mounted wearable computer (e.g., Google Glass®). The user device 1000 may include at least one or more wireless communication interfaces 1002, one or more memory circuits 1004, one or more input and/or output (I/O) devices/circuits 1006, and/or one or more processing circuits 1008 that may be communicatively coupled to one another. For example, the interface 1002, the memory circuit 1004, the I/O devices 1006, and the processing circuit 1008 may be communicatively coupled to each other through a bus 1010. The wireless communication interface 1002 allows the user device 1000 to communicate wirelessly with the wireless communication network 104. Thus, the interface 1002 allows the user device 1000 to communicate wirelessly with wireless wide area networks (WWAN), such as mobile telecommunication cellular networks, as well as short range, wireless local area networks (e.g., WiFi®, Zigbee®, Bluetooth®, etc.).

[0098] The memory circuit 1004 may include one or more volatile memory circuits and/or non-volatile memory circuits. Thus, the memory circuit 1004 may include dynamic random access memory (DRAM), static random access memory (SRAM), magnetoresistive random access memory (MRAM), electrically erasable programmable read-only memory (EEPROM), flash memory, etc. The memory circuit 1004 may store one or more cryptographic keys. The memory circuit 1004 may also store instructions that may be executed by the processing circuit 1008. The I/O devices/circuits 1006 may include one or more keyboards, mice, displays, touchscreen displays, printers, fingerprint scanners, and any other input and/or output devices.

[0099] The processing circuit 1008 (e.g., processor, central processing unit (CPU), application processing unit (APU), etc.) may execute instructions stored at the memory circuit 1006 and/or instructions stored at another computer-readable storage medium (e.g., hard disk drive, optical disk drive, solid-state drive, etc.) communicatively coupled to the user device 1000. The processing circuit 1008 may perform any one of the steps and/or processes of the user device 1000 described herein including those discussed with reference to FIGS. 2, 3, 4, 5, 6, 7, 8, 9, 11, and 12.

[00100] FIG. 11 illustrates a method 1100 operational at a device. The device may be an integrated circuit, a plurality of integrated circuits, or an electronic device that incorporates one or more integrated circuits. The method may be for performing service area updates involving control plane device relocation or a change of service area. First, entry into a new service area (e.g., new tracking area, new routing area, etc.) is identified 1102 at the device. Next, a service area update request is transmitted 1104 to a network device associated with a network. Then, a control plane message (one non-limiting, non-exclusive example includes a security mode command) is received 1106 from the network indicating control plane device relocation or a key refresh due to a service area change in response to transmitting the service area update request. Next, a first key (e.g., K_{ASME}) is derived 1108 based in part on data included in the control plane message received and a second key (e.g., K_{SKMF}) shared between the device and a key management device (e.g., SKMF), where the key management device is associated with the network. According to one aspect, the control plane message is received from a target control plane device (e.g., target MME) due to the service area change, the target control plane device being a different control plane device (e.g., source MME) from one currently serving the device. According to another aspect, the data included in the control plane message includes a control plane device identifier (e.g., MME identifier such as but not limited to GUMMEI) that identifies a control plane device that is and/or will be serving the device.

[00101] According to one aspect, deriving the first key is further based in part on a counter value Key Count maintained at the key management device and is included in the control plane message. According to another aspect, at least one of an evolved node B (eNB) key K_{eNB}, a non-access stratum key K_{NAS}, and/or a next hop (NH) key is derived based on the first key to secure communications between the device and the network. According to yet another aspect, the new service area is at least one of a new tracking area and/or a new routing area, and the service area update request is associated with at least one of a tracking area update and/or a routing area update.

[00102] According to one aspect, the control plane message is a security mode command, the target control plane device is a target MME, the key management device is an SKMF device, and the second key is a session root key for an authentication session. According to another aspect, a control plane device maintains a mobility management context and a session management context for the device, and the key management device maintains the second key.

[00103] FIG. 12 illustrates a method 1200 operational at a device for performing handover involving control plane device relocation or a change of service area. First, a handover command is received 1202 from a network device (e.g., source eNB) associated with the network, where the handover command indicates a new service area (e.g., new tracking area, new routing area, etc.). Next, a first key (e.g., K_{ASME}) is derived 1204 based on data included in the handover command and on a second key (e.g., K_{SKMF}) shared between the device and a key management device (e.g., SKMF), where the key management device is associated with the network. Then, a handover confirmation message that is secured based on the first key is sent 1206 to the network device.

[0100] According to one aspect, the handover command includes a target control plane device identifier (e.g., target MME identifier that may include GUMMEI) associated with a target control plane device (e.g., target MME) serving a target radio access node (e.g., target eNB) that is and/or will be serving the device. According to another aspect, deriving the first key is based in part on the target control plane device identifier. According to yet another aspect, the target control plane device is a target mobility management entity (MME), the key management device is a session key management function (SKMF) device, and the target control plane device identifier is an MME identifier associated with the target MME.

[0101] FIG. 13 illustrates a schematic block diagram of a network device 1300 according to one aspect of the disclosure. The network device 1300 may be an MME, a RAN, S-GW, and/or P-GW. The network device 1300 may include at least one or more wireless communication interfaces 1302, one or more memory circuits 1304, one or more input and/or output (I/O) devices/circuits 1306, and/or one or more processing circuits 1308 that may be communicatively coupled to one another. For example, the interface 1302, the memory circuit 1304, the I/O devices 1306, and the processing circuit 1308 may be communicatively coupled to each other through a bus 1310. The wireless communication interface 1302 allows the network device 1300 to communicate wirelessly with the user device 102. Thus, the interface 1302 allows the network device 1300 to communicate wirelessly through wireless wide area networks (WWAN), such as mobile telecommunication cellular networks, and/or short range, wireless local area networks (e.g., WiFi®, Zigbee®, Bluetooth®, etc.).

[0102] The memory circuit 1304 may include one or more volatile memory circuits and/or non-volatile memory circuits. Thus, the memory circuit 1304 may include DRAM, SRAM, MRAM, EEPROM, flash memory, etc. The memory circuit 1304 may store one or more cryptographic keys. The memory circuit 1304 may also store instructions that may be executed by the processing circuit 1308. The I/O devices/circuits 1306 may include one or more keyboards, mice, displays, touchscreen displays, printers, fingerprint scanners, and any other input and/or output devices.

[0103] The processing circuit 1308 (e.g., processor, central processing unit (CPU), application processing unit (APU), etc.) may execute instructions stored at the memory circuit 1306 and/or instructions stored at another computer-readable storage medium (e.g., hard disk drive, optical disk drive, solid-state drive, etc.) communicatively coupled to the network device 1300. The processing circuit 1308 may perform any one of the steps and/or processes of a network devices described herein including those discussed with reference to FIGS. 2, 3, 4, 5, 6, 7, 8, 9, 14, and 15.

[0104] FIG. 14 illustrates a method 1400 operational at a network device for performing a tracking area update involving control plane device relocation or a change of service area at the control plane device. First, a service area update request is received 1402 from a device (e.g., user equipment) for which the network device does not have a device context (e.g., UE context) or the device has changed service areas (e.g., tracking areas or routing areas). Next, a request for a first key (e.g., K_{ASME}) is transmitted 1404 to a key management device (e.g., SKMF). Then, the first key is received 1406 from the key management device, where the first key based in part on a second key (e.g., K_{SKMF}) shared between the key management device and the device. Next, a control plane message is transmitted 1408 to the device that includes data allowing the device to derive the first key. According to one aspect, the network device is a mobility management entity (MME) and the first key is further based on an MME identifier that identifies the MME. According to another aspect, a device context request is transmitted to a prior control plane device that previously served the device if the network device does not have the device context.

[0105] According to one aspect, the device context is received from the prior control plane device in response to transmitting the device context request. According to another aspect, the data includes a control plane device identifier that identifies the network device. According to yet another aspect, a counter value Key Count is received from the key management device along with the first key.

[0106] According to one aspect, the counter value Key Count is included in the data transmitted to the device. According to another aspect, a service area update is transmitted to the device after receiving notification from the device that the control plane message was successfully received. According to yet another aspect, the service area update request is associated with at least one of a tracking area update and/or a routing area update and changing service areas includes at least one of changing tracking areas and/or changing routing areas. According to another aspect, the control plane message is a non-access stratum security mode command, the key management device is a session key management function (SKMF) device, the device is a user equipment, the device context is a user equipment context associated with the user equipment, and the second key is a session root key for an authentication session.

[0107] FIG. 15 illustrates a method 1500 operational at a network device for performing handover involving a control plane device relocation or a change of service area at the control plane device. First, a forward relocation request is received 1502 at the network device from a source control plane device. Next, a request for a first key is transmitted 1504 to a key management (SKMF) device. Then, the first key is received 1506 from the key management device, where the first key is based in part on a second key shared between the key management device and a device. Next, a handover request is transmitted to a target radio access node (RAN) with a RAN session key derived from the first key. According to one aspect, a handover request acknowledgement message is received from the target RAN indicating the target RAN will serve the device. According to another aspect, an acknowledgement message is transmitted to the key management device indicating receipt of the first key only after receiving the handover request acknowledgement message from the target RAN.

[0108] According to one aspect, a forward relocation response is transmitted to the source control plane device that includes data utilized by the device to derive the first key. According to another aspect, the network device is a target control plane device that will serve the device and the data includes a target control plane device identifier that identifies the target control plane device. According to yet another aspect, the target control plane device is a target mobility management entity (MME), the source control plane device is a source MME, the target control plane device identifier is a globally unique MME identifier (GUMMEI), the key management device is a session key management function (SKMF) device, and the device is a user equipment. According to yet another aspect, a counter value Key Count is received along with the first key.

[0109] FIG. 16 illustrates a block diagram of a device 1600 (e.g., user device/equipment) according to one aspect of the disclosure. The device 1600 may include a service area identification circuit 1602, a service area update request transmission circuit 1604, a control plane message receiving circuit 1606, and/or a first key derivation circuit 1608, which may all be communicatively coupled via a communication bus 1610. Each of the circuits 1602, 1604, 1606, 1608 of the device 1600 may be specialized circuits (e.g., application specific integrated circuits (ASICs), field programmable gate arrays (FPGAs), etc.) that are specifically wired to perform their respective specific functions.

[0110] The service area identification circuit 1602 may be one example of a means for identifying entry into a new service area. The service area update request transmission circuit 1604 may be one example of a means for transmitting a service area update request to a network device associated with the network. The control plane message receiving circuit 1606 may be one example of a means for receiving a control plane message from the network indicating control plane device relocation or a key refresh due to a service area change in response to transmitting the service area update request. The first key derivation circuit 1608 may be one example of a means for deriving a first key based in part on data included in the control plane message received and a second key shared between the device and a key management device.

[0111] FIG. 17 illustrates a block diagram of a device 1700 (e.g., user device/equipment) according to one aspect of the disclosure. The device 1700 may include a handover command receiving circuit 1702, a first key derivation circuit 1704, and/or a handover confirmation transmission circuit 1706, which may all be communicatively coupled via a communication bus 1708. Each of the circuits 1702, 1704, 1706 of the device 1700 may be specialized circuits (e.g., ASICs, FPGAs, etc.) that are specifically wired to perform their respective specific functions.

[0112] The handover command receiving circuit 1702 may be one example of a means for receiving a handover command from a network device associated with the network, the handover command indicating a new service area. The first key derivation circuit 1704 may be one example of a means for deriving a first key based on data included in the handover command and on a second key shared between the device and a key management device. The handover confirmation transmission circuit 1706 may be one example of a means for sending a handover confirmation message that is secured based on the first key.

[0113] FIG. 18 illustrates a block diagram of a network device 1800 (e.g., MME) according to one aspect of the disclosure. The device 1800 may include a first key request transmission circuit 1802, a service area update request receiving circuit 1804, a first key receiving circuit 1806, and/or control plane message transmission circuit 1808, which may all be communicatively coupled via a communication bus 1810. Each of the circuits 1802, 1804, 1806, 1808 of the network device 1800 may be specialized circuits (e.g., ASICs, FPGAs, etc.) that are specifically wired to perform their respective specific functions.

[0114] The first key request transmission circuit 1802 may be one example of a means for transmitting a request for a first key to a key management device. The service area update request receiving circuit 1804 may be one example of a means for receiving a service area update request from a device for which the network device does not have a device context or the device has changed service areas. The first key receiving circuit 1806 may be one example of a means for receiving the first key from the key management device, the first key based in part on a second key shared between the key management device and the device. The control plane message transmission circuit 1808 may be one example of a means for transmitting a control plane message to the device that includes data allowing the device to derive the first key.

[0115] FIG. 19 illustrates a block diagram of a network device 1900 (e.g., MME) according to one aspect of the disclosure. The device 1900 may include a forward relocation request receiving circuit 1902, a first key request transmission circuit 1904, a first key receiving circuit 1906, and/or a handover request transmission circuit 1908, which may all be communicatively coupled via a communication bus 1910. Each of the circuits 1902, 1904, 1906, 1908 of the network device 1900 may be specialized circuits (e.g., ASICs, FPGAs, etc.) that are specifically wired to perform their respective specific functions.

[0116] The forward relocation request receiving circuit 1902 may be one example of a means for receiving a forward relocation request at the network device from a source control plane device. The first key request transmission circuit 1904 may be one example of a means for transmitting a request for a first key to a key management device. The first key receiving circuit 1906 may be one example of a means for receiving the first key from the key management device, the first key based in part on a second key shared between the key management device and a device. The handover request transmission circuit 1908 may be one example of a means for transmitting a handover request to a target radio access node (RAN) with a RAN session key derived from the first key.

[0117] One or more of the components, steps, features, and/or functions illustrated in FIGS. 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, and/or 19 may be rearranged and/or combined into a single component, step, feature or function or embodied in several components, steps, or functions. Additional elements, components, steps, and/or functions may also be added without departing from the invention. The apparatus, devices, and/or components illustrated in FIGS. 1, 3, 4, 5, 7, 8, 9, 10, 13, 16, 17, 18, and/or 19 may be configured to perform one or more of the methods, features, or steps described in FIGS. 2, 6, 7, 8, 9, 11, 12, 14, and/or 15. The algorithms described herein may also be efficiently implemented in software and/or embedded in hardware.

[0118] Also, it is noted that the aspects of the present disclosure may be described as a process that is depicted as a flowchart, a flow diagram, a structure diagram, or a block diagram. Although a flowchart may describe the operations as a sequential process, many of the operations can be performed in parallel or concurrently. In addition, the order of the operations may be re-arranged. A process is terminated when its operations are completed. A process may correspond to a method, a function, a procedure, a subroutine, a subprogram, etc. When a process corresponds to a function, its termination corresponds to a return of the function to the calling function or the main function.

[0119] Moreover, a storage medium may represent one or more devices for storing data, including read-only memory (ROM), random access memory (RAM), magnetic disk storage mediums, optical storage mediums, flash memory devices and/or other machine-readable mediums and, processor-readable mediums, and/or computer-readable mediums for storing information. The terms “machine-readable medium”, “computer-readable medium”, and/or “processor-readable medium” may include, but are not limited to non-transitory mediums such as portable or fixed storage devices, optical storage devices, and various other mediums capable of storing or containing instruction(s) and/or data. Thus, the various methods described herein may be fully or partially implemented by instructions and/or data that may be stored in a “machine-readable medium”, “computer-readable medium”, and/or “processor-readable medium” and executed by one or more processors, machines and/or devices.

[0120] Furthermore, aspects of the disclosure may be implemented by hardware, software, firmware, middleware, microcode, or any combination thereof. When implemented in software, firmware, middleware or microcode, the program code or code segments to perform the necessary tasks may be stored in a machine-readable medium such as a storage medium or other storage(s). A processor may perform the necessary tasks. A code segment may represent a procedure, a function, a subprogram, a program, a routine, a subroutine, a module, a software package, a class, or any combination of instructions, data structures, or program statements. A code segment may be coupled to another code segment or a hardware circuit by passing and/or receiving information, data, arguments, parameters, or memory contents. Information, arguments, parameters, data, etc. may be passed, forwarded, or transmitted via any suitable means including memory sharing, message passing, token passing, network transmission, etc.

[0121] The various illustrative logical blocks, modules, circuits, elements, and/or components described in connection with the examples disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic component, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing components, e.g., a combination of a DSP and a microprocessor, a number of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration.

[0122] The methods or algorithms described in connection with the examples disclosed herein may be embodied directly in hardware, in a software module executable by a processor, or in a combination of both, in the form of processing unit, programming instructions, or other directions, and may be contained in a single device or distributed across multiple devices. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. A storage medium may be coupled to the processor such that the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor.

[0123] Those of skill in the art would further appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the aspects disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system.

[0124] The various features of the invention described herein can be implemented in different systems without departing from the invention. It should be noted that the foregoing aspects of the disclosure are merely examples and are not to be construed as limiting the invention. The description of the aspects of the present disclosure is intended to be illustrative, and not to limit the scope of the claims. As such, the present teachings can be readily applied to other types of apparatuses and many alternatives, modifications, and variations will be apparent to those skilled in the art.

CLAIMS

1. A device comprising:

a wireless communication interface adapted to transmit and receive data wirelessly to and from a network; and

a processing circuit communicatively coupled to the wireless communication interface, the processing circuit adapted to:

identify entry into a new service area;

transmit a service area update request to a network device associated with the network;

receive a control plane message from the network indicating control plane device relocation or a key refresh due to a service area change in response to transmitting the service area update request; and

derive a first key based in part on data included in the control plane message received and a second key shared between the device and a key management device, the key management device associated with the network.

2. The device of claim 1, wherein the control plane message is received from a target control plane device due to the service area change, the target control plane device being a different control plane device from one currently serving the device.

3. The device of claim 1, wherein the data included in the control plane message includes a control plane device identifier that identifies a control plane device that is and/or will be serving the device.

4. The device of claim 1, wherein deriving the first key is further based in part on a counter value Key Count maintained at the key management device and included in the control plane message.

5. The device of claim 1, wherein the processing circuit is further adapted to:

derive at least one of an evolved node B (eNB) key K_{eNB}, a non-access stratum key K_{NAS}, and/or a next hop (NH) key based on the first key to secure communications between the device and the network.

6. The device of claim 1, wherein the new service area is at least one of a new tracking area and/or a new routing area, and the service area update request is associated with at least one of a tracking area update and/or a routing area update.

7. The device of claim 2, wherein the control plane message is a security mode command, the target control plane device is a target mobility management entity (MME), the key management device is a session key management function (SKMF) device, and the second key is a session root key for an authentication session.

8. The device of claim 1, wherein a control plane device maintains a mobility management context and a session management context for the device, and the key management device maintains the second key.

9. A device comprising:

a wireless communication interface adapted to transmit and receive data wirelessly to a network; and

a processing circuit communicatively coupled to the wireless communication interface, the processing circuit adapted to:

receive a handover command from a network device associated with the network, the handover command indicating a new service area;

derive a first key based on data included in the handover command and on a second key shared between the device and a key management device, the key management device associated with the network; and

send a handover confirmation message that is secured based on the first key.

10. The device of claim 9, wherein the handover command includes a target control plane device identifier associated with a target control plane device serving a target radio access node that is and/or will be serving the device.

11. The device of claim 10, wherein deriving the first key is based in part on the target control plane device identifier.

12. The device of claim 10, wherein the target control plane device is a target mobility management entity (MME), the key management device is a session key management function (SKMF) device, and the target control plane device identifier is an MME identifier associated with the target MME.

13. The device of claim 9, wherein deriving the first key is further based in part on a counter value Key Count maintained at the key management device.

14. The device of claim 9, wherein the second key is a session root key for an authentication session.

15. A network device associated with a network, the network device comprising:

a communication interface adapted to transmit and receive information; and

a processing circuit communicatively coupled to the communication interface, the processing circuit adapted to:

receive a service area update request from a device for which the network device does not have a device context or the device has changed service areas;

transmit a request for a first key to a key management device;

receive the first key from the key management device, the first key based in part on a second key shared between the key management device and the device; and

transmit a control plane message to the device that includes data allowing the device to derive the first key.

16. The network device of claim 15, wherein the network device is a mobility management entity (MME) and the first key is further based on an MME identifier that identifies the MME.

17. The network device of claim 15, wherein the processing circuit is further adapted to:

transmit a device context request to a prior control plane device that previously served the device if the network device does not have the device context; and

receive the device context from the prior control plane device in response to transmitting the device context request.

18. The network device of claim 15, wherein the data includes a control plane device identifier that identifies the network device.

19. The network device of claim 15, wherein the processing circuit is further adapted to:

receive a counter value Key Count from the key management device along with the first key; and

include the counter value Key Count in the data transmitted to the device.

20. The network device of claim 15, wherein the processing circuit is further adapted to:

transmit a service area update to the device after receiving notification from the device that the control plane message was successfully received.

21. The network device of claim 15, wherein the service area update request is associated with at least one of a tracking area update and/or a routing area update and changing service areas includes at least one of changing tracking areas and/or changing routing areas.

22. The device of claim 15, wherein the control plane message is a non-access stratum security mode command, the key management device is a session key management function (SKMF) device, the device is a user equipment, the device context is a user equipment context associated with the user equipment, and the second key is a session root key for an authentication session.

23. A network device associated with a network, the network device comprising:

a communication interface adapted to transmit and receive information; and a processing circuit communicatively coupled to the communication interface, the processing circuit adapted to:

receive a forward relocation request at the network device from a source control plane device;

transmit a request for a first key to a key management device;

receive the first key from the key management device, the first key based in part on a second key shared between the key management device and a device; and

transmit a handover request to a target radio access node (RAN) with a RAN session key derived from the first key.

24. The network device of claim 23, wherein the processing circuit is further adapted to:

receive a handover request acknowledgement message from the target RAN indicating the target RAN will serve the device.

25. The network device of claim 24, wherein the processing circuit is further adapted to:

transmit an acknowledgement message to the key management device indicating receipt of the first key only after receiving the handover request acknowledgement message from the target RAN.

26. The network device of claim 23, wherein the processing circuit is further adapted to:

transmit a forward relocation response to the source control plane device that includes data utilized by the device to derive the first key.

27. The network device of claim 26, wherein the network device is a target control plane device that will serve the device and the data includes a target control plane device identifier that identifies the target control plane device.

28. The network device of claim 27, wherein the target control plane device is a target mobility management entity (MME), the source control plane device is a source

MME, the target control plane device identifier is a globally unique MME identifier (GUMMEI), the key management device is a session key management function (SKMF) device, and the device is a user equipment.

29. The network device of claim 26, wherein the data includes a counter value Key Count maintained at the key management device.

30. The network device of claim 23, wherein the processing circuit adapted to receive the first key from the key management device is further adapted to receive a counter value Key Count along with the first key.

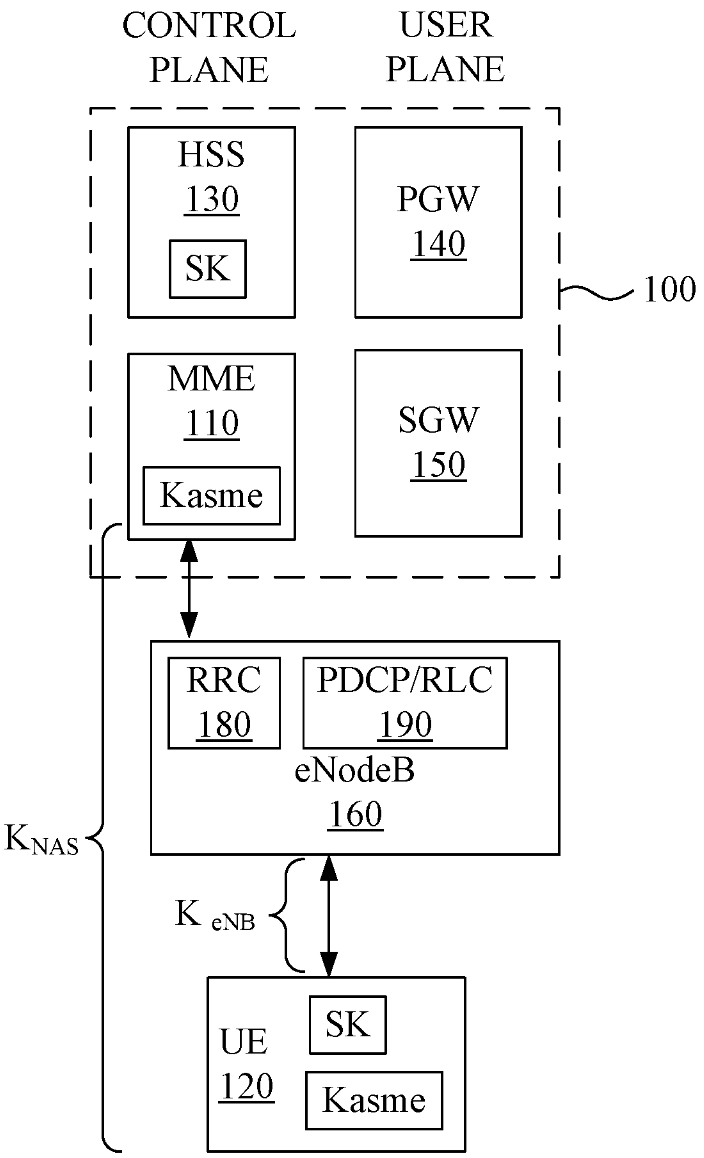

FIG. 1
(Prior Art)

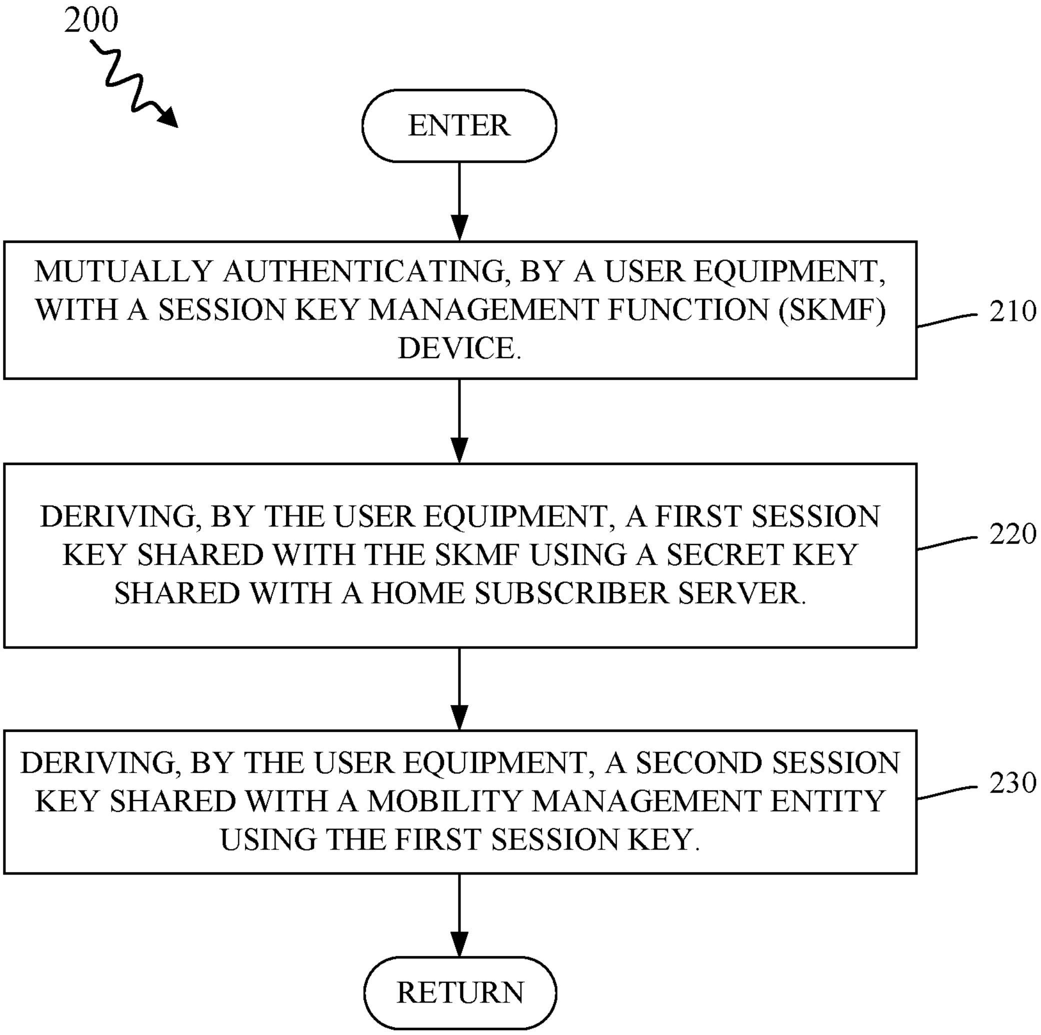
200
ENTER
MUTUALLY AUTHENTICATING, BY A USER EQUIPMENT, WITH A SESSION KEY MANAGEMENT FUNCTION (SKMF) DEVICE.
210
DERIVING, BY THE USER EQUIPMENT, A FIRST SESSION KEY SHARED WITH THE SKMF USING A SECRET KEY SHARED WITH A HOME SUBSCRIBER SERVER.
220
DERIVING, BY THE USER EQUIPMENT, A SECOND SESSION KEY SHARED WITH A MOBILITY MANAGEMENT ENTITY USING THE FIRST SESSION KEY.
230
RETURN

FIG. 2

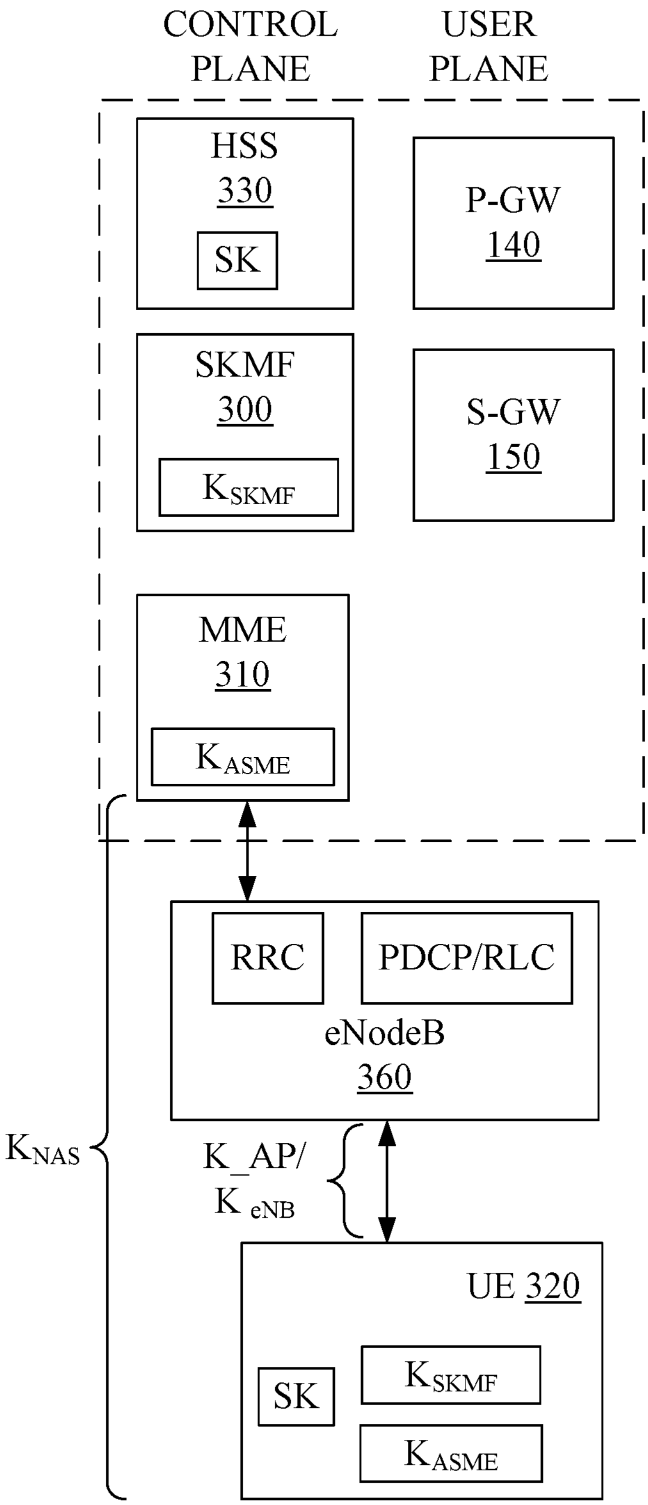
CONTROL PLANE
USER PLANE
HSS
330
SK
P-GW
140
SKMF
300
K_{SKMF}
S-GW
150
MME
310
K_{ASME}
RRC
PDCP/RLC
eNodeB
360
K_{NAS}
K_AP/
K_{eNB}
UE 320
SK
K_{SKMF}
K_{ASME}

FIG. 3

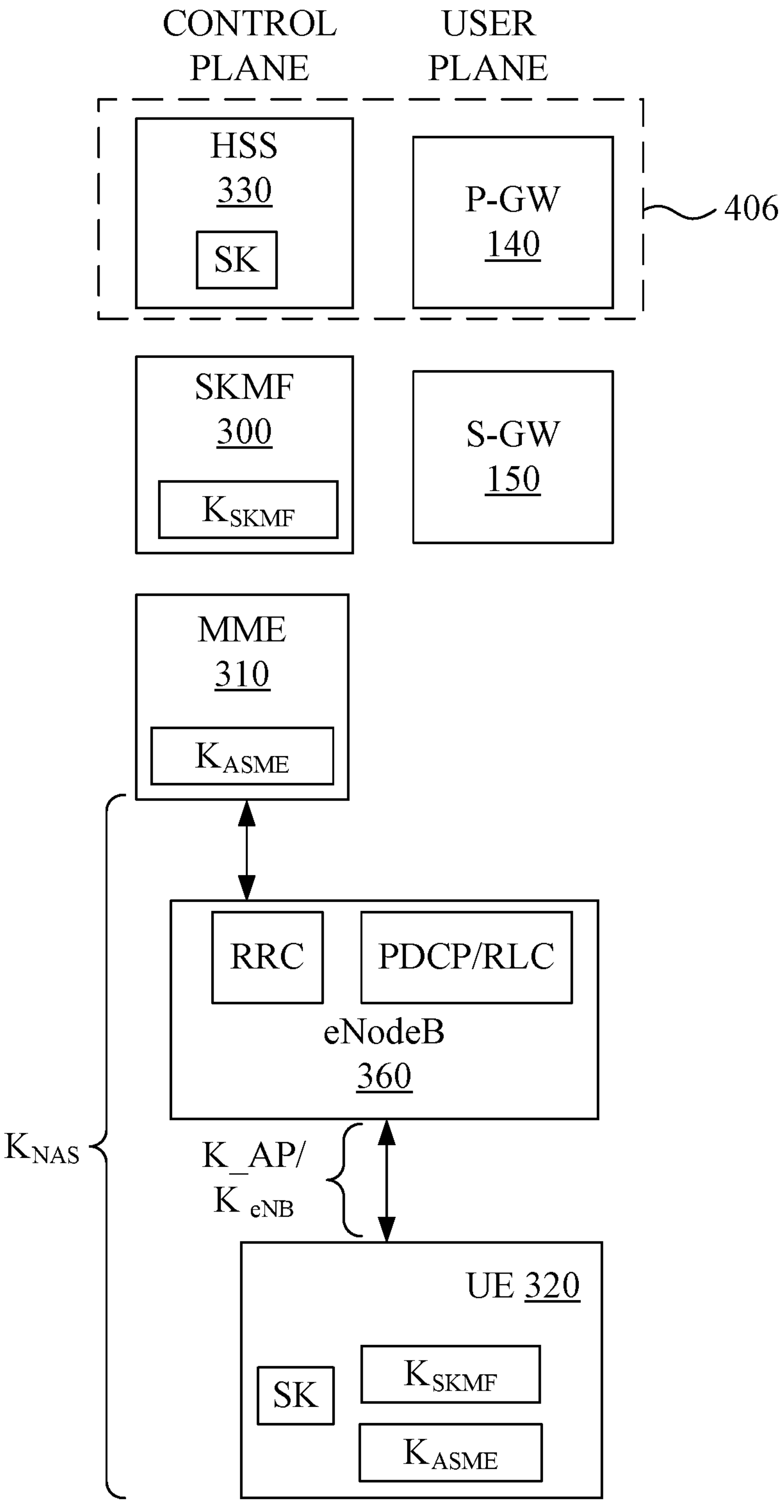
CONTROL PLANE
USER PLANE
HSS 330
SK
P-GW 140
406
SKMF 300
K_{SKMF}
S-GW 150
MME 310
K_{ASME}
RRC
PDCP/RLC
eNodeB 360
K_{NAS}
K_AP/ K_{eNB}
UE 320
SK
K_{SKMF}
K_{ASME}

FIG. 4

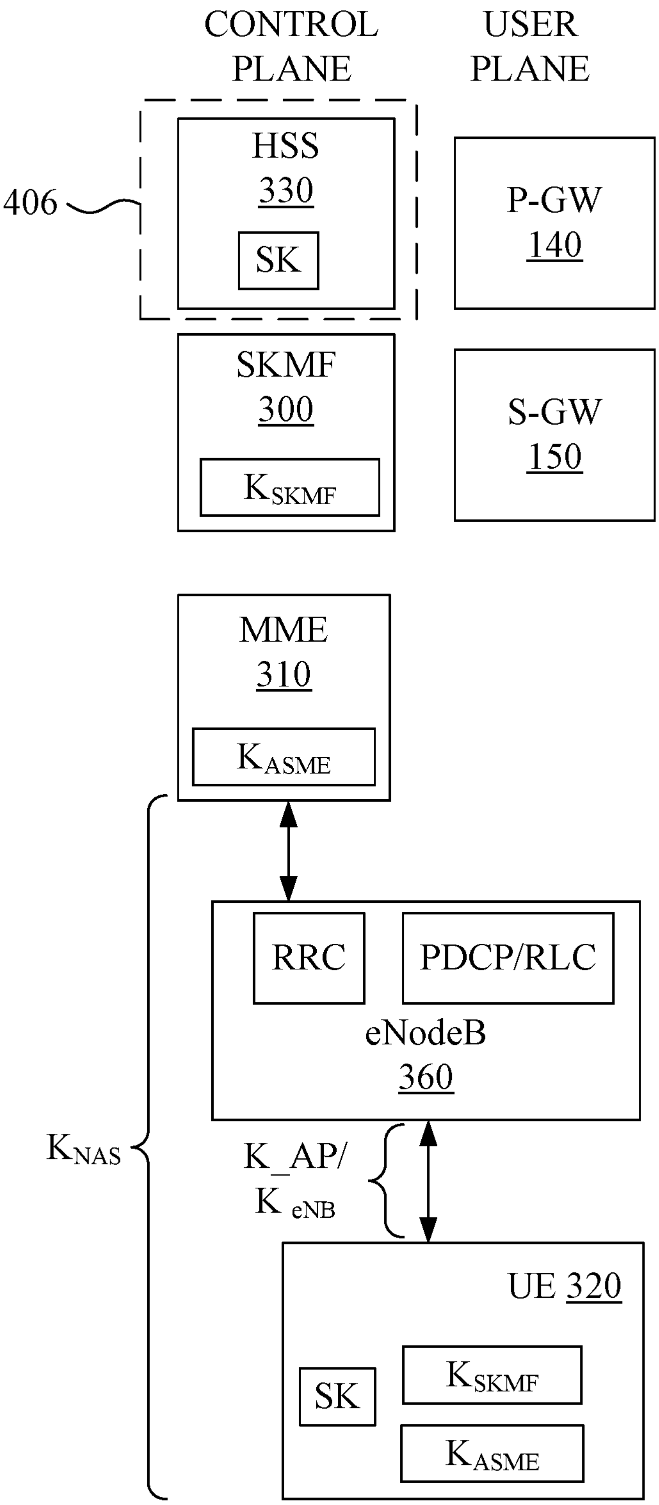
CONTROL PLANE
USER PLANE
406
HSS 330
SK
P-GW 140
SKMF 300
K_SKMF
S-GW 150
MME 310
K_ASME
RRC
PDCP/RLC
eNodeB 360
K_NAS
K_AP/ K eNB
UE 320
SK
K_SKMF
K_ASME

FIG. 5

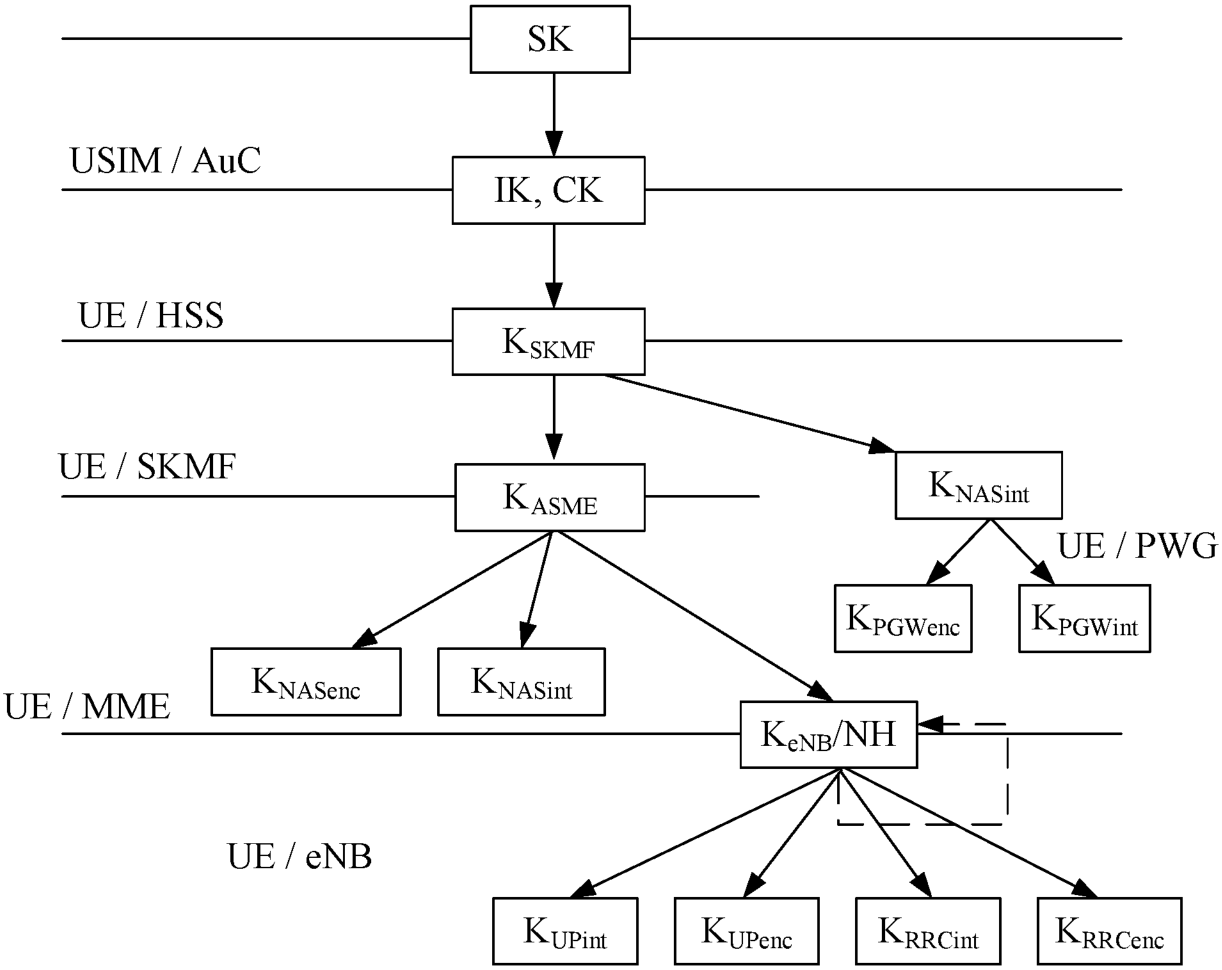
SK
USIM / AuC
IK, CK
UE / HSS
K_{SKMF}
UE / SKMF
K_{ASME}
K_{NASint}
UE / PWG
K_{PGWenc}
K_{PGWint}
K_{NASenc}
K_{NASint}
UE / MME
K_{eNB}/NH
UE / eNB
K_{UPint}
K_{UPenc}
K_{RRCint}
K_{RRCenc}

FIG. 6

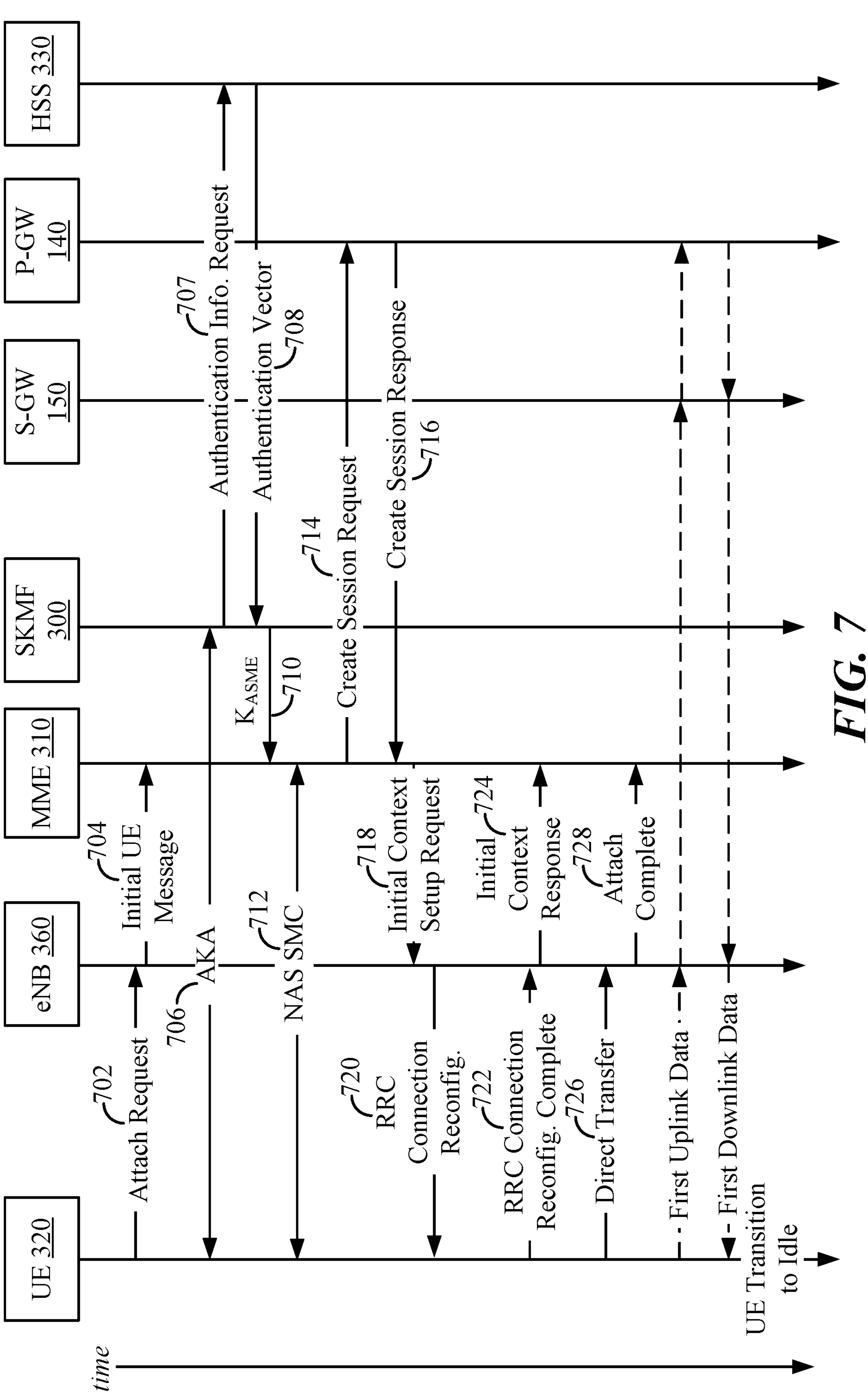
UE 320
eNB 360
MME 310
SKMF 300
S-GW 150
P-GW 140
HSS 330
time
702
Attach Request
704
Initial UE Message
706
AKA
707
Authentication Info. Request
Authentication Vector
708
KASME
710
712
NAS SMC
714
Create Session Request
Create Session Request
Create Session Response
716
718
Initial Context Setup Request
720
RRC Connection Reconfig.
722
RRC Connection Reconfig. Complete
724
Initial Context Response
726
Direct Transfer
728
Attach Complete
First Uplink Data
First Downlink Data
UE Transition to Idle

FIG. 7

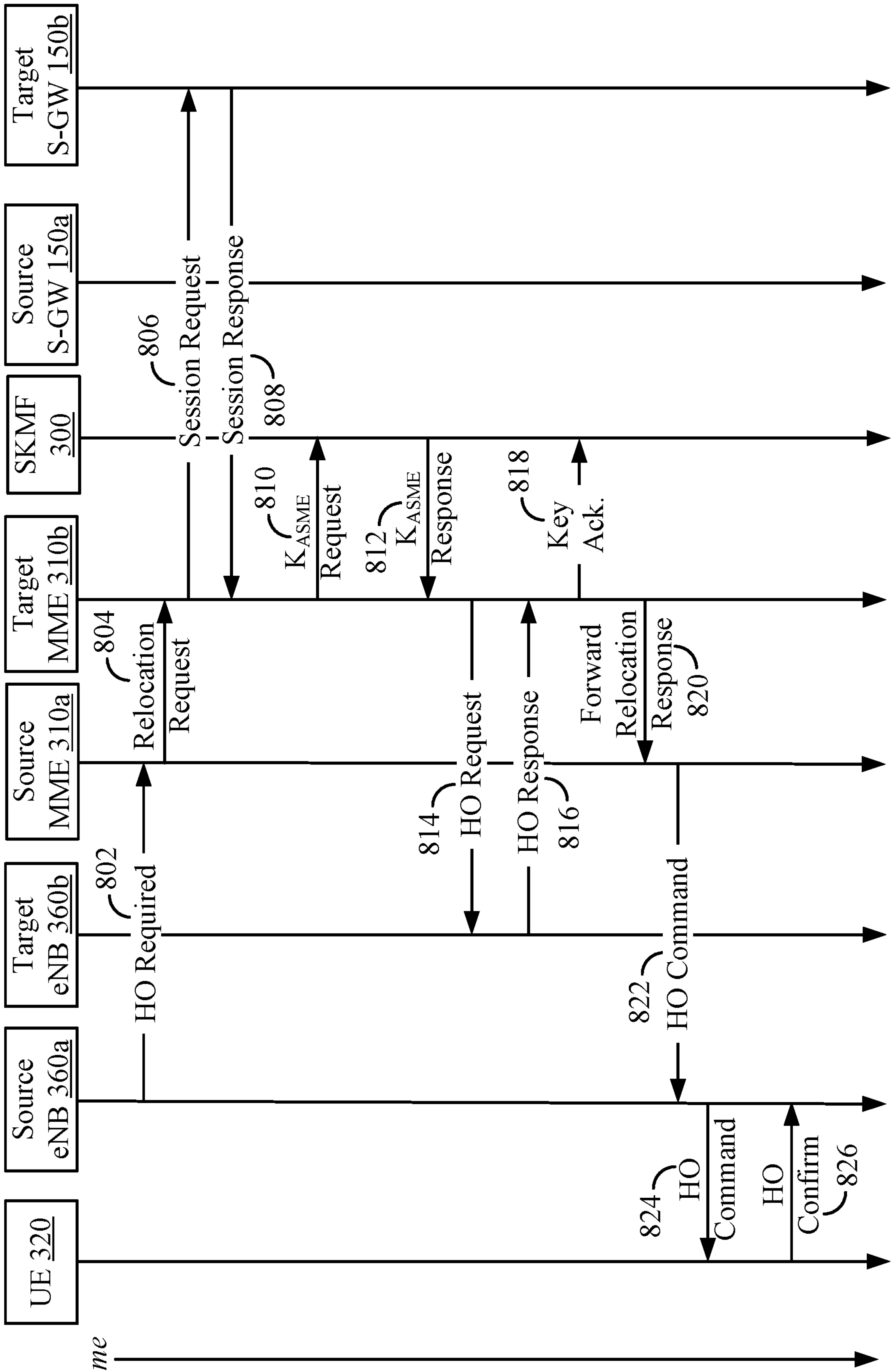
time
UE 320
Source eNB 360a
Target eNB 360b
Source MME 310a
Target MME 310b
SKMF 300
Source S-GW 150a
Target S-GW 150b
802
HO Required
804
Relocation Request
806
Session Request
Session Response
808
810
K_{ASME} Request
812
K_{ASME} Response
814
HO Request
HO Response
816
818
Key Ack.
Forward Relocation Response
820
822
HO Command
824
HO Command
HO Confirm
826

FIG. 8

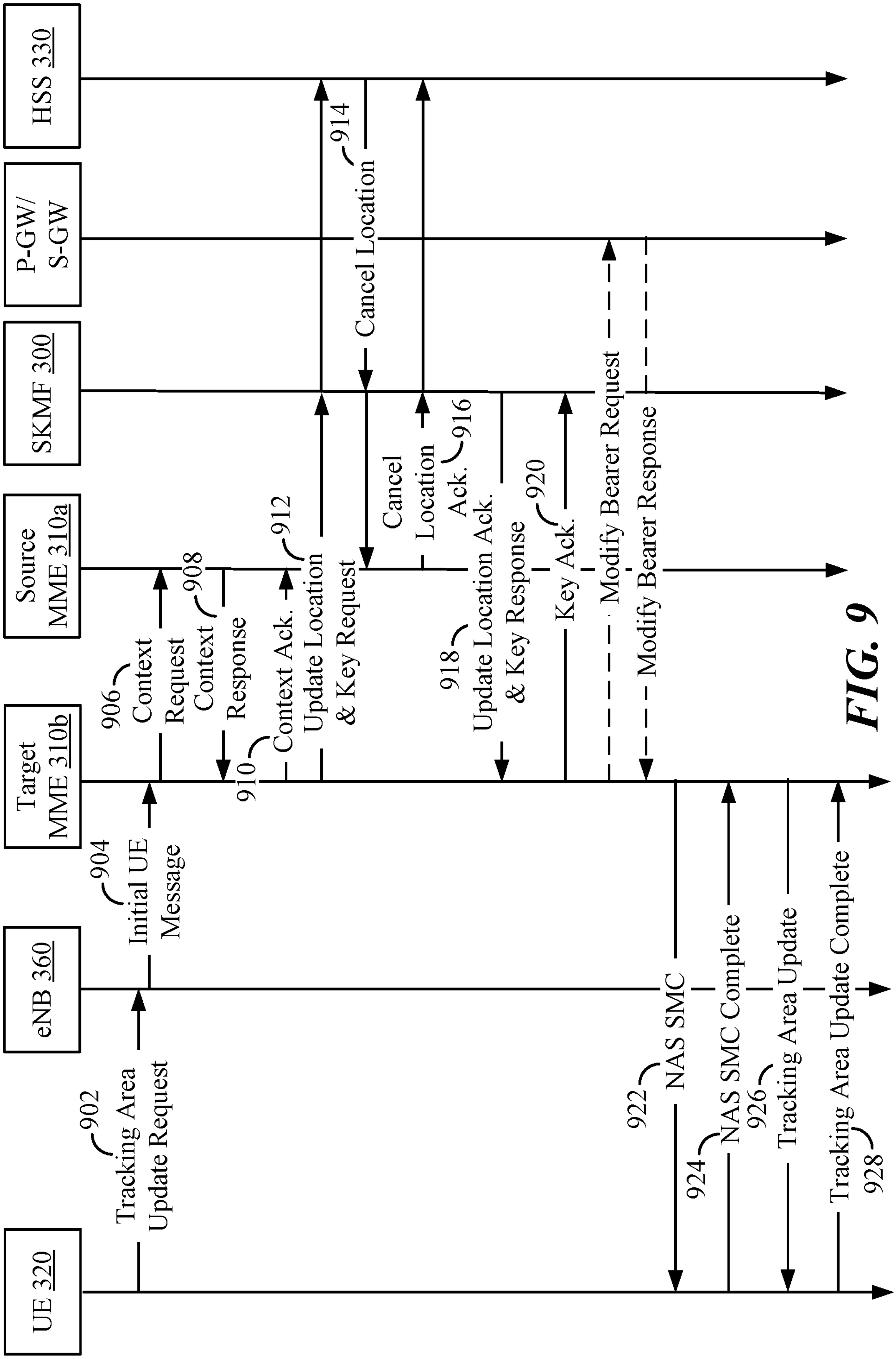
UE 320
eNB 360
Target MME 310b
Source MME 310a
SKMF 300
P-GW/ S-GW
HSS 330
902
Tracking Area Update Request
904
Initial UE Message
906
Context Request
908
Context Response
910
Context Ack.
912
Update Location & Key Request
914
Cancel Location
916
Cancel Location Ack.
918
Update Location Ack. & Key Response
920
Key Ack.
Modify Bearer Request
Modify Bearer Response
922
NAS SMC
924
NAS SMC Complete
926
Tracking Area Update
928
Tracking Area Update Complete

FIG. 9

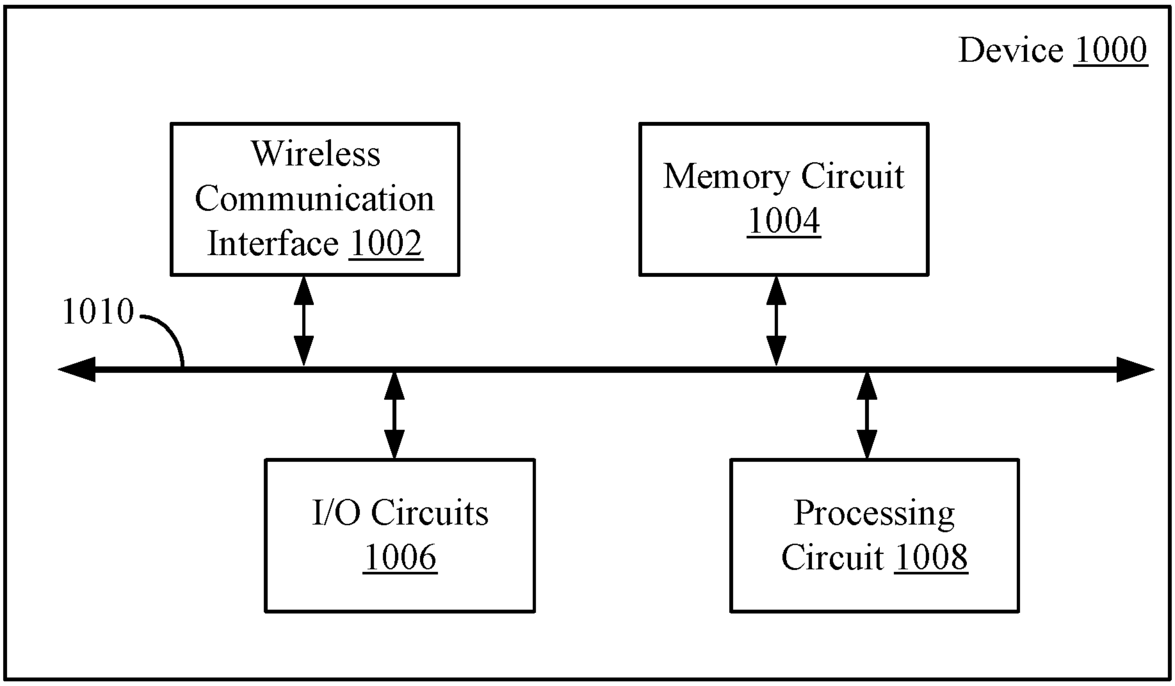
Device 1000
Wireless Communication Interface 1002
Memory Circuit 1004
1010
I/O Circuits 1006
Processing Circuit 1008

FIG. 10

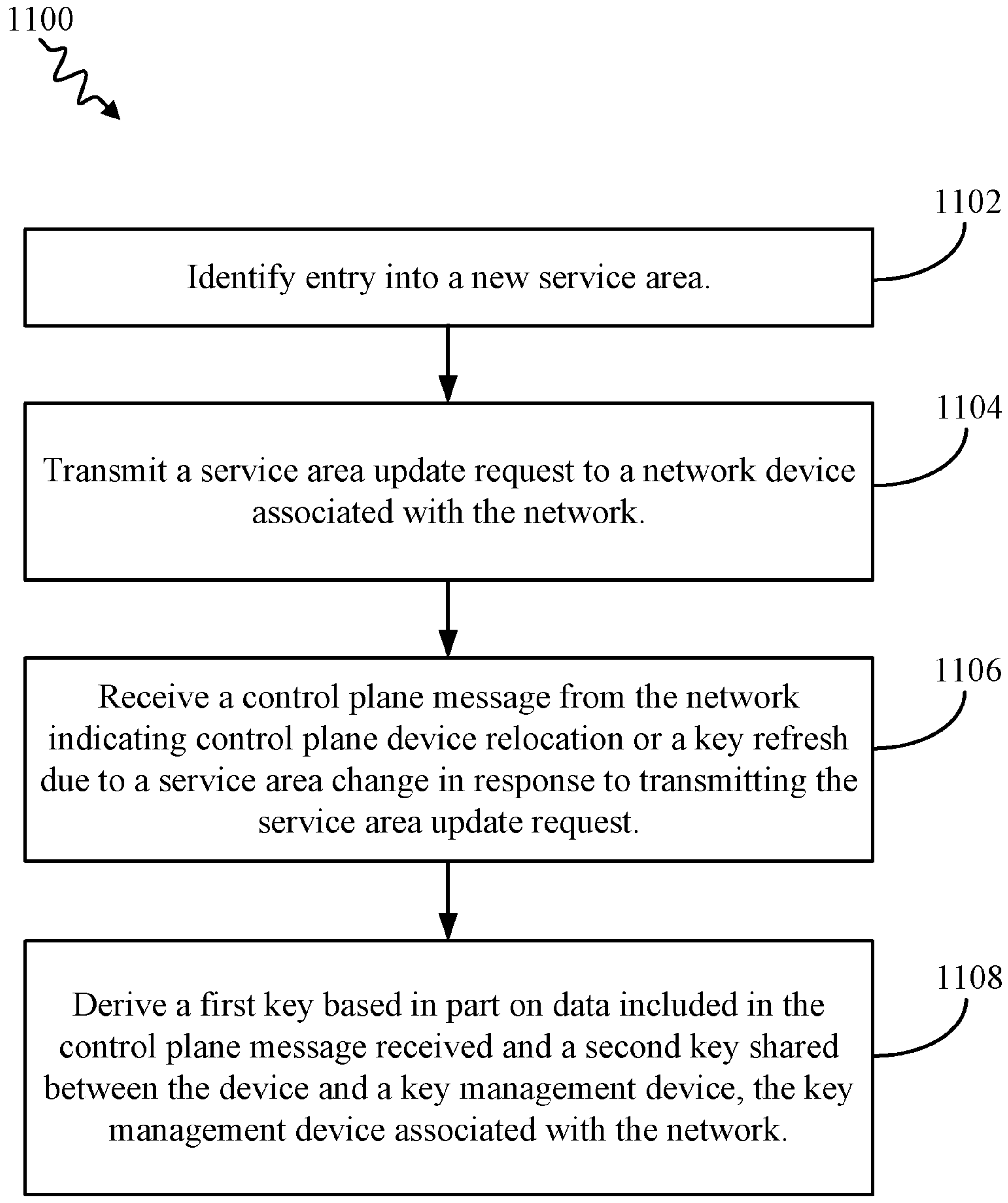
1100
1102
Identify entry into a new service area.
1104
Transmit a service area update request to a network device associated with the network.
1106
Receive a control plane message from the network indicating control plane device relocation or a key refresh due to a service area change in response to transmitting the service area update request.
1108
Derive a first key based in part on data included in the control plane message received and a second key shared between the device and a key management device, the key management device associated with the network.

FIG. 11

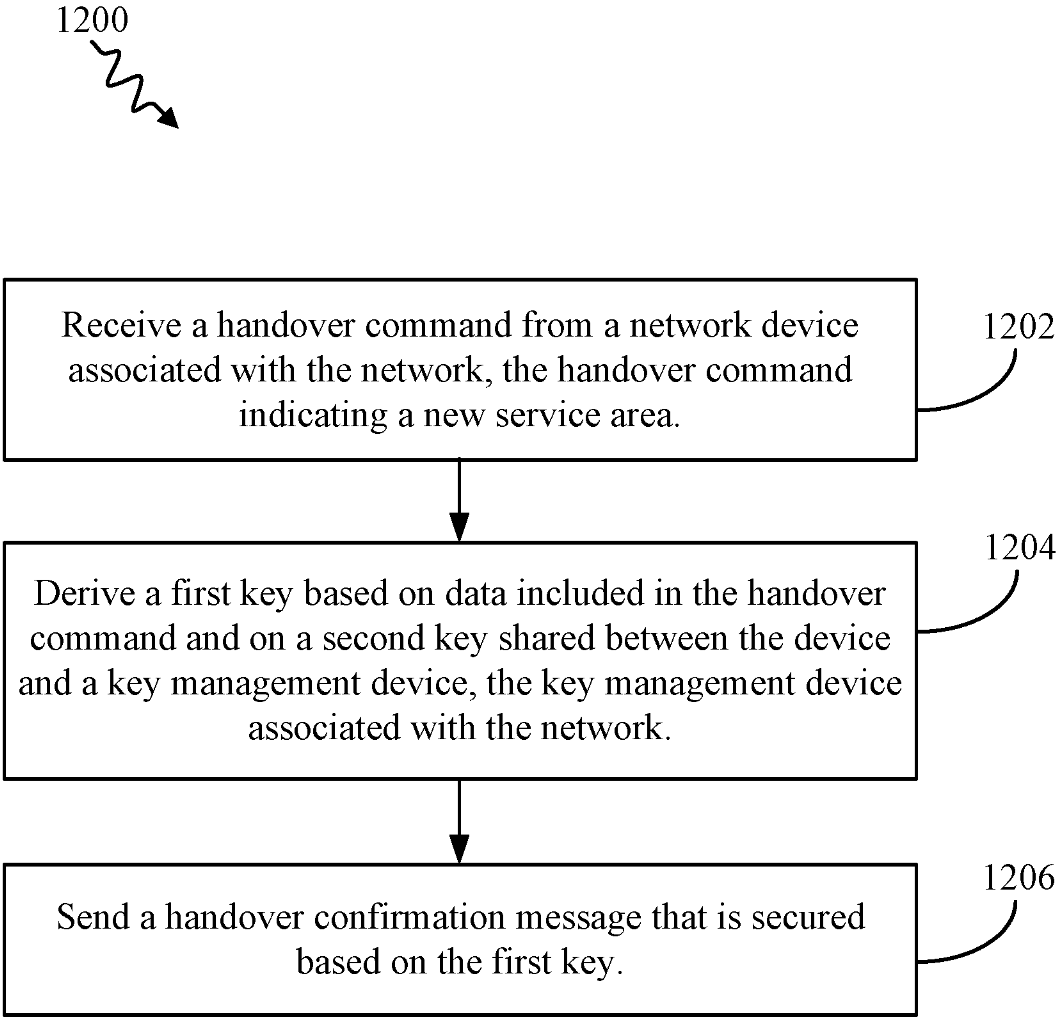
1200
Receive a handover command from a network device associated with the network, the handover command indicating a new service area.
1202
Derive a first key based on data included in the handover command and on a second key shared between the device and a key management device, the key management device associated with the network.
1204
Send a handover confirmation message that is secured based on the first key.
1206

FIG. 12

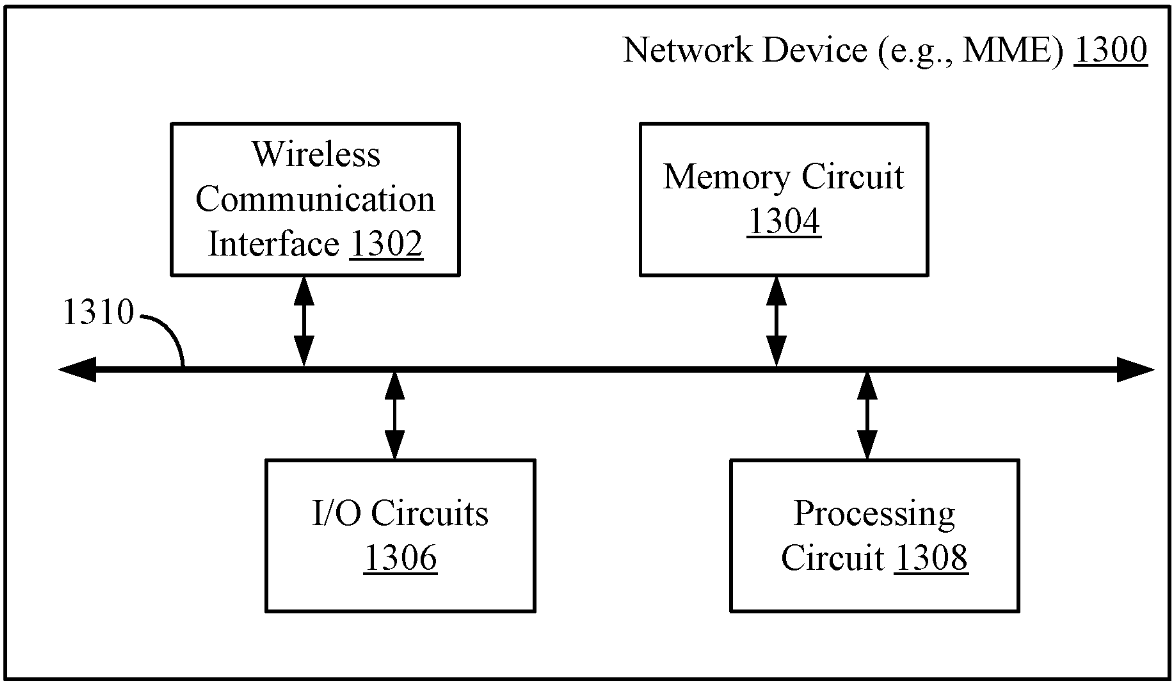
Network Device (e.g., MME) 1300
Wireless Communication Interface 1302
Memory Circuit 1304
1310
I/O Circuits 1306
Processing Circuit 1308

FIG. 13

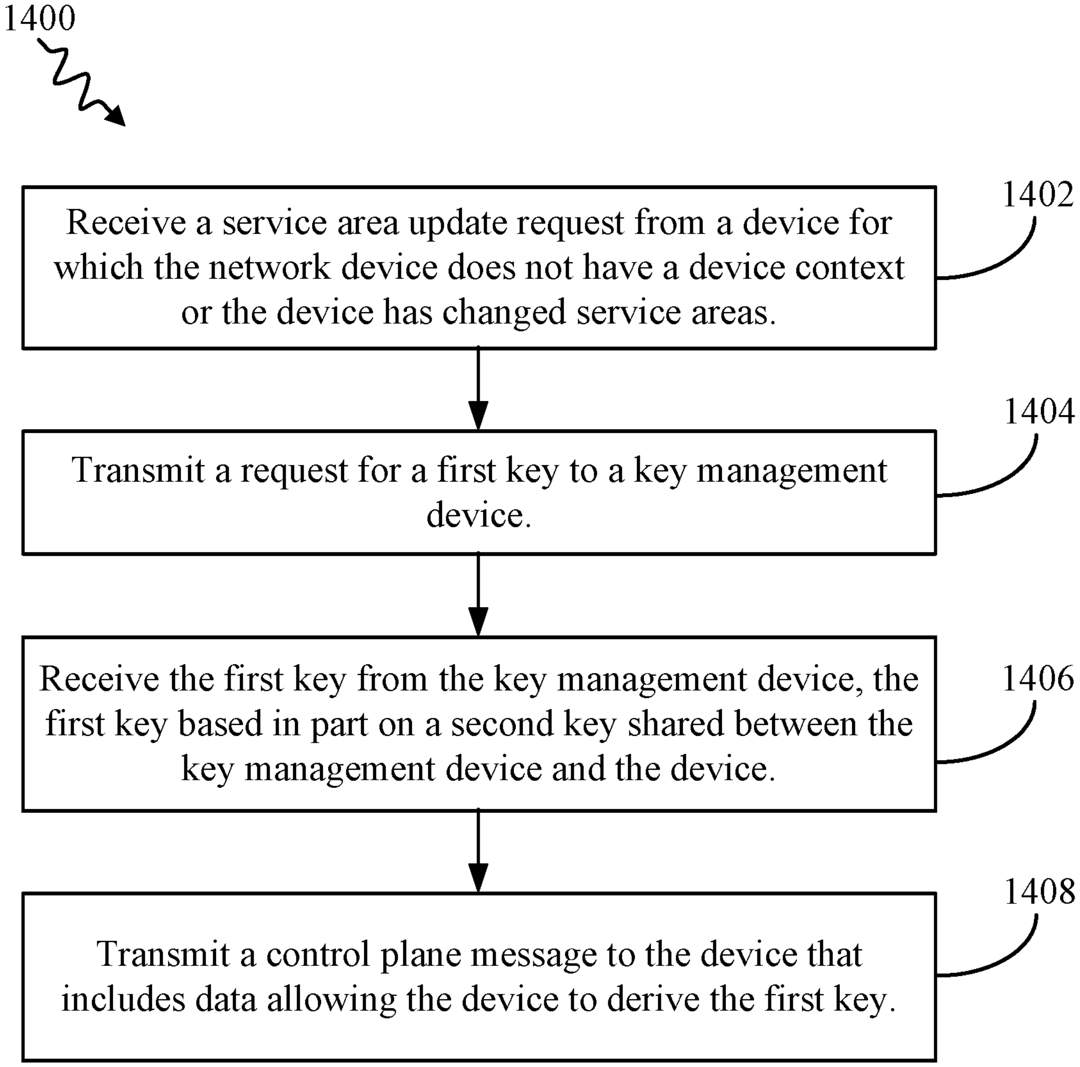
1400
1402
Receive a service area update request from a device for which the network device does not have a device context or the device has changed service areas.
1404
Transmit a request for a first key to a key management device.
1406
Receive the first key from the key management device, the first key based in part on a second key shared between the key management device and the device.
1408
Transmit a control plane message to the device that includes data allowing the device to derive the first key.

FIG. 14

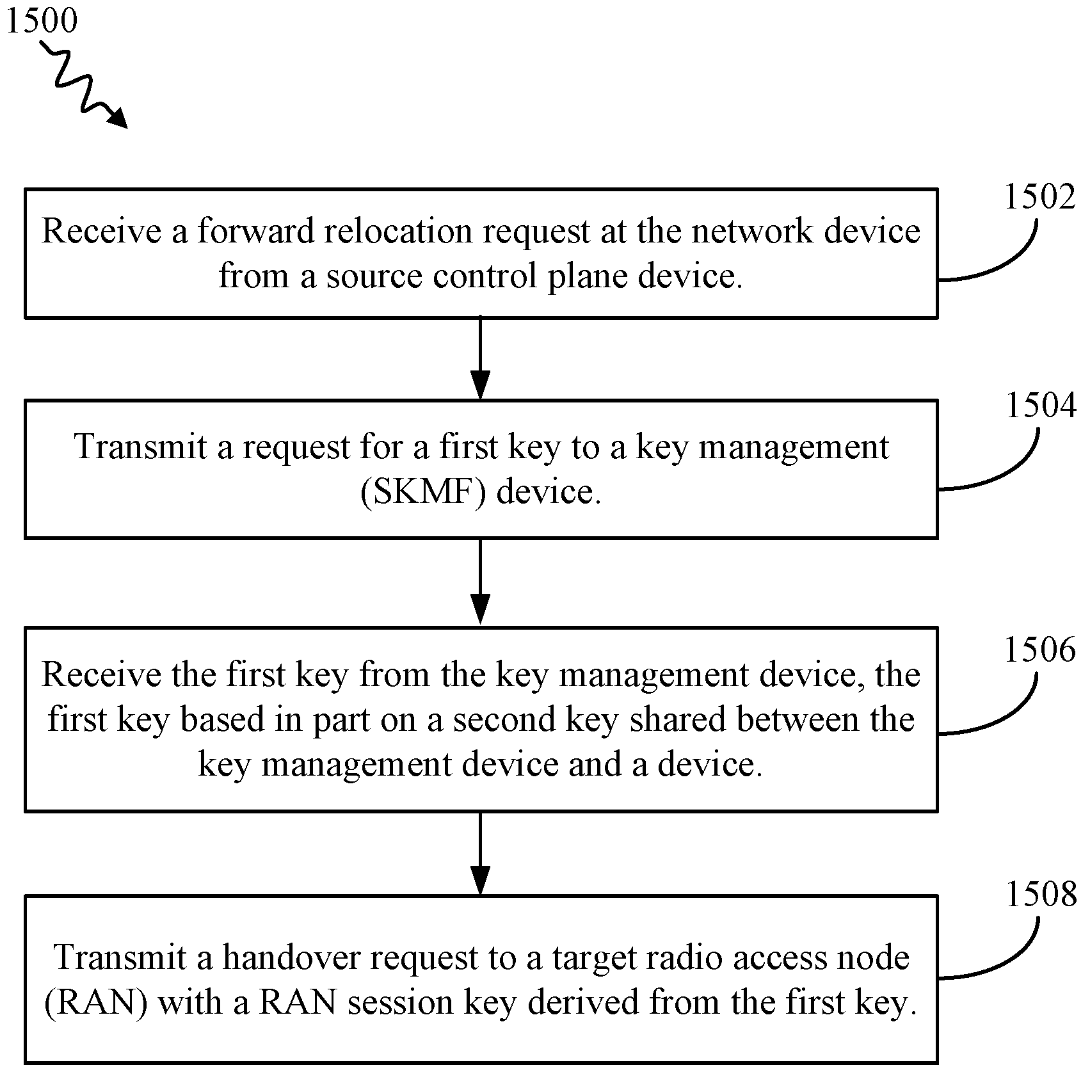
1500
Receive a forward relocation request at the network device from a source control plane device.
1502
Transmit a request for a first key to a key management (SKMF) device.
1504
Receive the first key from the key management device, the first key based in part on a second key shared between the key management device and a device.
1506
Transmit a handover request to a target radio access node (RAN) with a RAN session key derived from the first key.
1508

FIG. 15

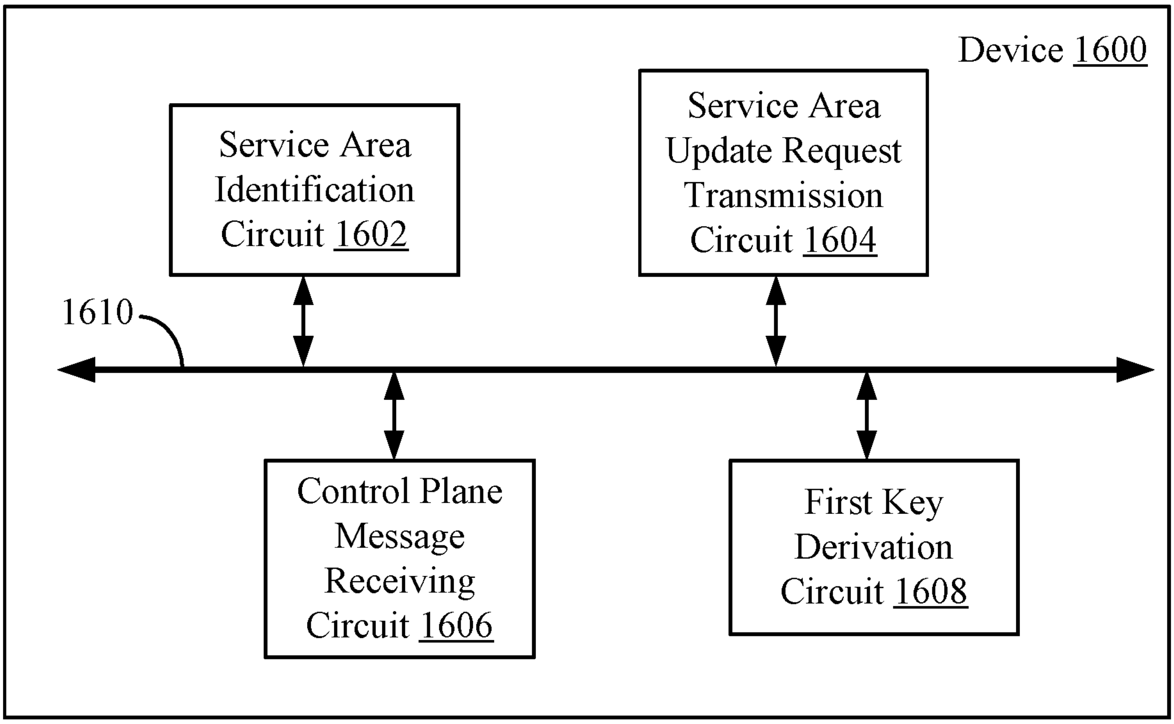
Device 1600
Service Area Identification Circuit 1602
Service Area Update Request Transmission Circuit 1604
1610
Control Plane Message Receiving Circuit 1606
First Key Derivation Circuit 1608

FIG. 16

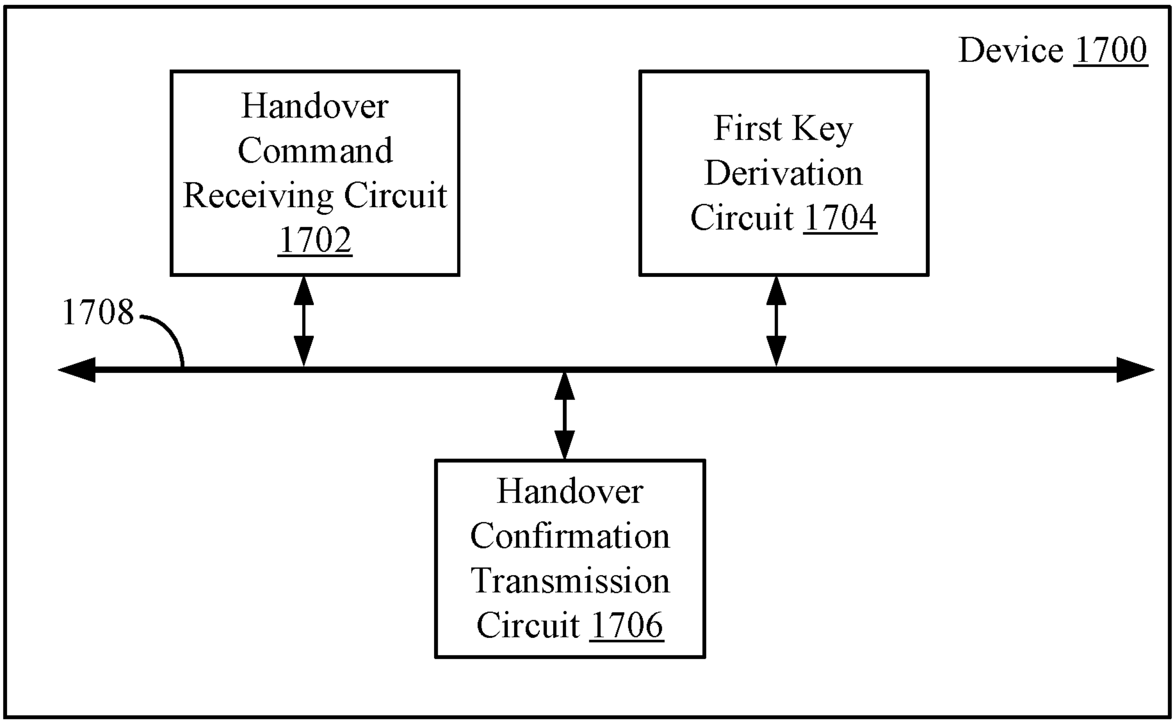
Device 1700
Handover Command Receiving Circuit 1702
First Key Derivation Circuit 1704
1708
Handover Confirmation Transmission Circuit 1706

FIG. 17

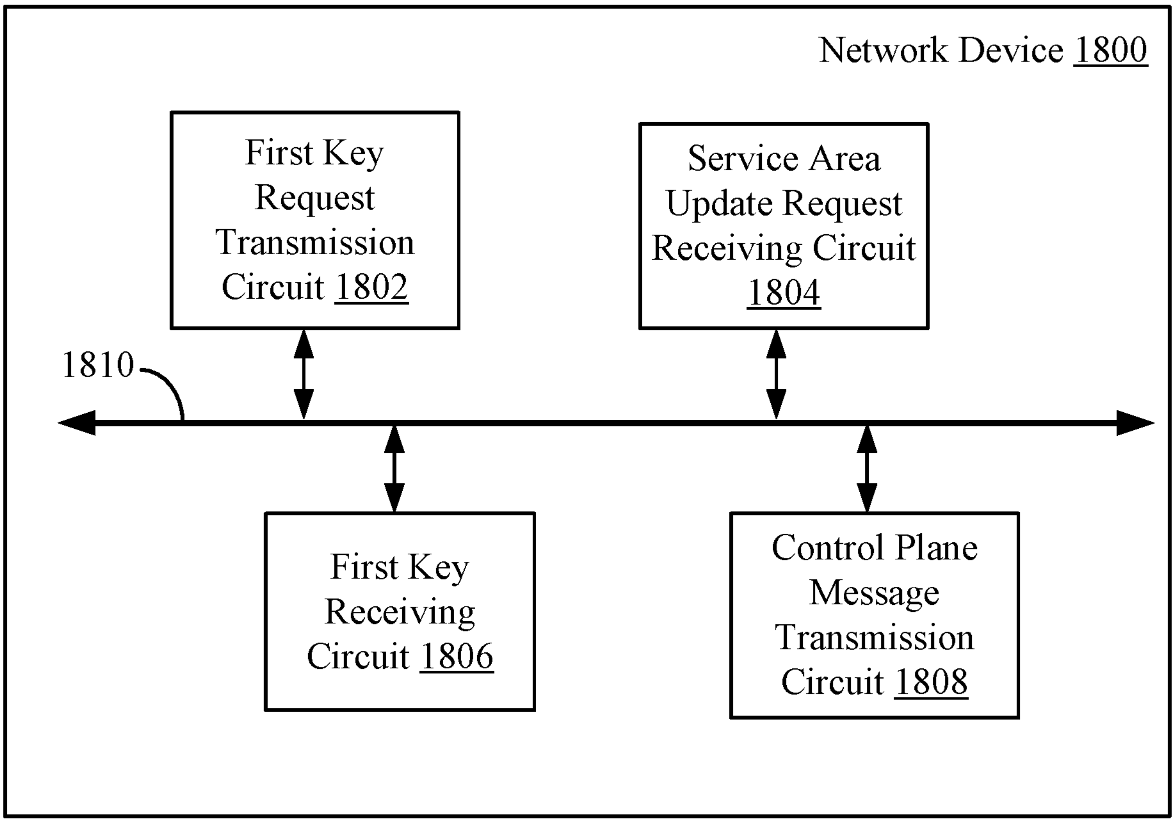
Network Device 1800
First Key Request Transmission Circuit 1802
Service Area Update Request Receiving Circuit 1804
1810
First Key Receiving Circuit 1806
Control Plane Message Transmission Circuit 1808

FIG. 18

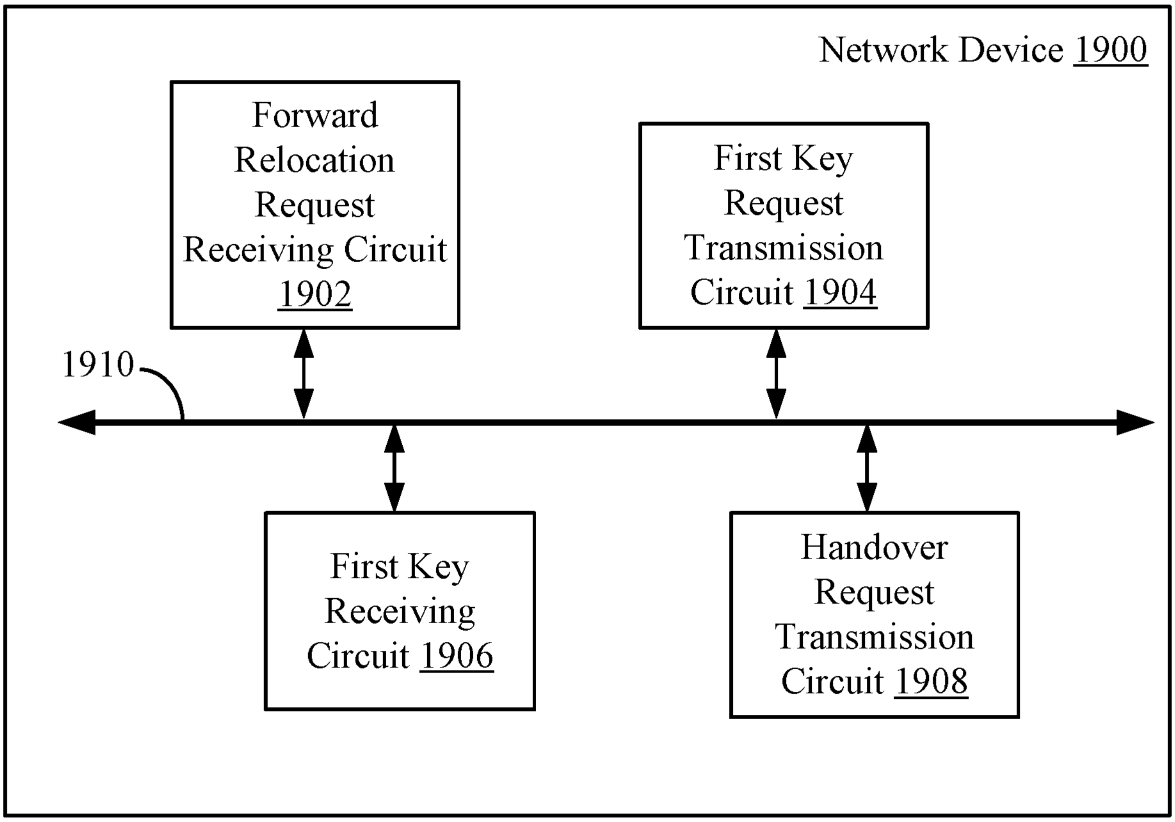
Network Device 1900
Forward Relocation Request Receiving Circuit 1902
First Key Request Transmission Circuit 1904
1910
First Key Receiving Circuit 1906
Handover Request Transmission Circuit 1908

FIG. 19

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/047101

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/02 H04W12/04
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 315 371 A2 (SAMSUNG ELECTRONICS CO LTD [KR]) 27 April 2011 (2011-04-27) paragraphs [0008], [0022] - [0039], [0047], [0051], [0069] figure 2 -----	1-30
X	US 2011/311053 A1 (ESCOTT ADRIAN EDWARD [GB] ET AL) 22 December 2011 (2011-12-22) paragraph [0039] - paragraph [0048] figures 5,9 ----- -/--	1-30

☒ 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 28 October 2016	Date of mailing of the international search report 08/11/2016
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Zembery, Peter

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2016/047101

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Dionisio Zumerle: "3GPP LTE Security Aspects", 3GPP Workshop, Bangalore, 30 May 2011, 30 May 2011 (2011-05-30), pages 1-27, XP055089219, Retrieved from the Internet: URL:http://www.3g4g.co.uk/Lte/LTE_Security_Pres_1105_3GPP.pdf [retrieved on 2013-11-19] "Key Derivation" on page 13 -----	1-30

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2016/047101

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2315371 A2	27-04-2011	CN 102187599 A	14-09-2011
		EP 2315371 A2	27-04-2011
		JP 5390611 B2	15-01-2014
		JP 2012500511 A	05-01-2012
		KR 20100021385 A	24-02-2010
		US 2011142239 A1	16-06-2011
		WO 2010019020 A2	18-02-2010
US 2011311053 A1	22-12-2011	AR 082018 A1	07-11-2012
		AU 2011268287 A1	17-01-2013
		CA 2802488 A1	22-12-2011
		CN 102948183 A	27-02-2013
		EP 2583480 A2	24-04-2013
		JP 5452769 B2	26-03-2014
		JP 2013535146 A	09-09-2013
		KR 20130030810 A	27-03-2013
		KR 20150013336 A	04-02-2015
		RU 2013102043 A	27-07-2014
		SG 186307 A1	30-01-2013
		TW 201218789 A	01-05-2012
		US 2011311053 A1	22-12-2011
		WO 2011159948 A2	22-12-2011