

SECURITY UPDATE FOR SUBSEQUENT LTM

TECHNICAL FIELD

[0001] The present disclosure relates to wireless communications, and more specifically to a base station, a user equipment, processors, and methods for security update for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), for example, security update for subsequent inter-central unit (CU) LTM.

BACKGROUND

[0002] A wireless communications system may include one or multiple network communication devices, such as base stations, which may be otherwise known as an eNodeB (eNB), a next-generation NodeB (gNB), or other suitable terminology. Each network communication devices, such as a base station may support wireless communications for one or multiple user communication devices, which may be otherwise known as user equipment (UE), or other suitable terminology. The wireless communications system may support wireless communications with one or multiple user communication devices by utilizing resources of the wireless communication system (e.g., time resources (e.g., symbols, slots, subframes, frames, or the like) or frequency resources (e.g., subcarriers, carriers). Additionally, the wireless communications system may support wireless communications across various radio access technologies including third generation (3G) radio access technology, fourth generation (4G) radio access technology, fifth generation (5G) radio access technology, among other suitable radio access technologies beyond 5G (e.g., sixth generation (6G)).

[0003] When a UE moves to a new cell with a change of packet data convergence protocol (PDCP) anchor, the UE and the network shall obtain a new security key for security update. For the intra-CU LTM (including the intra-CU intra-DU LTM and the intra-CU inter-DU LTM), no security update is needed due to the unchanged PDCP anchor, while for the inter-CU LTM, since the PDCP anchor relocation happens, the security update should be performed. However, for the subsequent inter-CU LTM, there is no radio resource control (RRC) reconfiguration message between the UE and a candidate CU. Thus, there are still some open problems in the LTM scheme that needs to be studied.

SUMMARY

[0004] The present disclosure relates to a base station, user equipment, methods and processors that support a security update for subsequent inter-CU LTM.

[0005] In a first aspect of the solution, a base station may comprise: a processor; and a transceiver coupled to the processor, wherein the base station is a first target base station for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), and the processor is configured to: determine a first security key to be used between a user equipment (UE) and a second target base station for the LTM and a next hop (NH) chaining counter (NCC) to be used for a key derivation for a cell switch by the UE; and transmit, via the transceiver and to the UE, the NCC.

[0006] In some implementations of the method and apparatuses described herein, the processor may be further configured to: transmit, via the transceiver and to the second target base station, the first security key and the NCC.

[0007] In some implementations of the method and apparatuses described herein, the first target base station may include a first target central unit (CU) and one or more distributed units (DUs), and the one or more DUs include a first target DU serving the UE.

[0008] In some implementations of the method and apparatuses described herein, the processor may include a first processor of the first target CU, and the first processor may be configured to: receive, from the first target DU, a cell switch decision message indicating a cell switch to a target cell; determine whether a security update is needed based on the received cell switch decision message; in response to determining that the security update is needed, perform a first security key derivation for determining the first security key and the NCC; and transmit, via the transceiver, the NCC to the first target DU such that the NCC is transmitted to the UE via the first target DU.

[0009] In some implementations of the method and apparatuses described herein, the first processor may be further configured to: transmit, via the transceiver and to the second target base station, the first security key and the NCC.

[0010] In some implementations of the method and apparatuses described herein, the first security key derivation may comprises: in the case that the first target CU has an unused {NH, NCC} pair, computing the first security key from the NH, and setting a

value of the NCC to be equal to a value of a NCC in the unused {NH, NCC} pair; or in the case that the first target CU does not have an unused {NH, NCC} pair, computing the first security key from a current security key used by the first target base station and the UE, and setting the value of the NCC to be equal to a value of a current NCC associated with the current security key.

[0011] In some implementations of the method and apparatuses described herein, the first processor may be configured to: determine that the security update is needed in the case that the target cell is managed by the second target base station; and determine that the security update is not needed in the case that the target cell is managed by the first target base station.

[0012] In some implementations of the method and apparatuses described herein, the processor may further include a second processor of the first target DU, and the second processor may be configured to: transmit, via the transceiver and to the UE, the NCC received from the first target CU, such that the NCC is used by the UE to perform a second security key derivation to determine a second security key to be used between the UE and the second target base station.

[0013] In some implementations of the method and apparatuses described herein, the first processor may be further configured to: transmit, via the transceiver and to the first target DU, a first indicator indicating whether the first target DU is to notify the UE that the security update is needed during the cell switch to the target cell.

[0014] In some implementations of the method and apparatuses described herein, the first indicator may include one of the following: a security update indicator indicating whether the security update is needed; a CU indicator indicating that a CU of the target cell is different from the first target CU; an inter-CU LTM indicator indicating that the cell switch is associated with an inter-CU LTM; or a CU node identifier (ID) indicating an ID of a CU of the target cell.

[0015] In some implementations of the method and apparatuses described herein, the second processor may be further configured to: transmit, via the transceiver and to the UE, a second indicator indicating whether the security update is needed during the cell switch to the target cell, wherein the second indicator is determined by the first target DU based on the first indicator.

[0016] In some implementations of the method and apparatuses described herein, the second indicator may include one of the following: a security update indicator indicating whether the security update is needed; a CU indicator indicating that a CU of the target cell is different from the first target CU; an inter-CU LTM indicator indicating that the cell switch is associated with an inter-CU LTM; and a CU node identifier (ID) indicating an ID of a CU of the target cell.

[0017] In some implementations of the method and apparatuses described herein, the NCC may be transmitted to the UE from the first target base station via a medium access control (MAC) control element (CE).

[0018] In some implementations of the method and apparatuses described herein, the MAC CE may be a LTM cell switch command.

[0019] In some implementations of the method and apparatuses described herein, the second processor may be further configured to: receive, via the transceiver and from the UE, a first security update failure message indicating a failure of the security update.

[0020] In some implementations of the method and apparatuses described herein, the processor may be further configured to: obtain, from an access and mobility management function (AMF), information on security update parameters; and transmit, via the transceiver and to the UE, the obtained information on security update parameters, wherein the information on security update parameters is used by the UE for updating a NH parameter associated with the first security key.

[0021] In some implementations of the method and apparatuses described herein, the information on security update parameters may indicate that a non-access stratum (NAS) security context different from a currently active NAS security context is activated by the AMF.

[0022] In some implementations of the method and apparatuses described herein, the security update parameters may include: a NH indicator indicating the NAS security context different from a currently active NAS security context is activated by the AMF; a ngKSI indicating the NAS security context used for deriving an updated NH parameter; or a downlink NAS COUNT including a NAS SQN and a NAS OVERFLOW, wherein the NAS SQN is a sequence number used for a security key used between the UE and the first target base station, and the NAS OVERFLOW is a

value which is incremented each time the NAS SQN is incremented from the maximum value.

[0023] In some implementations of the method and apparatuses described herein, the information on security update parameters may be transmitted to the UE via a medium access control (MAC) control element (CE) for a LTM cell switch command or a MAC CE for security update.

[0024] In some implementations of the method and apparatuses described herein, the processor may be further configured to: receive, via the transceiver and from the UE, a second security update failure message indicating a failure of updating the NH parameter.

[0025] In some implementations of the method and apparatuses described herein, the second security update failure message may be received via a medium access control (MAC) control element (CE).

[0026] In a second aspect of the solution, a base station comprises: a processor; and a transceiver coupled to the processor, wherein the base station is a first target base station for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), and the processor is configured to: determine whether a security update for LTM is needed; and transmit, via the transceiver, a security update information to a user equipment (UE), based on a result of the determination, wherein the security update information is associated with a first security key to be used between the UE and a second target base station for the LTM.

[0027] In some implementations of the method and apparatuses described herein, the first target base station may include a first target central unit (CU) and one or more distributed units (DUs), the one or more DUs include a first target DU serving the UE, the processor includes a first processor of the first target CU, and the first processor is configured to: receive, from the first target DU, a cell switch decision message indicating a cell switch to a target cell; and determine whether the security update is needed based on the received cell switch decision message.

[0028] In some implementations of the method and apparatuses described herein, the security update information may include a next hop (NH) chaining counter (NCC) to be used for a key derivation for a cell switch by the UE, and the first processor is

configured to: in response to determining that the security update is needed, perform a first security key derivation for determining the first security key and the NCC; and transmit, via the transceiver, the NCC to the first target DU such that the NCC is transmitted to the UE via the first target DU.

[0029] In some implementations of the method and apparatuses described herein, the first processor may be further configured to: transmit, via the transceiver, the first security key and the NCC to the second target base station.

[0030] In some implementations of the method and apparatuses described herein, the first processor may be further configured to: transmit, to the first target DU, a first indicator indicating whether the first target DU is to notify the UE that the security update is needed during the cell switch to the target cell.

[0031] In some implementations of the method and apparatuses described herein, the processor may further include a second processor of the first target DU, and the second processor is configured to: transmit, via the transceiver and to the UE, a second indicator indicating whether the security update is needed during the cell switch to the target cell, wherein the second indicator is determined by the first target DU based on the first indicator.

[0032] In some implementations of the method and apparatuses described herein, the processor may be configured to: determine that the security update is needed in response to obtaining, from an access and mobility management function (AMF), information on security update parameters, wherein the information on security update parameters is used by the UE for updating a next hop (NH) parameter associated with the first security key, wherein the security update information includes the received information on security update parameters.

[0033] In a third aspect of the solution, a processor for wireless communication comprises: at least one memory; and a controller coupled with the at least one memory and configured to cause the processor to: determine, at a first target base station for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), a first security key to be used between a user equipment (UE) and a second target base station for the LTM and a next hop (NH) chaining counter (NCC) to be used for a key derivation for a cell switch by the UE; and transmit, via the transceiver and to the UE, the NCC.

[0034] In a fourth aspect of the solution, a method performed by a first target base station for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), the method comprises: determining a first security key to be used between a user equipment (UE) and a second target base station for the LTM and a next hop (NH) chaining counter (NCC) to be used for a key derivation for a cell switch by the UE; and transmitting the NCC to the UE.

[0035] In a fifth aspect of the solution, a processor for wireless communication comprises: at least one memory; and a controller coupled with the at least one memory and configured to cause the processor to: determine, at a first target base station for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), whether a security update for LTM is needed; and transmit, via a transceiver, a security update information to a user equipment (UE), based on a result of the determination, wherein the security update information is associated with a first security key to be used between the UE and a second target base station for the LTM.

[0036] In a sixth aspect of the solution, a method performed by a first target base station for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), the method comprises: determining whether a security update for LTM is needed; and transmitting a security update information to a user equipment (UE), based on a result of the determination, wherein the security update information is associated with a first security key to be used between the UE and a second target base station for the LTM.

[0037] In a seventh aspect of the solution, a user Equipment (UE) comprises: a processor; and a transceiver coupled to the processor, wherein the processor is configured to: receive, via the transceiver and from a first target base station for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), a next hop (NH) chaining counter (NCC) to be used for a key derivation for a cell switch by the UE; and perform a key derivation by using the NCC to determine a first security key to be used between the UE and a second target base station for the LTM.

[0038] In some implementations of the method and apparatuses described herein, the key derivation may comprise: in the case that a value of the NCC is equal to a value of a current NCC associated with a current security key used by the first target base station and the UE, computing the security key from the current security key; or in the case that the value of the NCC is different from the value of the current NCC, synchronizing a locally kept NH parameter iteratively and increasing the value of the

current NCC, and computing the security key from the synchronized NH parameter in the case that the value of the current NCC matches the value of the NCC received from the first target base station.

[0039] In some implementations of the method and apparatuses described herein, the processor may be further configured to: receive, via the transceiver and from the first target base station, an indicator indicating whether a security update is needed during a cell switch to a target cell, and perform the key derivation in case the indicator indicates that the security update is needed.

[0040] In some implementations of the method and apparatuses described herein, the indicator may include one of the following: a security update indicator indicating whether the security update is needed; a CU indicator indicating that a CU of the target cell is different from the first target CU; an inter-CU LTM indicator indicating that the cell switch is associated with an inter-CU LTM; and a CU node identifier (ID) indicating an ID of a CU of the target cell.

[0041] In some implementations of the method and apparatuses described herein, the NCC may be received by the UE from the first target base station via a medium access control (MAC) control element (CE).

[0042] In some implementations of the method and apparatuses described herein, the MAC CE may be a LTM cell switch command.

[0043] In some implementations of the method and apparatuses described herein, the processor may be further configured to: transmit, via the transceiver and to the first target base station, a first security update failure message indicating a failure of the security update.

[0044] In some implementations of the method and apparatuses described herein, the processor may be further configured to: receive, via the transceiver and from the first target base station, information on security update parameters issued by an access and mobility management function (AMF); and update a NH parameter associated with the first security key based on the information on security update parameters.

[0045] In some implementations of the method and apparatuses described herein, the information on security update parameters may indicate that a non-access stratum

(NAS) security context different from a currently active NAS security context is activated by the AMF.

[0046] In some implementations of the method and apparatuses described herein, the security update parameters may include: a NH indicator indicating the NAS security context different from a currently active NAS security context is activated by the AMF; a ngKSI indicating the NAS security context used for deriving an updated NH parameter; or a downlink NAS COUNT including a NAS SQN and a NAS OVERFLOW, wherein the NAS SQN is a sequence number used for a security key used between the UE and the first target base station, and the NAS OVERFLOW is a value which is incremented each time the NAS SQN is incremented from the maximum value.

[0047] In some implementations of the method and apparatuses described herein, the information on security update parameters may be received by the UE via a medium access control (MAC) control element (CE) for a LTM cell switch command or a MAC CE for security update.

[0048] In some implementations of the method and apparatuses described herein, the processor may be further configured to: transmit, via the transceiver and to the first target base station, a second security update failure message indicating a failure of updating the NH parameter.

[0049] In some implementations of the method and apparatuses described herein, the second security update failure message may be transmitted via a medium access control (MAC) control element (CE).

[0050] In an eighth aspect of the solution, a user equipment (UE) comprises: a processor; and a transceiver coupled to the processor, wherein the processor is configured to: receive, via the transceiver and from a first target base station for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), a security update information; and perform an operation related to a security update for the LTM based on the security update information, wherein the security update information is associated with a first security key to be used between the UE and a second target base station for the LTM.

[0051] In some implementations of the method and apparatuses described herein, the security update information may include a next hop (NH) chaining counter (NCC) to

be used for a key derivation for a cell switch by the UE, and the operation related to the security update includes a key derivation operation for determining the first security key by using the NCC.

[0052] In some implementations of the method and apparatuses described herein, the security update information may further include an indicator indicating whether the security update is needed during a cell switch to a target cell.

[0053] In some implementations of the method and apparatuses described herein, the security update information may include an information on security update parameters used by the UE for updating a next hop (NH) parameter associated with the first security key; and the operation related to the security update includes updating the NH parameter by using the information on security update parameters.

[0054] In a ninth aspect of the solution, a processor for wireless communication comprises: at least one memory; and a controller coupled with the at least one memory and configured to cause the processor to: receive, via a transceiver and from a first target base station for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), a next hop (NH) chaining counter (NCC) to be used for a key derivation for a cell switch by the UE; and perform a key derivation by using the NCC to determine a first security key to be used between the UE and a second target base station for the LTM.

[0055] In a tenth aspect of the solution, a method performed by a user equipment (UE), the method comprises: receiving, from a first target base station for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), a next hop (NH) chaining counter (NCC) to be used for a key derivation for a cell switch by the UE; and performing a key derivation by using the NCC to determine a first security key to be used between the UE and a second target base station for the LTM.

[0056] In an eleventh aspect of the solution, a processor for wireless communication, comprising: at least one memory; and a controller coupled with the at least one memory and configured to cause the processor to: receive, via a transceiver and from a first target base station for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), a security update information; and perform an operation related to a security update for the LTM based on the security update information, wherein the security update information is associated with a first security key to be used between the UE and a second target base station for the LTM.

[0057] In a the twelfth aspect of the solution, a method performed by a user equipment (UE), the method comprises: receiving, from a first target base station for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), a security update information; and performing an operation related to a security update for the LTM based on the security update information, wherein the security update information is associated with a first security key to be used between the UE and a second target base station for the LTM.

[0058] It is to be understood that the summary section is not intended to identify key or essential features of embodiments of the present disclosure, nor is it intended to be used to limit the scope of the present disclosure. Other features of the present disclosure will become easily comprehensible through the following description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0059] FIG. 1 illustrates an example of a wireless communications system that supports a security update for subsequent LTM in accordance with aspects of the present disclosure.

[0060] FIG. 2 illustrates an example concept for LTM and subsequent LTM associated with aspects of the present disclosure.

[0061] FIGS. 3A to 3C illustrate example scenarios of LTM associated with aspects of the present disclosure.

[0062] FIG. 4 illustrates an example key derivation associated with aspects of the present disclosure.

[0063] FIG. 5 illustrates a signalling procedure for a security update for subsequent LTM in accordance with aspects of the present disclosure.

[0064] FIG. 6 illustrates a first example of signalling procedure for the security update for subsequent LTM in accordance with aspects of the present disclosure.

[0065] FIG. 7 illustrates a second example of signalling procedure for the security update for subsequent LTM in accordance with aspects of the present disclosure.

[0066] FIG. 8 illustrates a third example of signalling procedure for the security update for subsequent LTM in accordance with aspects of the present disclosure.

[0067] FIG. 9 illustrates a fourth example of signalling procedure for the security update for subsequent LTM in accordance with aspects of the present disclosure.

[0068] FIGS. 10 to 13 illustrate examples of devices that support the security update for subsequent LTM in accordance with aspects of the present disclosure.

[0069] FIGS. 14 to 17 illustrate examples of processors that support the security update for subsequent LTM in accordance with aspects of the present disclosure.

[0070] FIGS. 18 to 21 illustrate flowcharts of methods that support the security update for subsequent LTM in accordance with aspects of the present disclosure.

DETAILED DESCRIPTION

[0071] Principles of the present disclosure will now be described with reference to some embodiments. It is to be understood that these embodiments are described only for the purpose of illustration and help those skilled in the art to understand and implement the present disclosure, without suggesting any limitation as to the scope of the disclosure. The disclosure described herein may be implemented in various manners other than the ones described below.

[0072] In the following description and claims, unless defined otherwise, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skills in the art to which this disclosure belongs.

[0073] References in the present disclosure to “one embodiment,” “an example embodiment,” “an embodiment,” “some embodiments,” and the like indicate that the embodiment(s) described may include a particular feature, structure, or characteristic, but it is not necessary that every embodiment includes the particular feature, structure, or characteristic. Moreover, such phrases do not necessarily refer to the same embodiment(s). Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to affect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.

[0074] It shall be understood that although the terms “first” and “second” or the like may be used herein to describe various elements, these elements should not be limited by these terms. These terms are only used to distinguish one element from another

element. For example, a first element could also be termed as a second element, and similarly, a second element could also be termed as a first element, without departing from the scope of embodiments. As used herein, the term “and/or” includes any and all combinations of one or more of the listed terms.

[0075] The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of example embodiments. As used herein, the singular forms “a”, “an” and “the” are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms “comprises”, “comprising”, “has”, “having”, “includes” and/or “including”, when used herein, specify the presence of stated features, elements, and/or components etc., but do not preclude the presence or addition of one or more other features, elements, components and/ or combinations thereof.

[0076] As used herein, the term “communication network” refers to a network following any suitable communication standards, such as, 5G new radio (NR), long term evolution (LTE), LTE-advanced (LTE-A), wideband code division multiple access (WCDMA), high-speed packet access (HSPA), narrow band internet of things (NB-IoT), and so on. Further, the communications between a terminal device and a network device in the communication network may be performed according to any suitable generation communication protocols, including but not limited to, the first generation (1G), the second generation (2G), 2.5G, 2.75G, the third generation (3G), the fourth generation (4G), 4.5G, the fifth generation (5G) communication protocols, and/or any other protocols either currently known or to be developed in the future. Embodiments of the present disclosure may be applied in various communication systems. Given the rapid development in communications, there will also be future type communication technologies and systems in which the present disclosure may be embodied. It should not be seen as limiting the scope of the present disclosure to only the aforementioned systems.

[0077] As used herein, the term “network device” generally refers to a node in a communication network via which a terminal device can access the communication network and receive services therefrom. The network device may refer to a base station (BS) or an access point (AP), for example, a node B (NodeB or NB), a radio access network (RAN) node, an evolved NodeB (eNodeB or eNB), a NR NB (also referred to

as a gNB), a remote radio unit (RRU), a radio header (RH), an infrastructure device for a V2X (vehicle-to-everything) communication, a transmission and reception point (TRP), a reception point (RP), a remote radio head (RRH), a relay, an integrated access and backhaul (IAB) node, a low power node such as a femto BS, a pico BS, and so forth, depending on the applied terminology and technology.

[0078] As used herein, the term “terminal device” generally refers to any end device that may be capable of wireless communications. By way of example rather than a limitation, a terminal device may also be referred to as a communication device, a user equipment (UE), an end user device, a subscriber station (SS), an unmanned aerial vehicle (UAV), a portable subscriber station, a mobile station (MS), or an access terminal (AT). The terminal device may include, but is not limited to, a mobile phone, a cellular phone, a smart phone, a voice over IP (VoIP) phone, a wireless local loop phone, a tablet, a wearable terminal device, a personal digital assistant (PDA), a portable computer, a desktop computer, an image capture terminal device such as a digital camera, a gaming terminal device, a music storage and playback appliance, a vehicle-mounted wireless terminal device, a wireless endpoint, a mobile station, laptop-embedded equipment (LEE), laptop-mounted equipment (LME), a USB dongle, a smart device, wireless customer-premises equipment (CPE), an internet of things (IoT) device, a watch or other wearable, a head-mounted display (HMD), a vehicle, a drone, a medical device (for example, a remote surgery device), an industrial device (for example, a robot and/or other wireless devices operating in an industrial and/or an automated processing chain contexts), a consumer electronics device, a device operating on commercial and/or industrial wireless networks, and the like. In the following description, the terms: “terminal device,” “communication device,” “terminal,” “user equipment” and “UE,” may be used interchangeably.

[0079] As discussed above, when a UE moves from one cell to another cell, at some point, a serving cell change needs to be performed. In the legacy, the serving cell change is performed by explicit RRC reconfiguration signalling to trigger a synchronization of target cell based on L3 measurement reports. It leads to longer latency, larger overhead, and longer interruption time than beam-level mobility.

[0080] In the 3rd generation partnership project (3GPP), a new work item on further new radio (NR) mobility enhancements, named as layer 1/layer 2 (L1/L2)-triggered

mobility (LTM), was approved to change a serving cell via L1/L2 signalling, in order to reduce the latency, overhead and interruption time during a cell switch.

[0081] There are two definitions related to LTM, i.e., LTM and subsequent LTM. The LTM refers to a PCell (a primary cell of a master cell group) or PSCell (a primary cell of a secondary cell group) cell switch procedure that triggers via a medium access control (MAC) control element (CE) based on L1 measurements. The subsequent LTM refers to subsequent LTM cell switch procedures between candidate cells where the UE does not need to be reconfigured by the network.

[0082] FIG. 2 illustrates an example concept for LTM and subsequent LTM associated with aspects of the present disclosure.

[0083] In the LTM, when a UE connects to a source DU, the source CU corresponding to the source DU prepares all the candidate cell configurations within several candidate DUs (for example, 8 candidate DUs) and provides them to the UE through RRC signalling. As shown in FIG.2, for example, the LTM refers to a mobility from the source DU to a candidate DU1, the subsequent LTM refers to a mobility from the candidate DU1 to a candidate DU2, or a mobility from the candidate DU1 back to the source DU, without any further RRC signalling (e.g., RRCReconfiguration).

[0084] The potential applicable scenarios of LTM include intra-CU intra-DU LTM, intra-CU inter-DU LTM, and inter-CU LTM.

[0085] FIGS. 3A to 3C illustrate example scenarios of LTM associated with aspects of the present disclosure. FIG. 3A shows a scenario for intra-CU intra-DU LTM, FIG. 3B shows a scenario for intra-CU inter-DU LTM, and FIG. 3C shows a scenario for inter-CU inter-DU LTM.

[0086] As shown in FIG.3A, in the scenario for intra-CU intra-DU LTM, the UE moves between different cells within the same DU. As shown in FIG. 3B, in the scenario for intra-CU inter-DU LTM, the UE moves between different cells belonging to different DUs but within the same CU. As shown in FIG. 3C, in the scenario for inter-CU LTM, the UE moves between different cells belonging to different DUs, where the different DUs belong to different CUs.

[0087] FIG. 4 illustrates an example key derivation associated with aspects of the present disclosure.

[0088] With reference to FIG.4, a key used in above security related functions are organised and derived as follows:

- Key for access and mobility management function (AMF):
 - K_{AMF} is a key derived by mobile equipment (ME) and security anchor function (SEAF) from K_{SEAF} .
- Keys for NAS signalling:
 - K_{NASint} is a key derived by ME and AMF from K_{AMF} , which shall only be used for the protection of NAS signalling with a particular integrity algorithm;
 - K_{NASenc} is a key derived by ME and AMF from K_{AMF} , which shall only be used for the protection of NAS signalling with a particular encryption algorithm.

Key for gNB:

- K_{gNB} is a key derived by ME and AMF from K_{AMF} . K_{gNB} is further derived by ME and source gNB when performing horizontal or vertical key derivation.

Keys for UP traffic:

- K_{UPenc} is a key derived by ME and gNB from K_{gNB} , which shall only be used for the protection of UP traffic between ME and gNB with a particular encryption algorithm;
- K_{UPint} is a key derived by ME and gNB from K_{gNB} , which shall only be used for the protection of UP traffic between ME and gNB with a particular integrity algorithm.

Keys for RRC signalling:

- K_{RRCint} is a key derived by ME and gNB from K_{gNB} , which shall only be used for the protection of RRC signalling with a particular integrity algorithm;
- K_{RRCenc} is a key derived by ME and gNB from K_{gNB} , which shall only be used for the protection of RRC signalling with a particular encryption algorithm.

Intermediate keys:

- NH is a key derived by ME and AMF to provide forward security.
- K_{gNB}^* is a key derived by ME and gNB when performing a horizontal or vertical key derivation.

[0089] As described above, the primary authentication enables mutual authentication between the UE and the network and provide an anchor key called K_{SEAF} . From K_{SEAF} , K_{AMF} is created during e.g. primary authentication or NAS key re-keying and key refresh events. Based on K_{AMF} , K_{NASint} and K_{NASenc} are then derived when running a successful NAS security mode command (SMC) procedure.

[0090] Whenever an initial AS security context needs to be established between UE and gNB, the AMF and the UE derive a K_{gNB} and a next hop (NH) parameter. The K_{gNB} and the NH are derived from the K_{AMF} . A NH Chaining Counter (NCC) is associated with each K_{gNB} and NH parameter. Every K_{gNB} is associated with the NCC corresponding to the NH value from which it was derived. At initial setup, the K_{gNB} is derived directly from K_{AMF} , and is then considered to be associated with a virtual NH parameter with NCC value equal to zero. At initial setup, the derived NH value is associated with the NCC value one. On handovers, the basis for the K_{gNB} that will be used between the UE and the target gNB, called K_{gNB}^* , is derived from either the currently active K_{gNB} or from the NH parameter. If K_{gNB}^* is derived from the currently active K_{gNB} , this is referred to as a horizontal key derivation and is indicated to UE with an NCC that does not increase. If the K_{gNB}^* is derived from the NH parameter, the derivation is referred to as a vertical key derivation and is indicated to UE with an NCC increase. Finally, K_{RRCint} , K_{RRCenc} , K_{UPint} and K_{UPenc} are derived based on K_{gNB} after a new K_{gNB} is derived.

[0091] With such key derivation, a gNB with knowledge of a K_{gNB} , shared with a UE, is unable to compute any previous K_{gNB} that has been used between the same UE and a previous gNB, therefore providing backward security. Similarly, a gNB with knowledge of a K_{gNB} , shared with a UE, is unable to predict any future K_{gNB} that will be used between the same UE and another gNB after n or more handovers (since NH parameters are only computable by the UE and the AMF).

[0092] The AS SMC procedure is for RRC and user plane (UP) security algorithms negotiation and RRC security activation. When AS security context is to be established in the gNB, the AMF sends the complete UE 5G security capabilities to the gNB (i.e., all bits for every capability defined in TS 24.501 [28] and received in NAS signalling). At handover (or at UE Context retrieval), the complete UE 5G security capabilities are also sent by the source gNB to the target gNB (or by the last serving gNB to the receiving gNB respectively). The gNB chooses the ciphering algorithm which has the highest priority from its configured list and is also present in the UE 5G security capabilities. The gNB also chooses the integrity algorithm which has the highest priority from its configured list and is also present in the UE 5G security capabilities. The chosen algorithms are indicated to the UE in the AS SMC message and this message is integrity protected. RRC downlink ciphering (encryption) at the gNB starts after

sending the AS SMC message. RRC uplink deciphering (decryption) at the gNB starts after receiving and successful verification of the integrity protected AS security mode complete message from the UE. The UE verifies the validity of the AS SMC message from the gNB by verifying the integrity of the received message. RRC uplink ciphering (encryption) at the UE starts after sending the AS security mode complete message. RRC downlink deciphering (decryption) at the UE shall start after receiving and successful verification of the AS SMC message. The RRC Connection Reconfiguration procedure used to add data radio bearers (DRBs) shall be performed only after RRC security has been activated as part of the AS SMC procedure.

[0093] A UE connected to 5GC, shall support integrity protected DRBs at any data rate, up to and including the highest data rate supported by the UE for both uplink (UL) and downlink (DL). In case of failed integrity check (i.e. faulty or missing MAC-I), the concerned PDU shall be discarded by the receiving PDCP entity.

[0094] Key refresh is possible for K_{gNB} , $K_{RRCCenc}$, $K_{RRCCint}$, K_{UPenc} , and K_{UPint} and can be initiated by the gNB when a PDCP COUNTs are about to be re-used with the same Radio Bearer identity and with the same K_{gNB} . Key re-keying is also possible for the K_{gNB} , $K_{RRCCenc}$, $K_{RRCCint}$, K_{UPenc} , and K_{UPint} and can be initiated by the AMF when a 5G AS security context different from the currently active one shall be activated.

[0095] When the UE moves to a new cell with the change of PDCP anchor, the UE and the network shall obtain a new key for the security update. For the intra-CU LTM (including intra-CU intra-DU LTM and intra-CU inter-DU LTM), no security update is needed due to the unchanged PDCP anchor. However, for the inter-CU LTM, since the PDCP anchor relocation happens, the security update shall be performed.

[0096] Considering the security update for LTM, there are several issues should be considered as follows. The first issue is, for the subsequent inter-CU LTM (e.g., the UE moves from a candidate CU1 to another candidate CU2, or the UE moves from a candidate CU1 back to the source CU), there is not RRCReconfiguration message between the UE and the candidate CU. It is unclear how to synchronize the key between the UE and the candidate CU2 or the source CU.

[0097] The second issue is that no security update is needed for intra-CU LTM, but security update is mandatory for inter-CU LTM. It is unclear how to support the subsequent LTM for hybrid inter-CU LTM and intra-CU LTM cases. The third issue is

when the AMF has a new NAS security context, it shall derive a new NH parameter with a new NCC value equal to zero. It is unclear how to support the activation of the new NH by the UE for subsequent inter-CU LTM. Thus, it needs a solution to solve above issues to support subsequent LTM.

[0098] The present disclosure proposed a solution to support a security update for subsequent LTM, for example, for subsequent inter-CU LTM. In this solution, a security update information associated with a security key to be used between the UE and a target base station (for example, the candidate CU2 or the source CU mentioned above) for the subsequent LTM is introduced to facilitate the security update in at UE side and the target base station side. By implementing the example embodiments of the present disclosure, a security update for subsequent LTM may be realized.

[0099] Aspects of the present disclosure are described in the context of a wireless communications system.

[0100] FIG. 1 illustrates an example of a wireless communications system that supports a security update for subsequent LTM in accordance with aspects of the present disclosure. The wireless communications system 100 may include one or more network entities 102 (also referred to as network equipment (NE)), one or more UEs 104, a core network 106, and a packet data network 108. The wireless communications system 100 may support various radio access technologies. In some implementations, the wireless communications system 100 may be a 4G network, such as an LTE network or an LTE-advanced (LTE-A) network. In some other implementations, the wireless communications system 100 may be a 5G network, such as an NR network. In other implementations, the wireless communications system 100 may be a combination of a 4G network and a 5G network, or other suitable radio access technology including institute of electrical and electronics engineers (IEEE) 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20. The wireless communications system 100 may support radio access technologies beyond 5G. Additionally, the wireless communications system 100 may support technologies, such as time division multiple access (TDMA), frequency division multiple access (FDMA), or code division multiple access (CDMA), etc.

[0101] The one or more network entities 102 may be dispersed throughout a geographic region to form the wireless communications system 100. One or more of the network entities 102 described herein may be or include or may be referred to as a

network node, a base station, a network element, a radio access network (RAN), a base transceiver station, an access point, a NodeB, an eNodeB (eNB), a next-generation NodeB (gNB), or other suitable terminology. A network entity 102 and a UE 104 may communicate via a communication link 110, which may be a wireless or wired connection. For example, a network entity 102 and a UE 104 may perform wireless communication (e.g., receive signaling, transmit signaling) over a Uu interface.

[0102] A network entity 102 may provide a geographic coverage area 112 for which the network entity 102 may support services (e.g., voice, video, packet data, messaging, broadcast, etc.) for one or more UEs 104 within the geographic coverage area 112. For example, a network entity 102 and a UE 104 may support wireless communication of signals related to services (e.g., voice, video, packet data, messaging, broadcast, etc.) according to one or multiple radio access technologies. In some implementations, a network entity 102 may be moveable, for example, a satellite associated with a non-terrestrial network. In some implementations, different geographic coverage areas 112 associated with the same or different radio access technologies may overlap, but the different geographic coverage areas 112 may be associated with different network entities 102. Information and signals described herein may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

[0103] The one or more UEs 104 may be dispersed throughout a geographic region of the wireless communications system 100. A UE 104 may include or may be referred to as a mobile device, a wireless device, a remote device, a remote unit, a handheld device, or a subscriber device, or some other suitable terminology. In some implementations, the UE 104 may be referred to as a unit, a station, a terminal, or a client, among other examples. Additionally, or alternatively, the UE 104 may be referred to as an internet-of-things (IoT) device, an internet-of-everything (IoE) device, or machine-type communication (MTC) device, among other examples. In some implementations, a UE 104 may be stationary in the wireless communications system 100. In some other implementations, a UE 104 may be mobile in the wireless communications system 100.

[0104] The one or more UEs 104 may be devices in different forms or having different capabilities. Some examples of UEs 104 are illustrated in FIG. 1. A UE 104 may be capable of communicating with various types of devices, such as the network entities 102, other UEs 104, or network equipment (e.g., the core network 106, the packet data network 108, a relay device, an integrated access and backhaul (IAB) node, or another network equipment), as shown in FIG. 1. Additionally, or alternatively, a UE 104 may support communication with other network entities 102 or UEs 104, which may act as relays in the wireless communications system 100.

[0105] A UE 104 may also be able to support wireless communication directly with other UEs 104 over a communication link 114. For example, a UE 104 may support wireless communication directly with another UE 104 over a device-to-device (D2D) communication link. In some implementations, such as vehicle-to-vehicle (V2V) deployments, vehicle-to-everything (V2X) deployments, or cellular-V2X deployments, the communication link 114 may be referred to as a sidelink. For example, a UE 104 may support wireless communication directly with another UE 104 over a PC5 interface.

[0106] A network entity 102 may support communications with the core network 106, or with another network entity 102, or both. For example, a network entity 102 may interface with the core network 106 through one or more backhaul links 116 (e.g., via an S1, N2, N2, or another network interface). The network entities 102 may communicate with each other over the backhaul links 116 (e.g., via an X2, Xn, or another network interface). In some implementations, the network entities 102 may communicate with each other directly (e.g., between the network entities 102). In some other implementations, the network entities 102 may communicate with each other or indirectly (e.g., via the core network 106). In some implementations, one or more network entities 102 may include subcomponents, such as an access network entity, which may be an example of an access node controller (ANC). An ANC may communicate with the one or more UEs 104 through one or more other access network transmission entities, which may be referred to as a radio heads, smart radio heads, or transmission-reception points (TRPs).

[0107] In some implementations, a network entity 102 may be configured in a disaggregated architecture, which may be configured to utilize a protocol stack physically or logically distributed among two or more network entities 102, such as an

integrated access backhaul (IAB) network, an open radio access network (O-RAN) (e.g., a network configuration sponsored by the O-RAN Alliance), or a virtualized RAN (vRAN) (e.g., a cloud RAN (C-RAN)). For example, a network entity 102 may include one or more of a CU, a DU, a radio unit (RU), a RAN intelligent controller (RIC) (e.g., a near-real time RIC (Near-RT RIC), a non-real time RIC (Non-RT RIC)), a service management and orchestration (SMO) system, or any combination thereof.

[0108] An RU may also be referred to as a radio head, a smart radio head, a remote radio head (RRH), a remote radio unit (RRU), or a transmission reception point (TRP). One or more components of the network entities 102 in a disaggregated RAN architecture may be co-located, or one or more components of the network entities 102 may be located in distributed locations (e.g., separate physical locations). In some implementations, one or more network entities 102 of a disaggregated RAN architecture may be implemented as virtual units (e.g., a virtual CU (VCU), a virtual DU (VDU), a virtual RU (VRU)).

[0109] Split of functionality between a CU, a DU, and an RU may be flexible and may support different functionalities depending upon which functions (e.g., network layer functions, protocol layer functions, baseband functions, radio frequency functions, and any combinations thereof) are performed at a CU, a DU, or an RU. For example, a functional split of a protocol stack may be employed between a CU and a DU such that the CU may support one or more layers of the protocol stack and the DU may support one or more different layers of the protocol stack. In some implementations, the CU may host upper protocol layer (e.g., a layer 3 (L3), a layer 2 (L2)) functionality and signaling (e.g., radio resource control (RRC), service data adaptation protocol (SDAP), packet data convergence protocol (PDCP)). The CU may be connected to one or more DUs or RUs, and the one or more DUs or RUs may host lower protocol layers, such as a layer 1 (L1) (e.g., physical (PHY) layer) or an L2 (e.g., radio link control (RLC) layer, medium access control (MAC) layer) functionality and signaling, and may each be at least partially controlled by the CU 160.

[0110] Additionally, or alternatively, a functional split of the protocol stack may be employed between a DU and an RU such that the DU may support one or more layers of the protocol stack and the RU may support one or more different layers of the protocol stack. The DU may support one or multiple different cells (e.g., via one or

more RUs). In some implementations, a functional split between a CU and a DU, or between a DU and an RU may be within a protocol layer (e.g., some functions for a protocol layer may be performed by one of a CU, a DU, or an RU, while other functions of the protocol layer are performed by a different one of the CU, the DU, or the RU).

[0111] A CU may be functionally split further into CU control plane (CU-CP) and CU user plane (CU-UP) functions. A CU may be connected to one or more DUs via a midhaul communication link (e.g., F1, F1-c, F1-u), and a DU may be connected to one or more RUs via a fronthaul communication link (e.g., open fronthaul (FH) interface). In some implementations, a midhaul communication link or a fronthaul communication link may be implemented in accordance with an interface (e.g., a channel) between layers of a protocol stack supported by respective network entities 102 that are in communication via such communication links.

[0112] The core network 106 may support user authentication, access authorization, tracking, connectivity, and other access, routing, or mobility functions. The core network 106 may be an evolved packet core (EPC), or a 5G core (5GC), which may include a control plane entity that manages access and mobility (e.g., a mobility management entity (MME), an access and mobility management functions (AMF)) and a user plane entity that routes packets or interconnects to external networks (e.g., a serving gateway (S-GW), a packet data network (PDN) gateway (P-GW), or a user plane function (UPF)). In some implementations, the control plane entity may manage non-access stratum (NAS) functions, such as mobility, authentication, and bearer management (e.g., data bearers, signal bearers, etc.) for the one or more UEs 104 served by the one or more network entities 102 associated with the core network 106.

[0113] The core network 106 may communicate with the packet data network 108 over one or more backhaul links 116 (e.g., via an S1, N2, N2, or another network interface). The packet data network 108 may include an application server 118. In some implementations, one or more UEs 104 may communicate with the application server 118. A UE 104 may establish a session (e.g., a protocol data unit (PDU) session, or the like) with the core network 106 via a network entity 102. The core network 106 may route traffic (e.g., control information, data, and the like) between the UE 104 and the application server 118 using the established session (e.g., the established PDU session).

The PDU session may be an example of a logical connection between the UE 104 and the core network 106 (e.g., one or more network functions of the core network 106).

[0114] In the wireless communications system 100, the network entities 102 and the UEs 104 may use resources of the wireless communications system 100 (e.g., time resources (e.g., symbols, slots, subframes, frames, or the like) or frequency resources (e.g., subcarriers, carriers)) to perform various operations (e.g., wireless communications). In some implementations, the network entities 102 and the UEs 104 may support different resource structures. For example, the network entities 102 and the UEs 104 may support different frame structures. In some implementations, such as in 4G, the network entities 102 and the UEs 104 may support a single frame structure. In some other implementations, such as in 5G and among other suitable radio access technologies, the network entities 102 and the UEs 104 may support various frame structures (i.e., multiple frame structures). The network entities 102 and the UEs 104 may support various frame structures based on one or more numerologies.

[0115] One or more numerologies may be supported in the wireless communications system 100, and a numerology may include a subcarrier spacing and a cyclic prefix. A first numerology (e.g., $\mu=0$) may be associated with a first subcarrier spacing (e.g., 15 kHz) and a normal cyclic prefix. In some implementations, the first numerology (e.g., $\mu=0$) associated with the first subcarrier spacing (e.g., 15 kHz) may utilize one slot per subframe. A second numerology (e.g., $\mu=1$) may be associated with a second subcarrier spacing (e.g., 30 kHz) and a normal cyclic prefix. A third numerology (e.g., $\mu=2$) may be associated with a third subcarrier spacing (e.g., 60 kHz) and a normal cyclic prefix or an extended cyclic prefix. A fourth numerology (e.g., $\mu=3$) may be associated with a fourth subcarrier spacing (e.g., 120 kHz) and a normal cyclic prefix. A fifth numerology (e.g., $\mu=4$) may be associated with a fifth subcarrier spacing (e.g., 240 kHz) and a normal cyclic prefix.

[0116] A time interval of a resource (e.g., a communication resource) may be organized according to frames (also referred to as radio frames). Each frame may have a duration, for example, a 10 millisecond (ms) duration. In some implementations, each frame may include multiple subframes. For example, each frame may include 10 subframes, and each subframe may have a duration, for example, a 1 ms duration. In

some implementations, each frame may have the same duration. In some implementations, each subframe of a frame may have the same duration.

[0117] Additionally or alternatively, a time interval of a resource (e.g., a communication resource) may be organized according to slots. For example, a subframe may include a number (e.g., quantity) of slots. The number of slots in each subframe may also depend on the one or more numerologies supported in the wireless communications system 100. For instance, the first, second, third, fourth, and fifth numerologies (i.e., $\mu=0$, $\mu=1$, $\mu=2$, $\mu=3$, $\mu=4$) associated with respective subcarrier spacings of 15 kHz, 30 kHz, 60 kHz, 120 kHz, and 240 kHz may utilize a single slot per subframe, two slots per subframe, four slots per subframe, eight slots per subframe, and 16 slots per subframe, respectively. Each slot may include a number (e.g., quantity) of symbols (e.g., OFDM symbols). In some implementations, the number (e.g., quantity) of slots for a subframe may depend on a numerology. For a normal cyclic prefix, a slot may include 14 symbols. For an extended cyclic prefix (e.g., applicable for 60 kHz subcarrier spacing), a slot may include 12 symbols. The relationship between the number of symbols per slot, the number of slots per subframe, and the number of slots per frame for a normal cyclic prefix and an extended cyclic prefix may depend on a numerology. It should be understood that reference to a first numerology (e.g., $\mu=0$) associated with a first subcarrier spacing (e.g., 15 kHz) may be used interchangeably between subframes and slots.

[0118] In the wireless communications system 100, an electromagnetic (EM) spectrum may be split, based on frequency or wavelength, into various classes, frequency bands, frequency channels, etc. By way of example, the wireless communications system 100 may support one or multiple operating frequency bands, such as frequency range designations FR1 (410 MHz – 7.125 GHz), FR2 (24.25 GHz – 52.6 GHz), FR3 (7.125 GHz – 24.25 GHz), FR4 (52.6 GHz – 114.25 GHz), FR4a or FR4-1 (52.6 GHz – 71 GHz), and FR5 (114.25 GHz – 300 GHz). In some implementations, the network entities 102 and the UEs 104 may perform wireless communications over one or more of the operating frequency bands. In some implementations, FR1 may be used by the network entities 102 and the UEs 104, among other equipment or devices for cellular communications traffic (e.g., control information, data). In some implementations, FR2 may be used by the network entities 102 and the UEs 104, among other equipment or devices for short-range, high data rate capabilities.

[0119] FR1 may be associated with one or multiple numerologies (e.g., at least three numerologies). For example, FR1 may be associated with a first numerology (e.g., $\mu=0$), which includes 15 kHz subcarrier spacing; a second numerology (e.g., $\mu=1$), which includes 30 kHz subcarrier spacing; and a third numerology (e.g., $\mu=2$), which includes 60 kHz subcarrier spacing. FR2 may be associated with one or multiple numerologies (e.g., at least 2 numerologies). For example, FR2 may be associated with a third numerology (e.g., $\mu=2$), which includes 60 kHz subcarrier spacing; and a fourth numerology (e.g., $\mu=3$), which includes 120 kHz subcarrier spacing.

[0120] FIG. 5 illustrates an example signalling procedure 500 for a security update for subsequent LTM in accordance with aspects of the present disclosure. As shown in FIG. 5, a first target base station 102-1 determines, at step 502, whether a security update for LTM is needed. In some example embodiments, the first target base station 102-1 may be a base station for LTM (i.e., supporting LTM), and it may be, for example, a gNB, or other kinds of base station applicable for LTM. In present disclosure, the first target base station may be different from a source base station from which the UE receives the RRC message (e.g., RRCReconfiguration) for LTM.

[0121] In some example embodiments, the first target base station 102-1 may include a first target CU (also referred as candidate CU 1 as described above) and one or more DUs, the one or more DUs include a first target DU (also referred as candidate DU 1 as described above) serving a UE 104. In some example embodiments, the first target CU may receive, from the first target DU, a cell switch decision message indicating a cell switch to a target cell, and then determine whether the security update is needed based on the received cell switch decision message. In some example embodiments, the first target CU may determine that the security update is needed in response to obtaining, from an access and mobility management function (AMF) located in core network 106, information on security update parameters.

[0122] At step 504, the first target base station 102-1 may transmit a security update information to the UE 104, based on a result of the determination at step 502. For example, the first target base station 102-1 may transmit the security update information to the UE 104 in response to determining that the security update is needed. The UE 104 may receive, at step 506, the security update information, and perform, at step 508, an

operation related to a security update for the LTM based on the security update information.

[0123] In some example embodiments, the security update information may be associated with a first security key to be used between the UE and a second target base station. In present disclosure, the second target base station may also be a base station for LTM (i.e., supporting LTM), and it may be, for example, a gNB, or other kinds of base station applicable for LTM. In some example embodiments, the second target base station may also be a source base station from which the UE receives the RRC message (e.g., RRCReconfiguration) for LTM.

[0124] In some example embodiments, the security update information may include, for example, a NCC to be used for a key derivation for a cell switch by the UE, the NCC may be determined via a first key derivation by the first target CU in response to determining that the security update is needed. In such case, the NCC is transmitted to the first target DU first and then is forwarded to the UE via the first target DU, and the operation related to the security update performed by the UE 104 may include a key derivation operation for determining the first security key by using the NCC. A detailed description for this case will be described below with reference to FIGS. 6 to 8.

[0125] In some example embodiments, the security update information may include the information on security update parameters obtained from the AMF, and the information on security update parameters may be used by the UE for updating a NH parameter associated with the first security key. In such case, the operation related to the security update may include updating the NH parameter by using the information on security update parameters. A detailed description for this case will be described below with reference to FIG. 9.

[0126] Hereafter, further detailed descriptions regarding the security update for subsequent LTM are illustrated in FIGS. 6 to 9. FIG. 6 illustrates a first example of signalling procedure 600 for a security update for subsequent LTM in accordance with aspects of the present disclosure. In present disclosure, FIG. 6 is for the security update for subsequent LTM without a new NAS security context.

[0127] As shown in FIG. 6, a first target base station 102-1 may determine, at step 602, a first security key to be used between a UE 104 and a second target base station and a NCC to be used for a key derivation for a cell switch by the UE 104. Herein, both

the first target base station 102-1 and the second target base station may be base stations for LTM (i.e., supporting LTM), and they may be, for example, gNBs, or other kinds of base stations applicable for LTM.

[0128] At step 604, the first target base station 102-1 may transmit the NCC to the UE 104. The UE 104 may receive, at step 606, the NCC from the first target base station 102-1 and perform, at step 608, a key derivation by using the NCC to determine a first security key to be used between the UE 104 and a second target base station.

[0129] Hereafter, a detailed description regarding steps 602-608 in procedure 600 is explained with reference to FIGS. 7 and 8. FIG. 7 illustrates a second example of signalling procedure 700 for a security update for subsequent LTM in accordance with aspects of the present disclosure. FIG. 7 is for the security update for subsequent LTM without a new NAS security context.

[0130] As shown in FIG. 7, the signalling procedure 700 involves a UE 104, a first target base station 102-1 and a second target base station 102-2. Herein, both the first target base station 102-1 and the second target base station 102-2 may be base stations for LTM (i.e., supporting LTM), and they may be, for example, gNBs, or other kinds of base stations applicable for LTM.

[0131] In some example embodiments, the first target base station 102-1 may include a first target CU 102-10 and one or more DUs, the one or more DUs include a first target DU (also referred as candidate DU 1 as described above) 102-11 serving the UE 104. The second target base station 102-2 may include a second target CU 102-20.

[0132] In some example embodiments, at step 702, the first target DU 102-11 may determine to perform a cell switch to a target cell, e.g., based on L1 measurement reports of the candidate cells received from the UE 104, that is, make a LTM cell switch decision. Then at step 704, the first target DU 102-11 may signal the first target CU 102-10 about the LTM cell switch decision by sending a cell switch decision message indicating the cell switch to the target cell, e.g. a UE Context Modification Required message including the target cell, a LTM Cell Change Notification message, or other messages that may indicate the cell switch.

[0133] The first target CU 102-10 may receive, at step 706, from the first target DU 102-11, the cell switch decision message, and determine whether a security update is needed based on the received cell switch decision message.

[0134] In some example embodiments, the first target CU 102-10 may determine that the security update is not needed in the case that the target cell is managed by the first target base station, and in such case, the first target CU 102-10 will do not perform a first key derivation. In some example embodiments, the first target CU 102-10 may determine that the security update is needed in the case that the target cell is managed by the second target base station, and in such case, the first target CU 102-10 will perform the first security key derivation.

[0135] In response to determining that the security update is needed, the first target CU 102-10 may perform, at step 708, a first security key derivation for determining the first security key (i.e., K_{gNB2}^*) and the NCC for LTM cell switch. In present disclosure, the step 708 corresponds to step 602 in FIG. 6.

[0136] In some example embodiments, for the first security key derivation, in the case that the first target CU 102-10 has an unused {NH, NCC} pair, the first target CU 102-10 may compute the first security key (i.e., K_{gNB2}^*) from the NH, and set a value of the NCC to be equal to a value of a NCC in the unused {NH, NCC} pair; otherwise in the case that the first target CU does not have an unused {NH, NCC} pair, the first target CU 102-10 may compute the first security key (i.e., K_{gNB2}^*) from a current security key (i.e., K_{gNB1}) used by the first target base station and the UE, and set the value of the NCC to be equal to a value of a current NCC associated with the current security key (i.e., K_{gNB1}).

[0137] Thereafter, the first target CU 102-10 may transmit, at step 710, the NCC to the first target DU 102-11 such that the NCC could be transmitted to the UE 104 via the first target DU 102-11. The first target CU 102-10 may further transmit, at step 724, the first security key and the NCC to the second target CU 102-20, thus at step 726, the NCC is received by the second target CU 102-20. The order of step 710 and step 724 may be different from that shown in FIG. 7. For example, step 710 may be performed before step 724, or step 710 and step 724 may be performed simultaneously.

[0138] In some example embodiments, the first target CU 102-10 may signal the NCC to the first target DU 102-11 by sending a UE Context Modification Confirm

message as shown in FIG. 7. However, the first target CU 102-10 may send the NCC to the first target DU102-11 via other messages, e.g., UE Context Modification Request message. In some example embodiments, the first target CU 102-10 may transmit the first security key and the NCC, i.e., $\{K_{gNB2}^*, NCC\}$ pair, to the second target CU 102-20 via a UE-associated signalling, e.g., Security Information Notification message as shown in FIG. 7.

[0139] The first target DU 102-11 may receive, at step 712, the NCC from the first target CU 102-10, and may transmit, at step 714, the NCC received from the first target CU 102-10 to the UE 104, such that the NCC may be used by the UE 104 to perform a second security key derivation to determine a second security key to be used between the UE and the second target base station.

[0140] In some example embodiments, the NCC is transmitted to the UE 104 from the first target base station 102-1 (particularly, the first target DU 102-11) via a MAC CE, and the MAC CE may be a LTM cell switch command, that is, the NCC may be included in the LTM cell switch command. However, it is to be understood by those skilled in the art that the NCC may also be transmitted to the UE 104 via messages other than the LTM cell switch command. The UE 104 may receive the NCC from the first target DU 102-11(e.g., via a MAC CE) at step 716 and perform the second security key derivation by using the received NCC at step 718.

[0141] In some example embodiments, for the second key derivation, in the case that a value of the NCC is equal to a value of a current NCC associated with a current security key (i.e., K_{gNB1}) used by the first target base station 102-1 and the UE 104, the UE 104 may compute first security key (i.e. K_{gNB2}^*) from the current security key (i.e., K_{gNB1}); otherwise in the case that the value of the NCC is different from the value of the current NCC, the UE 104 may synchronize a locally kept NH parameter iteratively and increase the value of the current NCC, and compute the first security key(i.e. K_{gNB2}^*) from the synchronized NH parameter in the case that the value of the current NCC matches the value of the NCC received from the first target base station.

[0142] However, if the UE 104 do not receive the NCC, for example, if the NCC is not included in the MAC CE, the UE 104 will not perform the second key derivation, that is, the UE 104 will use the current security key (i.e., K_{gNB1}) when it connects to the target cell. If the security update fails, for example, the security key derived by the UE

104 at step 718 may be different from the first security key transmitted to the second target CU 102-20 at step 724, the UE 104 may, at step 720, transmit a first security update failure message indicating a failure of the security update, e.g., via a MAC CE, to the first target DU 102-11. Thereby the first target DU 102-11 will receive, at step 722, the first security update failure message indicating a failure of the security update from the UE 104. In some example embodiments, the first target DU 102-11 may transmit a third security update failure message indicating a failure of the security update to the first target CU 102-10, which is not shown in FIG. 7. In some example embodiments, the first target DU 102-11 may forward the first security update failure message indicating a failure of the security update to the first target CU 102-10, which is not shown in FIG. 7.

[0143] FIG. 8 illustrates a second example of signalling procedure 800 for a security update for subsequent LTM in accordance with aspects of the present disclosure. FIG. 8 is also for the security update for subsequent LTM without a new NAS security context. As shown in FIG. 8, some steps in FIG. 8 are the same to those in FIG. 7, e.g., steps 802 to 808, and 818 to 826 correspond to steps 702 to 708, and 718 to 726, respectively. Thus, the description regarding these steps will be omitted for concision and only the steps different from those in FIG. 7 will be described in detail as below.

[0144] With reference to FIG. 8, if the first target CU 102-10 determines that a security update is needed at step 806, and performs the first security key derivation at step 808, it may transmit, at step 810, and to the first target DU 102-11, a first indicator indicating whether the first target DU 102-11 is to notify the UE 104 that the security update is needed during the cell switch to the target cell.

[0145] In some example embodiments, the first indicator may be transmitted to the first target DU 102-11 together with the NCC at step 810 as shown in FIG. 8. For example, the first target CU 102-10 may transmit the NCC along with the first indicator to the first target DU 102-11 via the UE Context Modification Confirm message as shown in FIG. 8. However, the first target CU 102-10 may also transmit the NCC along with the first indicator to the first target DU 102-11 via other messages, e.g., UE Context Modification Request message. As another example, the first target CU 102-10 may transmit the first indicator to the first target DU 102-11 separately from the NCC, e.g., via a different message from the message including the NCC.

[0146] In some example embodiments, the first indicator may include a security update indicator, a CU indicator, an inter-CU LTM indicator, or a CU node identifier (ID). For instance, the security update indicator can indicate whether the security update is needed, and for example, if the security update indicator is set to TRUE or 1, the first target DU 102-11 is to notify the UE 104 that the security update is needed during the LTM cell switch. Also, the CU indicator may indicate that a CU of the target cell is different from the first target CU, and for example, if the CU indicator is set to TRUE or 1, the first target DU 102-11 is to notify the UE 104 that the security update is needed during the LTM cell switch.

[0147] In addition, the inter-CU LTM indicator can indicate that the cell switch is associated with an inter-CU LTM, and for example, if the inter-CU LTM indicator is set to TRUE or 1, the first target DU 102-11 is to notify the UE 104 that the security update is needed during the LTM cell switch. Further, the CU node identifier (ID) may indicate an ID of a CU of the target cell, and for example, if the CU node ID is different from the current CU node ID, first target DU 102-11 is to notify the UE 104 that the security update is needed during the LTM cell switch.

[0148] After received the first indicator at step 812, the first target DU 102-11 may determine a second indicator indicating whether the security update is needed during the cell switch to the target cell, and may transmit, to the UE 104, the second indicator at step 814.

[0149] In some example embodiments, the second indicator may be determined by the first target DU 102-11 based on the first indicator. In some example embodiments, the second indicator may be transmitted to the UE 104 together with the NCC at step 814 as shown in FIG. 8. For example, the first target DU 102-11 may transmit the NCC along with the second indicator to the UE 104 via a MAC CE used for the LTM cell switch command as shown in FIG. 8, that is, the NCC and the second indicator may be included in the LTM cell switch command. However, the first target DU 102-11 may also transmit the NCC along with the second indicator to the first target DU 102-11 via other messages. As another example, the first target CU 102-10 may transmit the first indicator to the first target DU 102-11 separately from the NCC, e.g., via a different message from the message including the NCC.

[0150] In some example embodiments, the second indicator may include a security update indicator, a CU indicator, an inter-CU LTM indicator, or a CU node identifier (ID). For instance, the security update indicator can indicate whether the security update is needed, and for example, if the security update indicator is set to 1, it means that the security update is needed and the UE 104 shall perform the security update during the LTM cell switch. Also, the CU indicator may indicate that a CU of the target cell is different from the first target CU; and for example, If the CU indicator is set to 1, it means that the security update is needed and the UE 104 shall perform the security update during the LTM cell switch.

[0151] In addition, the inter-CU LTM indicator can indicate that the cell switch is associated with an inter-CU LTM, and for example, if the inter-CU LTM indicator is set to 1, it means that the security update is needed and the UE 104 shall perform the security update during the LTM cell switch. Further, the CU node identifier (ID) may indicate an ID of a CU of the target cell, and for example, if the CU node ID is different from the current CU node ID, it means that the security update is needed and the UE 104 shall perform the security update during the LTM cell switch.

[0152] In some example embodiments, the second indicator may be the same with the first indicator. For example, the second indicator and the first indicator are both the security update indicator set to 1. In some example embodiments, the second indicator may be different from the first indicator. For example, the first indicator is a CU node ID different from the current CU node ID (that is, CU node ID for the first target CU 102-10), and the second indicator is a security update indicator set to 1 which indicate that the security update is needed.

[0153] The UE 104 may receive the second indicator from first target DU 102-11 at step 816 and then determine whether a security update is needed based on the second indicator. If the second indicator indicates the security update is not needed, the UE does not perform the second key derivation. That is, the UE will use the current security key (i.e., K_{gNB1}) when it connects to the target cell. However, if the second indicator indicates a security update is needed, the UE 104 performs the second key derivation as described with reference to FIG. 7.

[0154] Although it is described that the first indicator and the second indicator are transmitted in the case that the NCC is transmitted in above description, the first

indicator and the second indicator may be transmitted when the NCC is not transmitted. For example, when the first target CU 102-10 determines that a security update is not needed and thus the first key derivation is not performed, the NCC is not generated. In such case, the first target CU 102-10 may only send, to the first target DU 102-11, the first indicator indicating that the first target DU 102-11 is to notify the UE 104 that the security update is not needed during the cell switch to the target cell, and accordingly, the first target DU 102-11 may only send, to the UE 104, the second indicator indicating that the security update is not needed during the cell switch to the target cell.

[0155] In some example embodiments, in the case that the second indicator indicating that the security update is not needed, and the current security key (i.e., K_{gNB1}) used by the UE 104 is different from the security key used at the second target CU 102-2, the UE 104 may, at step 820, like in step 720, transmit a first security update failure message indicating a failure of the security update to the first target DU 102-11.

[0156] FIG. 9 illustrates a third example of signalling procedure 900 for a security update for subsequent LTM in accordance with aspects of the present disclosure. The signalling procedure 900 is for a case with a new NAS security context.

[0157] As shown in FIG. 9, if an AMF 103 has activated a new NAS security context different from the currently active NAS security context, it sends a message to the first target CU 102-10 at step 902. The message may carry information on security update parameters which may indicate that a NAS security context different from a currently active NAS security context is activated by the AMF 103, and may be used by the UE 104 for updating a NH parameter associated with the first security key. For example, the message may include security update parameters such as a NH indicator, a ngKSI and/or a downlink NAS COUNT. The NH indicator may indicate a new NAS security context is activated by the AMF, and the ngKSI may indicate the new NAS security context used for deriving an updated NH parameter (i.e. a new NH parameter). In addition, the downlink NAS COUNT may include a NAS SQN and a NAS OVERFLOW, wherein the NAS SQN is a sequence number used for a security key used between the UE and the first target base station, and the NAS OVERFLOW is a value which is incremented each time the NAS SQN is incremented from the maximum value.

[0158] In some example embodiments, the message may be for example, a Path Switch Request Acknowledge message, or a Handover Request message. However, other messages will be applicable if they could perform the same the function.

[0159] The first target CU 102-10 may obtain, from the AMF 103, the information on security update parameters (including the NH indicator, the ngKSI and the downlink NAS COUNT) at step 904, and transmit it to the first target DU 102-11 at step 906.

[0160] In some example embodiments, the first target CU 102-10 may send the information on security update parameters (i.e., the received NH indicator, ngKSI and/or downlink NAS COUNT) to the first target DU 102-11, via, for example, a UE Context Modification Request message or other messages. The the first target DU 102-11 may receive the information on security update parameters at step 908, and then reply with a response message, such as a UE Context Modification Response message, at step 910. At step 912, the first target CU 102-10 receives the response message.

[0161] At step 914, the first target DU 102-11 may transmit the information on security update parameters (i.e., the received NH indicator, ngKSI and/or downlink NAS COUNT) to the UE 104, via, for example, a MAC CE. In one example, it may be a MAC CE used for the LTM cell switch command, that is, the NH indicator, ngKSI and/or downlink NAS COUNT may be included in the LTM cell switch command. In another example, it may be a MAC CE used for the security update, that is, the MAC CE includes the ngKSI and the downlink NAS COUNT.

[0162] The UE 104 receives the information on security update parameters (i.e., the NH indicator, ngKSI and downlink NAS COUNT) at step 916, and performs, at step 918, a NH update using the NAS security context identified by the ngKSI and the downlink NAS COUNT, to obtain a new (i.e., updated) NH. The NH parameter is associated with the first security key.

[0163] In some example embodiments, if the NH update fails (for example, the UE 104 cannot perform the NF update for some reasons), the UE 104 may transmit a second security update failure message indicating a failure of updating the NH parameter (or a second security update failure message indicating a failure of the security update) to the first target DU 102-11 at step 920, and then the first target DU 102-11 may receive the second security update failure message at step 922. In some example embodiments, the first target DU 102-11 may transmit a fourth security update failure message indicating

a failure of the security update to the first target CU 102-10, which is not shown in FIG. 9. In some example embodiments, the first target DU 102-11 may forward the second security update failure message indicating a failure of the security update to the first target CU 102-10, which is not shown in FIG. 9.

[0164] In some example embodiments, the second security update failure message may be transmitted via a MAC CE.

[0165] FIGS. 10 to 13 illustrate examples of devices that support a security update for subsequent LTM in accordance with aspects of the present disclosure.

[0166] FIG. 10 illustrates an example of a device 1000 that supports a security update for subsequent LTM in accordance with aspects of the present disclosure. The device 1000 may be an example of a first target base station 102-1 as described herein. The device 1000 may support wireless communication with one or more network entities 102 (for example, the second target base station 102-2 or AMF 103 as above), UE 104, or any combination thereof. The device 1000 may include components for bi-directional communications including components for transmitting and receiving communications, such as a processor 1002 (including a first processor of the first target CU 102-10 and a second processor of the first target DU 102-11), a memory 1004, a transceiver 1006, and, optionally, an I/O controller 1008. These components may be in electronic communication or otherwise coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces (e.g., buses).

[0167] The processor 1002, the memory 1004, the transceiver 1006, or various combinations thereof or various components thereof may be examples of means for performing various aspects of the present disclosure as described herein. For example, the processor 1002, the memory 1004, the transceiver 1006, or various combinations or components thereof may support a method for performing one or more of the operations described herein.

[0168] In some implementations, the processor 1002, the memory 1004, the transceiver 1006, or various combinations or components thereof may be implemented in hardware (e.g., in communications management circuitry). The hardware may include a processor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a field-programmable gate array (FPGA) or other programmable logic device, a discrete gate or transistor logic, discrete hardware components, or any combination

thereof configured as or otherwise supporting a means for performing the functions described in the present disclosure. In some implementations, the processor 1002 and the memory 1004 coupled with the processor 1002 may be configured to perform one or more of the functions described herein (e.g., executing, by the processor 1002, instructions stored in the memory 1004).

[0169] For example, the processor 1002 may support wireless communication at the device 1000 in accordance with examples as disclosed herein. The processor 1002 may be configured to operable to support a means for determining a first security key to be used between a UE and a second target base station for the LTM and a NCC to be used for a key derivation for a cell switch by the UE; and means for transmitting the NCC to the UE.

[0170] The processor 1002 may include an intelligent hardware device (e.g., a general-purpose processor, a DSP, a CPU, a microcontroller, an ASIC, an FPGA, a programmable logic device, a discrete gate or transistor logic component, a discrete hardware component, or any combination thereof). In some implementations, the processor 1002 may be configured to operate a memory array using a memory controller. In some other implementations, a memory controller may be integrated into the processor 1002. The processor 1002 may be configured to execute computer-readable instructions stored in a memory (e.g., the memory 1004) to cause the device 1000 to perform various functions of the present disclosure.

[0171] The memory 1004 may include random access memory (RAM) and read-only memory (ROM). The memory 1004 may store computer-readable, computer-executable code including instructions that, when executed by the processor 1002 cause the device 1000 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as system memory or another type of memory. In some implementations, the code may not be directly executable by the processor 1002 but may cause a computer (e.g., when compiled and executed) to perform functions described herein. In some implementations, the memory 1004 may include, among other things, a basic I/O system (BIOS) which may control basic hardware or software operation such as the interaction with peripheral components or devices.

[0172] The I/O controller 1008 may manage input and output signals for the device 1000. The I/O controller 1008 may also manage peripherals not integrated into the device 1000. In some implementations, the I/O controller 1008 may represent a physical connection or port to an external peripheral. In some implementations, the I/O controller 1008 may utilize an operating system such as iOS®, ANDROID®, MS-WINDOWS®, OS/2®, UNIX®, LINUX®, or another known operating system. In some implementations, the I/O controller 1008 may be implemented as part of a processor, such as the processor 1006. In some implementations, a user may interact with the device 1000 via the I/O controller 1008 or via hardware components controlled by the I/O controller 1008.

[0173] In some implementations, the device 1000 may include a single antenna 1010. However, in some other implementations, the device 1000 may have more than one antenna 1010 (i.e., multiple antennas), including multiple antenna panels or antenna arrays, which may be capable of concurrently transmitting or receiving multiple wireless transmissions. The transceiver 1006 may communicate bi-directionally, via the one or more antennas 1010, wired, or wireless links as described herein. For example, the transceiver 1006 may represent a wireless transceiver and may communicate bi-directionally with another wireless transceiver. The transceiver 1006 may also include a modem to modulate the packets, to provide the modulated packets to one or more antennas 1010 for transmission, and to demodulate packets received from the one or more antennas 1010. The transceiver 1006 may include one or more transmit chains, one or more receive chains, or a combination thereof.

[0174] A transmit chain may be configured to generate and transmit signals (e.g., control information, data, packets). The transmit chain may include at least one modulator for modulating data onto a carrier signal, preparing the signal for transmission over a wireless medium. The at least one modulator may be configured to support one or more techniques such as amplitude modulation (AM), frequency modulation (FM), or digital modulation schemes like phase-shift keying (PSK) or quadrature amplitude modulation (QAM). The transmit chain may also include at least one power amplifier configured to amplify the modulated signal to an appropriate power level suitable for transmission over the wireless medium. The transmit chain may also include one or more antennas 1010 for transmitting the amplified signal into the air or wireless medium.

[0175] A receive chain may be configured to receive signals (e.g., control information, data, packets) over a wireless medium. For example, the receive chain may include one or more antennas 1010 for receive the signal over the air or wireless medium. The receive chain may include at least one amplifier (e.g., a low-noise amplifier (LNA)) configured to amplify the received signal. The receive chain may include at least one demodulator configured to demodulate the receive signal and obtain the transmitted data by reversing the modulation technique applied during transmission of the signal. The receive chain may include at least one decoder for decoding the processing the demodulated signal to receive the transmitted data.

[0176] FIG. 11 illustrates an example of a device 1100 that supports a security update for subsequent LTM in accordance with aspects of the present disclosure. The device 1100 may be an example of a first target base station 102-1 as described herein. The device 1100 may support wireless communication with one or more network entities 102 (for example, the second target base station 102-2 or AMF 103 as above), UE 104, or any combination thereof. The device 1100 may include components for bi-directional communications including components for transmitting and receiving communications, such as a processor 1102 (including a first processor of the first target CU 102-10 and a second processor of the first target DU 102-11), a memory 1104, a transceiver 1106, and, optionally, an I/O controller 1108. These components may be in electronic communication or otherwise coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces (e.g., buses).

[0177] The processor 1102, the memory 1104, the transceiver 1106, or various combinations thereof or various components thereof may be examples of means for performing various aspects of the present disclosure as described herein. For example, the processor 1102, the memory 1104, the transceiver 1106, or various combinations or components thereof may support a method for performing one or more of the operations described herein.

[0178] In some implementations, the processor 1102, the memory 1104, the transceiver 1106, or various combinations or components thereof may be implemented in hardware (e.g., in communications management circuitry). The hardware may include a processor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a field-programmable gate array (FPGA) or other programmable logic device, a

discrete gate or transistor logic, discrete hardware components, or any combination thereof configured as or otherwise supporting a means for performing the functions described in the present disclosure. In some implementations, the processor 1102 and the memory 1104 coupled with the processor 1102 may be configured to perform one or more of the functions described herein (e.g., executing, by the processor 1102, instructions stored in the memory 604).

[0179] For example, the processor 1102 may support wireless communication at the device 1100 in accordance with examples as disclosed herein. The processor 1102 may be configured to operable to support a means for determining whether a security update for LTM is needed; and means for transmitting a security update information to a user equipment (UE), based on a result of the determination, the security update information is associated with a first security key to be used between the UE and a second target base station for the LTM.

[0180] The processor 1102 may include an intelligent hardware device (e.g., a general-purpose processor, a DSP, a CPU, a microcontroller, an ASIC, an FPGA, a programmable logic device, a discrete gate or transistor logic component, a discrete hardware component, or any combination thereof). In some implementations, the processor 1102 may be configured to operate a memory array using a memory controller. In some other implementations, a memory controller may be integrated into the processor 1102. The processor 602 may be configured to execute computer-readable instructions stored in a memory (e.g., the memory 1104) to cause the device 1100 to perform various functions of the present disclosure.

[0181] The memory 1104 may include random access memory (RAM) and read-only memory (ROM). The memory 1104 may store computer-readable, computer-executable code including instructions that, when executed by the processor 1102 cause the device 1100 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as system memory or another type of memory. In some implementations, the code may not be directly executable by the processor 1102 but may cause a computer (e.g., when compiled and executed) to perform functions described herein. In some implementations, the memory 1104 may include, among other things, a basic I/O system (BIOS) which may control basic

hardware or software operation such as the interaction with peripheral components or devices.

[0182] The I/O controller 1108 may manage input and output signals for the device 1100. The I/O controller 1108 may also manage peripherals not integrated into the device 1100. In some implementations, the I/O controller 1108 may represent a physical connection or port to an external peripheral. In some implementations, the I/O controller 1108 may utilize an operating system such as iOS®, ANDROID®, MS-WINDOWS®, OS/2®, UNIX®, LINUX®, or another known operating system. In some implementations, the I/O controller 1108 may be implemented as part of a processor, such as the processor 1106. In some implementations, a user may interact with the device 1100 via the I/O controller 1108 or via hardware components controlled by the I/O controller 1108.

[0183] In some implementations, the device 1100 may include a single antenna 1110. However, in some other implementations, the device 1100 may have more than one antenna 1110 (i.e., multiple antennas), including multiple antenna panels or antenna arrays, which may be capable of concurrently transmitting or receiving multiple wireless transmissions. The transceiver 1106 may communicate bi-directionally, via the one or more antennas 1110, wired, or wireless links as described herein. For example, the transceiver 1106 may represent a wireless transceiver and may communicate bi-directionally with another wireless transceiver. The transceiver 1106 may also include a modem to modulate the packets, to provide the modulated packets to one or more antennas 1110 for transmission, and to demodulate packets received from the one or more antennas 1110. The transceiver 1106 may include one or more transmit chains, one or more receive chains, or a combination thereof.

[0184] A transmit chain may be configured to generate and transmit signals (e.g., control information, data, packets). The transmit chain may include at least one modulator for modulating data onto a carrier signal, preparing the signal for transmission over a wireless medium. The at least one modulator may be configured to support one or more techniques such as amplitude modulation (AM), frequency modulation (FM), or digital modulation schemes like phase-shift keying (PSK) or quadrature amplitude modulation (QAM). The transmit chain may also include at least one power amplifier configured to amplify the modulated signal to an appropriate power

level suitable for transmission over the wireless medium. The transmit chain may also include one or more antennas 1110 for transmitting the amplified signal into the air or wireless medium.

[0185] A receive chain may be configured to receive signals (e.g., control information, data, packets) over a wireless medium. For example, the receive chain may include one or more antennas 1110 for receive the signal over the air or wireless medium. The receive chain may include at least one amplifier (e.g., a low-noise amplifier (LNA)) configured to amplify the received signal. The receive chain may include at least one demodulator configured to demodulate the receive signal and obtain the transmitted data by reversing the modulation technique applied during transmission of the signal. The receive chain may include at least one decoder for decoding the processing the demodulated signal to receive the transmitted data.

[0186] FIG. 12 illustrates an example of a device 1200 that supports a security update for subsequent LTM in accordance with aspects of the present disclosure. The device 1200 may be an example of a UE 104 as described herein. The device 1200 may support wireless communication with one or more network entities 102 (for example, the first target base station 102-1 as above), or any combination thereof. The device 600 may include components for bi-directional communications including components for transmitting and receiving communications, such as a processor 1202, a memory 1204, a transceiver 1206, and, optionally, an I/O controller 1208. These components may be in electronic communication or otherwise coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces (e.g., buses).

[0187] The processor 1202, the memory 1204, the transceiver 1206, or various combinations thereof or various components thereof may be examples of means for performing various aspects of the present disclosure as described herein. For example, the processor 1202, the memory 1204, the transceiver 1206, or various combinations or components thereof may support a method for performing one or more of the operations described herein.

[0188] In some implementations, the processor 1202, the memory 1204, the transceiver 1206, or various combinations or components thereof may be implemented in hardware (e.g., in communications management circuitry). The hardware may include a processor, a digital signal processor (DSP), an application-specific integrated circuit

(ASIC), a field-programmable gate array (FPGA) or other programmable logic device, a discrete gate or transistor logic, discrete hardware components, or any combination thereof configured as or otherwise supporting a means for performing the functions described in the present disclosure. In some implementations, the processor 1202 and the memory 1204 coupled with the processor 1202 may be configured to perform one or more of the functions described herein (e.g., executing, by the processor 1202, instructions stored in the memory 604).

[0189] For example, the processor 1202 may support wireless communication at the device 1200 in accordance with examples as disclosed herein. The processor 1202 may be configured to operable to support a means for receiving, from a first target base station for LTM, a NCC to be used for a key derivation for a cell switch by the UE; and means for performing a key derivation by using the NCC to determine a first security key to be used between the UE and a second target base station for the LTM.

[0190] The processor 1202 may include an intelligent hardware device (e.g., a general-purpose processor, a DSP, a CPU, a microcontroller, an ASIC, an FPGA, a programmable logic device, a discrete gate or transistor logic component, a discrete hardware component, or any combination thereof). In some implementations, the processor 1202 may be configured to operate a memory array using a memory controller. In some other implementations, a memory controller may be integrated into the processor 1202. The processor 1202 may be configured to execute computer-readable instructions stored in a memory (e.g., the memory 1204) to cause the device 1200 to perform various functions of the present disclosure.

[0191] The memory 1204 may include random access memory (RAM) and read-only memory (ROM). The memory 1204 may store computer-readable, computer-executable code including instructions that, when executed by the processor 1202 cause the device 1200 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as system memory or another type of memory. In some implementations, the code may not be directly executable by the processor 1202 but may cause a computer (e.g., when compiled and executed) to perform functions described herein. In some implementations, the memory 1204 may include, among other things, a basic I/O system (BIOS) which may control basic

hardware or software operation such as the interaction with peripheral components or devices.

[0192] The I/O controller 1208 may manage input and output signals for the device 1200. The I/O controller 1208 may also manage peripherals not integrated into the device 1200. In some implementations, the I/O controller 1208 may represent a physical connection or port to an external peripheral. In some implementations, the I/O controller 1208 may utilize an operating system such as iOS®, ANDROID®, MS-WINDOWS®, OS/2®, UNIX®, LINUX®, or another known operating system. In some implementations, the I/O controller 1208 may be implemented as part of a processor, such as the processor 1206. In some implementations, a user may interact with the device 1200 via the I/O controller 1208 or via hardware components controlled by the I/O controller 1208.

[0193] In some implementations, the device 1200 may include a single antenna 1210. However, in some other implementations, the device 1200 may have more than one antenna 1210 (i.e., multiple antennas), including multiple antenna panels or antenna arrays, which may be capable of concurrently transmitting or receiving multiple wireless transmissions. The transceiver 1206 may communicate bi-directionally, via the one or more antennas 1210, wired, or wireless links as described herein. For example, the transceiver 1206 may represent a wireless transceiver and may communicate bi-directionally with another wireless transceiver. The transceiver 1206 may also include a modem to modulate the packets, to provide the modulated packets to one or more antennas 1210 for transmission, and to demodulate packets received from the one or more antennas 1210. The transceiver 1206 may include one or more transmit chains, one or more receive chains, or a combination thereof.

[0194] A transmit chain may be configured to generate and transmit signals (e.g., control information, data, packets). The transmit chain may include at least one modulator for modulating data onto a carrier signal, preparing the signal for transmission over a wireless medium. The at least one modulator may be configured to support one or more techniques such as amplitude modulation (AM), frequency modulation (FM), or digital modulation schemes like phase-shift keying (PSK) or quadrature amplitude modulation (QAM). The transmit chain may also include at least one power amplifier configured to amplify the modulated signal to an appropriate power

level suitable for transmission over the wireless medium. The transmit chain may also include one or more antennas 1210 for transmitting the amplified signal into the air or wireless medium.

[0195] A receive chain may be configured to receive signals (e.g., control information, data, packets) over a wireless medium. For example, the receive chain may include one or more antennas 1210 for receive the signal over the air or wireless medium. The receive chain may include at least one amplifier (e.g., a low-noise amplifier (LNA)) configured to amplify the received signal. The receive chain may include at least one demodulator configured to demodulate the receive signal and obtain the transmitted data by reversing the modulation technique applied during transmission of the signal. The receive chain may include at least one decoder for decoding the processing the demodulated signal to receive the transmitted data.

[0196] FIG. 13 illustrates an example of a device 1300 that supports a security update for subsequent LTM in accordance with aspects of the present disclosure. The device 1300 may be an example of a UE 104 as described herein. The device 1300 may support wireless communication with one or more network entities 102 (for example, the first target base station 102-1 as above), UE 104, or any combination thereof. The device 1300 may include components for bi-directional communications including components for transmitting and receiving communications, such as a processor 1302, a memory 1304, a transceiver 1306, and, optionally, an I/O controller 1308. These components may be in electronic communication or otherwise coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces (e.g., buses).

[0197] The processor 1302, the memory 1304, the transceiver 1306, or various combinations thereof or various components thereof may be examples of means for performing various aspects of the present disclosure as described herein. For example, the processor 1302, the memory 1304, the transceiver 1306, or various combinations or components thereof may support a method for performing one or more of the operations described herein.

[0198] In some implementations, the processor 1302, the memory 1304, the transceiver 1306, or various combinations or components thereof may be implemented in hardware (e.g., in communications management circuitry). The hardware may include

a processor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a field-programmable gate array (FPGA) or other programmable logic device, a discrete gate or transistor logic, discrete hardware components, or any combination thereof configured as or otherwise supporting a means for performing the functions described in the present disclosure. In some implementations, the processor 1302 and the memory 1304 coupled with the processor 1302 may be configured to perform one or more of the functions described herein (e.g., executing, by the processor 1302, instructions stored in the memory 604).

[0199] For example, the processor 1302 may support wireless communication at the device 1300 in accordance with examples as disclosed herein. The processor 1302 may be configured to operable to support a means for receiving, from a first target base station for LTM, a security update information; and means for perform an operation related to a security update for the LTM based on the security update information, the security update information is associated with a first security key to be used between the UE and a second target base station for the LTM.

[0200] The processor 1302 may include an intelligent hardware device (e.g., a general-purpose processor, a DSP, a CPU, a microcontroller, an ASIC, an FPGA, a programmable logic device, a discrete gate or transistor logic component, a discrete hardware component, or any combination thereof). In some implementations, the processor 1302 may be configured to operate a memory array using a memory controller. In some other implementations, a memory controller may be integrated into the processor 1302. The processor 1302 may be configured to execute computer-readable instructions stored in a memory (e.g., the memory 1304) to cause the device 1300 to perform various functions of the present disclosure.

[0201] The memory 1304 may include random access memory (RAM) and read-only memory (ROM). The memory 1304 may store computer-readable, computer-executable code including instructions that, when executed by the processor 1302 cause the device 1300 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as system memory or another type of memory. In some implementations, the code may not be directly executable by the processor 1302 but may cause a computer (e.g., when compiled and executed) to perform functions described herein. In some implementations, the memory 1304 may

include, among other things, a basic I/O system (BIOS) which may control basic hardware or software operation such as the interaction with peripheral components or devices.

[0202] The I/O controller 1308 may manage input and output signals for the device 1300. The I/O controller 1308 may also manage peripherals not integrated into the device 1300. In some implementations, the I/O controller 1308 may represent a physical connection or port to an external peripheral. In some implementations, the I/O controller 1308 may utilize an operating system such as iOS®, ANDROID®, MS-WINDOWS®, OS/2®, UNIX®, LINUX®, or another known operating system. In some implementations, the I/O controller 1308 may be implemented as part of a processor, such as the processor 1306. In some implementations, a user may interact with the device 1300 via the I/O controller 1308 or via hardware components controlled by the I/O controller 1308.

[0203] In some implementations, the device 1300 may include a single antenna 1310. However, in some other implementations, the device 1300 may have more than one antenna 1310 (i.e., multiple antennas), including multiple antenna panels or antenna arrays, which may be capable of concurrently transmitting or receiving multiple wireless transmissions. The transceiver 1306 may communicate bi-directionally, via the one or more antennas 1310, wired, or wireless links as described herein. For example, the transceiver 1306 may represent a wireless transceiver and may communicate bi-directionally with another wireless transceiver. The transceiver 1306 may also include a modem to modulate the packets, to provide the modulated packets to one or more antennas 1310 for transmission, and to demodulate packets received from the one or more antennas 1310. The transceiver 1306 may include one or more transmit chains, one or more receive chains, or a combination thereof.

[0204] A transmit chain may be configured to generate and transmit signals (e.g., control information, data, packets). The transmit chain may include at least one modulator for modulating data onto a carrier signal, preparing the signal for transmission over a wireless medium. The at least one modulator may be configured to support one or more techniques such as amplitude modulation (AM), frequency modulation (FM), or digital modulation schemes like phase-shift keying (PSK) or quadrature amplitude modulation (QAM). The transmit chain may also include at least

one power amplifier configured to amplify the modulated signal to an appropriate power level suitable for transmission over the wireless medium. The transmit chain may also include one or more antennas 1310 for transmitting the amplified signal into the air or wireless medium.

[0205] A receive chain may be configured to receive signals (e.g., control information, data, packets) over a wireless medium. For example, the receive chain may include one or more antennas 1310 for receive the signal over the air or wireless medium. The receive chain may include at least one amplifier (e.g., a low-noise amplifier (LNA)) configured to amplify the received signal. The receive chain may include at least one demodulator configured to demodulate the receive signal and obtain the transmitted data by reversing the modulation technique applied during transmission of the signal. The receive chain may include at least one decoder for decoding the processing the demodulated signal to receive the transmitted data.

[0206] FIG. 14 illustrates an example of a processor 1400 that supports a security update for subsequent LTM in accordance with aspects of the present disclosure. The processor 1400 (including a first processor of the first target CU 102-10 and a second processor of the first target DU 102-11) may be an example of a processor configured to perform various operations in accordance with examples as described herein. The processor 1400 may include a controller 1402 configured to perform various operations in accordance with examples as described herein. The processor 1400 may optionally include at least one memory 1404, such as L1/L2/L3 cache. Additionally, or alternatively, the processor 1400 may optionally include one or more arithmetic-logic units (ALUs) 1400. One or more of these components may be in electronic communication or otherwise coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces (e.g., buses).

[0207] The processor 1400 may be a processor chipset and include a protocol stack (e.g., a software stack) executed by the processor chipset to perform various operations (e.g., receiving, obtaining, retrieving, transmitting, outputting, forwarding, storing, determining, identifying, accessing, writing, reading) in accordance with examples as described herein. The processor chipset may include one or more cores, one or more caches (e.g., memory local to or included in the processor chipset (e.g., the processor 1400) or other memory (e.g., random access memory (RAM), read-only memory (ROM), dynamic RAM (DRAM), synchronous dynamic RAM (SDRAM), static RAM

(SRAM), ferroelectric RAM (FeRAM), magnetic RAM (MRAM), resistive RAM (RRAM), flash memory, phase change memory (PCM), and others).

[0208] The controller 1402 may be configured to manage and coordinate various operations (e.g., signaling, receiving, obtaining, retrieving, transmitting, outputting, forwarding, storing, determining, identifying, accessing, writing, reading) of the processor 1400 to cause the processor 1400 to support various operations of a base station in accordance with examples as described herein. For example, the controller 1402 may operate as a control unit of the processor 1400, generating control signals that manage the operation of various components of the processor 1400. These control signals include enabling or disabling functional units, selecting data paths, initiating memory access, and coordinating timing of operations.

[0209] The controller 1402 may be configured to fetch (e.g., obtain, retrieve, receive) instructions from the memory 1404 and determine subsequent instruction(s) to be executed to cause the processor 1400 to support various operations in accordance with examples as described herein. The controller 1402 may be configured to track memory address of instructions associated with the memory 1404. The controller 1402 may be configured to decode instructions to determine the operation to be performed and the operands involved. For example, the controller 1402 may be configured to interpret the instruction and determine control signals to be output to other components of the processor 1400 to cause the processor 1400 to support various operations in accordance with examples as described herein. Additionally, or alternatively, the controller 1402 may be configured to manage flow of data within the processor 1400. The controller 1402 may be configured to control transfer of data between registers, arithmetic logic units (ALUs), and other functional units of the processor 1400.

[0210] The memory 1404 may include one or more caches (e.g., memory local to or included in the processor 1400 or other memory, such RAM, ROM, DRAM, SDRAM, SRAM, MRAM, flash memory, etc. In some implementation, the memory 1404 may reside within or on a processor chipset (e.g., local to the processor 1400). In some other implementations, the memory 1404 may reside external to the processor chipset (e.g., remote to the processor 1400).

[0211] The memory 1404 may store computer-readable, computer-executable code including instructions that, when executed by the processor 1400, cause the processor

1400 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as system memory or another type of memory. The controller 1402 and/or the processor 1400 may be configured to execute computer-readable instructions stored in the memory 1404 to cause the processor 1400 to perform various functions. For example, the processor 1400 and/or the controller 1402 may be coupled with or to the memory 1404, and the processor 1400, the controller 1402, and the memory 1404 may be configured to perform various functions described herein. In some examples, the processor 1400 may include multiple processors and the memory 1404 may include multiple memories. One or more of the multiple processors may be coupled with one or more of the multiple memories, which may, individually or collectively, be configured to perform various functions herein.

[0212] The one or more ALUs 1400 may be configured to support various operations in accordance with examples as described herein. In some implementation, the one or more ALUs 1400 may reside within or on a processor chipset (e.g., the processor 1400). In some other implementations, the one or more ALUs 1400 may reside external to the processor chipset (e.g., the processor 1400). One or more ALUs 1400 may perform one or more computations such as addition, subtraction, multiplication, and division on data. For example, one or more ALUs 1400 may receive input operands and an operation code, which determines an operation to be executed. One or more ALUs 1400 be configured with a variety of logical and arithmetic circuits, including adders, subtractors, shifters, and logic gates, to process and manipulate the data according to the operation. Additionally, or alternatively, the one or more ALUs 1400 may support logical operations such as AND, OR, exclusive-OR (XOR), not-OR (NOR), and not-AND (NAND), enabling the one or more ALUs 1400 to handle conditional operations, comparisons, and bitwise operations.

[0213] The processor 1400 may support wireless communication in accordance with examples as disclosed herein. The processor 1400 may be configured to or operable to support a means for determining a first security key to be used between a UE and a second target base station for the LTM and a NCC to be used for a key derivation for a cell switch by the UE; and means for transmitting the NCC to the UE.

[0214] FIG. 15 illustrates an example of a processor 1500 that supports a security update for subsequent LTM in accordance with aspects of the present disclosure. The processor 1500 (including a first processor of the first target CU 102-10 and a second

processor of the first target DU 102-11) may be an example of a processor configured to perform various operations in accordance with examples as described herein. The processor 1500 may include a controller 1502 configured to perform various operations in accordance with examples as described herein. The processor 1500 may optionally include at least one memory 1504, such as L1/L2/L3 cache. Additionally, or alternatively, the processor 1500 may optionally include one or more arithmetic-logic units (ALUs) 1500. One or more of these components may be in electronic communication or otherwise coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces (e.g., buses).

[0215] The processor 1500 may be a processor chipset and include a protocol stack (e.g., a software stack) executed by the processor chipset to perform various operations (e.g., receiving, obtaining, retrieving, transmitting, outputting, forwarding, storing, determining, identifying, accessing, writing, reading) in accordance with examples as described herein. The processor chipset may include one or more cores, one or more caches (e.g., memory local to or included in the processor chipset (e.g., the processor 1500) or other memory (e.g., random access memory (RAM), read-only memory (ROM), dynamic RAM (DRAM), synchronous dynamic RAM (SDRAM), static RAM (SRAM), ferroelectric RAM (FeRAM), magnetic RAM (MRAM), resistive RAM (RRAM), flash memory, phase change memory (PCM), and others).

[0216] The controller 1502 may be configured to manage and coordinate various operations (e.g., signaling, receiving, obtaining, retrieving, transmitting, outputting, forwarding, storing, determining, identifying, accessing, writing, reading) of the processor 1500 to cause the processor 1500 to support various operations of a base station in accordance with examples as described herein. For example, the controller 1502 may operate as a control unit of the processor 1500, generating control signals that manage the operation of various components of the processor 1500. These control signals include enabling or disabling functional units, selecting data paths, initiating memory access, and coordinating timing of operations.

[0217] The controller 1502 may be configured to fetch (e.g., obtain, retrieve, receive) instructions from the memory 1504 and determine subsequent instruction(s) to be executed to cause the processor 1500 to support various operations in accordance with examples as described herein. The controller 1502 may be configured to track memory

address of instructions associated with the memory 1504. The controller 1502 may be configured to decode instructions to determine the operation to be performed and the operands involved. For example, the controller 1502 may be configured to interpret the instruction and determine control signals to be output to other components of the processor 1500 to cause the processor 1500 to support various operations in accordance with examples as described herein. Additionally, or alternatively, the controller 1502 may be configured to manage flow of data within the processor 1500. The controller 1502 may be configured to control transfer of data between registers, arithmetic logic units (ALUs), and other functional units of the processor 1500.

[0218] The memory 1504 may include one or more caches (e.g., memory local to or included in the processor 1500 or other memory, such RAM, ROM, DRAM, SDRAM, SRAM, MRAM, flash memory, etc. In some implementation, the memory 1504 may reside within or on a processor chipset (e.g., local to the processor 1500). In some other implementations, the memory 1504 may reside external to the processor chipset (e.g., remote to the processor 1500).

[0219] The memory 1504 may store computer-readable, computer-executable code including instructions that, when executed by the processor 1500, cause the processor 1500 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as system memory or another type of memory. The controller 1502 and/or the processor 1500 may be configured to execute computer-readable instructions stored in the memory 1504 to cause the processor 1500 to perform various functions. For example, the processor 1500 and/or the controller 1502 may be coupled with or to the memory 1504, and the processor 1500, the controller 1502, and the memory 1504 may be configured to perform various functions described herein. In some examples, the processor 1500 may include multiple processors and the memory 1504 may include multiple memories. One or more of the multiple processors may be coupled with one or more of the multiple memories, which may, individually or collectively, be configured to perform various functions herein.

[0220] The one or more ALUs 1500 may be configured to support various operations in accordance with examples as described herein. In some implementation, the one or more ALUs 1500 may reside within or on a processor chipset (e.g., the processor 1500). In some other implementations, the one or more ALUs 1500 may

reside external to the processor chipset (e.g., the processor 1500). One or more ALUs 1500 may perform one or more computations such as addition, subtraction, multiplication, and division on data. For example, one or more ALUs 1500 may receive input operands and an operation code, which determines an operation to be executed. One or more ALUs 1500 be configured with a variety of logical and arithmetic circuits, including adders, subtractors, shifters, and logic gates, to process and manipulate the data according to the operation. Additionally, or alternatively, the one or more ALUs 1500 may support logical operations such as AND, OR, exclusive-OR (XOR), not-OR (NOR), and not-AND (NAND), enabling the one or more ALUs 1500 to handle conditional operations, comparisons, and bitwise operations.

[0221] The processor 1500 may support wireless communication in accordance with examples as disclosed herein. The processor 1500 may be configured to or operable to support a means for determining whether a security update for LTM is needed; and means for transmitting a security update information to a UE, based on a result of the determination, the security update information is associated with a first security key to be used between the UE and a second target base station for the LTM.

[0222] FIG. 16 illustrates an example of a processor 1600 that supports a security update for subsequent LTM in accordance with aspects of the present disclosure. The processor 1600 may be an example of a processor configured to perform various operations in accordance with examples as described herein. The processor 1600 may include a controller 1602 configured to perform various operations in accordance with examples as described herein. The processor 1600 may optionally include at least one memory 1604, such as L1/L2/L3 cache. Additionally, or alternatively, the processor 1600 may optionally include one or more arithmetic-logic units (ALUs) 1600. One or more of these components may be in electronic communication or otherwise coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces (e.g., buses).

[0223] The processor 1600 may be a processor chipset and include a protocol stack (e.g., a software stack) executed by the processor chipset to perform various operations (e.g., receiving, obtaining, retrieving, transmitting, outputting, forwarding, storing, determining, identifying, accessing, writing, reading) in accordance with examples as described herein. The processor chipset may include one or more cores, one or more caches (e.g., memory local to or included in the processor chipset (e.g., the processor

1600) or other memory (e.g., random access memory (RAM), read-only memory (ROM), dynamic RAM (DRAM), synchronous dynamic RAM (SDRAM), static RAM (SRAM), ferroelectric RAM (FeRAM), magnetic RAM (MRAM), resistive RAM (RRAM), flash memory, phase change memory (PCM), and others).

[0224] The controller 1602 may be configured to manage and coordinate various operations (e.g., signaling, receiving, obtaining, retrieving, transmitting, outputting, forwarding, storing, determining, identifying, accessing, writing, reading) of the processor 1600 to cause the processor 1600 to support various operations of a base station in accordance with examples as described herein. For example, the controller 1602 may operate as a control unit of the processor 1600, generating control signals that manage the operation of various components of the processor 1600. These control signals include enabling or disabling functional units, selecting data paths, initiating memory access, and coordinating timing of operations.

[0225] The controller 1602 may be configured to fetch (e.g., obtain, retrieve, receive) instructions from the memory 1604 and determine subsequent instruction(s) to be executed to cause the processor 1600 to support various operations in accordance with examples as described herein. The controller 1602 may be configured to track memory address of instructions associated with the memory 1604. The controller 1602 may be configured to decode instructions to determine the operation to be performed and the operands involved. For example, the controller 1602 may be configured to interpret the instruction and determine control signals to be output to other components of the processor 1600 to cause the processor 1600 to support various operations in accordance with examples as described herein. Additionally, or alternatively, the controller 1602 may be configured to manage flow of data within the processor 1600. The controller 1602 may be configured to control transfer of data between registers, arithmetic logic units (ALUs), and other functional units of the processor 1600.

[0226] The memory 1604 may include one or more caches (e.g., memory local to or included in the processor 1600 or other memory, such RAM, ROM, DRAM, SDRAM, SRAM, MRAM, flash memory, etc. In some implementation, the memory 1604 may reside within or on a processor chipset (e.g., local to the processor 1600). In some other implementations, the memory 1604 may reside external to the processor chipset (e.g., remote to the processor 1600).

[0227] The memory 1604 may store computer-readable, computer-executable code including instructions that, when executed by the processor 1600, cause the processor 1600 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as system memory or another type of memory. The controller 1602 and/or the processor 1600 may be configured to execute computer-readable instructions stored in the memory 1604 to cause the processor 1600 to perform various functions. For example, the processor 1600 and/or the controller 1602 may be coupled with or to the memory 1604, and the processor 1600, the controller 1602, and the memory 1604 may be configured to perform various functions described herein. In some examples, the processor 1600 may include multiple processors and the memory 1604 may include multiple memories. One or more of the multiple processors may be coupled with one or more of the multiple memories, which may, individually or collectively, be configured to perform various functions herein.

[0228] The one or more ALUs 1600 may be configured to support various operations in accordance with examples as described herein. In some implementation, the one or more ALUs 1600 may reside within or on a processor chipset (e.g., the processor 1600). In some other implementations, the one or more ALUs 1600 may reside external to the processor chipset (e.g., the processor 1600). One or more ALUs 1600 may perform one or more computations such as addition, subtraction, multiplication, and division on data. For example, one or more ALUs 1600 may receive input operands and an operation code, which determines an operation to be executed. One or more ALUs 1600 be configured with a variety of logical and arithmetic circuits, including adders, subtractors, shifters, and logic gates, to process and manipulate the data according to the operation. Additionally, or alternatively, the one or more ALUs 1600 may support logical operations such as AND, OR, exclusive-OR (XOR), not-OR (NOR), and not-AND (NAND), enabling the one or more ALUs 1600 to handle conditional operations, comparisons, and bitwise operations.

[0229] The processor 1600 may support wireless communication in accordance with examples as disclosed herein. The processor 1600 may be configured to or operable to support a means for receiving, from a first target base station for LTM, a NCC to be used for a key derivation for a cell switch by the UE; and means for performing a key derivation by using the NCC to determine a first security key to be used between the UE and a second target base station for the LTM.

[0230] FIG. 17 illustrates an example of a processor 1700 that supports a security update for subsequent LTM in accordance with aspects of the present disclosure. The processor 1700 may be an example of a processor configured to perform various operations in accordance with examples as described herein. The processor 1700 may include a controller 1702 configured to perform various operations in accordance with examples as described herein. The processor 1700 may optionally include at least one memory 1704, such as L1/L2/L3 cache. Additionally, or alternatively, the processor 1700 may optionally include one or more arithmetic-logic units (ALUs) 1700. One or more of these components may be in electronic communication or otherwise coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces (e.g., buses).

[0231] The processor 1700 may be a processor chipset and include a protocol stack (e.g., a software stack) executed by the processor chipset to perform various operations (e.g., receiving, obtaining, retrieving, transmitting, outputting, forwarding, storing, determining, identifying, accessing, writing, reading) in accordance with examples as described herein. The processor chipset may include one or more cores, one or more caches (e.g., memory local to or included in the processor chipset (e.g., the processor 1700) or other memory (e.g., random access memory (RAM), read-only memory (ROM), dynamic RAM (DRAM), synchronous dynamic RAM (SDRAM), static RAM (SRAM), ferroelectric RAM (FeRAM), magnetic RAM (MRAM), resistive RAM (RRAM), flash memory, phase change memory (PCM), and others).

[0232] The controller 1702 may be configured to manage and coordinate various operations (e.g., signaling, receiving, obtaining, retrieving, transmitting, outputting, forwarding, storing, determining, identifying, accessing, writing, reading) of the processor 1700 to cause the processor 1700 to support various operations of a base station in accordance with examples as described herein. For example, the controller 1702 may operate as a control unit of the processor 1700, generating control signals that manage the operation of various components of the processor 1700. These control signals include enabling or disabling functional units, selecting data paths, initiating memory access, and coordinating timing of operations.

[0233] The controller 1702 may be configured to fetch (e.g., obtain, retrieve, receive) instructions from the memory 1704 and determine subsequent instruction(s) to be

executed to cause the processor 1700 to support various operations in accordance with examples as described herein. The controller 1702 may be configured to track memory address of instructions associated with the memory 1704. The controller 1702 may be configured to decode instructions to determine the operation to be performed and the operands involved. For example, the controller 1702 may be configured to interpret the instruction and determine control signals to be output to other components of the processor 1700 to cause the processor 1700 to support various operations in accordance with examples as described herein. Additionally, or alternatively, the controller 1702 may be configured to manage flow of data within the processor 1700. The controller 1702 may be configured to control transfer of data between registers, arithmetic logic units (ALUs), and other functional units of the processor 1700.

[0234] The memory 1704 may include one or more caches (e.g., memory local to or included in the processor 1700 or other memory, such RAM, ROM, DRAM, SDRAM, SRAM, MRAM, flash memory, etc. In some implementation, the memory 1704 may reside within or on a processor chipset (e.g., local to the processor 1700). In some other implementations, the memory 1704 may reside external to the processor chipset (e.g., remote to the processor 1700).

[0235] The memory 1704 may store computer-readable, computer-executable code including instructions that, when executed by the processor 1700, cause the processor 1700 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as system memory or another type of memory. The controller 1702 and/or the processor 1700 may be configured to execute computer-readable instructions stored in the memory 1704 to cause the processor 1700 to perform various functions. For example, the processor 1700 and/or the controller 1702 may be coupled with or to the memory 1704, and the processor 1700, the controller 1702, and the memory 1704 may be configured to perform various functions described herein. In some examples, the processor 1700 may include multiple processors and the memory 1704 may include multiple memories. One or more of the multiple processors may be coupled with one or more of the multiple memories, which may, individually or collectively, be configured to perform various functions herein.

[0236] The one or more ALUs 1700 may be configured to support various operations in accordance with examples as described herein. In some implementation,

the one or more ALUs 1700 may reside within or on a processor chipset (e.g., the processor 1700). In some other implementations, the one or more ALUs 1700 may reside external to the processor chipset (e.g., the processor 1700). One or more ALUs 1700 may perform one or more computations such as addition, subtraction, multiplication, and division on data. For example, one or more ALUs 1700 may receive input operands and an operation code, which determines an operation to be executed. One or more ALUs 1700 be configured with a variety of logical and arithmetic circuits, including adders, subtractors, shifters, and logic gates, to process and manipulate the data according to the operation. Additionally, or alternatively, the one or more ALUs 1700 may support logical operations such as AND, OR, exclusive-OR (XOR), not-OR (NOR), and not-AND (NAND), enabling the one or more ALUs 1700 to handle conditional operations, comparisons, and bitwise operations.

[0237] The processor 1700 may support wireless communication in accordance with examples as disclosed herein. The processor 1700 may be configured to or operable to support a means for receiving, from a first target base station for LTM, a security update information; and means for performing an operation related to a security update for the LTM based on the security update information, the security update information is associated with a first security key to be used between the UE and a second target base station for the LTM.

[0238] FIG. 18 illustrates a flowchart of a method 1800 that supports a security update for subsequent LTM in accordance with aspects of the present disclosure. The operations of the method 1800 may be implemented by a device or its components as described herein. For example, the operations of the method 1800 may be performed by a first target base station 102-1 as described herein. In some implementations, the device may execute a set of instructions to control the function elements of the device to perform the described functions. Additionally, or alternatively, the device may perform aspects of the described functions using special-purpose hardware.

[0239] At 1805, the method may include determining a first security key to be used between a UE 104 and a second target base station 102-2 for the LTM and a NCC to be used for a key derivation for a cell switch by the UE 104. The operations of 1805 may be performed in accordance with examples as described herein. In some

implementations, aspects of the operations of 2005 may be performed by a device as described with reference to FIG. 1.

[0240] At 1810, the method may include transmitting the NCC to the UE 104. The operations of 1810 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 2010 may be performed by a device as described with reference to FIG. 1.

[0241] FIG. 19 illustrates a flowchart of a method 1900 that supports a security update for subsequent LTM in accordance with aspects of the present disclosure. The operations of the method 1900 may be implemented by a device or its components as described herein. For example, the operations of the method 1900 may be performed by a first target base station 102-1 as described herein. In some implementations, the device may execute a set of instructions to control the function elements of the device to perform the described functions. Additionally, or alternatively, the device may perform aspects of the described functions using special-purpose hardware.

[0242] At 1905, the method may include determining whether a security update for LTM is needed. The operations of 1905 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1905 may be performed by a device as described with reference to FIG. 1.

[0243] At 1910, the method may include transmitting a security update information to a UE 104, based on a result of the determination, the security update information is associated with a first security key to be used between the UE 104 and a second target base station 102-2 for the LTM. The operations of 1910 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1910 may be performed by a device as described with reference to FIG. 1.

[0244] FIG. 20 illustrates a flowchart of a method 2000 that supports a security update for subsequent LTM in accordance with aspects of the present disclosure. The operations of the method 2000 may be implemented by a device or its components as described herein. For example, the operations of the method 2000 may be performed by a UE 104 as described herein. In some implementations, the device may execute a set of instructions to control the function elements of the device to perform the described functions. Additionally, or alternatively, the device may perform aspects of the described functions using special-purpose hardware.

[0245] At 2005, the method may include receiving, from a first target base station 102-1 for LTM, a NCC to be used for a key derivation for a cell switch by the UE 104. The operations of 2205 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 2205 may be performed by a device as described with reference to FIG. 1.

[0246] At 2010, the method may include performing a key derivation by using the NCC to determine a first security key to be used between the UE 104 and a second target base station 102-2 for the LTM. The operations of 2010 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 2010 may be performed by a device as described with reference to FIG. 1.

[0247] FIG. 21 illustrates a flowchart of a method 2100 that supports a security update for subsequent LTM in accordance with aspects of the present disclosure. The operations of the method 2100 may be implemented by a device or its components as described herein. For example, the operations of the method 2100 may be performed by a UE 104 as described herein. In some implementations, the device may execute a set of instructions to control the function elements of the device to perform the described functions. Additionally, or alternatively, the device may perform aspects of the described functions using special-purpose hardware.

[0248] At 2105, the method may include receiving, from a first target base station 102-1 for LTM, a security update information. The operations of 2105 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 2105 may be performed by a device as described with reference to FIG. 1.

[0249] At 2110, the method may include performing an operation related to a security update for the LTM based on the security update information, the security update information is associated with a first security key to be used between the UE 104 and a second target base station 102-2 for the LTM. The operations of 2110 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 2110 may be performed by a device as described with reference to FIG. 1.

[0250] It should be noted that the methods described herein describes possible implementations, and that the operations and the steps may be rearranged or otherwise

modified and that other implementations are possible. Further, aspects from two or more of the methods may be combined.

[0251] The various illustrative blocks and components described in connection with the disclosure herein may be implemented or performed with a general-purpose processor, a DSP, an ASIC, a CPU, an FPGA or other programmable logic device, 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 processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices (e.g., a combination of a DSP and a microprocessor, multiple microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration).

[0252] The functions described herein may be implemented in hardware, software executed by a processor, firmware, or any combination thereof. If implemented in software executed by a processor, the functions may be stored on or transmitted over as one or more instructions or code on a computer-readable medium. Other examples and implementations are within the scope of the disclosure and appended claims. For example, due to the nature of software, functions described herein may be implemented using software executed by a processor, hardware, firmware, hardwiring, or combinations of any of these. Features implementing functions may also be physically located at various positions, including being distributed such that portions of functions are implemented at different physical locations.

[0253] Computer-readable media includes both non-transitory computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A non-transitory storage medium may be any available medium that may be accessed by a general-purpose or special-purpose computer. By way of example, non-transitory computer-readable media may include RAM, ROM, electrically erasable programmable ROM (EEPROM), flash memory, compact disk (CD) ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other non-transitory medium that may be used to carry or store desired program code means in the form of instructions or data structures and

that may be accessed by a general-purpose or special-purpose computer, or a general-purpose or special-purpose processor.

[0254] As used herein, including in the claims, an article “a” before an element is unrestricted and understood to refer to “at least one” of those elements or “one or more” of those elements. The terms “a,” “at least one,” “one or more,” and “at least one of one or more” may be interchangeable. As used herein, including in the claims, “or” as used in a list of items (e.g., a list of items prefaced by a phrase such as “at least one of” or “one or more of” or “one or both of”) indicates an inclusive list such that, for example, a list of at least one of A, B, or C means A or B or C or AB or AC or BC or ABC (i.e., A and B and C). Also, as used herein, the phrase “based on” shall not be construed as a reference to a closed set of conditions. For example, an example step that is described as “based on condition A” may be based on both a condition A and a condition B without departing from the scope of the present disclosure. In other words, as used herein, the phrase “based on” shall be construed in the same manner as the phrase “based at least in part on. Further, as used herein, including in the claims, a “set” may include one or more elements.

[0255] The description herein is provided to enable a person having ordinary skill in the art to make or use the disclosure. Various modifications to the disclosure will be apparent to a person having ordinary skill in the art, and the generic principles defined herein may be applied to other variations without departing from the scope of the disclosure. Thus, the disclosure is not limited to the examples and designs described herein but is to be accorded the broadest scope consistent with the principles and novel features disclosed herein.

CLAIMS

What is claimed is:

1. A base station, comprising:
a processor; and
a transceiver coupled to the processor,
wherein the base station is a first target base station for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), and the processor is configured to:
determine a first security key to be used between a user equipment (UE)
and a second target base station for the LTM and a next hop (NH) chaining counter (NCC) to be used for a key derivation for a cell switch by the UE; and
transmit, via the transceiver and to the UE, the NCC.
2. The base station of claim 1, wherein the processor is further configured to:
transmit, via the transceiver and to the second target base station, the first security key and the NCC.
3. The base station of claim 2, wherein the first target base station includes a first target central unit (CU) and one or more distributed units (DUs), and the one or more DUs include a first target DU serving the UE.
4. The base station of claim 3, wherein the processor further includes a second processor of the first target DU, and the second processor is configured to:
transmit, via the transceiver and to the UE, the NCC received from the first target CU, such that the NCC is used by the UE to perform a second security key derivation to determine a second security key to be used between the UE and the second target base station.
5. The base station of claim 4, wherein the second processor is further configured to:
transmit, via the transceiver and to the UE, a second indicator indicating whether the security update is needed during the cell switch to the target cell, wherein the second indicator is determined by the first target DU based on the first indicator.

6. The base station of claim 5, wherein the second indicator includes one of the following:

- a security update indicator indicating whether the security update is needed;
- a CU indicator indicating that a CU of the target cell is different from the first target CU;
- an inter-CU LTM indicator indicating that the cell switch is associated with an inter-CU LTM; and
- a CU node identifier (ID) indicating an ID of a CU of the target cell.

7. The base station of claim 1, wherein the NCC is transmitted to the UE from the first target base station via a medium access control (MAC) control element (CE).

8. The base station of claim 7, wherein the MAC CE is a LTM cell switch command.

9. The base station of claim 4, wherein the second processor is further configured to:

- receive, via the transceiver and from the UE, a first security update failure message indicating a failure of the security update.

10. A method performed by a first target base station for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), the method comprising:

- determining a first security key to be used between a user equipment (UE) and a second target base station for the LTM and a next hop (NH) chaining counter (NCC) to be used for a key derivation for a cell switch by the UE; and
- transmitting the NCC to the UE.

11. A user Equipment (UE), comprising:

- a processor; and
 - a transceiver coupled to the processor,
- wherein the processor is configured to:

receive, via the transceiver and from a first target base station for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), a next hop (NH) chaining counter (NCC) to be used for a key derivation for a cell switch by the UE; and

perform a key derivation by using the NCC to determine a first security key to be used between the UE and a second target base station for the LTM.

12. The UE of claim 11, wherein the key derivation comprises:

in the case that a value of the NCC is equal to a value of a current NCC associated with a current security key used by the first target base station and the UE, computing the security key from the current security key; or

in the case that the value of the NCC is different from the value of the current NCC, synchronizing a locally kept NH parameter iteratively and increasing the value of the current NCC, and computing the security key from the synchronized NH parameter in the case that the value of the current NCC matches the value of the NCC received from the first target base station.

13. The UE of claim 11, wherein the processor is further configured to:

receive, via the transceiver and from the first target base station, an indicator indicating whether a security update is needed during a cell switch to a target cell, and

perform the key derivation in case the indicator indicates that the security update is needed.

14. The UE of claim 13, wherein the indicator includes one of the following:

a security update indicator indicating whether the security update is needed;

a CU indicator indicating that a CU of the target cell is different from the first target CU;

an inter-CU LTM indicator indicating that the cell switch is associated with an inter-CU LTM; and

a CU node identifier (ID) indicating an ID of a CU of the target cell.

15. The UE of claim 11, wherein the NCC is received by the UE from the first target base station via a medium access control (MAC) control element (CE).

16. The UE of claim 15, wherein the MAC CE is a LTM cell switch command.

17. The UE of claim 13, wherein the processor is further configured to:
transmit, via the transceiver and to the first target base station, a first security update failure message indicating a failure of the security update.

18. The UE of claim 11, wherein the processor is further configured to:
receive, via the transceiver and from the first target base station, information on security update parameters issued by an access and mobility management function (AMF); and
update a NH parameter associated with the first security key based on the information on security update parameters.

19. The UE of claim 18, wherein the information on security update parameters indicates that a non-access stratum (NAS) security context different from a currently active NAS security context is activated by the AMF.

20. A method performed by a user equipment (UE), the method comprising:
receiving, from a first target base station for layer 1/layer 2 (L1/L2)-triggered mobility (LTM), a next hop (NH) chaining counter (NCC) to be used for a key derivation for a cell switch by the UE; and
performing a key derivation by using the NCC to determine a first security key to be used between the UE and a second target base station for the LTM.