SECURITY RELATED MECHANISM FOR LTM

TECHNICAL FIELD

[0001] The present disclosure relates to wireless communications, and more specifically to master nodes (MN), secondary node (SN), methods, apparatuses, and computer readable medium for a security related mechanism for inter-MN layer 1/2 triggered mobility (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 the 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 done by explicit radio resource control (RRC) reconfiguration signalling to trigger the synchronization of target cell based on layer 3 (L3) measurements report, which may lead to longer latency, larger overhead, and longer interruption time than beam level mobility. Therefore, in the third generation partner project (3GPP), a work item on further new radio (NR) mobility enhancements, named as LTM, was approved to change a serving cell via L1/L2 signalling, in order to reduce the latency, overhead and interruption time.

[0004] Security key(s) may be used for communication between a UE and the network, for ciphering and integrity protections. In case the UE is connected to both MN and SN with

dual connectivity (DC), and the LTM procedure is occurred, details about the security keys should be further studied.

SUMMARY

[0005] The present disclosure relates to master nodes, user equipment (UE), core network entity, methods, apparatuses, processors, and computer readable medium for a security related mechanism. According to embodiments in the present disclosure, the security keys for subsequent LTM procedure can be determined and used.

[0006] In some implementations, there is provided a first MN. The first MN comprises at least one memory; and at least one processor coupled with the at least one memory and configured to cause the first MN to: determine that a UE with DC is to be handed over from the first MN to a second MN during an LTM procedure, wherein the first MN has become a serving MN for the UE after an LTM cell switch towards the first MN; transmit, to the second MN, a first message comprising a first security key and a first value associated with the first security key, wherein the first security key is to be used between the UE and the second MN after the second MN has become a serving MN for the UE; and transmit, to the UE, a second message indicating: the first value, which is to be used by the UE for derivation of the first security key associated with the second MN, and a second value, which is to be used by the UE for derivation of a second security key associated with an SN, wherein the SN remains unchanged after the second MN has become the serving MN for the UE.

[0007] In some implementations, there is provided a second MN. The second MN comprises at least one memory; and at least one processor coupled with the at least one memory and configured to cause the second MN to: receive, from a first MN, a first message comprising a first security key and a first value associated with the first security key, wherein a UE with DC is to be handed over from the first MN to the second MN during an LTM procedure, the first MN has become a serving MN for the UE after an LTM cell switch towards the first MN, and wherein the first security key is to be used between the UE and the second MN after the second MN has become a serving MN for the UE, and the first value is to be used by the UE for derivation of the first security key; determine, based on the first security key, a second security key associated with an SN and a second value associated with the second security key, wherein the SN remains unchanged after the second MN has become the serving MN for the UE; and transmit, to the SN, the second security key.

[0008] In some implementations, there is provided a UE. The UE comprises at least one

memory; and at least one processor coupled with the at least one memory and configured to cause the UE to: receive, from a first MN, a second message indicating: a first value, which is to be used by the UE for derivation of a first security key associated with a second MN, wherein the UE with DC is to be handed over from the first MN to the second MN during an LTM procedure, the first MN has become a serving MN for the UE after an LTM cell switch towards the first MN, and wherein the first security key is to be used between the UE and the second MN after the second MN has become a serving MN for the UE, and a second value, which is to be used by the UE for derivation of a second security key associated with an SN, wherein the SN remains unchanged after the second MN has become the serving MN for the UE; and determine the first security key and the second security key based on the second message.

[0009] In some implementations, there is provided a method performed by the first MN. The method comprises: determining that a UE with DC is to be handed over from the first MN to a second MN during an LTM procedure, wherein the first MN has become a serving MN for the UE after an LTM cell switch towards the first MN; transmitting, to the second MN, a first message comprising a first security key and a first value associated with the first security key, wherein the first security key is to be used between the UE and the second MN after the second MN has become a serving MN for the UE; and transmitting, to the UE, a second message indicating: the first value, which is to be used by the UE for derivation of the first security key associated with the second MN, and a second value, which is to be used by the UE for derivation of a second security key associated with an SN, wherein the SN remains unchanged after the second MN has become the serving MN for the UE.

[0010] In some implementations, there is provided a method performed by the second MN. The method comprises: receiving, from a first MN, a first message comprising a first security key and a first value associated with the first security key, wherein a UE with DC is to be handed over from the first MN to the second MN during an LTM procedure, the first MN has become a serving MN for the UE after an LTM cell switch towards the first MN, and wherein the first security key is to be used between the UE and the second MN after the second MN has become a serving MN for the UE, and the first value is to be used by the UE for derivation of the first security key; determining, based on the first security key, a second security key associated with an SN and a second value associated with the second security key, wherein the SN remains unchanged after the second MN has become the serving MN for the UE; and transmitting, to the SN, the second security key.

[0011] In some implementations, there is provided a method performed by the UE. The method comprises: receiving, from a first MN, a second message indicating: a first value, which is to be used by the UE for derivation of a first security key associated with a second MN, wherein the UE with DC is to be handed over from the first MN to the second MN during an LTM procedure, the first MN has become a serving MN for the UE after an LTM cell switch towards the first MN, and wherein the first security key is to be used between the UE and the second MN after the second MN has become a serving MN for the UE, and a second value, which is to be used by the UE for derivation of a second security key associated with an SN, wherein the SN remains unchanged after the second MN has become the serving MN for the UE; and determining the first security key and the second security key based on the second message.

[0012] In some implementations, there is provided a processor for wireless communication. The processor comprises at least one controller coupled with at least one memory and configured to cause the processor to: determine that a UE with DC is to be handed over from the first MN to a second MN during an LTM procedure, wherein the first MN has become a serving MN for the UE after an LTM cell switch towards the first MN; transmit, to the second MN, a first message comprising a first security key and a first value associated with the first security key, wherein the first security key is to be used between the UE and the second MN after the second MN has become a serving MN for the UE; and transmit, to the UE, a second message indicating: the first value, which is to be used by the UE for derivation of the first security key associated with the second MN, and a second value, which is to be used by the UE for derivation of a second security key associated with an SN, wherein the SN remains unchanged after the second MN has become the serving MN for the UE.

[0013] In some implementations, there is provided a processor for wireless communication. The processor comprises at least one controller coupled with at least one memory and configured to cause the processor to: receive, from a first MN, a first message comprising a first security key and a first value associated with the first security key, wherein a UE with DC is to be handed over from the first MN to the second MN during an LTM procedure, the first MN has become a serving MN for the UE after an LTM cell switch towards the first MN, and wherein the first security key is to be used between the UE and the second MN after the second MN has become a serving MN for the UE, and the first value is to be used by the UE for derivation of the first security key; determine, based on the first security key, a second security key associated with an SN and a second value associated with the second security

key, wherein the SN remains unchanged after the second MN has become the serving MN for the UE; and transmit, to the SN, the second security key.

[0014] In some implementations, there is provided a processor for wireless communication. The processor comprises at least one controller coupled with at least one memory and configured to cause the processor to: receive, from a first MN, a second message indicating: a first value, which is to be used by the UE for derivation of a first security key associated with a second MN, wherein the UE with DC is to be handed over from the first MN to the second MN during an LTM procedure, the first MN has become a serving MN for the UE after an LTM cell switch towards the first MN, and wherein the first security key is to be used between the UE and the second MN after the second MN has become a serving MN for the UE, and a second value, which is to be used by the UE for derivation of a second security key associated with an SN, wherein the SN remains unchanged after the second MN has become the serving MN for the UE; and determine the first security key and the second security key based on the second message.

[0015] In some implementations of the methods and the first MN described herein, further comprising: receiving, from the second MN, a first response indicating an acknowledge (ACK) of the first message, wherein the first response comprises the index of the second value.

[0016] In some implementations of the methods and the first MN described herein, further comprising: receiving, from the second MN, a first response indicating an acknowledge of the first message.

[0017] In some implementations of the methods, the first MN, and the second MN described herein, further comprising: receiving, from a source MN of the LTM procedure, a cell switch notification comprising one of: a target cell ID associated with the first MN, or an ID of the first MN.

[0018] In some implementations of the methods and the second MN described herein, further comprising: transmitting, to the first MN, a first response indicating an acknowledge of the first message, wherein the first response comprises an index of the second value in a second list associated with the second MN.

[0019] In some implementations of the methods and the second MN described herein, further comprising: receiving, from a source MN of the LTM procedure during an LTM preparation phase, a handover request associated with the UE; and transmitting, to the source

MN, a handover request acknowledge comprising: the second list associated with the second MN, and a counter value to be used by the UE for derivation of a further security key between the UE and the second MN after the UE hands over from the source MN to the second MN.

[0020] In some implementations of the methods and the second MN described herein, further comprising: transmitting, to the first MN, a first response indicating an acknowledge of the first message.

[0021] In some implementations of the methods and the UE described herein, further comprising: receiving, from a source MN of the LTM procedure, an RRC reconfiguration message comprising: a second list associated with the second MN, and a counter value to be used by the UE for derivation of a further security key between the UE and the second MN after the second MN has become the serving MN for the UE.

[0022] In some implementations of the methods and the UE described herein, further comprising: determining the updated list by removing, from the second list, the counter value associated with the second MN that is comprised in the RRC reconfiguration message; and selecting the first counter value in the updated list.

[0023] In some implementations of the methods and the UE described herein, further comprising: determining the number of LTM cell switch during the LTM procedure; and determining the second value from the second list based on the number, wherein a location of the second value in the second list is the number.

[0024] In some implementations of the methods, the first MN, the second MN, and the UE described herein, the second message indicates to the UE to determine the second value based on a first counter value in an updated list associated with the second MN.

[0025] In some implementations of the methods, the first MN, the second MN, and the UE described herein, the first counter value is different from a counter value that is provided to the UE during an LTM preparation phase which is initiated by a source MN of the LTM procedure.

[0026] In some implementations of the methods, the first MN, the second MN, and the UE described herein, the second message indicates to the UE to determine the second value based on a number of LTM cell switch and a second list associated with the second MN.

[0027] In some implementations of the methods, the first MN, the second MN, and the UE described herein, the second message comprises an index of the second value in a second list

associated with the second MN.

[0028] In some implementations of the methods, the first MN, the second MN, and the UE described herein, the second list associated with the second MN is provided to the UE from the second MN via a source MN of the LTM procedure during an LTM preparation phase.

[0029] In some implementations of the methods, the first MN, the second MN, and the UE described herein, each of the first response and the second message comprises the second value.

[0030] In some implementations of the methods, the first MN, the second MN, and the UE described herein, each of the first response and the second message indicates that the second value corresponds to a counter value provided to the UE from the second MN via a source MN of the LTM procedure during an LTM preparation phase.

[0031] In some implementations of the methods, the first MN, the second MN, and the UE described herein, the first message further comprises one of: an identifier (ID) of the UE, or a node ID of the SN.

[0032] In some implementations of the methods, the first MN, the second MN, and the UE described herein, the ID of the UE comprises an identifier of the UE allocated by a source MN of the LTM procedure during an LTM preparation phase.

[0033] In some implementations of the methods, the first MN, the second MN, and the UE described herein, the second message comprises an LTM cell switch command.

[0034] In some implementations of the methods, the first MN, the second MN, and the UE described herein, the first value comprises a value of next hop chaining counter (NCC), and the second value comprises a value of a security key counter.

[0035] In some implementations of the methods, the first MN, the second MN, and the UE described herein, the first message is transmitted to the second MN via a source MN of the LTM procedure.

[0036] In some implementations of the methods, the first MN, the second MN, and the UE described herein, the second value is determined based on a first counter value in an updated list associated with the second MN, wherein the updated list is determined based on a second list associated with the second MN which is generated during an LTM preparation phase.

[0037] In some implementations of the methods, the first MN, the second MN, and the UE described herein, the second value is determined based on a number of LTM cell switch

during the LTM procedure and a second list associated with the second MN.

[0038] In some implementations, there is provided a core network entity, such as an access and mobility management function (AMF). The core network entity comprises at least one memory; and at least one processor coupled with the at least one memory and configured to cause the core network entity to: receive, from a source MN of a UE, a first message indicating a list of candidate cells for an LTM procedure of the UE; and transmit, to the source MN, a second message comprising a list of value pairs, wherein a first value pair in the list of value pairs comprises paired first value and second value, wherein the first value pair is used for a first candidate cell in the list of candidate cells, and wherein the first value and the second value are to be used for derivation of a security key between the UE and a first candidate MN associated with the first candidate cell after the UE hands over to the first candidate MN.

[0039] In some implementations, there is provided a source MN. The source MN comprises at least one memory; and at least one processor coupled with the at least one memory and configured to cause the source MN to: transmit, to a core network entity, a first message indicating a list of candidate cells for an LTM procedure of a UE; and receive, from the core network entity, a second message comprising a list of value pairs, wherein a first value pair in the list of value pairs comprises paired first value and second value, wherein the first value pair is used for a first candidate cell in the list of candidate cells, and wherein the first value and the second value are to be used for derivation of a security key between the UE and a first candidate MN associated with the first candidate cell after the UE hands over to the first candidate MN.

[0040] In some implementations, there is provided a first MN. The first MN comprises at least one memory; and at least one processor coupled with the at least one memory and configured to cause the first MN to: perform, for a UE, an LTM cell switch towards the first MN during an LTM procedure, wherein the first MN has become a serving MN for the UE after the LTM cell switch; transmit, to a core network entity, a path switch request; and receive, from the core network entity, a path switch response indicating an acknowledge of the path switch request without a reconfigured value pair for use.

[0041] In some implementations, there is provided a method performed by the core network entity. The method comprises: receiving, from a source MN of a UE, a first message indicating a list of candidate cells for an LTM procedure of the UE; and transmitting, to the

source MN, a second message comprising a list of value pairs, wherein a first value pair in the list of value pairs comprises paired first value and second value, wherein the first value pair is used for a first candidate cell in the list of candidate cells, and wherein the first value and the second value are to be used for derivation of a security key between the UE and a first candidate MN associated with the first candidate cell after the UE hands over to the first candidate MN.

[0042] In some implementations, there is provided a method performed by the source MN. The method comprises: transmitting, to a core network entity, a first message indicating a list of candidate cells for an LTM procedure of a UE; and receiving, from the core network entity, a second message comprising a list of value pairs, wherein a first value pair in the list of value pairs comprises paired first value and second value, wherein the first value pair is used for a first candidate cell in the list of candidate cells, and wherein the first value and the second value are to be used for derivation of a security key between the UE and a first candidate MN associated with the first candidate cell after the UE hands over to the first candidate MN.

[0043] In some implementations, there is provided a method performed by the first MN. The method comprises: performing, for a UE, an LTM cell switch towards the first MN during an LTM procedure, wherein the first MN has become a serving MN for the UE after the LTM cell switch; transmitting, to a core network entity, a path switch request; and receiving, from the core network entity, a path switch response indicating an acknowledge of the path switch request without a reconfigured value pair for use.

[0044] In some implementations, there is provided a processor for wireless communication. The processor comprises at least one controller coupled with at least one memory and configured to cause the processor to: receive, from a source MN of a UE, a first message indicating a list of candidate cells for an LTM procedure of the UE; and transmit, to the source MN, a second message comprising a list of value pairs, wherein a first value pair in the list of value pairs comprises paired first value and second value, wherein the first value pair is used for a first candidate cell in the list of candidate cells, and wherein the first value and the second value are to be used for derivation of a security key between the UE and a first candidate MN associated with the first candidate cell after the UE hands over to the first candidate MN.

[0045] In some implementations, there is provided a processor for wireless communication. The processor comprises at least one controller coupled with at least one memory and

configured to cause the processor to: transmit, to a core network entity, a first message indicating a list of candidate cells for an LTM procedure of a UE; and receive, from the core network entity, a second message comprising a list of value pairs, wherein a first value pair in the list of value pairs comprises paired first value and second value, wherein the first value pair is used for a first candidate cell in the list of candidate cells, and wherein the first value and the second value are to be used for derivation of a security key between the UE and a first candidate MN associated with the first candidate cell after the UE hands over to the first candidate MN.

[0046] In some implementations, there is provided a processor for wireless communication. The processor comprises at least one controller coupled with at least one memory and configured to cause the processor to: perform, for a UE, an LTM cell switch towards the first MN during an LTM procedure, wherein the first MN has become a serving MN for the UE after the LTM cell switch; transmit, to a core network entity, a path switch request; and receive, from the core network entity, a path switch response indicating an acknowledge of the path switch request without a reconfigured value pair for use.

[0047] In some implementations of the methods and the core network entity described herein, further comprising: receiving, from the first candidate MN, a path switch request; and transmitting, to the first candidate MN, a path switch response indicating an acknowledge of the path switch request.

[0048] In some implementations of the methods and the source MN described herein, further comprising: determining, based on the second message, the security key between the UE and the first candidate MN; and transmitting, to the first candidate MN, a third message comprising the security key and the second value.

[0049] In some implementations of the methods, the core network entity, the source MN, and the first MN described herein, the path switch request comprises a first indicator indicating that a cause of a path switch to the first candidate MN is an LTM.

[0050] In some implementations of the methods, the core network entity, the source MN, and the first MN described herein, the path switch response comprises a further value pair which should not be used by the first candidate MN.

[0051] In some implementations of the methods, the core network entity, the source MN, and the first MN described herein, the path switch response comprises a second indicator indicating that the further value pair should be neglected.

[0052] In some implementations of the methods, the core network entity, the source MN, and the first MN described herein, the first value comprises a value of next hop (NH), and the second value comprises a value of NCC.

[0053] In some implementations, there is provided a first MN. The first MN comprises at least one memory; and at least one processor coupled with the at least one memory and configured to cause the first MN to: receive, from a source MN of a UE, a handover request for an LTM procedure, wherein the handover request comprises a first security key, a first value, and a list of a plurality of candidate cells, wherein the first security key is to be used between the UE and the first MN after the UE hands over from the source MN to the first MN, and wherein the first value is to be used by the UE for derivation of the first security key; and transmit, to each of a plurality of candidate MNs associated with the plurality of candidate cells, a further handover request comprising a corresponding security key and a corresponding value for a corresponding candidate MN, wherein the corresponding security key is to be used between the UE and the corresponding candidate MN after the UE hands over from the first MN to the corresponding candidate MN, and wherein the corresponding value is to be used by the UE for derivation of the corresponding security key.

[0054] In some implementations, there is provided a method performed by the first MN. The method comprises: receiving, from a source MN of a UE, a handover request for an LTM procedure, wherein the handover request comprises a first security key, a first value, and a list of a plurality of candidate cells, wherein the first security key is to be used between the UE and the first MN after the UE hands over from the source MN to the first MN, and wherein the first value is to be used by the UE for derivation of the first security key; and transmitting, to each of a plurality of candidate MNs associated with the plurality of candidate cells, a further handover request comprising a corresponding security key and a corresponding value for a corresponding candidate MN, wherein the corresponding security key is to be used between the UE and the corresponding candidate MN after the UE hands over from the first MN to the corresponding candidate MN, and wherein the corresponding value is to be used by the UE for derivation of the corresponding security key.

[0055] In some implementations, there is provided a processor for wireless communication. The processor comprises at least one controller coupled with at least one memory and configured to cause the processor to: receive, from a source MN of a UE, a handover request for an LTM procedure, wherein the handover request comprises a first security key, a first value, and a list of a plurality of candidate cells, wherein the first security key is to be used

between the UE and the first MN after the UE hands over from the source MN to the first MN, and wherein the first value is to be used by the UE for derivation of the first security key; and transmit, to each of a plurality of candidate MNs associated with the plurality of candidate cells, a further handover request comprising a corresponding security key and a corresponding value for a corresponding candidate MN, wherein the corresponding security key is to be used between the UE and the corresponding candidate MN after the UE hands over from the first MN to the corresponding candidate MN, and wherein the corresponding value is to be used by the UE for derivation of the corresponding security key.

[0056] In some implementations of the methods and the first MN described herein, further comprising: receiving, from the corresponding candidate MN, a further handover request acknowledge comprising a further corresponding value, wherein the further corresponding value is to be used by the UE for derivation of a security key between the UE and an SN after the UE hands over from the first MN to the corresponding candidate MN.

[0057] In some implementations of the methods and the first MN described herein, further comprising: transmitting, to the source MN, a handover request acknowledge message comprising: the first value and a second value associated with the first MN, wherein the second value is to be used by the UE for derivation a security key between the UE and the SN after the UE hands over from the source MN to the first MN, and the corresponding value and the further corresponding value associated with the corresponding candidate MN.

[0058] In some implementations of the methods and the first MN described herein, further comprising: transmitting, to the SN, an SN addition request message comprising a second security key which is determined based on the first security key and the second value, wherein the second security key is to be used between the UE and the SN after the UE hands over from the source MN to the first MN.

[0059] In some implementations of the methods and the first MN described herein, the further corresponding value comprises a value of a security key counter.

[0060] In some implementations of the methods and the first MN described herein, the first value comprises a value of NCC.

BRIEF DESCRIPTION OF THE DRAWINGS

[0061] FIG. 1 illustrates an example of a wireless communications system in which some embodiments of the present disclosure can be implemented;

[0062] FIG. 2A illustrates an example schematic of 5G key derivation;

[0063] FIG. 2B illustrates an example schematic of intra-CU intra-DU mobility;

[0064] FIG. 2C illustrates an example schematic of intra-CU inter-DU mobility;

[0065] FIG. 2D illustrates an example schematic of inter-CU mobility;

[0066] FIG. 2E illustrates an example schematic of subsequent LTM procedure;

[0067] FIG. 2F illustrates an overall procedure for LTM;

[0068] FIG. 2G illustrates an example schematic of a dual connectivity protocol architecture for multi-radio dual connectivity (MR-DC) with 5GC;

[0069] FIG. 2H illustrates an example schematic of security aspects in SN Addition/Modification procedures;

[0070] FIG. 2I illustrates a schematic diagram of an example communication network in which some embodiments of the present disclosure can be implemented;

[0071] FIG. 3 illustrates a signalling chart illustrating communication process in accordance with some example embodiments of the present disclosure;

[0072] FIGS. 4A-4B illustrate signalling charts illustrating some detailed processes in accordance with some example embodiments of the present disclosure;

[0073] FIG. 5 illustrates another signalling chart illustrating communication process in accordance with some example embodiments of the present disclosure;

[0074] FIG. 6 illustrates a further signalling chart illustrating communication process in accordance with some example embodiments of the present disclosure;

[0075] FIG. 7 illustrates an example of a device that is suitable for implementing embodiments of the present disclosure;

[0076] FIG. 8 illustrates an example of a processor that is suitable for implementing some embodiments of the present disclosure;

[0077] FIG. 9 illustrates a flowchart of an example method implemented at a first MN in accordance with aspects of the present disclosure;

[0078] FIG. 10 illustrates a flowchart of an example method implemented at a second MN in accordance with aspects of the present disclosure;

[0079] FIG. 11 illustrates a flowchart of an example method implemented at a UE in

accordance with aspects of the present disclosure;

[0080] FIG. 12 illustrates a flowchart of an example method implemented at a core network entity (such as AMF) in accordance with aspects of the present disclosure;

[0081] FIG. 13 illustrates a flowchart of an example method implemented at a source MN in accordance with aspects of the present disclosure;

[0082] FIG. 14 illustrates a flowchart of an example method implemented at a first MN in accordance with aspects of the present disclosure; and

[0083] FIG. 15 illustrates a flowchart of an example method implemented at a first MN in accordance with aspects of the present disclosure.

[0084] Throughout the drawings, the same or similar reference numerals represent the same or similar element.

DETAILED DESCRIPTION

[0085] 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 can be implemented in various manners other than the ones described below. 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.

[0086] 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.

[0087] 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. In some examples, values, procedures, or apparatuses are referred to as "best," "lowest," "highest," "minimum," "maximum," or the like. It will be appreciated that such descriptions are intended to indicate that a selection among many used functional alternatives can be made, and such selections need not be better, smaller, higher, or otherwise preferable to other selections.

[0088] The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of 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, components and/or the like, but do not preclude the presence or addition of one or more other features, elements, components and/or combinations thereof. For example, the term "includes" and its variants are to be read as open terms that mean "includes, but is not limited to." The term "based on" is to be read as "based at least in part on." The term "one embodiment" and "an embodiment" are to be read as "at least one embodiment." The term "another embodiment" is to be read as "at least one other embodiment." The use of an expression such as "A and/or B" can mean either "only A" or "only B" or "both A and B." Other definitions, explicit and implicit, may be included below.

[0089] FIG. 1 illustrates an example of a wireless communications system 100 in which some embodiments of the present disclosure can be implemented. 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 (CN) 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 a long term evolution (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 a new radio (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.

[0090] 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.

[0091] 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, message, 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.

[0092] 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.

[0093] 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 CN 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.

[0094] 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 (SL). For example, a UE 104 may support wireless communication directly with another UE 104 over a PC5 interface.

[0095] A network entity 102 may support communications with the CN 106, or with another network entity 102, or both. For example, a network entity 102 may interface with the CN 106 through one or more backhaul links 116 (e.g., via an S1, N2, N3, 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 CN 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).

[0096] 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 RAN (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 central unit (CU), a distributed unit (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.

[0097] 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)).

[0098] 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 adaption 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.

[0099] 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).

[00100] 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.

[00101] The CN 106 may support user authentication, access authorization, tracking, connectivity, and other access, routing, or mobility functions. The CN 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 CN 106.

[00102] The CN 106 may communicate with the packet data network 108 over one or more backhaul links 116 (e.g., via an S1, N2, N3, 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 CN 106 via a network entity 102. The CN 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 CN 106 (e.g., one or more network functions of the CN 106).

[00103] 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.

[00104] 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., μ=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., μ=0) associated with the first subcarrier spacing (e.g., 15 kHz) may utilize one slot per subframe. A second numerology (e.g., μ=1) may be associated with a second subcarrier spacing (e.g., 30 kHz) and a normal cyclic prefix. A third numerology (e.g., μ=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., μ=3) may be associated with a fourth subcarrier spacing (e.g., 120 kHz) and a normal cyclic prefix. A fifth numerology (e.g., μ=4) may be associated with a fifth subcarrier spacing (e.g., 240 kHz) and a normal cyclic prefix.

[00105] 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.

[00106] 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., μ=0, μ=1, μ=2, μ=3, μ=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., orthogonal frequency-division multiplexing (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., μ=0) associated with a first subcarrier spacing (e.g., 15 kHz) may be used interchangeably between subframes and slots.

[00107] 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.

[00108] 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., μ=0), which includes 15 kHz subcarrier spacing; a second numerology (e.g., μ=1), which includes 30 kHz subcarrier spacing; and a third numerology (e.g., μ=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., μ=2), which includes 60 kHz subcarrier spacing; and a fourth numerology (e.g., μ=3), which

includes 120 kHz subcarrier spacing.

[00109] The following principles apply to NR connected to 5G core (5GC) security:

- For user data (DRBs), ciphering provides user data confidentiality and integrity protection provides user data integrity;
- For RRC signalling (SRBs), ciphering provides signalling data confidentiality and integrity protection signalling data integrity;

NOTE: Ciphering and integrity protections are optionally configured except for RRC signalling for which integrity protection is always configured. Ciphering and integrity protection can be configured per DRB but all DRBs belonging to a PDU session for which the User Plane Security Enforcement information indicates that UP integrity protection is required, are configured with integrity protection.

- For key management and data handling, any entity processing cleartext shall be protected from physical attacks and located in a secure environment;
- The gNB (AS) keys are cryptographically separated from the 5GC (NAS) keys;
- Separate AS and NAS level Security Mode Command (SMC) procedures are used;
- A sequence number (COUNT) is used as input to the ciphering and integrity protection and a given sequence number must only be used once for a given key (except for identical re-transmission) on the same radio bearer in the same direction.

[00110] The keys are organised and derived as follows:

- Key for AMF:
  - K_{AMF} is a key derived by ME and 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.

[00111] FIG. 2A illustrates an example schematic of 5G key derivation 201. 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 SMC procedure.

[00112] Whenever an initial AS security context needs to be established between UE and gNB, AMF and the UE derive a K_{gNB} and a Next Hop parameter (NH). 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.

[00113] 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).

[00114] The AS SMC procedure is for RRC and 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 3GPP specification 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 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 DRBs shall be performed only after RRC security has been activated as part of the AS SMC procedure.

[00115] 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 UL and 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.

[00116] Key refresh is possible for K_{gNB}, $K_{RRC\text{-}enc}$, $K_{RRC\text{-}int}$, $K_{UP\text{-}enc}$, and $K_{UP\text{-}int}$ 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}, $K_{RRC\text{-}enc}$, $K_{RRC\text{-}int}$, $K_{UP\text{-}enc}$, and $K_{UP\text{-}int}$ and can be initiated by the AMF when a 5G AS security context different from the currently active one shall be activated.

[00117] LTM refers to a cell switch procedure that the network triggers via medium access control – control element (MAC CE) based on L1 measurements. The potential applicable scenarios of LTM include intra-CU intra-DU mobility, intra-CU inter-DU mobility, and inter-CU mobility, as shown in FIGS. 2B-2D respectively. FIG. 2B illustrates an example schematic of intra-CU intra-DU mobility 202, in which the UE moves between different cells within a DU. FIG. 2C illustrates an example schematic of intra-CU inter-DU mobility 203 in which the UE moves between different cells belonging to different DUs but within a CU. FIG. 2D illustrates an example schematic of inter-CU mobility 204, in which the UE moves between different cells belonging to different DUs, where the DUs belongs to different CUs.

[00118] Subsequent LTM refers to LTM cell switch procedures between candidate cells without RRC reconfiguration by the network in between. FIG. 2E illustrates an example schematic of subsequent LTM procedure 205. When the UE connects to the source gNB, the source gNB prepares all the candidate configurations within the candidate gNB and provides them to the UE through RRC signalling. As shown, the LTM refers to the mobility from the source gNB to the candidate gNB1. The subsequent LTM refers to the mobility from the candidate gNB1 to the candidate gNB2, or the mobility from the candidate gNB1 back to the source gNB, without any further RRC reconfiguration.

[00119] LTM is a procedure in which a gNB receives L1 measurement report(s) from a UE, and on their basis the gNB changes UE serving cell by a cell switch command signalled via a MAC CE. The cell switch command indicates an LTM candidate configuration that the gNB previously prepared and provided to the UE through RRC signalling. Then the UE switches to the target configuration according to the cell switch command. The LTM procedure can be used to reduce the mobility latency.

[00120] When configured by the network, it is possible to activate transmission configuration indication (TCI) states of one or multiple cells that are different from the current serving cell. For instance, the TCI states of the LTM candidate cells can be activated

in advance before any of those cells become the serving cell. This allows the UE to be DL synchronized with those cells, thereby facilitating a faster cell switch to one of those cells when cell switch is triggered.

[00121] When configured by the network, it is possible to initiate UL time advance (TA) acquisition (called early TA) procedure of one or multiple cells that are different from the current serving cells. If the cell has the same NTA as the current serving cells or NTA=0, early TA acquisition procedure is not required. The network may request the UE to perform early TA acquisition of a candidate cell before a cell switch. The early TA acquisition procedure is triggered by PDCCH order or realized through UE-based TA measurement as configured by RRC. In the former case, the gNB to which the candidate cell belongs calculates the TA value and sends it to the gNB to which the serving cell belongs. The serving cell sends the TA value in the LTM cell switch command MAC CE when triggering LTM cell switch. In the latter case, the UE performs TA measurement for the candidate cells after being configured by RRC but the exact time the UE performs TA measurement is up to UE implementation. The UE applies the TA value measured by itself and performs RACH-less LTM upon receiving the cell switch command. The network may also send a TA value in the LTM cell switch command MAC CE without early TA acquisition.

[00122] Depending on the availability of a valid TA value, the UE performs either a RACH-less LTM or RACH-based LTM cell switch. If the TA value is provided in the cell switch command, the UE applies the TA value as instructed by the network. In the case where UE-based TA measurement is configured, but no TA value is provided in the cell switch command, the UE applies the TA value by itself if available. Meanwhile, the UE performs RACH-less LTM cell switch upon receiving the cell switch command. If no valid TA value is available, the UE performs RACH-based LTM cell switch.

[00123] Regardless of whether the UE is configured for UE-based TA measurement for a certain candidate cell, it will still follow the PDCCH order, which includes requesting a random access procedure towards the candidate cells. This also applies to the candidate cells for which the UE is capable of deriving TA values by itself. Additionally, regardless of whether the UE has already performed a random access procedure towards the candidate cells, it will still follow the UE-based measurement configuration if configured by the network.

[00124] For RACH-less LTM, the UE accesses the target cell using either a configured grant

or a dynamic grant. The configured grant is provided in the LTM candidate configuration, and the UE selects the configured grant occasion associated with the beam indicated in the cell switch command. Upon initiation of LTM cell switch to the target cell, the UE starts to monitor PDCCH on the target cell for dynamic scheduling. Before RACH-less LTM procedure completion, the UE shall not trigger random access procedure if it does not have a valid PUCCH resource for triggered SRs.

[00125] The following principles apply to LTM: Security key is maintained upon an LTM cell switch; and Subsequent LTM is supported.

[00126] LTM supports both intra-gNB-DU and intra-gNB-CU inter-gNB-DU mobility. LTM supports both intra-frequency and inter-frequency mobility, including mobility to inter-frequency cell that is not a current serving cell. LTM is supported only for licensed spectrum. The following scenarios are supported: -PCell change in non-CA scenario and non-DC scenario; -PCell and SCell(s) change in CA scenario; -Dual connectivity scenario, PCell and MCG SCell(s) change and intra-SN PSCell and SCG SCell(s) change without MN involvement. LTM for simultaneous PCell and PSCell change is not supported. While the UE has stored LTM candidate configurations the UE can also execute any L3 handover command sent by the network.

[00127] Cell switch command is conveyed in a MAC CE, which contains the necessary information to perform the LTM cell switch. FIG. 2F illustrates an overall procedure for LTM 206. Subsequent LTM is done by repeating the early synchronization, LTM cell switch execution, and LTM cell switch completion steps without releasing other LTM candidate cell configurations after each LTM cell switch completion. The general procedure over the air interface is applicable to SCG LTM.

[00128] At step 1 in FIG. 2F, the UE sends a MeasurementReport message to the gNB. The gNB decides to configure LTM and initiates candidate cell(s) preparation. At step 2, the gNB transmits an RRCReconfiguration message to the UE including the LTM candidate cell configurations of one or multiple candidate cells. At step 3, the UE stores the LTM candidate cell configurations and transmits an RRCReconfigurationComplete message to the gNB.

[00129] At step 4a, the UE may performs DL synchronization with candidate cell(s) before receiving the cell switch command. It is understood that DL synchronization for candidate cell(s) before cell switch command is supported, at least based on synchronization signal

block (SSB).

[00130] At step 4b, if requested by the network, the UE performs early TA acquisition with candidate cell(s) before receiving the cell switch command. This is done via CFRA triggered by a PDCCH order from the source cell, following which the UE sends preamble towards the indicated candidate cell. In order to minimize the data interruption of the source cell due to CFRA towards the candidate cell(s), the UE doesn't receive RAR for the purpose of TA value acquisition and the TA value of the candidate cell is indicated in the cell switch command. The UE doesn't maintain the TA timer for the candidate cell and relies on network implementation to guarantee the TA validity.

[00131] At step 5, the UE performs L1 measurements on the configured candidate cell(s) and transmits L1 measurement reports to the gNB. L1 measurement should be performed as long as apply the RRC reconfiguration in step 2.

[00132] At step 6, the gNB decides to execute cell switch to a target cell and transmits a MAC CE triggering cell switch by including the candidate configuration index of the target cell. The UE switches to the target cell and applies the configuration indicated by candidate configuration index.

[00133] At step 7, the UE performs the random access procedure towards the target cell, if UE does not have valid TA of the target cell.

[00134] At step 8, the UE completes the LTM cell switch procedure by sending RRCReconfigurationComplete message to target cell. If the UE has performed a RA procedure in step 7, the UE considers that LTM execution is successfully completed when the random access procedure is successfully completed. For RACH-less LTM, the UE considers that LTM execution is successfully completed when the UE determines that the network has successfully received its first UL data. The UE determines successful reception of its first UL data by receiving a PDCCH addressing the UE's C-RNTI in the target cell, which schedules a new transmission following the first UL data.

[00135] In some cases, the steps 4-8 can be performed multiple times for subsequent LTM using the LTM candidate cell configuration(s) provided in step 2.

[00136] The procedure over the air interface is applicable to both intra-DU LTM and inter-DU LTM. The overall LTM procedures over F1-C and Xn interface are captured in prior art which will be repeated in the present disclosure.

[00137] In 3GPP release 18 (R18), the LTM focuses on the intra-CU LTM (including intra-CU intra-DU LTM and intra-CU inter-DU LTM) only. In R19, the LTM will focus on the inter-CU LTM, including specify support for inter-CU Layer 2 Mobility (LTM):

- Prioritize the case when CU is acting as MN when DC is not configured.
- As secondary priority, support the case when NR-DC is configured and CU is acting as SN and MCG is unchanged.
- As secondary priority, support the case when NR-DC is configured, CU is acting as MN and SCG is unchanged or SCG is released. Note: The case that LTM is configured in both MCG and SCG is excluded.
- Specify support for subsequent LTM mobility procedures aiming to avoid RRC configuration between cell switches as per Rel-18 LTM. Coordination with SA3 needed with respect to security key handling.
- Note: Rel. 18 intra-CU LTM procedure is considered as baseline for adding inter-CU support.

[00138] FIG. 2G illustrates an example schematic of a dual connectivity protocol architecture 207 for MR-DC with 5GC. Details of the architecture illustrating MCG, SCG, and Split bearers for both SRBs and DRBs are shown. The architecture has the following variants.

[00139] NG-RAN E-UTRA-NR Dual Connectivity (NGEN-DC) is the variant when the UE is connected to one ng-eNB that acts as a Master Node (MN) and one gNB that acts as a Secondary Node (SN). The ng-eNB is connected to the 5GC and the gNB is connected to the ng-eNB via Xn interface.

[00140] NR-E-UTRA Dual Connectivity (NE-DC) is the variant when the UE is connected to one gNB that acts as a MN and one ng-eNB that acts as a SN. The MN (i.e., gNB) is connected to 5GC and the ng-eNB (i.e., SN) is connected to the gNB via Xn interface.

[00141] NR-NR Dual Connectivity (NR-DC) is the variant when the UE is connected to one gNB that acts as a MN and one gNB that acts as a SN. The MN is connected to 5GC while the SN is connected to MN via Xn interface.

[00142] When the MN establishes security context between an SN and the UE for the first time for a given AS security context shared between the MN and the UE, the MN generates the K_{SN} for the SN and sends it to the SN over the Xn-C. To generate the K_{SN}, the MN

associates a counter, called an SN Counter or an SK counter, with the current AS security context. The SN Counter is used as freshness input into K_{SN} derivations. The MN sends the value of the SN Counter to the UE over the RRC signalling path when it is required to generate a new K_{SN}. The K_{SN} is used to derive further RRC and UP keys that are used between the UE and SN.

[00143] When the MN is executing the Secondary Node Addition procedure (i.e. initial offload of one or more radio bearers to the SN), or the Secondary Node Modification procedure which requires an update of the K_{SN}, the MN shall derive an K_{SN}. The MN shall maintain the SN Counter. In the case of Conditional PSCell Change and conditional PSCell addition, if there are more than one candidate SNs, for each SN, the MN shall derive a different K_{SN} via using different SN counter.

[00144] When executing the procedure for adding subsequent radio bearer(s) to the same SN, the MN shall, for each new radio bearer, assign a radio bearer identity that has not previously been used since the last K_{SN} change. If the MN cannot allocate an unused radio bearer identity for a new radio bearer in the SN, due to radio bearer identity space exhaustion, the MN shall increment the SN Counter and compute a fresh K_{SN}, and then shall perform a SN Modification procedure to update the K_{SN}.

[00145] FIG. 2H illustrates an example schematic of security aspects 208 in SN Addition/Modification procedures (MN initiated). The dual connectivity procedure with activation of encryption/decryption and integrity protection follows the steps below.

[00146] 1. The UE and the MN establish the RRC connection.

[00147] 2. The MN sends SN Addition/Modification Request to the SN over the Xn-C to negotiate the available resources, configuration, and algorithms at the SN. The MN computes and delivers the K_{SN} to the SN if a new key is needed. The UE security capabilities and the UP security policy received from the SMF shall also be sent to SN. In case of PDU split, UP integrity protection and ciphering activation decision from MN may be also included. When the MN decides to configure CPA or CPC, if there are more than one candidate SNs, for each SN, the MN shall derive a different K_{SN} and delivers the K_{SN} to each SN separately.

[00148] 3. The SN allocates the necessary resources and chooses the ciphering algorithm and integrity algorithm which has the highest priority from its configured list and is also present in the UE security capability. If a new K_{SN} was delivered to the SN then the SN

calculates the needed RRC. The UP keys may be derived at the same time when RRC key derived. The SN shall activate the UP security policy.

[00149] 4. The SN sends SN Addition/Modification Acknowledge to the MN indicating availability of requested resources and the identifiers for the selected algorithm(s) for the requested DRBs and/or SRB for the UE. The UP integrity protection and encryption indications shall be send to the MN.

[00150] 5. The MN sends the RRC Connection Reconfiguration Request to the UE instructing it to configure the new DRBs and/or SRB for the SN. The MN shall include the SN Counter parameter to indicate a new K_{SN} is needed and the UE shall compute the K_{SN} for the SN. The MN forwards the UE configuration parameters (which contains the algorithm identifier(s) received from the SN in step 4), and UP integrity protection and encryption indications (received from the SN in step 4) to the UE. If an SN sends more than one candidate PScell SCG configuration, the MN signals to the UE that all these configurations are associated with the same SN counter value. It is noted that since the message is sent over the RRC connection between the MN and the UE, it is integrity protected using the K_{RRCint} of the MN. Hence the SN Counter cannot be tampered with.

[00151] 6. The UE accepts the RRC Connection Reconfiguration Request after validating its integrity. The UE shall compute the K_{SN} for the SN if an SN Counter parameter was included. The UE shall also compute the needed RRC and UP keys and activate the RRC and UP protection as per the indications received for the associated SRB and/or DRBs respectively. The UE sends the RRC Reconfiguration Complete to the MN. The UE activates the chosen encryption/decryption and integrity protection keys with the SN at this point.

[00152] 7. MN sends SN Reconfiguration Complete to the SN over the Xn-C to inform the SN of the configuration result. On receipt of this message, SN may activate the chosen encryption/decryption and integrity protection with UE.

[00153] 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.

[00154] Embodiments of the present disclosure provide a solution of communication. In

the solution, a first MN, which is a source MN for a subsequent LTM in the LTM procedure of a UE in DC, may determine that the UE is to be handed over from the first MN to a second MN. The first MN transmits a first message to the second MN, and the first message may include a first security key and an associated first value, where the first security key is to be used between the UE and the second MN after the UE hands over from the first MN to the second MN, and the first value is to be used by the UE for derivation of the first security key. The first MN transmits a second message to the UE, and the second message may indicate the first value and a second value, wherein the second value is to be used by the UE for derivation of a second security key which is to be used between the UE and the SN after the UE hands over from the first MN to the second MN. As such, the security keys for subsequent MNs in the subsequent LTM can be determined and used. Therefore, a communication of the UE can be secured, and the safety can be guaranteed. Principles and implementations of the present disclosure will be described in detail below with reference to the figures.

[00155] FIG. 2I illustrates a schematic diagram of an example communication network 200 in which some embodiments of the present disclosure can be implemented. As shown in FIG. 2I, the communication network 200 may include a UE 230, base stations 210, 211, 212, and 220, and an AMF 250 in CN. Each of the base stations 210, 211, 212, and 220 may be a gNB.

[00156] In some cases, the UE 230 may be in a DC, e.g., served by both MN and SN. For the UE 230 in DC, it may be configured with a master cell group (MCG) associated with the MN, and a secondary cell group (SCG) associated with the SN. For example, the base stations 210, 211, and 212 can be master nodes, and the base station 220 can be a secondary node. For example, the MN 210 and the SN 220 can serve the UE 230. In some cases, the UE 230 may be served by MN only, without SN. For example, the MN 210 can serve the UE 230, without the SN 220.

[00157] While considering a mobility of the UE 230, the mobility may be an inter-MN mobility. The MN 210 may be a source MN (S-MN), and the MN 211 and/or the MN 212 can be a candidate (or target) MN (T-MN).

[00158] In case a subsequent LTM is performed, the UE 230 may hand over (or switch) from a source MN to a candidate MN, then to another candidate MN. For example, the UE 230 may hand over from the S-MN 210 to the T-MN 211, and then the UE 230 hands over from

the T-MN 211 to the T-MN 212.

[00159] In the present disclosure, it is assumed that the UE 230 is in DC with the SCG configuration unchanged. In the present disclosure, the S-MN is an MN which triggers the LTM preparation, i.e., sending the RRC reconfiguration to the UE including the LTM candidate configurations. In the following description, it is assumed that the base station 210 is the S-MN 210. In the present disclosure, the candidate MN is an MN which is responsible for the LTM candidate cell(s). The LTM candidate cells with be in the same candidate MN or different candidate MNs. In the following description, the candidate MN may also be called as a target MN (T-MN), and it is assumed that the base stations 211 and 212 are T-MN 211 and T-MN 212 respectively. It is also assumed that a candidate cell 1 is in the T-MN 211 and a candidate cell 2 is in the T-MN 212, for ease of description. It is to be understood that the UE 230 may be served by MN without SN. In this case, the procedures between the MN and the SN could be ignored.

[00160] The AMF 250 is also shown in FIG. 2I, however, it is to be noted the it may have a different name in the actual scenario. The name of "AMF" is only for illustration without any limitation.

[00161] It is to be understood that the number of devices in FIG. 2I is given for the purpose of illustration without suggesting any limitations to the present disclosure. For example, there may be more candidate MNs for the UE 230 during the inter-MN mobility.

[00162] In the present disclosure, the term "NCC" may be used as a counter used for next hop access key derivation, the term "NH" may be a key used for the next hop communication, and the term "sk-counter" may be used as a counter used upon initial configuration of K_{SN}, as well as upon refresh of K_{SN}. The key "K_{MN}" may be that used for the communication between the UE and the MN, the key "K_{SN}" may be that used for the communication between the UE and the SN, and the key "K_{MN}*" may be that used for the communication between the UE and the target MN on handover. However, it should be appreciated that the terms and the keys may be in some different forms, and the present disclosure does not limit for this aspect. It is to be understood that the security key (i.e., NH, K_{MN}, K_{SN}, K_{MN}*) and/or the counter (e.g., NCC, sk-counter) are associated with a cell, i.e., different cells are associated with different security keys and counters. For ease of description, in the following description, it is assumed that each target MN or SN has a candidate cell, e.g., the candidate cell 1 is in the T-MN 211 and the candidate cell 2 is in the T-MN 212.

[00163] FIG. 3 illustrates a signalling chart illustrating communication process 300 in accordance with some example embodiments of the present disclosure. The process 300 may involve the UE 230, the S-MN 210, the T-MN 211, the T-MN 212, and the SN 220 as discussed with reference to FIG. 2I. It would be appreciated that the process 300 may be applied to other communication scenarios, which will not be described in detail.

[00164] The UE 230 may be initially connected to the S-MN 210 and the SN 220 with DC. The UE 230 may be subject to an LTM procedure with unchanged SN 220. The LTM procedure may include an LTM preparation phase and one or more LTM cell switch phases. For example, the LTM preparation phase may be performed, e.g., initiated by the S-MN 210. For example, the one or more LTM cell switch phases may include an initial LTM cell switch (e.g. an initial LTM) phase and one or multiple LTM subsequent LTM cell switch (e.g. subsequent LTM) phases. For example, in the initial LTM cell switch (e.g. an initial LTM) phase, a serving MN for the UE 230 may be changed from the source MN 210 to a candidate MN (e.g. T-MN 211 in the present disclosure), that is, an initial LTM cell switch towards the T-MN 211 may be performed with the S-MN 210 being a serving MN for the UE 230. For example, in a subsequent LTM cell switch (e.g. subsequent LTM) phase, a serving MN for the UE 230 may be changed from a candidate MN (e.g. T-MN 211 in the present disclosure) to another candidate MN (e.g. T-MN 212 in the present disclosure), that is, a subsequent LTM cell switch towards the T-MN 212 may be performed with the T-MN 211 being a serving MN for the UE 230. It is to be understood that the LTM cell switch phase also refers to LTM execution phase.

[00165] As shown in FIG. 3, the UE 230 may be handed over from the S-MN 210 to the T-MN 211 with the SCG configuration unchanged, e.g. at 305, during the LTM procedure. It is understood that the T-MN 211 becomes the serving MN for the UE 230 after 305.

[00166] In the process 300, the T-MN 211 determines that the UE 230 is to be handed over from T-MN 211 to T-MN 212 at 310. For example, a subsequent LTM phase from T-MN 211 to T-MN 212 is to be performed. For example, the T-MN 211 is a source of the subsequent LTM phase, and the T-MN 212 is a target of the subsequent LTM phase.

[00167] In addition or alternatively, the T-MN 211 may determine a first security key and a first value, e.g. at 308, for the subsequent LTM phase. The first security key will be used for the communication between the UE 230 and the T-MN 212 after the UE 230 hands over from the T-MN 211 to the T-MN 212. The first value may be used by the UE 230 for

derivation of the first security key. In some implementations, the T-MN 211 may determine (or generate) the first value, and then determine (or generate) the first security key based on the first value. In some examples, a security key for the communication between the UE 230 and the T-MN 211 may be represented as $K_{T\text{-}MN1}$, and the first security key may be determined based on the first value and $K_{T\text{-}MN1}$. For example, the first security key may be represented as $K_{T\text{-}MN1}$*@T-MN2. In some examples, the first value may be NCC, for example, the first value may be represented as NCC@T-MN2. It is to be noted that the step 308 is illustrated before the step 310 in FIG. 3, however, in some cases, it may be performed after 310, and the present disclosure does not limit for this aspect.

[00168] In the process 300, the T-MN 211 transmits a first message to the T-MN 212 at 320. In some implementations, the first message may include the first security key and the first value. In some examples, the first message may be a security information notification, however, it may be another type which is not limited in the present disclosure.

[00169] In some implementations, the first message may include an ID of the UE 230, in this case, it may indicate that the security information in the first message is for which UE. In some examples, the ID of the UE 230 may be a NG-RAN node UE XnAP ID which is allocated by the S-MN 210, e.g. S-MN UE XnAP ID. In some examples, the ID of the UE 230 may be a common UE ID that is different from the S-MN UE XnAP ID. For example, the common UE ID was provided by the S-MN 210 to the T-MN 211 and the T-MN 212, e.g., during the LTM preparation phase.

[00170] In the process 300, the T-MN 212 determines a second security key and a second value at 330. The second security key will be used for the communication between the UE 230 and the SN 220 after the UE 230 hands over from the T-MN 211 to the T-MN 212. The second value may be used by the UE 230 for derivation of the second security key. In some implementations, the T-MN 212 may determine (or generate) the second value, and then determine (or generate) the second security key based on the first security key and the second value. For example, the second security key may be represented as K_{SN}@T-MN2. In some examples, the second value may be a sk-counter, for example, the second value may be represented as sk-counter@T-MN2.

[00171] In some implementations, the second value may be determined by any of various manners. In some example embodiments, the second value may be a counter value which is different from a value provided to the source MN 210 during the LTM preparation phase.

In some example embodiments, the second value may be a counter value that is the same as that provided to the source MN 210 during the LTM preparation phase.

[00172] In some example embodiments, a counter list has been provided by the T-MN 212 to the source MN 210 during the LTM preparation phase, and the second value may be determined (or selected) from the counter list associated with the T-MN 212.

[00173] In some examples, the T-MN 212 may select the second value from the counter list, and accordingly an index of the second value in the counter list can be determined.

[00174] In some examples, the T-MN 212 may determine the second value based on a number of handovers have been performed by the UE 230 during the LTM procedure. For example, a counter may be used for counting the number, e.g., based on the times that receiving security information notifications from other candidate MNs, or times that receiving cell switch messages. For example, for p-th subsequent LTM phase of the UE 230, the p-th counter value in the counter list can be selected as the second value.

[00175] In some examples, the T-MN 212 may determine the second value based on the first counter value in the counter list, optionally by considering the value provided to the source MN 210 during the LTM preparation phase. For example, if the counter list does not include the value provided to the source MN 210 during the LTM preparation phase, then the first counter value in the counter list can be selected as the second value. For another example, if the counter list includes the value provided to the source MN 210 during the LTM preparation phase, an updated counter list may be determined by removing the value provided to the source MN 210 during the LTM preparation phase, and in addition, the first counter value in the updated counter list can be selected as the second value.

[00176] In some other examples, the T-MN 212 may determine the second value by using a different manner, such as an algorithm, in some instances, a plurality of manners (algorithms) may be provided by the S-MN 210 e.g. during the LTM preparation phase.

[00177] In the process 300, the T-MN 212 transmits a third message to the SN 220 at 340, where the third message includes the second security key. As such, the SN 220 will use the second security key for communication between the UE 230 and the SN 220 after the UE 230 hands over to the T-MN 212.

[00178] In addition or alternatively, the T-MN 212 transmits a first response to the T-MN 211 at 345. The first response may be a confirm message or an acknowledge message of the first message. In some implementations, the first response may indicate the second value.

[00179] In some examples, the first response may include the second value, e.g. which is different from the value provided to the source MN 210 during the LTM preparation phase. In some examples, the first response may include an indication indicates that the second value is the same as the value provided to the source MN 210 during the LTM preparation phase. In some examples, the first response may include an index of the second value in the counter list which was provided to the source MN 210 during the LTM preparation phase. In some examples, the first response may include a first indication, which may indicate that the second value is determined based on a number of handovers of the UE 230. In some examples, the first response may include a second indication, which may indicate that the second value is determined based on the first counter value in the counter list, by considering the value provided to the source MN 210 during the LTM preparation phase. In some examples, the first response may indicate the manner (e.g. algorithm) which is used for determining the second value. In some other examples, the first response may include the first value.

[00180] In the process 300, the T-MN 211 transmits a second message to the UE 230 at 350. In some implementations, the second message may include the first value, e.g., NCC@T-MN2 discussed at 308. In some implementations, the second message may indicate the second value.

[00181] In some examples, the second message may include the second value. In some examples, the second message may include an indication indicates that the second value is the same as the value provided to the source MN 210 during the LTM preparation phase. In some examples, the second message may include an index of the second value in the counter list which was provided to the source MN 210 during the LTM preparation phase. In some examples, the second message may include a first indication, which may indicate that the second value is determined based on a number of handovers of the UE 230. In some examples, the second message may include a second indication, which may indicate that the second value is determined based on the first counter value in the counter list, by considering the value provided to the source MN 210 during the LTM preparation phase. In some other examples, the second message may indicate the manner (e.g. algorithm) which is used for determining the second value.

[00182] In some examples, the second message may be implemented as an LTM cell switch command, e.g. MAC CE. For example, the second message may be used for indicating to the UE 230 to switch from the T-MN 121 to the T-MN 122.

[00183] In addition, the UE 230 determine the first security key and the second security key at 360. Specifically, the UE 230 may determine the first value and the second value based on the second message 350, and further determine the first and second security keys based on the first and second value respectively.

[00184] In some examples, in case the second message include information (e.g. the second value, the index, the indication, the first indication, the second indication, the manner, etc.) of the second value, the UE 230 may determine the second value accordingly. In some other examples, in case the second message does not include any information about the second value, a default manner may be used by the UE 230 for determining the second value. It is to be understood that the default manner is used by both the UE 230 and the T-MN 122 (e.g. at 330), for example, the default manner may be indicated by the S-MN 210 during the LTM preparation phase.

[00185] The UE 230 may be handed over from the T-MN 211 to the T-MN 212 with the SCG configuration unchanged, e.g. at 365. After the UE 230 hands over to the T-MN 212, the first security key ($K_{T\text{-}MN1*}$@T-MN2) will be used for communication between the UE 230 and the T-MN 212, and the second security key (K_{SN}@T-MN2) will be used for communication between the UE 230 and the SN 220.

[00186] It is to be understood that the embodiments with reference to FIG. 3 are only for illustration without any limitation, for example, some step(s) in FIG. 3 may be omitted, reordered, modified, or combined, some further step(s) may be also included, the present disclosure does not limit for this aspect. For example, although it is illustrated that the T-MN 211 is a serving MN for the UE 230 after an initial LTM phase, in some cases, the T-MN 211 may be a serving MN for the UE 230 after a subsequent LTM phase. For example, the UE 230 may be handed over from the S-MN 210 to a candidate MN m, and then be handed over from the candidate MN m to the T-MN 211.

[00187] As detailed examples, FIGS. 4A-4B are provided below with an assumption that the UE 230 with DC hands over from the S-MN 210 to the T-MN 211 in an initial LTM phase, and hands over from the T-MN 211 to the T-MN 212 in a subsequent LTM phase, with the SCG configuration unchanged. In other words, the T-MN 211 is a source of the subsequent LTM and the T-MN 212 is a target of the subsequent LTM.

[00188] FIG. 4A illustrates a signalling chart illustrating communication process 400 which involves the UE 230, the S-MN 210, the T-MN 211 (T-MN1), the T-MN 212 (T-MN2), and

the SN 220 as discussed with reference to FIG. 2I. The UE 230 is initially connected to the S-MN 210 and the SN 220 with DC.

[00189] In the process 400, the S-MN 210 may start the LTM preparation procedure, e.g. for a candidate cell 1 and a candidate cell 2.

[00190] In the process 400, the S-MN 210 transmits a handover request to the T-MN 211 and the T-MN 212 respectively at 401. In some implementations, the handover request to the T-MN 211 at 401a may include $K_{S\text{-}MN}$*1 (e.g. represented as $K_{S\text{-}MN}$*@T-MN1) to be used between the UE 230 and the T-MN 211 on handover from the S-MN 210 to the T-MN 211, and NCC1 (e.g. represented as NCC1@T-MN1) to be used for next hop access key derivation by the UE 230 when the UE 230 connects to the T-MN 211. In some implementations, the handover request to the T-MN 212 at 401b may include $K_{S\text{-}MN}$*2 (e.g. represented as $K_{S\text{-}MN}$*@T-MN2) to be used between the UE 230 and the T-MN 212 on handover from the S-MN 210 to the T-MN 212, and NCC2 (e.g. represented as NCC2@T-MN2) to be used for next hop access key derivation by the UE 230 when the UE 230 connects to the T-MN 212.

[00191] In the process 400, each of the T-MN 211 and T-MN 212 transmits an SN addition request message to the SN 220 at 402. In some implementations, the SN addition request message from T-MN 211 at 402a may include $K_{SN}1$ (e.g. represented as K_{SN1}@T-MN1) used for the communication between the UE 230 and the SN 220 when the serving MN becoming the T-MN 211. In some examples, $K_{SN}1$ is determined by the T-MN 211 based on the $K_{S\text{-}MN}$*1 and a sk-counter 1 (e.g. represented as SK-counter1@T-MN1), where the sk-counter 1 is selected by the T-MN 211. In some implementations, the SN addition request message from T-MN 212 at 402b may include $K_{SN}2$ (e.g. represented as K_{SN2}@T-MN2) used for the communication between the UE 230 and the SN 220 when the serving MN becoming the T-MN 212. In some examples, $K_{SN}2$ is determined by the T-MN 212 based on the $K_{S\text{-}MN}$*2 and a sk-counter 2 (e.g. represented as SK-counter2@T-MN2), where the sk-counter 2 is selected by the T-MN 212.

[00192] In the process 400, the SN 220 replies with an SN addition request ACK to each of the T-MN 211 and T-MN 212 at 403. In some implementations, the SN addition request ACK at 403a may indicate that the SN addition request at 402a is successfully received. In some implementations, the SN addition request ACK at 403b may indicate that the SN addition request at 402b is successfully received.

[00193] In the process 400, each of the T-MN 211 and T-MN 212 transmits a handover request ACK to the S-MN 210 at 404. In some implementations, the handover request ACK from T-MN 211 at 404a may include the NCC1 (e.g. NCC1@T-MN1) and the sk-counter 1 (e.g. SK-counter1@T-MN1) associated with the LTM candidate cell 1. In some examples, the handover request ACK from T-MN 211 at 404a may include an LTM configuration associated with the LTM candidate cell 1. For example, the LTM configuration, the NCC1, and the sk-counter 1 associated with the LTM candidate cell 1 may be included in the HandoverCommand message embedded in the handover request ACK message at 404a. In some implementations, the handover request ACK from T-MN 212 at 404b may include the NCC2 (e.g. NCC2@T-MN2) and the sk-counter 2 (e.g. SK-counter2@T-MN2) associated with the LTM candidate cell 2. In some examples, the handover request ACK from T-MN 212 at 404b may include an LTM configuration associated with the LTM candidate cell 2. For example, the LTM configuration, the NCC2, and the sk-counter 2 associated with the LTM candidate cell 2 may be included in the HandoverCommand message embedded in the handover request ACK message at 404b.

[00194] In the process 400, the S-MN 210 transmits an RRC reconfiguration message to the UE 230 at 405. In some implementations, the RRC reconfiguration message includes: the LTM candidate configuration, the NCC1, and the sk-counter 1 associated with the LTM candidate cell 1; and the LTM candidate configuration, the NCC2, and the sk-counter 2 associated with the LTM candidate cell 2. Upon receiving the RRC reconfiguration message, the UE 230 may reply with an RRC reconfiguration complete message to the S-MN 210 at 406.

[00195] At 407, an LTM cell switch is performed, and the UE 230 may hand over from the S-MN 210 to the T-MN 211. In some examples, the S-MN 210, the SN 220, and the UE 230 may perform LTM cell switch to the LTM candidate cell 1 with the SCG configuration. In some examples, at 407, the T-MN 211 performs path switch procedure towards the AMF 250, to obtain a new <NH, NCC> pair from the AMF 250.

[00196] Optionally, the S-MN 210 transmits an LTM cell switch notification to each of the T-MN 211 and T-MN 212 at 408. In some examples, the LTM cell switch notification to T-MN 211 at 408a may include an ID of the LTM candidate cell 1, e.g. a target cell ID. In some examples, the LTM cell switch notification to T-MN 212 at 408b may include an ID of the LTM candidate cell 1 (e.g. a target cell ID) and/or a node ID of T-MN 211 (e.g., T-MN1 ID).

[00197] In the process 400, the T-MN 211 transmits a first message, which is illustrated as a security information notification in FIG. 4A, to the T-MN 212 at 409. In some implementations, the security information notification may include $K_{T\text{-}MN1}$* (e.g. represented as $K_{T\text{-}MN1}$*@T-MN2) to be used between the UE 230 and the T-MN 212 on handover from the T-MN 211 to the T-MN 212, and the NCC3 (e.g. represented as NCC3@T-MN2) used for next hop access key derivation by the UE 230 when the UE 230 connects to the T-MN 212.

[00198] In some implementations, the security information notification may include an indicator indicating that the security information notification is for which UE. In some examples, the indicator may be an NG-RAN node UE XnAP ID allocated by the S-MN 210 (i.e., S-MN UE XnAP ID). For example, the S-MN UE XnAP ID provided to the T-MN 211 and the T-MN 212 may be the same. In some other examples, the indicator may be a common UE ID different from the S-MN UE XnAP ID. For example, the common UE ID may be provided to the T-MN 211 at 401a and to the T-MN 212 at 401b from the S-MN 210.

[00199] In some implementations, the security information notification may include a node ID of the S-MN 210, which may be an NG-RAN node ID of the S-MN 210 (i.e., S-MN node ID).

[00200] As mentioned above, the steps 408a-408b are optional. In some implementations, if the steps 408a-408b are included, then the security information notification at 409 may be transmitted from the T-MN 211 to the T-MN 212 directly. In some other implementations, if the steps 408a-408b are not included, the security information notification at 409 may be transmitted via the S-MN 210. In some examples, the T-MN 211 may transmit the $K_{T\text{-}MN1}$* and the NCC3 to the S-MN 210, and then the S-MN 210 may send the $K_{T\text{-}MN1}$* and the NCC3 to the T-MN 212.

[00201] In the process 400, the T-MN 212 transmits an SN modification request to the SN 220 at 410, and the SN 220 replies with an SN modification request ACK at 411. In some implementations, the SN modification request may include $K_{SN}3$ (e.g., represented as K_{SN3}@T-MN2) used for the communication between the UE 230 and the SN 220 when the serving MN becomes the T-MN 212. In some examples, the $K_{SN}3$ is determined by the T-MN 212 based on the $K_{T\text{-}MN1}$* and a sk-counter, which may be different from the sk-counter 2 that used at step 402b or may be the same as the sk-counter 2 that used at step 402b. For example, the sk-counter for determining $K_{SN}3$ may be sk-counter 3 (e.g. represented as SK-counter3@T-MN2) or sk-counter 2.

[00202] In addition or alternatively, the T-MN 212 transmits a security information confirm to the T-MN 211 at 412. In some examples, the security information confirm may be transmitted from the T-MN 212 to the T-MN 211 directly. In some other examples, the security information confirm may be transmitted from the T-MN 212 to the T-MN 211 via the S-MN 210. For example, the T-MN 212 may send the security information confirm to the S-MN 210, and then the S-MN 210 may send the security information confirm to the T-MN 211.

[00203] In some implementations, if sk-counter 3 is used for determining $K_{SN}3$, the security information confirm may include the sk-counter 3.

[00204] In some other implementations, if sk-counter 2 is used for determining $K_{SN}3$, then the security information confirm may include the sk-counter 2, or the security information confirm may include a first indicator indicating that the sk-counter is unchanged (i.e. the same as that determined in the LTM preparation procedure), or the security information confirm is not transmitted.

[00205] In some instances, the first indicator may indicate that the sk-counter used for generating K_{SN} is unchanged. For example, the first indicator may be the same sk-counter IE with the value set to TRUE/YES. For example, the first indicator may be the same SN IE with the value set to TRUE/YES. For example, the first indicator may be the node ID of the SN 220.

[00206] From a perspective of T-MN 211, if the security information confirm is not received, it may determine that the sk-counter used for generating K_{SN} is unchanged.

[00207] In the process 400, at 413, the T-MN 211 may determine to trigger the LTM cell switch for the UE 230, e.g., from LTM candidate cell 1 towards LTM candidate cell 2.

[00208] In the process 400, the T-MN 211 transmits a second message, which is illustrated as an LTM cell switch command in FIG. 4A, to the UE 230 at 414. In some implementations, the LTM cell switch command may be in a form of MAC CE. In some implementations, the LTM cell switch command may include NCC3.

[00209] In some implementations, if the security information confirm at 412 includes sk-counter 3, then the LTM cell switch command may include sk-counter 3.

[00210] In some other implementations, if the security information confirm at 412 include sk-counter 2 or a first indicator indicating that the sk-counter is unchanged, then the LTM

cell switch command may include a second indicator indicating that the sk-counter used for generating K_{SN} is unchanged. In some instances, the second indicator may be similar as the first indicator. For example, the second indicator may be the same sk-counter IE with the value set to TRUE/YES. For example, the second indicator may be the same SN IE with the value set to TRUE/YES. For example, the second indicator may be the node ID of the SN 220.

[00211] In the process 400, at 415, an LTM cell switch (e.g., a subsequent LTM cell switch) is performed, and the UE 230 may hand over from the T-MN 211 to the T-MN 212. In some implementations, the UE 230 may perform a key derivation for cell switch to the LTM candidate cell 2 with the SCG configuration, and perform cell switch to the T-MN 212 and the SN 220.

[00212] It is to be appreciated that the process 400 in FIG. 4A is only for illustration without any limitation. In some examples, the steps 408a-408b may be not performed. In some examples, the step 413 may be performed before step 409. In some examples, a name of any message may be changed. In some examples, some additional steps may be included. For example, the T-MN 211 may receive, from the AMF 250, a pair of NH and NCC after the step 407. It is to be understood that some further embodiments may be obtained and are still in the protection scope of the present disclosure.

[00213] FIG. 4B illustrates a signalling chart illustrating communication process 450 which involves the UE 230, the S-MN 210, the T-MN 211 (T-MN1), the T-MN 212 (T-MN2), and the SN 220 as discussed with reference to FIG. 2I. The UE 230 is initially connected to the S-MN 210 and the SN 220 with DC.

[00214] In the process 450, the S-MN 210 may start the LTM preparation procedure, e.g. for a candidate cell 1 and a candidate cell 2. The steps 401, 402, 403, 406, 407, 408, 409, 411, 413, and 415 shown in FIG. 4B may refer to those discussed in FIG. 4A, detailed of which will not be repeated herein.

[00215] In the process 450, each of the T-MN 211 and T-MN 212 transmits a handover request ACK to the S-MN 210 at 424. In some implementations, the handover request ACK from T-MN 211 at 424a may include an LTM configuration, the NCC1 (e.g. NCC1@T-MN1), and a first counter list (e.g. SK-counter list1@T-MN1) associated with the LTM candidate cell 1. For example, the LTM configuration, the NCC1, and the first counter list associated with the LTM candidate cell 1 may be included in the HandoverCommand message

embedded in the handover request ACK message at 424a. In some examples, the first counter list may include multiple counter values in a specific order with the sk-counter 1 being the first one. In some other examples, the first counter list may include multiple counter values in a specific order where the sk-counter 1 is not in the first counter list, in this case, the handover request ACK from T-MN 211 at 424a may further include the sk-counter 1. In some embodiments, the first counter list may include multiple counter values each with a corresponding index.

[00216] In some implementations, the handover request ACK from T-MN 212 at 424b may include an LTM configuration, the NCC2 (e.g. NCC2@T-MN2) and a second counter list (e.g. SK-counter list2@T-MN2) associated with the LTM candidate cell 2. For example, the LTM configuration, the NCC2, and the second counter list associated with the LTM candidate cell 2 may be included in the HandoverCommand message embedded in the handover request ACK message at 424b. In some examples, the second counter list may include multiple counter values in a specific order with the sk-counter 2 being the first one. In some other examples, the second counter list may include multiple counter values in a specific order where the sk-counter 2 is not in the second counter list, in this case, the handover request ACK from T-MN 212 at 424b may further include the sk-counter 2. In some embodiments, the second counter list may include multiple counter values each with a corresponding index.

[00217] In the process 450, the S-MN 210 transmits an RRC reconfiguration message to the UE 230 at 425. In some implementations, the RRC reconfiguration message includes: the LTM candidate configuration, the NCC1, and the first counter list associated with the LTM candidate cell 1; and the LTM candidate configuration, the NCC2, and the second counter list associated with the LTM candidate cell 2. In some embodiments, the first counter list may include multiple counter values each with a corresponding index. In some embodiments, the second counter list may include multiple counter values each with a corresponding index.

[00218] In some examples, if the first counter list does not include the sk-counter 1, then the RRC reconfiguration message may further include the sk-counter 1 associated with the LTM candidate cell 1. In some examples, if the second counter list does not include the sk-counter 2, then the RRC reconfiguration message may further include the sk-counter 2 associated with the LTM candidate cell 2.

[00219] After receiving the security information notification from the T-MN 211 at 409, the T-MN 212 transmits, at 430, an SN modification request to the SN 220. In some implementations, the SN modification request may include $K_{SN}3$ (e.g., represented as K_{SN3}@T-MN2) used for the communication between the UE 230 and the SN 220 when the serving MN becomes the T-MN 212. In some examples, the $K_{SN}3$ is determined by the T-MN 212 based on the $K_{T\text{-}MN1}$* and a sk-counter, which may be sk-counter 3 that is included in the second counter list discussed at step 424b.

[00220] Specifically, the T-MN 212 may select the sk-counter 3 from the second counter list.

[00221] In some example embodiments, each counter value in the second counter list has a corresponding index, and thus the T-MN 212 may determine an index of the sk-counter 3 accordingly.

[00222] In some example embodiments, the sk-counter 3 may be selected based on a number of handovers that have been performed by the UE 230. In some examples, there is a counter of LTM for counting a number of received security information notification from other candidate MNs. For instance, if the T-MN 212 receives the first security information notification (i.e. the first time), then the first counter value in the second counter list is selected if the sk-counter 2 is not included in the second counter list, or the second counter value in the second counter list is selected if the sk-counter 2 is included in the second counter list. In some other examples, there is a counter of LTM for a number of LTM cell switch messages to the same LTM candidate cell (i.e., LTM candidate cell 2), that is, the number of the LTM cell switch to the LTM candidate cell 2, e.g. for a case with the step 413 performed before step 409.

[00223] In some example embodiments, the sk-counter 3 may be selected based on the first counter value in the second counter list. In some examples, if the first counter value in the second counter list is sk-counter 2, then the T-MN 212 may select the second counter value in the second counter list. For example, the T-MN 212 can remove the sk-counter 2 from the second counter list to generate an updated second counter list, and then may select the first counter value from the updated second counter list. In some examples, if the first counter value in the second counter list is not sk-counter 2, then the T-MN 212 may select the first counter value in the second counter list.

[00224] In addition or alternatively, the T-MN 212 transmits a security information confirm to the T-MN 211 at 432. In some examples, the security information confirm may be

transmitted from the T-MN 212 to the T-MN 211 directly. In some other examples, the security information confirm may be transmitted from the T-MN 212 to the T-MN 211 via the S-MN 210. For example, the T-MN 212 may send the security information confirm to the S-MN 210, and then the S-MN 210 may send the security information confirm to the T-MN 211.

[00225] In some example embodiments, the security information confirm may include an index of sk-counter 3.

[00226] In some example embodiments, the security information confirm may be omitted (not transmitted) or the security information confirm may include a first indication indicating that the counter value used for derivation of the $K_{SN}3$ is determined based on a number of handovers that have been performed by the UE 230.

[00227] In some example embodiments, the security information confirm may be omitted (not transmitted) or the security information confirm may include a second indication indicating that the counter value used for derivation of the $K_{SN}3$ is determined based on the first counter value in the second counter list.

[00228] In the process 450, the T-MN 211 transmits a second message, which is illustrated as an LTM cell switch command in FIG. 4B, to the UE 230 at 434. In some implementations, the LTM cell switch command may be in a form of MAC CE. In some implementations, the LTM cell switch command may include NCC3.

[00229] In some example embodiments, the security information confirm at 432 includes an index of sk-counter 3, then the LTM cell switch command may include the index of the sk-counter 3.

[00230] In some example embodiments, the security information confirm at 432 may include a first indication, then the LTM cell switch command may include the first indication.

[00231] In some example embodiments, the security information confirm at 432 may include a second indication, then the LTM cell switch command may include the second indication.

[00232] In the process 450, the UE 230 selects the sk-counter 3 from the second counter list at 435, based on the LTM cell switch command from T-MN 212.

[00233] In some example embodiments, if the LTM cell switch command includes the index of the sk-counter 3, then the UE 230 may determine the sk-counter 3 based on the index.

[00234] In some example embodiments, if the LTM cell switch command includes the first indication, then the UE 230 may determine the sk-counter 3 based on a number of handovers in the LTM procedure.

[00235] In some example embodiments, if the LTM cell switch command includes the second indication, then the UE 230 may determine the sk-counter 3 based on the first counter value in the second counter list.

[00236] It is to be understood that the selection operation for the sk-counter 3 at the UE 230 and at the T-MN 212 should be aligned. In this way, the UE 230 can select the sk-counter 3 in a same way as that of the T-MN 212, and thus the selected counter value (i.e. sk-counter 3) by the T-MN 212 and the UE 230 will be the same, ensuring a correct communication between the UE 230 and the SN 220.

[00237] It is to be appreciated that the process 450 in FIG. 4B is only for illustration without any limitation. In some examples, the steps 408a-408b may be not performed. In some examples, the step 413 may be performed before step 409. In some examples, a name of any message may be changed. In some examples, some additional steps may be included. For example, the T-MN 211 may receive, from the AMF 250, a pair of NT and NCC after the step 407. It is to be understood that some further embodiments may be obtained and are still in the protection scope of the present disclosure.

[00238] According to some embodiments with reference to FIGS. 3-4B, security keys for both MN and SN can be determined for a subsequent LTM in the LTM procedure, in addition a first value and a second value can be determined accordingly for derivation the security keys by the UE. As such, the correct and accurate communication for the UE with DC can be guaranteed. In some examples, there is no need to transmit the second value explicitly in the message to the UE, but an index or an indication may be used, in this case, the safety of the second value can be guaranteed, avoiding information stealing from a third party.

[00239] Reference is further made to FIG. 5, which illustrates a signalling chart illustrating communication process 500 which involves the UE 230, the S-MN 210, the T-MN 211 (T-MN1), T-MN 212 (T-MN2), the SN 220, and the AMF 250, as discussed with reference to FIG. 2I. The UE 230 is initially connected to the S-MN 210 and the SN 220 with DC.

[00240] In the process 500, the S-MN 210 transmits, to the AMF 250, a first message including a list of candidate cells for LTM procedure of the UE 230 (which is illustrated as LTM candidate list in FIG. 5) at 501. In some example embodiments, the list of candidate

cells for LTM procedure may include one or multiple candidate cells, for example, it may include a candidate cell 1 associated with T-MN 121 and a candidate cell 2 associated with T-MN 122.

[00241] In the process 500, the AMF 250 transmit, to the S-MN 210, a second message including a list of value pairs (which is illustrated as list of <NH, NCC> pairs) at 502.

[00242] In some implementations, the number of value pairs may be not less than the number of candidate cells. For example, one or more value pairs are associated with a candidate cell. In this case, the second message may include one or multiple lists of value pairs at 502, and each list of value pairs is associated with a candidate cell in the LTM candidate list at 501.

[00243] In some implementations, each value pair in the list may include two paired values, e.g. associated with a candidate cell in the LTM candidate list at 501. In some implementations, each value pair in the list may be associated with an index.

[00244] As a specific example, a specific value pair may include a first value and a second value being used for a first candidate cell associated with a first candidate MN. In this example, the first value and the second value may be used for derivation of a security key between the UE 230 and the first candidate MN after the UE 230 hands over to the first candidate MN. For example, the first value may be implemented as a NH, and the second value may be implemented as a NCC.

[00245] For ease of description, it is assumed that the second message includes a <NH1, NCC1> pair for candidate cell 1, and a <NH2, NCC2> pair for candidate cell 2.

[00246] The S-MN 210 may start the LTM preparation procedure, e.g. for a candidate cell 1 and a candidate cell 2.

[00247] In the process 500, the S-MN 210 transmits a handover request to the T-MN 211 and the T-MN 212 respectively at 503. In some implementations, the handover request to the T-MN 211 at 503a may include $K_{S\text{-}MN}$*1 (e.g. represented as $K_{S\text{-}MN*}$@T-MN1) to be used between the UE 230 and the T-MN 211 on handover from the S-MN 210 to the T-MN 211, and NCC1 (e.g. represented as NCC1@T-MN1) to be used for next hop access key derivation by the UE 230 when the UE 230 connects to the T-MN 211. In some examples, the $K_{S\text{-}MN}$*1 is derived based on the NH1 which is corresponding to (paired with) the NCC1. In some implementations, the handover request to the T-MN 212 at 503b may include $K_{S\text{-}MN}$*2 (e.g. represented as $K_{S\text{-}MN*}$@T-MN2) to be used between the UE 230 and the T-MN 212 on

handover from the S-MN 210 to the T-MN 212, and NCC2 (e.g. represented as NCC2@T-MN2) to be used for next hop access key derivation by the UE 230 when the UE 230 connects to the T-MN 212. In some examples, the K_{S-MN}*2 is derived based on the NH2 which is corresponding to (paired with) the NCC2. It is to be understood that the S-MN 210 may transmit multiple <K_{S-MN}*, NCC> pairs to the T-MN 211 and the T-MN 212 respectively at 503, if the S-MN 210 receives multiple <NH, NCC> pairs at 502.

[00248] In the process 500, each of the T-MN 211 and T-MN 212 transmits an SN addition request message to the SN 220 at 504. In some implementations, the SN addition request message from T-MN 211 at 504a may include $K_{SN}1$ (e.g. represented as K_{SN1}@T-MN1) used for the communication between the UE 230 and the SN 220 when the serving MN becoming the T-MN 211. In some examples, $K_{SN}1$ is determined by the T-MN 211 based on the K_{S-MN}*1 and a sk-counter 1 (e.g. represented as SK-counter1@T-MN1), where the sk-counter 1 is selected by the T-MN 211. In some implementations, the SN addition request message from T-MN 212 at 504b may include $K_{SN}2$ (e.g. represented as K_{SN2}@T-MN2) used for the communication between the UE 230 and the SN 220 when the serving MN becoming the T-MN 212. In some examples, $K_{SN}2$ is determined by the T-MN 212 based on the K_{S-MN}*2 and a sk-counter 2 (e.g. represented as SK-counter2@T-MN2), where the sk-counter 2 is selected by the T-MN 212. It is to be understood that the T-MN 211 or the T-MN 212 may determine multiple K_{SN} based on the received multiple K_{S-MN}* at 503 and the sk-counters, and the sk-counters may be the same.

[00249] In the process 500, the SN 220 replies with an SN addition request ACK to each of the T-MN 211 and T-MN 212 at 505. In some implementations, the SN addition request ACK at 505a may indicate that the SN addition request at 504a is successfully received. In some implementations, the SN addition request ACK at 505b may indicate that the SN addition request at 504b is successfully received.

[00250] In the process 500, each of the T-MN 211 and T-MN 212 transmits a handover request ACK to the S-MN 210 at 506. In some implementations, the handover request ACK from T-MN 211 at 506a may include the NCC1 (e.g. NCC1@T-MN1) and the sk-counter 1 (e.g. SK-counter1@T-MN1) associated with the LTM candidate cell 1. In some examples, the handover request ACK from T-MN 211 at 506a may include an LTM configuration associated with the LTM candidate cell 1. For example, the LTM configuration, the NCC1, and the sk-counter 1 associated with the LTM candidate cell 1 may be included in the HandoverCommand message embedded in the handover request ACK message at 506a. In

some implementations, the handover request ACK from T-MN 212 at 506b may include the NCC2 (e.g. NCC2@T-MN2) and the sk-counter 2 (e.g. SK-counter2@T-MN2) associated with the LTM candidate cell 2. In some examples, the handover request ACK from T-MN 212 at 506b may include an LTM configuration associated with the LTM candidate cell 2. For example, the LTM configuration, the NCC2, and the sk-counter 2 associated with the LTM candidate cell 2 may be included in the HandoverCommand message embedded in the handover request ACK message at 506b. It is to be understood that one or multiple NCCs associated with the LTM candidate cell may be included in the HandoverCommand message, and each NCC may be associated with an index. It is to be understood that one or multiple <NCC, sk-counter> pairs associated with the LTM candidate cell may be included in the HandoverCommand message, and each <NCC, sk-counter> pair may be associated with an index.

[00251] In the process 500, the S-MN 210 transmits an RRC reconfiguration message to the UE 230 at 507. In some implementations, the RRC reconfiguration message includes: the LTM candidate configuration, the NCC1, and the sk-counter 1 associated with the LTM candidate cell 1; and the LTM candidate configuration, the NCC2, and the sk-counter 2 associated with the LTM candidate cell 2. Upon receiving the RRC reconfiguration message, the UE 230 may reply with an RRC reconfiguration complete message to the S-MN 210 at 508. It is to be understood that one or multiple NCCs associated with the LTM candidate cell may be included in the RRC reconfiguration message, and each NCC may be associated with an index. It is to be understood that one or multiple <NCC, sk-counter> pairs associated with the LTM candidate cell may be included in the RRC reconfiuration message, and each <NCC, sk-counter> pair may be associated with an index.

[00252] At 509, an LTM cell switch is performed, and the UE 230 may hand over from the S-MN 210 to the T-MN 211. In some examples, the S-MN 210, the SN 220, and the UE 230 may perform LTM cell switch to the LTM candidate cell 1 with the SCG configuration.

[00253] In the process 500, the T-MN 211 transmits a path switch request to the AMF 250 at 510. In some implementations, the path switch request may inform the AMF 250 of the new serving MN.

[00254] In some implementations, the path switch request may include a first indicator which indicates a cause of the path switch to the T-MN 211, for example, the cause may be LTM. In other words, the first indicator may indicate that the path switch is due to the LTM.

[00255] The AMF 250 transmits a path switch response, which is illustrated as a path switch response ANK in FIG. 5, to the T-MN 211 at 511. In some implementations, the path switch response may indicate that the path switch request has been successfully completed in the core network. In some implementations, there is no need to reconfigure a value for the T-MN 211 at 511.

[00256] In some example embodiments, the path switch response may include a further value pair which should not be used by the T-MN 211, for example a new pair <NH_{new}, NCC_{new}> may be included in the path switch response. However, the new pair should not be used by the T-MN 211. In some examples, the path switch response may include a second indicator, which indicates that the further value pair should be neglected (not be used) by the T-MN 211. In some other examples, a default behavior for the further value pair in the path switch response may be pre-defined, for examples, the default behavior may include not using the further value pair or neglecting the further value pair.

[00257] As such, although the path switch response may include a further value pair, the T-MN 211 will not use the further value pair for subsequent LTM.

[00258] In the process 500, at 512, the T-MN 211 may determine to trigger the LTM cell switch for the UE 230, e.g., from LTM candidate cell 1 towards LTM candidate cell 2. In the process 500, the T-MN 211 transmits an LTM cell switch command to the UE 230 at 513. In some implementations, the LTM cell switch command may be in a form of MAC CE. In some examples, the LTM cell switch command may include the index of the <NCC, sk-counter> pair. In some other examples, the LTM cell switch command may include the index of the NCC.

[00259] In addition, an LTM cell switch (e.g., a subsequent LTM cell switch) is performed, and the UE 230 may hand over from the T-MN 211 to the T-MN 212 at 514. In some implementations, the UE 230 may perform a key derivation for cell switch to the LTM candidate cell 2 with the SCG configuration, and perform cell switch to the T-MN 212 and the SN 220.

[00260] According some embodiments with reference to FIG. 5, the list of value pairs may be provided by the AMF, e.g. before the LTM preparation phase of the LTM procedure, in this case, the value pair may be used for subsequent LTM, and no new value pair is needed. Therefore, the overhead can be reduced and the communication efficiency can be guaranteed.

[00261] Reference is further made to FIG. 6, which illustrates a signalling chart illustrating communication process 600 which involves the UE 230, the S-MN 210, the T-MN 211 (T-MN1), T-MN 212 (T-MN2), and the SN 220, as discussed with reference to FIG. 2I. The UE 230 is initially connected to the S-MN 210 and the SN 220 with DC.

[00262] In the process 600, the S-MN 210 may start the LTM preparation procedure, e.g. for a candidate cell 1.

[00263] In the process 600, the S-MN 210 transmits a handover request message to the T-MN 211 at 601. In some implementations, the handover request message may include a first security key, a first value, and a list of candidate cells. The first security key may be $K_{S\text{-}MN}*1$ (e.g. represented as $K_{S\text{-}MN*}$@T-MN1), which is to be used between the UE 230 and the T-MN 211 on handover from the S-MN 210 to the T-MN 211. The first value may be NCC1 (e.g. represented as NCC1@T-MN1) is to be used for next hop access key derivation by the UE 230 when the UE 230 connects to the T-MN 211. The list of candidate cells (also called as an LTM candidate cell list) may include one or more candidate cells, e.g., each of which is different from candidate cell 1. For example, the one or more candidate cells may be used for subsequent LTM.

[00264] In the process 600, the T-MN 211 transmits an SN addition request message to the SN 220 at 602. In some implementations, the SN addition request message may include $K_{SN}1$ (e.g. represented as K_{SN1}@T-MN1) used for the communication between the UE 230 and the SN 220 when the serving MN becoming the T-MN 211. In some examples, $K_{SN}1$ is determined by the T-MN 211 based on the $K_{S\text{-}MN}*1$ and a sk-counter 1 (e.g. represented as SK-counter1@T-MN1), where the sk-counter 1 is selected by the T-MN 211.

[00265] In the process 600, the SN 220 replies with an SN addition request ACK to the T-MN 211 at 603. In some implementations, the SN addition request ACK may indicate that the SN addition request is successfully received.

[00266] In the process 600, the T-MN 211 may start subsequent LTM preparation procedure, e.g. by transmitting a further handover request message to each candidate MN of each candidate cell. In some embodiments, for a candidate cell x (e.g. any one candidate cell in the list of candidate cells), a candidate MN x can be determined, and the T-MN 211 may transmit a further handover request message to the candidate MN x. In some examples, the further handover request message to the candidate MN x may include a security key x1 and a value x2, where the security key x1 is to be used between the UE 230 and the candidate

MN x after the UE hands over from the T-MN 2111 to the candidate MN x, and the value x2 is to be used by the UE 230 for derivation of the security key x1.

[00267] As shown in FIG. 6, the T-MN 211 transmits a handover request to the T-MN 212 at 604. In some implementations, the handover request at 604 may include a further security key (such as $K_{T\text{-}MN1}$*) and a further value (such as NCC2) corresponding to the T-MN 212. In some implementations, the further security key $K_{T\text{-}MN1}$* (e.g. represented as $K_{T\text{-}MN1}$*@T-MN2) is to be used between the UE 230 and the T-MN 212 on handover from the T-MN 211 to the T-MN 212, and the further value NCC3 (e.g. represented as NCC3@T-MN2) is to be used for next hop access key derivation by the UE 230 when the UE 230 connects to the T-MN 212.

[00268] The T-MN 212 transmits an SN Addition Request message to the SN 220 at 605. In some examples, the SN Addition Request message at 605 may include the $K_{SN}2$ to be used for the communication between the UE 230 and the SN 220 when the serving MN becoming the T-MN 212. The $K_{SN}2$ is determined by the T-MN 212 based on the $K_{T\text{-}MN1}$* and a sk-counter 2, where the sk-counter 2 is selected by the T-MN 212. The SN 220 may reply with an SN addition request ACK message to the T-MN 212 at 606.

[00269] In the process 600, the T-MN 212 transmits a handover request ACK message to the T-MN 211 at 607. In some embodiments, the handover request ACK at 607 may include LTM candidate configuration for subsequent LTM, the NCC2, and the sk-counter 2 associated with the LTM candidate cell 2. In some examples, the LTM candidate configuration for subsequent LTM, the NCC2, and the sk-counter 2 associated with the LTM candidate cell 2 may be included in the HandoverCommand message embedded in the handover request ACK message.

[00270] It is understandable that the T-MN 211 may receive, from each candidate MN of candidate cell, a corresponding handover request ACK message.

[00271] In the process 600, the T-MN 211 transmits a handover request ACK message to the S-MN 210 at 608. In some implementations, the handover request ACK message to the S-MN 210 may include a first value and a second value associated with the T-MN 211, where the first value is to be used by the UE 230 for derivation of a security key between the UE 230 and the T-MN 211 after the UE 230 hands over from the S-MN 210 to the T-MN 211, and the second value is to be used by the UE 230 for derivation of a security key between the UE 230 and the SN 220 after the UE 230 hands over from the S-MN 210 to the T-MN 211.

[00272] In some implementations, the handover request ACK message to the S-MN 210 may further include following information associated with each candidate MN: a corresponding value to be used by the UE 230 for derivation of a security key between the UE 230 and the corresponding candidate MN after the UE 230 hands over from the T-MN 211 to the corresponding candidate MN, and a further corresponding value to be used by the UE 230 for derivation of a security key between the UE 230 and the SN 220 after the UE 230 hands over from the T-MN 211 to the corresponding candidate MN.

[00273] As an illustrated example, the handover request ACK message to the S-MN 210 may include (1) the LTM candidate configuration, the NCC1, and the sk-counter 1 associated with the LTM candidate cell 1; and (2) the LTM candidate configuration, the NCC2, and the sk-counter 2 associated with the LTM candidate cell 2 for subsequent LTM.

[00274] The steps 601-608 above are discussed for an LTM preparation procedure initiated by the S-MN 210 for the candidate cell 1. It is understood that the LTM preparation procedure for the candidate cell 2 may be also initiated by the S-MN 210 in a similar way, e.g., the S-MN 210 may transmit a handover request message to the T-MN 212. It is to be noted that the LTM preparation procedure for the candidate cell 2 is similar with steps 601-608, e.g., by exchanging the roles of T-MN 211 and T-MN 212, which will not be repeated t herein for brevity.

[00275] In the process 600, the S-MN 210 transmits an RRC reconfiguration message to the UE 230 at 609. In some implementations, the RRC reconfiguration message includes information received from each candidate MN, e.g., by a handover request ACK message. For examples, the RRC reconfiguration message may include, e.g. corresponding to steps 601-608, the LTM candidate configuration, the NCC1, and the sk-counter 1 associated with the LTM candidate cell 1; and the LTM candidate configuration, the NCC2, and the sk-counter 2 associated with the LTM candidate cell 2.

[00276] Upon receiving the RRC reconfiguration message, the UE 230 may reply with an RRC reconfiguration complete message to the S-MN 210 at 610.

[00277] At 611, an LTM cell switch is performed, and the UE 230 may hand over from the S-MN 210 to the T-MN 211. In some examples, the S-MN 210, the SN 220, and the UE 230 may perform LTM cell switch to the LTM candidate cell 1 with the SCG configuration.

[00278] At 612, the T-MN 211 may determine to trigger the LTM cell switch for the UE 230, e.g., from LTM candidate cell 1 towards LTM candidate cell 2. In addition, the T-MN 211

transmits an LTM cell switch command (i.e. MAC CE) to the UE 230 at 613. Accordingly, at 614, an LTM cell switch (e.g., a subsequent LTM cell switch) is performed, and the UE 230 may hand over from the T-MN 211 to the T-MN 212.

[00279] According to embodiments with reference to FIG. 6, information needed for key derivation is determined and provided to the UE 230 at the LTM preparation procedure. For example, the S-MN provides the LTM candidate cell list to the candidate MN for subsequent LTM preparation. For example, each candidate MN can prepare the NCC and the sk-counter for subsequent LTM. As such, the information can be used for each handover (e.g. subsequent LTM) and there is no need to update the security information during the LTM procedure frequently. Therefore, the efficiency of the handover can be guaranteed.

[00280] According to some embodiments discussed above, a solution for supporting subsequent LTM with unchanged SCG configuration is provided. It is to be appreciated that the processes discussed with reference to FIGS. 3-6 are only for illustration without any limitation. For example, some step(s) may be omitted, reordered, modified, or combined, or some further step(s) may be also included, the present disclosure does not limit for this aspect.

[00281] In the present disclosure, the terms procedure, process, phase, and stage may be used interchangeably in some embodiments.

[00282] FIG. 7 illustrates an example of a device 700 that is suitable for implementing embodiments of the present disclosure. The device 700 may be an example of a UE, an MN, an SN, or a core network entity (such as an AMF) as described herein. The device 700 may support wireless communication with the S-MN 210, the T-MN 211/212, the SN 220, the UE 230, the AMF 250, or any combination thereof. The device 700 may include components for bi-directional communications including components for transmitting and receiving communications, such as a processor 702, a memory 704, a transceiver 706, and, optionally, an I/O controller 708. 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).

[00283] The processor 702, the memory 704, the transceiver 706, 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 702, the memory 704, the transceiver 706, or various combinations or components thereof may

support a method for performing one or more of the operations described herein.

[00284] In some implementations, the processor 702, the memory 704, the transceiver 706, 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 702 and the memory 704 coupled with the processor 702 may be configured to perform one or more of the functions described herein (e.g., executing, by the processor 702, instructions stored in the memory 704).

[00285] For example, the processor 702 may support wireless communication at the device 700 in accordance with examples as disclosed herein. The processor 702 may be configured to operable to support a means for operations discussed above.

[00286] The processor 702 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 702 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 702. The processor 702 may be configured to execute computer-readable instructions stored in a memory (e.g., the memory 704) to cause the device 700 to perform various functions of the present disclosure.

[00287] The memory 704 may include random access memory (RAM) and read-only memory (ROM). The memory 704 may store computer-readable, computer-executable code including instructions that, when executed by the processor 702 cause the device 700 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 702 but may cause a computer (e.g., when compiled and executed) to perform functions described herein. In some implementations, the memory 704 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.

[00288] The I/O controller 708 may manage input and output signals for the device 700. The I/O controller 708 may also manage peripherals not integrated into the device 700. In some implementations, the I/O controller 708 may represent a physical connection or port to an external peripheral. In some implementations, the I/O controller 708 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 708 may be implemented as part of a processor, such as the processor 702. In some implementations, a user may interact with the device 700 via the I/O controller 708 or via hardware components controlled by the I/O controller 708.

[00289] In some implementations, the device 700 may include a single antenna 710. However, in some other implementations, the device 700 may have more than one antenna 710 (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 706 may communicate bi-directionally, via the one or more antennas 710, wired, or wireless links as described herein. For example, the transceiver 706 may represent a wireless transceiver and may communicate bi-directionally with another wireless transceiver. The transceiver 706 may also include a modem to modulate the packets, to provide the modulated packets to one or more antennas 710 for transmission, and to demodulate packets received from the one or more antennas 710. The transceiver 706 may include one or more transmit chains, one or more receive chains, or a combination thereof.

[00290] 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 710 for transmitting the amplified signal into the air or wireless medium.

[00291] 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 710 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.

[00292] FIG. 8 illustrates an example of a processor 800 that is suitable for implementing some embodiments of the present disclosure. The processor 800 may be an example of a processor configured to perform various operations in accordance with examples as described herein. The processor 800 may include a controller 802 configured to perform various operations in accordance with examples as described herein. The processor 800 may optionally include at least one memory 804, such as L1/L2/L3 cache. Additionally, or alternatively, the processor 800 may optionally include one or more arithmetic-logic units (ALUs) 806. 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).

[00293] The processor 800 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 800) 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).

[00294] The controller 802 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 800 to cause the processor 800 to support various operations in accordance with examples as described herein. For example, the controller 802 may operate as a control unit of the processor 800, generating

control signals that manage the operation of various components of the processor 800. These control signals include enabling or disabling functional units, selecting data paths, initiating memory access, and coordinating timing of operations.

[00295] The controller 802 may be configured to fetch (e.g., obtain, retrieve, receive) instructions from the memory 804 and determine subsequent instruction(s) to be executed to cause the processor 800 to support various operations in accordance with examples as described herein. The controller 802 may be configured to track memory address of instructions associated with the memory 804. The controller 802 may be configured to decode instructions to determine the operation to be performed and the operands involved. For example, the controller 802 may be configured to interpret the instruction and determine control signals to be output to other components of the processor 800 to cause the processor 800 to support various operations in accordance with examples as described herein. Additionally, or alternatively, the controller 802 may be configured to manage flow of data within the processor 800. The controller 802 may be configured to control transfer of data between registers, arithmetic logic units (ALUs), and other functional units of the processor 800.

[00296] The memory 804 may include one or more caches (e.g., memory local to or included in the processor 800 or other memory, such RAM, ROM, DRAM, SDRAM, SRAM, MRAM, flash memory, etc. In some implementations, the memory 804 may reside within or on a processor chipset (e.g., local to the processor 800). In some other implementations, the memory 804 may reside external to the processor chipset (e.g., remote to the processor 800).

[00297] The memory 804 may store computer-readable, computer-executable code including instructions that, when executed by the processor 800, cause the processor 800 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 802 and/or the processor 800 may be configured to execute computer-readable instructions stored in the memory 804 to cause the processor 800 to perform various functions. For example, the processor 800 and/or the controller 802 may be coupled with or to the memory 804, the processor 800, the controller 802, and the memory 804 may be configured to perform various functions described herein. In some examples, the processor 800 may include multiple processors and the memory 804 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.

[00298] The one or more ALUs 806 may be configured to support various operations in accordance with examples as described herein. In some implementations, the one or more ALUs 806 may reside within or on a processor chipset (e.g., the processor 800). In some other implementations, the one or more ALUs 806 may reside external to the processor chipset (e.g., the processor 800). One or more ALUs 806 may perform one or more computations such as addition, subtraction, multiplication, and division on data. For example, one or more ALUs 806 may receive input operands and an operation code, which determines an operation to be executed. One or more ALUs 806 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 806 may support logical operations such as AND, OR, exclusive-OR (XOR), not-OR (NOR), and not-AND (NAND), enabling the one or more ALUs 806 to handle conditional operations, comparisons, and bitwise operations.

[00299] The processor 800 may support wireless communication in accordance with examples as disclosed herein. The processor 800 may be configured to or operable to support a means for operations described in some embodiments of the present disclosure.

[00300] FIG. 9 illustrates a flowchart of a method 900 performed by a first MN in accordance with aspects of the present disclosure. The operations of the method 900 may be implemented by a device or its components as described herein. For example, the operations of the method 900 may be performed by the T-MN 211 in FIG. 2I. 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.

[00301] At 910, the method may include determining that a UE with DC is to be handed over from the first MN to a second MN during an LTM procedure, wherein the first MN has become a serving MN for the UE after an LTM cell switch towards the first MN. The operations of 910 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 910 may be performed by the T-MN 211 as described with reference to FIG. 2I.

[00302] At 920, the method may include transmitting, to the second MN, a first message comprising a first security key and a first value associated with the first security key, wherein the first security key is to be used between the UE and the second MN after the second MN

has become a serving MN for the UE. The operations of 920 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 920 may be performed by the T-MN 211 as described with reference to FIG. 2I.

[00303] At 930, the method may include transmitting, to the UE, a second message indicating: the first value, which is to be used by the UE for derivation of the first security key associated with the second MN, and a second value, which is to be used by the UE for derivation of a second security key associated with an SN, wherein the SN remains unchanged after the second MN has become the serving MN for the UE. The operations of 930 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 930 may be performed by the T-MN 211 as described with reference to FIG. 2I.

[00304] FIG. 10 illustrates a flowchart of a method 1000 performed by a second MN in accordance with aspects of the present disclosure. The operations of the method 1000 may be implemented by a device or its components as described herein. For example, the operations of the method 1000 may be performed by the T-MN 212 in FIG. 2I. 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.

[00305] At 1010, the method may include receiving, from a first MN, a first message comprising a first security key and a first value associated with the first security key, wherein a UE with DC is to be handed over from the first MN to the second MN during an LTM procedure, the first MN has become a serving MN for the UE after an LTM cell switch towards the first MN, and wherein the first security key is to be used between the UE and the second MN after the second MN has become a serving MN for the UE, and the first value is to be used by the UE for derivation of the first security key. The operations of 1010 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1010 may be performed by the T-MN 212 as described with reference to FIG. 2I.

[00306] At 1020, the method may include determining, based on the first security key, a second security key associated with an SN and a second value associated with the second security key, wherein the SN remains unchanged after the second MN has become the serving MN for the UE. The operations of 1020 may be performed in accordance with examples as

described herein. In some implementations, aspects of the operations of 1020 may be performed by the T-MN 212 as described with reference to FIG. 2I.

[00307] At 1030, the method may include transmitting, to the SN, the second security key. The operations of 1030 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1030 may be performed by the T-MN 212 as described with reference to FIG. 2I.

[00308] FIG. 11 illustrates a flowchart of a method 1100 performed by a UE in accordance with aspects of the present disclosure. The operations of the method 1100 may be implemented by a device or its components as described herein. For example, the operations of the method 1100 may be performed by the UE 230 in FIG. 2I. 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.

[00309] At 1110, the method may include receiving, from a first MN, a second message indicating: a first value, which is to be used by the UE for derivation of a first security key associated with a second MN, wherein the UE with DC is to be handed over from the first MN to the second MN during an LTM procedure, the first MN has become a serving MN for the UE after an LTM cell switch towards the first MN, and wherein the first security key is to be used between the UE and the second MN after the second MN has become a serving MN for the UE, and a second value, which is to be used by the UE for derivation of a second security key associated with an SN, wherein the SN remains unchanged after the second MN has become the serving MN for the UE. The operations of 1110 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1110 may be performed by the UE 230 as described with reference to FIG. 2I.

[00310] At 1120, the method may include determining the first security key and the second security key based on the second message. The operations of 1120 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1120 may be performed by the UE 230 as described with reference to FIG. 2I.

[00311] FIG. 12 illustrates a flowchart of a method 1200 performed by a core network entity in accordance with aspects of the present disclosure. The operations of the method 1200 may be implemented by a device or its components as described herein. For example, the operations of the method 1200 may be performed by the AMF 250 in FIG. 2I. 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.

[00312] At 1210, the method may include receiving, from a source MN of a UE, a first message indicating a list of candidate cells for an LTM procedure of the UE. The operations of 1210 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1210 may be performed by the AMF 250 as described with reference to FIG. 2I.

[00313] At 1220, the method may include transmitting, to the source MN, a second message comprising a list of value pairs, wherein a first value pair in the list of value pairs comprises paired first value and second value, wherein the first value pair is used for a first candidate cell in the list of candidate cells, and wherein the first value and the second value are to be used for derivation of a security key between the UE and a first candidate MN associated with the first candidate cell after the UE hands over to the first candidate MN. The operations of 1220 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1220 may be performed by the AMF 250 as described with reference to FIG. 2I.

[00314] FIG. 13 illustrates a flowchart of a method 1300 performed by a source MN in accordance with aspects of the present disclosure. The operations of the method 1300 may be implemented by a device or its components as described herein. For example, the operations of the method 1300 may be performed by the S-MN 210 in FIG. 2I. 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.

[00315] At 1310, the method may include transmitting, to a core network entity, a first message indicating a list of candidate cells for an LTM procedure of a UE. The operations of 1310 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1310 may be performed by the S-MN 210 as described with reference to FIG. 2I.

[00316] At 1320, the method may include receiving, from the core network entity, a second message comprising a list of value pairs, wherein a first value pair in the list of value pairs comprises paired first value and second value, wherein the first value pair is used for a first

candidate cell in the list of candidate cells, and wherein the first value and the second value are to be used for derivation of a security key between the UE and a first candidate MN associated with the first candidate cell after the UE hands over to the first candidate MN. The operations of 1320 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1320 may be performed by the S-MN 210 as described with reference to FIG. 2I.

[00317] FIG. 14 illustrates a flowchart of a method 1400 performed by a first MN in accordance with aspects of the present disclosure. The operations of the method 1400 may be implemented by a device or its components as described herein. For example, the operations of the method 1400 may be performed by the T-MN 211 in FIG. 2I. 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.

[00318] At 1410, the method may include performing, for a UE, an LTM cell switch towards the first MN during an LTM procedure, wherein the first MN has become a serving MN for the UE after the LTM cell switch. The operations of 1410 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1410 may be performed by the T-MN 211 as described with reference to FIG. 2I.

[00319] At 1420, the method may include transmitting, to a core network entity, a path switch request. The operations of 1420 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1420 may be performed by the T-MN 211 as described with reference to FIG. 2I.

[00320] At 1430, the method may include receiving, from the core network entity, a path switch response indicating an acknowledge of the path switch request without a reconfigured value pair for use. The operations of 1430 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1430 may be performed by the T-MN 211 as described with reference to FIG. 2I.

[00321] FIG. 15 illustrates a flowchart of a method 1500 performed by a first MN in accordance with aspects of the present disclosure. The operations of the method 1500 may be implemented by a device or its components as described herein. For example, the operations of the method 1500 may be performed by the T-MN 211 in FIG. 2I. 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.

[00322] At 1510, the method may include receiving, from a source MN of a UE, a handover request for an LTM procedure, wherein the handover request comprises a first security key, a first value, and a list of a plurality of candidate cells, wherein the first security key is to be used between the UE and the first MN after the UE hands over from the source MN to the first MN, and wherein the first value is to be used by the UE for derivation of the first security key. The operations of 1510 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1510 may be performed by the T-MN 211 as described with reference to FIG. 2I.

[00323] At 1520, the method may include transmitting, to each of a plurality of candidate MNs associated with the plurality of candidate cells, a further handover request comprising a corresponding security key and a corresponding value for a corresponding candidate MN, wherein the corresponding security key is to be used between the UE and the corresponding candidate MN after the UE hands over from the first MN to the corresponding candidate MN, and wherein the corresponding value is to be used by the UE for derivation of the corresponding security key. The operations of 1520 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1520 may be performed by the T-MN 211 as described with reference to FIG. 2I.

[00324] 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.

[00325] 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.

[00326] 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.

[00327] 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.

[00328] 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.

[00329] 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 first master node (MN) comprising:

at least one memory; and

at least one processor coupled with the at least one memory and configured to cause the first MN to:

determine that a user equipment (UE) with dual connectivity (DC) is to be handed over from the first MN to a second MN during a layer 1 or layer 2 triggered mobility (LTM) procedure, wherein the first MN has become a serving MN for the UE after an LTM cell switch towards the first MN;

transmit, to the second MN, a first message comprising a first security key and a first value associated with the first security key, wherein the first security key is to be used between the UE and the second MN after the second MN has become a serving MN for the UE; and

transmit, to the UE, a second message indicating:

the first value, which is to be used by the UE for derivation of the first security key associated with the second MN, and

a second value, which is to be used by the UE for derivation of a second security key associated with a secondary node (SN), wherein the SN remains unchanged after the second MN has become the serving MN for the UE.

2. The first MN of claim 1, wherein the second message comprises an index of the second value in a second list associated with the second MN.

3. The first MN of claim 2, wherein the at least one processor is further configured to cause the first MN to:

receive, from the second MN, a first response indicating an acknowledge of the first message, wherein the first response comprises the index of the second value.

4. The first MN of claims 2, wherein the second list associated with the second MN is provided to the UE from the second MN via a source MN of the LTM procedure during an LTM preparation phase.

5. The first MN of claim 1, wherein the first message further comprises one of:

an identifier (ID) of the UE, or

a node ID of the SN.

6. The first MN of claim 5, wherein the ID of the UE comprises an identifier of the UE allocated by a source MN of the LTM procedure during an LTM preparation phase.

7. The first MN of claim 1, wherein the at least one processor is further configured to cause the first MN to:

receive, from a source MN of the LTM procedure, a cell switch notification comprising one of:

a target cell ID associated with the first MN, or

an ID of the first MN.

8. The first MN of claim 1, wherein the second message comprises an LTM cell switch command.

9. The first MN of claim 1, wherein the first value comprises a value of next hop chaining counter (NCC), and the second value comprises a value of a security key counter.

10. A user equipment (UE) comprising:

at least one memory; and

at least one processor coupled with the at least one memory and configured to cause the UE to:

receive, from a first master node (MN), a second message indicating:

a first value, which is to be used by the UE for derivation of a first security key associated with a second MN, wherein the UE with dual connectivity (DC) is to be handed over from the first MN to the second MN during a layer 1 or layer 2 triggered mobility (LTM) procedure, the first MN has become a serving MN for the UE after an LTM cell switch towards the first MN, and wherein the first security key is to be used between the UE and the second MN after the second MN has become a serving MN for the UE, and

a second value, which is to be used by the UE for derivation of a second security key associated with a secondary node (SN), wherein the SN remains unchanged after the second MN has become the serving MN for the UE; and

determine the first security key and the second security key based on the second message.

11. The UE of claim 10, wherein the at least one processor is further configured to cause the UE to:

receive, from a source MN of the LTM procedure, a radio resource control (RRC) reconfiguration message comprising:

a second list associated with the second MN, and

a counter value to be used by the UE for derivation of a further security key between the UE and the second MN after the second MN has become the serving MN for the UE.

12. The UE of claim 11, wherein the second message indicates to the UE to determine the second value based on a first counter value in an updated list associated with the second MN, wherein the updated list is determined based on the second list associated with the second MN.

13. The UE of claim 12, wherein the at least one processor is further configured to cause the UE to:

determine the updated list by removing, from the second list, the counter value associated with the second MN that is comprised in the RRC reconfiguration message; and

select the first counter value in the updated list.

14. The UE of claim 11, wherein the second message indicates to the UE to determine the second value based on a number of LTM cell switch and the second list associated with the second MN.

15. The UE of claim 11, wherein the second message comprises an index of the second value in the second list.

16. The UE of claim 10, wherein the second message comprises an LTM cell switch command.

17. The UE of claim 10, wherein the first value comprises a value of next hop chaining counter (NCC), and the second value comprises a value of a security key counter.

18. A source master node (MN) comprising:

at least one memory; and

at least one processor coupled with the at least one memory and configured to cause the source MN to:

transmit, to a core network entity, a first message indicating a list of candidate cells for a layer 1 or layer 2 triggered mobility (LTM) procedure of a user equipment (UE); and

receive, from the core network entity, a second message comprising a list of value pairs, wherein a first value pair in the list of value pairs comprises paired first value and second value, wherein the first value pair is used for a first candidate cell in the list of candidate cells, and wherein the first value and the second value are to be used for derivation of a security key between the UE and a first candidate MN associated with the first candidate cell after the UE hands over to the first candidate MN.

19. The source MN of claim 18, wherein the at least one processor is further configured to cause the source MN to:

determine, based on the second message, the security key between the UE and the first candidate MN; and

transmit, to the first candidate MN, a third message comprising the security key and the second value.

20. The source MN of claim 18, wherein the first value comprises a value of next hop (NH), and the second value comprises a value of next hop chaining counter (NCC).