SELECTING UNIFORM CRYPTOGRAPHIC ALGORITHMS AND KEY SIZES DURING USER EQUIPMENT (UE) MOBILITY SCENARIOS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Patent Application No. 63/551,874, filed on February 9, 2024, entitled SELECTING UNIFORM CRYPTOGRAPHIC ALGORITHMS AND KEY SIZES DURING USER EQUIPMENT (UE) MOBILITY SCENARIOS, which is incorporated by reference in its entirety.

TECHNICAL FIELD

[0002] The present disclosure relates to wireless communications, and more specifically to selecting uniform cryptographic algorithms and key sizes during user equipment (UE) mobility scenarios.

BACKGROUND

[0003] A wireless communications system may include one or multiple network communication devices, such as base stations, which 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, or the like)). 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)).

[0004] Wireless communications systems apply a security context for communications between UEs and base stations or other network communications devices. For example, to activate security for a UE, a Non Access Stratum (NAS) security context may be

established between the UE and an Application Mobility and Management Function (AMF) of a network. The security context, which can include authentication, integrity protection, and ciphering applied to communications, may be created during a primary authentication and/or key agreement procedure between the UE and the AMF (or other network function).

SUMMARY

[0005] 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.

[0006] The present disclosure relates to methods, apparatuses, and systems that enable a UE to indicate its security capabilities (e.g., 256-bit security capabilities) to a network during a mobility procedure, such as an Xn handover or N2 handover.

[0007] Some implementations of the method and apparatuses described herein may further include a base station for wireless communication, comprising at least one memory and at least one processor coupled with the at least one memory and configured to cause the base station to initiate a handover procedure for a user equipment UE, determine a security capability of the UE, select a target base station based on the security capability of the UE, and transmit the determined security capability of the UE to the selected target base station.

[0008] In some implementations of the method and apparatuses described herein, the at least one processor is further configured to cause the base station to complete the handover procedure for the UE with the selected target base station.

[0009] In some implementations of the method and apparatuses described herein, the determined security capability of the UE includes only 128-bit security algorithms, the at least one processor is further configured to cause the base station to select a target base station that has a configuration to support 128-bit algorithms.

[0010] In some implementations of the method and apparatuses described herein, the determined security capability of the UE includes128-bit security algorithms and 256-bit security algorithms, the at least one processor is further configured to cause the base station to select a target base station that has a configuration to support 256-bit algorithms.

[0011] In some implementations of the method and apparatuses described herein, the determined security capability of the UE includes only 256-bit security algorithms, the at least one processor is further configured to cause the base station to select a target base station that has a configuration to support 256-bit algorithms.

[0012] In some implementations of the method and apparatuses described herein, the determined security capability of the UE includes support of one or more of 256-bit encryption algorithms, 256-bit integrity algorithms, 128-bit encryption algorithms, 128-bit integrity algorithms, 256-bit integrity algorithms, 256-bit security key sizes, or use 256-bit Access Stratum (AS) key size indications.

[0013] In some implementations of the method and apparatuses described herein, the at least one processor is configured to cause the base station to select the target base station based on matching the security capability of the UE to apply uniform ciphering and integrity protection algorithms for AS security supported by the target base station.

[0014] In some implementations of the method and apparatuses described herein, the base station is an NR Node B (gNB) and the handover procedure is an Xn handover procedure.

[0015] Some implementations of the method and apparatuses described herein may further include a base station for wireless communication, comprising at least one memory and at least one processor coupled with the at least one memory and configured to cause the base station to initiate, for a UE, a handover procedure from the base station to a target base station, generate a source to target transparent container (STC) that indicates support of 256-bit security algorithms at the UE, and transmit the generated STC to an Access and Mobility Management Function (AMF) associated with the base station that initiated the handover procedure.

[0016] In some implementations of the method and apparatuses described herein, the STC indicates support of 256-bit encryption algorithms, 256-bit integrity algorithms, 256-bit encryption algorithms selected and used at the base station, 256-bit integrity algorithms selected and used at the base station, 256-bit security key sizes, or use 256-bit AS key indications at the UE.

[0017] In some implementations of the method and apparatuses described herein, the at least one processor is configured to cause the base station to select the target base station based on determining the target base station supports 256-bit ciphering and integrity protection algorithms for AS security.

[0018] Some implementations of the method and apparatuses described herein may further include a network function for wireless communication, comprising at least one memory and at least one processor coupled with the at least one memory and configured to cause the network function to receive, from a source base station during a handover procedure for a UE, an STC that indicates support of 256-bit security algorithms at the UE, and transmit the generated STC to a target base station during the handover procedure.

[0019] In some implementations of the method and apparatuses described herein, the STC indicates support of 256-bit encryption algorithms, 256-bit integrity algorithms, 256-bit encryption algorithms selected and used at the target base station, 256-bit integrity algorithms selected and used at the target base station, 256-bit security key sizes, or use 256-bit AS key indications at the UE.

[0020] In some implementations of the method and apparatuses described herein, the at least one processor is configured to cause the network function to select the target base station based on determining the target base station supports 256-bit ciphering and integrity protection algorithms for AS security.

[0021] In some implementations of the method and apparatuses described herein, the network function is a source AMF associated with the source base station.

[0022] In some implementations of the method and apparatuses described herein, the at least one processor is configured to cause the network function to transmit the generated STC to the target base station via a target AMF associated with the target base station.

[0023] Some implementations of the method and apparatuses described herein may further include a base station for wireless communication, comprising at least one memory; and at least one processor coupled with the at least one memory and configured to cause the base station to receive an indication that a UE served by the base station has moved out of a RAN-based notification area (RNA) associated with the base station, initiate an RNA update procedure for the UE to a new base station, and transmit a 256-bit security capability of the UE to the new base station during the initiated RNA update procedure.

[0024] In some implementations of the method and apparatuses described herein, the 256-bit security capability of the UE identifies support of 256-bit encryption algorithms, 256-bit integrity algorithms, 256-bit security key sizes, or use 256-bit AS key indications at the UE.

[0025] Some implementations of the method and apparatuses described herein may further include a base station for wireless communication, comprising at least one memory and at least one processor coupled with the at least one memory and configured to cause the base station to transmit a security capability of a UE to a secondary base station, wherein the UE is also connected to the base station, receive, from the secondary base station, 256-bit ciphering and integrity protection algorithms selected by the secondary base station to apply 256-bit security for the UE, and transmit the 256-bit ciphering and integrity protection algorithms selected by the secondary base station to the UE.

[0026] In some implementations of the method and apparatuses described herein, the security capability of the UE identifies support of 256-bit encryption algorithms, 256-bit integrity algorithms, 256-bit security key sizes, or use 256-bit AS key indications at the UE.

[0027] In some implementations of the method and apparatuses described herein, the secondary base station supports 256-bit ciphering and integrity protection algorithms for AS security.

[0028] In some implementations of the method and apparatuses described herein, the at least one processor is further configured to cause the base station to select the secondary base station based on an operator policy associated with the secondary base station that prioritizes the security algorithm supported by the secondary base station.

[0029] In some implementations of the method and apparatuses described herein, the base station is a master node and the secondary base station is a secondary node.

[0030] In some implementations of the method and apparatuses described herein, the at least one processor is configured to cause the base station to transmit the security capability of UE to the secondary base station during a random access procedure between the UE and the secondary base station.

[0031] In some implementations of the method and apparatuses described herein, the base station is an NR Node B (gNB) and the secondary base station is an NR Node B (gNB).

BRIEF DESCRIPTION OF THE DRAWINGS

[0032] Figure 1 illustrates an example of a wireless communications system in accordance with aspects of the present disclosure.

[0033] Figure 2 illustrates a messaging flow of an Xn handover procedure in accordance with aspects of the present disclosure.

[0034] Figure 3 illustrates a messaging flow of an N2 handover procedure with an AMF change in accordance with aspects of the present disclosure.

[0035] Figure 4 illustrates a messaging flow of an N2 handover procedure without an AMF change in accordance with aspects of the present disclosure.

[0036] Figure 5 illustrates a messaging flow of an RNA update procedure in accordance with aspects of the present disclosure.

[0037] Figure 6 illustrates a messaging flow of a dual connectivity procedure in accordance with aspects of the present disclosure.

[0038] Figure 7 illustrates an example of a UE in accordance with aspects of the present disclosure.

[0039] Figure 8 illustrates an example of a processor in accordance with aspects of the present disclosure.

[0040] Figure 9 illustrates an example of a network equipment (NE) in accordance with aspects of the present disclosure.

[0041] Figure 10 illustrates a flowchart of a method performed by a NE in accordance with aspects of the present disclosure.

[0042] Figure 11 illustrates a flowchart of a method performed by a NE in accordance with aspects of the present disclosure.

[0043] Figure 12 illustrates a flowchart of another method performed by a NE in accordance with aspects of the present disclosure.

[0044] Figure 13 illustrates a flowchart of another method performed by a NE in accordance with aspects of the present disclosure.

[0045] Figure 14 illustrates a flowchart of another method performed by a NE in accordance with aspects of the present disclosure.

DETAILED DESCRIPTION

[0046] Legacy cryptographic algorithms for ciphering and integrity protection (e.g., of AS and NAS layer connections) in 5G systems utilize 128-bit algorithms (e.g., AES-128). The security of these algorithms, such as AES-128, can be compromised by quantum

computing and other powerful computing systems. To counter such threats to symmetric cryptography (e.g., from bad actors using quantum computers), the 5G systems may update their algorithms by doubling the key-size of an algorithm, and thus doubling the number of bits used in classical security mechanisms.

[0047] Recently, 265-bit algorithms and other security mechanisms have been introduced to wireless communications systems, such as to core networks and radio access networks (RANs). The introduction of 265-bit capabilities enables 256-bit capable UEs to connect to base stations (e.g., gNBs) that support the 256-bit algorithms and/or Access and Mobility Management Functions (AMFs) that support the 256-bit algorithms. However, such support for 256-bit capabilities is not ubiquitous across networks or UEs.

[0048] Thus, there may be scenarios where a UE supports 256-bit security, but a network entity or function does not support 256-bit security (e.g., a gNB or AMF only supports 128-bit security). Similarly, there may be scenarios where one or more network nodes support 256-bit security, but the UE, or another network node, does not support 256-bit security (e.g., the UE only supports 128-bit security).

[0049] Further, during UE mobility (e.g., Xn handover, N2 handover, and so on), the UE may connect with different gNBs/RAN nodes or different AMFs, where each RAN node or AMF utilizes an independent selection process or algorithm during the handover. When the selection processes are not based on or aware of the security capabilities (e.g., 256-bit security capabilities) of the UE, various problems may arise. For example:

[0050] When the UE supports 256-bit algorithms and a source gNB supports 256-bit security handovers to a target gNB that only supports 128-bit algorithms, the AS connection for the UE may have a reduced level of security;

[0051] When the UE supports both 256-bit algorithms and 128-bit algorithms and a source gNB supports 256-bit security handovers the UE to a target gNB that supports both 128-bit algorithms and 256-bit algorithms, the target gNB may select and use 128-bit algorithms, and the AS connection for the UE may have a reduced level of security;

[0052] Currently, 256-bit radio resource control (RRC) keys (K_{RRCint} and K_{RRCenc}), and user plane (UP) keys (K_{UPint} and K_{UPenc}) are truncated by the gNB/ng-eNB and used with

128-bit algorithms for ciphering and integrity protection. Thus, during mobility of the UE, when any RAN node similarly truncates and uses 128-bit keys for ciphering and integrity protection (e.g., even using a 256-bit algorithm), the AS connection for the UE may have a reduced level of security due to a lack of entropy;

[0053] Also, 256-bit Non Access Stratum (NAS) keys (K_{NASint} and K_{NASenc}) are truncated by the AMF and used with 128-bit algorithms for ciphering and integrity protection. Thus, during mobility of the UE, when an AMF similarly truncates and uses 128-bit keys for ciphering and integrity protection (e.g., even using a 256-bit algorithm), the NAS connection for the UE may have a reduced level of security due to a lack of entropy; and so on.

[0054] The technology described herein provides solutions to such problems, by enabling a UE to indicate its security capabilities (e.g., 256-bit security capabilities) to a network during a mobility procedure, such as an Xn handover or N2 handover. For example, the UE may send an indication to the network in a NAS message or N1 transport.

[0055] The security capabilities (256-bit capabilities) for the UE may include support of a 256-bit key size (e.g., a 256-bit permanent key, a 256-bit key derivation function, such as HMAC-SHA-256) and indicate the supported security capabilities via a “256-bit key size supported” indication. Further, the security capabilities (256-bit capabilities) for the UE may include 256-bit cryptographic algorithms for ciphering and integrity protection (e.g., a 256-bit SNOW 3G based algorithm, a 256-bit AES based algorithm, a 256-bit ZUC based algorithm, and so on) and indicate the supported security capabilities via a “256-bits cryptographic algorithms support” indication, along with algorithm identities/identifiers.

[0056] Thus, the systems and method described herein can mitigate or avoid reduced levels of security during mobility procedures arising from the introduction or roll out of an enhanced level of security (e.g., 256-bit) to a network and/or various network entities, among other benefits.

[0057] Aspects of the present disclosure are described in the context of a wireless communications system.

[0058] Figure 1 illustrates an example of a wireless communications system 100 in accordance with aspects of the present disclosure. The wireless communications system 100 may include one or more NE 102, one or more UE 104, and a core network (CN) 106. The wireless communications system 100 may support various radio access technologies. In some implementations, the wireless communications system 100 may be a 4G network, such as an LTE network or an LTE-Advanced (LTE-A) network. In some other implementations, the wireless communications system 100 may be a NR network, such as a 5G network, a 5G-Advanced (5G-A) network, or a 5G ultrawideband (5G-UWB) 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, for example, 6G. 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.

[0059] The one or more NE 102 may be dispersed throughout a geographic region to form the wireless communications system 100. One or more of the NE 102 described herein may be or include or may be referred to as a network node, a base station, a network element, a network function, a network entity, a radio access network (RAN), a NodeB, an eNodeB (eNB), a next-generation NodeB (gNB), or other suitable terminology. An NE 102 and a UE 104 may communicate via a communication link, which may be a wireless or wired connection. For example, an NE 102 and a UE 104 may perform wireless communication (e.g., receive signaling, transmit signaling) over a Uu interface.

[0060] An NE 102 may provide a geographic coverage area for which the NE 102 may support services for one or more UEs 104 within the geographic coverage area. For example, an NE 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, an NE 102 may be moveable, for example, a satellite associated with a non-terrestrial network (NTN). In some

implementations, different geographic coverage areas associated with the same or different radio access technologies may overlap, but the different geographic coverage areas may be associated with different NE 102.

[0061] The one or more UE 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 remote unit, a mobile device, a wireless device, a remote device, a subscriber device, a transmitter device, a receiver 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.

[0062] A UE 104 may be able to support wireless communication directly with other UEs 104 over a communication link. 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 may be referred to as a sidelink. For example, a UE 104 may support wireless communication directly with another UE 104 over a PC5 interface.

[0063] An NE 102 may support communications with the CN 106, or with another NE 102, or both. For example, an NE 102 may interface with other NE 102 or the CN 106 through one or more backhaul links (e.g., S1, N2, N3, or network interface). In some implementations, the NE 102 may communicate with each other directly. In some other implementations, the NE 102 may communicate with each other indirectly (e.g., via the CN 106). In some implementations, one or more NE 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).

[0064] 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 NE 102 associated with the CN 106.

[0065] The CN 106 may communicate with a packet data network over one or more backhaul links (e.g., via an S1, N2, N3, or another network interface). The packet data network may include an application server. In some implementations, one or more UEs 104 may communicate with the application server. A UE 104 may establish a session (e.g., a protocol data unit (PDU) session, or the like) with the CN 106 via an NE 102. The CN 106 may route traffic (e.g., control information, data, and the like) between the UE 104 and the application server 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).

[0066] In the wireless communications system 100, the NEs 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 NEs 102 and the UEs 104 may support different resource structures. For example, the NEs 102 and the UEs 104 may support different frame structures. In some implementations, such as in 4G, the NEs 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 NEs 102 and the UEs 104 may support various frame structures (i.e., multiple frame structures). The NEs 102 and the UEs 104 may support various frame structures based on one or more numerologies.

[0067] 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.

[0068] 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.

[0069] 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., 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.

[0070] 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 NEs 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 NEs 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 NEs 102 and the UEs 104, among other equipment or devices for short-range, high data rate capabilities.

[0071] 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.

[0072] As described herein, the systems and method exchange levels/capabilities/strengths supported by UEs and networks during UE mobility procedures, to prevent or avoid reduced levels of security when the UE moves from a source base station to a target base station, among other benefits.

[0073] In some embodiments, a source (or serving) gNB (or other base station) determines to initiate a handover for the UE 104. The source gNB checks the security capabilities of the UE 104. When the security capabilities of the UE 104 include only 128-bit algorithms, the source gNB selects a target gNB that has a capability/configuration to support 128-bit algorithms. Also, when the security capabilities of the UE 104 include 128-bit algorithms and 256-bit algorithms, the source gNB selects a target gNB that has a capability/configuration to support 256-bit algorithms. Finally, when the security capabilities of the UE 104 include only 256-bit algorithms, the source gNB selects a target gNB that has a capability/configuration to support 256-bit algorithms.

[0074] The source gNB transmits or otherwise provides the target gNB with the security capabilities of the UE 104, such as the support of 256-bit encryption algorithms, 256-bit integrity algorithms, and a 256-bit key size indication and/or Use 256 bit AS key indication. The target gNB, using the information provided by the source gNB, applies uniform 256-bit ciphering and integrity protection algorithms using 256 bit AS keys (e.g., RRC keys (K_{RRCint} and K_{RRCenc}), UP Keys (K_{UPint} and K_{UPenc})) for the AS security (e.g., RRC and User Plane security), and so on.

[0075] Figure 2 illustrates a messaging flow 200 of an Xn handover procedure in accordance with aspects of the present disclosure. In some cases, the messaging flow 200 represents how to implement uniform application of a 256-bit algorithm for AS security (e.g., RRC and UP ciphering and integrity protection) during an Xn handover scenario for the UE 104 (e.g., where the UE 104 moves from a source gNB to a target gNB).

[0076] Further, the messaging flow 200 depicts the UE 104 and a new target gNB uniformly using 256-bit AS security keys (e.g., RRC keys (K_{RRCint} and K_{RRCenc}) and UP Keys (K_{UPint} and K_{UPenc})) while using 256-bit algorithms for the RRC and UP ciphering and integrity protection. The messaging flow 200 also depicts how a source gNB selects a target gNB with sufficient security capabilities/configurations (e.g., to apply 256-bit algorithms and security) to serve the UE 104, when the UE 104 can support 256-bit cryptographic algorithms (or 256-bit security).

[0077] In some cases, before commencement of step 1, when the UE 104 can support 256-bit security, the UE 104 transmits or shares the corresponding UE 256-bit security capabilities to the network in a NAS message/N1 transport (e.g., Registration Request/Mobility Registration update/Periodic Registration update/any initial NAS message/PDU session establishment/modification request message, and so on), along with a UE identifier (subscription concealed identifier (SUCI), 5G globally unique temporary UE identity (5G-GUTI)).

[0078] As described herein, the UE 256-bit security capabilities may include (1) the UE 104 supporting a 256-bit key size (e.g., 256 bit permanent key, 256 bits key derivation function, such as HMAC-SHA-256), (2) the UE 104 supporting 256-bit cryptographic algorithms (e.g., 256-bit SNOW 3G based algorithm, 256-bit AES based algorithm, 256-bit ZUC based algorithm, and so on).

[0079] For example, a UE supported ciphering algorithms list can be part of an Encryption Algorithms information element (IE) in a UE Security Capabilities IE and include: NEA0 (Null ciphering algorithm), 128-NEA1 (128-bit SNOW 3G based algorithm), 128-NEA2 (128-bit AES based algorithm), 128-NEA3 (128-bit ZUC based algorithm), 256-NEA1/4 (256-bit SNOW 3G based algorithm), 256-NEA2/5 (256-bit AES based algorithm), 256-NEA3/6 (256-bit ZUC based algorithm), and so on.

[0080] As another example, a UE supported integrity protection algorithms list can be part of an Integrity Algorithms IE in a UE Security Capabilities IE and include: NIA0 (Null integrity protection algorithm), 128-NIA1 (128-bit SNOW 3G based algorithm), 128-NIA2 (128-bit AES based algorithm), 128-NIA3 (128-bit ZUC based algorithm), 256-NIA1/4 (256-bit SNOW 3G based algorithm), 256-NIA2/5 (256-bit AES based algorithm), 256-NIA3/6 (256-bit ZUC based algorithm), and so on.

[0081] Further, in some cases, the UE 104 and the network (e.g., via the NE 102) may perform primary authentication, NAS and AS security establishment (e.g., via a security mode command procedure) to connect the UE to the network. Due to the mobility of the UE 104, or due to other reasons, the serving gNB may initiate a handover for the UE (e.g., towards a target gNB), as described herein.

[0082] In step 1, during handover from a source RAN, or gNB/ng-eNB 210 over Xn to a target RAN, or gNB/ng-eNB 220, the source gNB/ng-eNB 210 includes the 5G security capabilities of the UE 104 with the 256-bit security capabilities of the UE 104. For example, the source gNB 210 may include a "Use 256 bit AS key" indication and 256-bit ciphering and 256-bit integrity algorithms used in the source gNB 210 in a handover request message sent to the target gNB 220.

[0083] When the UE 104 supports 256-bit security capabilities, the source gNB/ng-eNB 210 may select a target gNB/ng-eNB having the 256-bit algorithm configurations/support to enable uniform security, to ensure a same level of protection (e.g., a same cryptographic key length) for AS, as described herein.

[0084] In step 2, target gNB/ng-eNB 220 determines to select and apply a 256-bit cryptographic algorithm (e.g., for AS security, such as RRC integrity and ciphering protection and UP integrity and ciphering protection) upon receipt of UE security capabilities to support 256 algorithms from the source gNB/ng-eNB 210 (e.g., in the handover request) and/or when an operator configuration policy includes 256-bit algorithms in a prioritized list.

[0085] When the target gNB/ng-eNB 220 determines to apply 256-bit cryptographic algorithm for AS (RRC and UP) security, based on a received, "Use 256-bit AS key" indication, the target gNB/ng-eNB 220, following the RRC integrity and encryption key derivation (K_{RRCint} and K_{RRCenc}) and UP integrity and encryption key derivation (K_{UPint} and K_{UPenc}), retains the 256-bit keys of K_{RRCint} and K_{RRCenc} and skips RRC key truncation. The target gNB/ng-eNB 220 may also retain the 256-bit keys of K_{UPint} and K_{UPenc} and skip the UP key truncation.

[0086] The target gNB/ng-eNB 220 may select the 256-bit algorithm with a highest priority from the received 5G security capabilities (e.g., supported 256-bit cryptographic algorithm) of the UE 104 according to the prioritized locally configured list of 256-bit algorithms (e.g., applicable for both integrity and ciphering algorithms).

[0087] In some cases, the source gNB/ng-eNB 210 selects a suitable target gNB/ng-eNB 220 based on the security capabilities of the target gNB/ng-eNB 220 (e.g., when the

target gNB/ng-eNB 220 supports 256-bit security/256-bit key size handling/256-bit ciphering and integrity algorithms). In these cases, the target gNB/ng-eNB 220 is selected to perform UE Xn handover to enable application of a same level of AS security (RRC and UP) for the UE 104. An example gNB /ng-eNB security capabilities exchange procedure is described herein.

[0088] In step 3, the target gNB/ng-eNB 220 sends to the source gNB/ng-eNB 210 the handover request acknowledge message, which includes a "handover command" with selected 256-bits RRC and UP encryption and integrity algorithms and may also contain the "Use 256-bit AS key" indication. The handover command may be a transparent container sent by the target gNB/ng-eNB 220 that is forwarded to the UE 104 by the source gNB/ng-eNB 210.

[0089] The target gNB/ng-eNB 220 may skip truncation for newly derived RRC keys (K_{RRCint} and K_{RRCenc}) and UP keys (K_{UPint} and K_{UPenc}) based on the received "Use 256 bit AS key" indication. The handover command message may be integrity protected with a 256-bit RRC integrity key based on the new RRC keys (K_{RRCint}) and the selected 256-bit cryptographic algorithm for integrity protection (e.g., if the target gNB/ng-eNB 220 selects and uses the 256-bit integrity algorithm). The handover command message may be also ciphered with 256-bit RRC encryption key based on the new RRC keys (K_{RRCenc}) and the selected 256-bit cryptographic algorithm for ciphering protection (e.g., if the target gNB/ng-eNB 220 selects and uses the 256-bit ciphering algorithm).

[0090] In step 4, the chosen algorithms (e.g., 256-bit RRC and UP encryption and integrity algorithms), such as when the target gNB/ng-eNB 220 selects different algorithms from the source gNB/ng-eNB 210, and the "Use 256-bit AS key" indication is indicated to the UE 104 in the handover command message. When the UE 104 does not receive a selection of integrity and ciphering algorithms, the UE 104 continues to use the same algorithms as before the handover (see TS 38.331 for a gNB or TS 36.331 for an ng-eNB) and uses 256-bit keys for RRC and UP security with no truncation to 128-bits (e.g., based on the "Use 256-bit AS key" indication received in the handover command). When a Xn-handover takes place from a ng-eNB to a gNB or vice versa, then the selected 256-bit

algorithms in the target node and the “Use 256-bit AS key” indication may be signaled in the handover command to the UE 104.

[0091] In step 5, the UE 104 determines to derive and retain 256-bit keys (for AS keys, such as RRC keys: K_{RRCint}, K_{RRCenc} and UP Keys: K_{UPint} and K_{UPenc}) and skips the RRC and UP key truncation based on the received selected RRC and UP algorithms (indicating 256-bit integrity and 256-bit ciphering algorithms) and/or based on the received “Use 256-bit AS key” indication in the handover command message.

[0092] The UE 104 determines to use 256-bit algorithms for ciphering and integrity protection based on the 256-bit integrity algorithm and the 256-bit ciphering algorithm indicated by the target gNB/ng-eNB 220 in the handover command message. For example, the UE 104 uses the integrity protection with the indicated (256-bit) RRC integrity algorithm and the RRC integrity key for further RRC connections with the target gNB/ng-eNB 220 in step 6.

[0093] In step 6a, the UE 104 sends the RRC Reconfiguration complete and/or Handover complete message to the target gNB/ng-eNB 220. In step 6b, the target gNB/ng-eNB 220 may send a handover success message to the source gNB/ng-eNB 210.

[0094] In step 7, the target gNB/ng-eNB 220 sends a Path-Switch message with the 5G security capabilities of the UE 104, including 256-bit security capabilities, received from the source gNB/ng-eNB 210 to a source AMF 230.

[0095] In step 8, the AMF 230 verifies that the 5G security capabilities of the UE 104 such as 256-bit security capabilities, received from the target gNB/ng-eNB 220 are the same as the security capabilities of the UE 104 locally stored at the source AMF 230.

[0096] In step 9, when there is a mismatch, the source AMF 230 sends its locally stored 5G security capabilities (e.g., 256-bit security capabilities) of the UE 104 to the target gNB/ng-eNB 330 in the Path-Switch Acknowledge message. The source AMF 230 supports logging capabilities for this event and may take additional measures, such as raising an alarm.

[0097] In step 10, when the target gNB/ng-eNB 220 receives 5G security capabilities (e.g., 256-bit security capabilities) of the UE 104 from the AMF 230 in the Path-Switch Acknowledge message, the target gNB/ng-eNB 220 updates the AS security context of the UE 104 with these 5G security capabilities containing the 256-bit security capabilities of the UE 104. The target gNB/ng-eNB 220 selects the 256-bit algorithm with a highest priority from these 5G security capabilities, containing the 256-bit security capabilities, according to the locally configured prioritized list of algorithms (applicable for both integrity and ciphering algorithms).

[0098] When the algorithms selected by the target gNB/ng-eNB 220 are different than the algorithms used at the source gNB/ng-eNB 210, then the target gNB/ng-eNB 220 may initiate an intra-cell handover procedure, which can include an RRC Connection Reconfiguration procedure indicating the selected 256-bit algorithms and a Next Hop Chaining Counter (NCC) parameter to the UE 104. Further, the target gNB/ng-eNB 220 can send the source gNB/ng-eNB 210 the UE context release message.

[0099] In some cases, by transferring the 256-bit ciphering and integrity algorithms used in a source RAN along with a “Use 256 bit AS key” indication to a target RAN, the handover request message allows for the target RAN to decipher and verify the integrity of the RRC Reestablishment Complete message on SRB1 in a potential RRC Connection Re-establishment procedure using the 256-bit integrity and ciphering algorithms and to use the 256-bit RRC keys. The target RAN may also use the information to determine whether to include a new selection of 256-bit security algorithms in the Handover Command message.

[0100] In some embodiments, a source or serving gNB may determine to initiate an N2 handover (with an AMF change). The source gNB may generate a source to target transparent container (STC) with the security capabilities of the UE 104 (as described herein). The source gNB may send the STC to a source AMF, which forwards the STC to a target gNB via a target AMF.

[0101] Figure 3 illustrates a messaging flow 300 of an N2 handover procedure with an AMF change in accordance with aspects of the present disclosure. In some cases, the messaging flow 300 depicts how a 256-bit algorithm can be uniformly applied for NAS

security (e.g., NAS ciphering and integrity protection) and AS security (e.g., RRC and UP ciphering and integrity protection) during an N2 handover scenario for the UE 104. The messaging flow 300 also depicts how the UE 104 and a target AMF 310 can uniformly use/apply 256-bit NAS security keys (K_{NASint} and K_{NASenc}) while using 256-bit algorithms for NAS ciphering and integrity protection.

[0102] Further, the messaging flow 300 may depict how the UE 104 and the target gNB 230 can uniformly use 256-bit AS security keys (e.g,, RRC keys (K_{RRCint} and K_{RRCenc}) or UP Keys (K_{UPint} and K_{UPenc})) while using 256-bit algorithms for the RRC and UP ciphering and integrity protection; and/or how the source AMF 230 selects a target AMF 310 having sufficient or matching security capabilities/configurations (e.g., to apply 256-bit algorithms based ciphering and integrity protection) to serve the UE 104, which can support 256-bit cryptographic algorithms (or 256-bit security).

[0103] In step 1, at handover from the source gNB/ng-eNB 210 to the target gNB/ng-eNB 220 over N2 (e.g., including an AMF change), the source gNB/ng-eNB 210 includes the 5G security capabilities (e.g., UE 256-bit security capabilities, via a “Use 256 bit AS key” indication) of the UE 104 and 256-bit ciphering and 256-bit integrity algorithms used by the source gNB/ng-eNB 210 in the handover request message.

[0104] In some cases, the source gNB/ng-eNB 210 may send the 5G security capabilities of the UE 104, with 256-bit security capabilities, and 256-bit ciphering and 256-bit integrity algorithms used by the gNB/ng-eNB 210 inside or contained in a source to target transparent container (STC), where the STC is sent to the source AMF 230 in the handover request message. The STC can enable transparent forwarding to the target 220 gNB/ng-eNB via the source AMF 230 and the target AMF 310 in a transparent manner. The receiving target gNB/ng-eNB 220 can use the information received in the STC to select the necessary cryptographic algorithms and key size (e.g., 256-bit ciphering algorithms and 256-bit key size in this case) and perform the AS security establishment.

[0105] In step 2, the source AMF 230 sends to the target AMF 310 the Namf_Communication_CreateUEContext Request message, which includes 5G security capabilities of the UE 104 with the UE 256-bit security capabilities, Use 256 bit NAS key

indications. The request message may include an STC, such as “STC(Used AS algorithms-Indicating 256-bit Integrity algorithm, 256-bit Ciphering algorithm, Use 256 bit AS key indication).”

[0106] In some cases, when the UE 104 supports 256-bit security capabilities, the source AMF 230 may select a target AMF having the 256-bit algorithm configurations/support to enable uniform security, such as to ensure the same level of protection (e.g., cryptographic key length) for the NAS (based on the AMF configuration exchanged over N14 interface as part of a configuration transfer, as described herein).

[0107] In some cases, the source AMF 230 selects a suitable target AMF based on the security capabilities of the target AMF (e.g., supporting 256-bit security/256-bit key size handling/256-bit ciphering and integrity algorithms). The target AMF (e.g., the target AMF 310) is selected to perform UE N2 handover to enable application of a same level of NAS security (e.g., NAS ciphering and integrity protection) for the UE 104.

[0108] In step 3, the target AMF 310 selects and applies a 256-bit cryptographic algorithm (for NAS security, such as integrity and ciphering protection) upon receipt of UE security capabilities that support 256-bit algorithm from the source AMF 230 and/or when the operator configuration policy includes 256-bit algorithms in a prioritized list.

[0109] When the target AMF 310 determines to apply a 256-bit cryptographic algorithm for NAS security, based on a “Use 256-bit NAS key” indication, the target AMF 310 follows the NAS integrity and encryption key derivation (K_{NASint} and K_{NASenc}) and retains the 256-bit keys of K_{NASint} and K_{NASenc}, skipping NAS key truncation. The target AMF 310 may select the 256-bit algorithm with a highest priority from the received 5G security capabilities (e.g., based on supported 256-bit cryptographic algorithm) of the UE 104 according to the prioritized locally configured list of 256-bit algorithms (applicable to both integrity and ciphering algorithms).

[0110] In step 4, when the change of the AMF at N2-Handover (or mobility registration update) results in a change of an algorithm to be used for establishing NAS security, the target AMF 310 indicates the 256-bit selected algorithm to the UE 104 as described herein

for N2-Handover (e.g., using a NAS Container (NASC)). The target AMF 310 may select the NAS algorithm having highest priority according to the ordered lists.

[0111] In some cases, such as a mobility registration update (e.g., using NAS SMC), the target AMF 310 indicates the 256-bit selected algorithm to the UE 104 along with the "Use 256-bit NAS key" indication. The target AMF 310 may create a NASC containing the selected 256-bit NAS security algorithms (for integrity and ciphering protection, which indicate selected 256-bit integrity algorithms and/or256-bit ciphering algorithms), and a "Use 256-bit NAS key" indication, along with other information (e.g., related to AMF key derivation) and NAS MAC.

[0112] In some cases, the target AMF 310 sends the 5G security capabilities (e.g., 256-bit security capabilities) of the UE 104, the STC (e.g., used AS algorithms and/or an indication of 256-bit integrity algorithm, 256-bit Ciphering algorithm), a "Use 256 bit AS key" indication, a NASC (e.g., indicating a selected 256-bit integrity algorithm, 256-bit ciphering algorithm, "Use 256 bit NAS key" indication, and so on), along with other information (e.g., related to AMF key derivation) and NAS MAC, in a NGAP HANDOVER REQUEST message to the target ng-eNB/gNB 220. The use of the NASC may be similar to use of a NAS SMC message.

[0113] In step 5, upon receipt of the NGAP HANDOVER REQUEST message from the target AMF 310, the target ng-eNB/gNB 220 uses the information received in the STC, such as used AS algorithms (e.g., an indication of 256-bit integrity algorithm, 256-bit ciphering algorithm, "Use 256 bit AS key" indication). The target gNB/ng-eNB 220 determines to select and apply the 256-bit cryptographic algorithm (for AS security, such as RRC integrity and ciphering protection and UP integrity and ciphering protection) upon receipt of UE security capabilities to support of 256-bit algorithms from the source gNB/ng-eNB 210 (in the STC) via the target AMF 310 and if an operator configuration policy includes 256-bit algorithms in a prioritized list.

[0114] If the target gNB/ng-eNB 220 determines to apply 256-bit cryptographic algorithm for AS (RRC and UP) security, based on the "Use 256-bit AS key" indication and when the target gNB/ng-eNB 220 follows the RRC integrity and encryption key

derivation (K_{RRCint} and K_{RRCenc}) and UP integrity and encryption key derivation (K_{UPint} and K_{UPenc}), the target gNB/ng-eNB 220 retains the 256-bit keys of K_{RRCint} and K_{RRCenc} and skips RRC key truncation. Similarly retains the 256-bit keys of K_{UPint} and K_{UPenc} and skips the UP key truncation. The target gNB/ng-eNB 220 selects the 256-bit algorithm with a highest priority from the received 5G security capabilities (based on supported 256-bit cryptographic algorithm) of the UE 104 according to the prioritized locally configured list of 256-bit algorithms (applicable to both integrity and ciphering algorithms).

[0115] In some cases, the target ng-eNB/gNB 220 constructs a 'Target to Source transparent Container' (TSC), which contains the selected 256-bit integrity algorithm, 256-bit ciphering algorithm for AS, and "Use 256 bit AS key" indication. The TSC provided by the target gNB/ng-eNB 220 enables transparent forwarding to the source gNB/ng-eNB 210 via the target AMF 310 and source AMF 230 in a transparent manner. Thus, the receiving source gNB/ng-eNB 210 can provide the information received in the TSC to the UE 104 in a handover command message (see step 9) to enable the UE 104 to select suitable cryptographic algorithms and key sizes (e.g., 256-bit ciphering algorithms and 256-bit key size), similar to the target gNB/ng-eNB 220 for a successful AS security establishment.

[0116] In step 6, the target gNB/ng-eNB 220 can send to the target AMF 310 a Handover Request Acknowledge message, which includes the TSC (e.g., selected 256-bit integrity algorithm, 256-bit ciphering algorithm for AS, and "Use 256 bit AS key" indication), and the NASC (e.g., Indicate selected 256-bit integrity algorithm, 256-bit ciphering algorithm, "Use 256 bit NAS key indication"), along with other information (e.g., related to AMF key derivation) and NAS MAC that is received in step 4.

[0117] In step 7, the target AMF 310 sends to the source AMF 230, Namf_Communication_CreateUEContext Response message, which includes the TSC (Selected 256-bit Integrity algorithm, 256-bit Ciphering algorithm for AS, and Use 256-bit AS key indication), and the NASC (Indicate selected 256-bit Integrity algorithm, 256-bit Ciphering algorithm, Use 256-bit NAS key indication, along with other information (e.g., related to AMF key derivation) and NAS MAC).

[0118] In step 8, the source AMF 230 sends the received TSC (Selected 256-bit Integrity algorithm, 256-bit Ciphering algorithm for AS, and Use 256-bit AS key indication), and the NASC (Indicate selected 256-bit Integrity algorithm, 256-bit Ciphering algorithm, Use 256-bit NAS key indication, along with other information (e.g., related to AMF key derivation) and NAS MAC) to the source gNB/ng-eNB 210 in a handover command message.

[0119] In step 9, the source gNB/ng-eNB 210 sends the chosen algorithms (e.g., 256-bit RRC and UP encryption and integrity algorithms), when the target gNB/ng-eNB 220 selects different algorithms compared to the source gNB/ng-eNB 210, and a "Use 256-bit AS key" indication (received in TSC in step 8) is indicated to the UE 104 along with the received NASC in the Handover Command message. For example, the source gNB/ng-eNB 210 sends the UE Handover Command message with the selected 256-bit integrity algorithm, 256-bit ciphering algorithm for AS, "Use 256 bit AS key" indication, and the NASC (indicate selected 256-bit integrity algorithm, 256-bit ciphering algorithm, "Use 256 bit NAS key" indication).

[0120] In step 10, the UE 104 derives and retains 256-bit keys (for NAS keys, such as K_{NASint}, K_{NASenc}) and skips the NAS key truncation based on the received selected NAS algorithms (indicating 256-bit integrity and 256-bit ciphering algorithms) and/or based on the received "Use 256-bit NAS key" indication (as part of the NASC) in the handover command message. The UE 104 may determine to use 256-bit algorithms for ciphering and integrity protection based on the 256-bit integrity algorithm, 256-bit ciphering algorithm indicated by the target AMF 310 (as part of the NASC) in the handover command message.

[0121] In some cases, The UE 104 derives and retains 256-bit keys (for AS keys, such as RRC keys: K_{RRCint}, K_{RRCenc}, and UP Keys: K_{UPint} and K_{UPenc}) and skips the RRC and UP key truncation based on the received selected RRC and UP algorithms (indicating 256-bit integrity and 256-bit ciphering algorithms) and/or based on the received "Use 256-bit AS key" indication in the handover command message. The UE 104 may determine to use 256-bit algorithms for ciphering and integrity protection based on the 256-bit integrity algorithm, 256-bit ciphering algorithm indicated by the target gNB/ng-eNB 220 in the handover command message. For example, the UE 104 may utilize the integrity protection

with the indicated (256-bit) RRC integrity algorithm and the RRC integrity key for further RRC connections with the target gNB/ng-eNB 220 in step 11 (e.g., for the handover confirm message).

[0122] In some cases, when the UE 104 does not receive a selection of integrity and ciphering algorithms, the UE 104 continues to use the same algorithms as before the handover (see TS 38.331 for gNB or TS 36.331 for ng-eNB) and uses 256-bit keys for RRC and UP security with no truncation to 128-bits (based on the "Use 256-bit AS key" indication received in the handover command).

[0123] In step 11, the UE 104 sends a handover confirm message to the target gNB/ng-eNB 220 by applying the newly selected 256-bit integrity and ciphering algorithms with 256-bit RRC keys (K_{RRCint}, K_{RRCenc}).

[0124] In step 12, the target gNB/ng-eNB 220 may send a handover notify message to the target AMF 310.

[0125] In step 13a, the target AMF 310 may send a Namf_Communication_N2InfoNotify to the source AMF. In step 13b, the source AMF 230 may send a Namf_Communication_N2InfoNotify acknowledgement to the target AMF 310.

[0126] In step 14a, the source AMF 230 may send a UE context release command to the source gNB/ng-eNB 210. In step 14b, the source gNB/ng-eNB 210 may send a UE context release complete to the source AMF 230.

[0127] In some embodiments, a source or serving gNB may determine to initiate an N2 handover (without an AMF change). The source gNB may generate a source to target transparent container (STC) with the security capabilities of the UE 104 (as described herein). The source gNB may send the STC to a source AMF, which forwards the STC to a target gNB.

[0128] Figure 4 illustrates a messaging flow 400 of an N2 handover procedure without an AMF change in accordance with aspects of the present disclosure. In some cases, the messaging flow 400 depicts how a 256-bit algorithm can be uniformly applied for AS

security (e.g., RRC and UP ciphering and integrity protection) during an N2 handover scenario for the UE 104.

[0129] Further, the messaging flow 400 may depict how the UE 104 and the target gNB 230 can uniformly use 256-bit AS security keys (e.g,, RRC keys (K_{RRCint} and K_{RRCenc}) or UP Keys (K_{UPint} and K_{UPenc})) while using 256-bit algorithms for the RRC and UP ciphering and integrity protection; and/or how the source AMF 230 selects a target gNB having sufficient or matching security capabilities/configurations (e.g., to apply 256-bit algorithms based ciphering and integrity protection) to serve the UE 104, which can support 256-bit cryptographic algorithms (or 256-bit security).

[0130] In step 1, during handover from the source gNB/ng-eNB 210 to the target gNB/ng-eNB 220 over N2 (via a same AMF 410), the source gNB/ng-eNB 210 includes the 5G security capabilities of the UE 104 (e.g., 256-bit security capabilities, “Use 256 bit AS key” indication), and 256-bit ciphering and 256-bit integrity algorithms used by the source gNB/ng-eNB 210 in the handover request message.

[0131] In some cases, the source gNB/ng-eNB 210 may send the 5G security capabilities (e.g., 256-bit security capabilities and/or “Use 256 bit AS key” indication), and 256-bit ciphering and 256-bit integrity algorithms used by the source gNB/ng-eNB 210 inside an STC, which is sent by the AMF 410 in the handover request message. The STC enables transparent forwarding to the target gNB/ng-eNB 220 via the AMF 410 in a transparent manner. The receiving target gNB/ng-eNB 220 may use the information received in the STC to select the suitable cryptographic algorithms and key size (e.g., 256-bit ciphering algorithms and 256-bit key size in this case) and perform an AS security establishment.

[0132] In step 2, the AMF 410 sends to the target gNB/ng-eNB 220 the Handover Request message, which includes the 5G security capabilities (e.g., 256-bit security capabilities of the UE 104), and STC (used AS algorithms, indicating 256-bit integrity algorithm, 256-bit ciphering algorithm, “Use 256 bit AS key” indication) received in step 1. When the UE 104 supports 256-bit security capabilities, the AMF 410 may select a target gNB/ng-eNB 220 having 256-bit algorithm configurations/support to enable uniform

security, such as to ensure the same level of protection (e.g., cryptographic key length) for AS (based on the N2 configuration exchanged over N2/NGAP interface as part of a configuration transfer described herein).

[0133] In step 3, upon receipt of an NGAP HANDOVER REQUEST message from the AMF 410, the target ng-eNB/gNB 220 uses the information received in the STC. The target gNB/ng-eNB 220 selects and applies a 256-bit cryptographic algorithm (for AS security, such as RRC integrity and ciphering protection and UP integrity and ciphering protection) upon receipt of UE security capabilities to support 256-bit algorithms from the source gNB/ng-eNB 210 (in the STC) via the AMF 410 and/or when the operator configuration policy includes 256-bit algorithms in a prioritized list.

[0134] If the target gNB/ng-eNB 220 determines to apply a 256-bit cryptographic algorithm for AS (RRC and UP) security, based on the "Use 256-bit AS key" indication and the target gNB/ng-eNB 220 follows the RRC integrity and encryption key derivation (K_{RRCint} and K_{RRCenc}) and UP integrity and encryption key derivation (K_{UPint} and K_{UPenc}), the target gNB/ng-eNB 220 retains the 256-bit keys of K_{RRCint} and K_{RRCenc} and skips an RRC key truncation. Similarly, the target gNB/ng-eNB 220 retains the 256-bit keys of K_{UPint} and K_{UPenc}, and skips a UP key truncation.

[0135] The target gNB/ng-eNB 220 may select the 256-bit algorithm with highest priority from the received 5G security capabilities (based on supported 256-bit cryptographic algorithm) of the UE according to the prioritized locally configured list of 256-bit algorithms (this applies for both integrity and ciphering algorithms).

[0136] The target ng-eNB/gNB 220 may construct a TSC, which contains the selected 256-bit integrity algorithm, 256-bit ciphering algorithm for AS, and "Use 256 bit AS key" indication. In some cases, the TSC provided by the target gNB/ng-eNB 220 enables transparent forwarding to the source gNB/ng-eNB 210 via the AMF 410 in a transparent manner. Thus, the receiving source gNB/ng-eNB 210 can provide the information received in the TSC to the UE 104 in a handover command message (see step 6) to enable the UE 104 to select suitable or matching cryptographic algorithms and key sizes (e.g., 256-bit

ciphering algorithms and 256-bit key size), similar to the target gNB 220 for a successful AS security establishment.

[0137] In step 4, the target ng-eNB/gNB 220 can send to the AMF 410 a Handover Request Acknowledge message, which includes the TSC (e.g., selected 256-bit integrity algorithm, 256-bit ciphering algorithm for AS, and "Use 256 bit AS key" indication).

[0138] In step 5, the AMF 410 sends the received TSC to the source gNB/ng-eNB 210 in a handover command message.

[0139] In step 6, the source gNB/ng-eNB 210 sends the chosen algorithms (e.g., 256-bit RRC and UP encryption and integrity algorithms), when the target gNB/ng-eNB 220 selects different algorithms compared to the source gNB/ng-eNB 210 and the "Use 256-bit AS key" indication (received in TSC in step 5) is indicated to the UE 104 along with the received NASC in the Handover Command message. For example, the source gNB/ng-eNB 210 sends the UE Handover Command message with selected 256-bit integrity algorithm, 256-bit ciphering algorithm for AS, and "Use 256 bit AS key" indication.

[0140] In step 7, the UE 104 derives and retains 256-bit keys (for AS keys, such as RRC keys: K_{RRCint}, K_{RRCenc} and UP Keys: K_{UPint} and K_{UPenc}) and skips the RRC and UP key truncation based on the received selected RRC and UP algorithms (indicating 256-bit integrity and 256-bit ciphering algorithms) and/or based on the received "Use 256-bit AS key" indication in the handover command message. Further, the UE 104 determines to use 256-bit algorithms for ciphering and integrity protection based on the 256-bit integrity algorithm, 256-bit ciphering algorithm indicated by the target gNB/ng-eNB 220 in the handover command message. This may include using the integrity protection with the indicated (256-bit) RRC integrity algorithm and the RRC integrity key for further RRC connections with the target gNB/ng-eNB 220 in step 8 (e.g., for the handover confirm message).

[0141] In some cases, when the UE 104 does not receive a selection of integrity and ciphering algorithms, the UE 104 may use the same algorithms as before the handover (see TS 38.331 for gNB or TS 36.331 for ng-eNB) and uses 256-bit keys for RRC and UP

security with no truncation to 128-bits (based on the “Use 256-bit AS key” indication received in the handover command).

[0142] In step 8, the UE 104 sends a handover confirm message to the target gNB/ng-eNB 220 by applying the newly selected 256-bit integrity and ciphering algorithms with 256-bit RRC keys (K_{RRCint}, K_{RRCenc}).

[0143] In step 9, the target gNB/ng-eNB 220 may send a handover notify message to the AMF 410.

[0144] In step 10a, the AMF 410 may send a UE context release command to the source gNB/ng-eNB 210, and in step 10b, the source gNB/ng-eNB 210 may send a UE context release complete to the AMF 410.

[0145] In some embodiments, a UE triggered RAN-based notification area (RNA) update procedure can involve context retrieval over an Xn interface, which can facilitate 256-bit security and algorithm negotiation between the UE 104 and the network. In some cases, the RNA update procedure may be triggered when the UE 104 moves out of a configured RNA, or periodically regardless of the location of the UE 104. Figure 5 illustrates a messaging flow 500 of an RNA update procedure in accordance with aspects of the present disclosure.

[0146] In step 1, the UE 104 resumes from RRC_INACTIVE, providing an I-RNTI allocated by a last serving gNB 520 and appropriate cause value, e.g., RAN notification area update. The UE 104 sends a RRC resume request to a new gNB 510 with the RNA update.

[0147] In step 2, the new gNB 510, if able to resolve a gNB identity contained in the I-RNTI, requests the last serving gNB 620 to provide UE Context, providing the cause value received in step 1 by sending a retrieve UE context request message.

[0148] In step 3, the last serving gNB 520 may provide the UE context. For example, the last serving gNB 520 provides the UE 5G security capabilities (e.g., 256-bit Security capabilities, Used AS algorithms, such as an indicate 256-bit integrity algorithm, 256-bit

ciphering algorithm, and “Use 256 bit AS key” indication) to the new gNB 510 in the Retrieve UE Context Response message.

[0149] Alternatively, in some cases, the last serving gNB 520 may decide to move the UE 104 to RRC_IDLE (and the procedure follows steps 3 and later of figure 9.2.2.5-3 of TS 38.300, i.e., Case A) or, if the UE 104 is still within the previously configured RNA, to keep the UE context in the last serving gNB 520 and to keep the UE 104 in RRC_INACTIVE (and the procedure follows steps 3 and later of figure 9.2.2.5-2 of TS 38.300, i.e., Case B). Case A: Instead of providing the UE context, the last serving gNB 520 provides an *RRCRelease* message to move the UE 104 to RRC_IDLE. Case B: The last serving gNB 520 stores received information to be used in the next resume attempt (e.g. C-RNTI and PCI related to the resumption cell), and responds to the last serving gNB 520 with the RETRIEVE UE CONTEXT FAILURE message including an encapsulated *RRCRelease* message. The *RRCRelease* message includes Suspend Indication.

[0150] In step 4, the new gNB 510 may move the UE 104 to RRC_CONNECTED or may send the UE 104 back to RRC_IDLE (in which case an *RRCRelease* message is sent by the gNB 510) or send the UE 104 back to RRC_INACTIVE as assumed in the following.

[0151] In some cases, during transitions from RRC_INACTIVE to RRC_CONNECTED states the new gNB, or ng-eNB, 510 selects and applies a 256-bit cryptographic algorithm (for AS security, such as RRC integrity and ciphering protection and UP integrity and ciphering protection) when it receives UE security capabilities to support 256-bit algorithms from the last serving gNG 520 and if an operator configuration policy includes 256-bit algorithms in a prioritized list.

[0152] When the new gNB 510 determines to apply a 256-bit cryptographic algorithm for AS (RRC and UP) security, based on a “Use 256-bit AS key” indication” and the gNB 510 follows the RRC integrity and encryption key derivation (K_{RRCint} and K_{RRCenc}) and UP integrity and encryption key derivation (K_{UPint} and K_{UPenc}), the new gNB 510 retains the 256-bit keys of K_{RRCint} and K_{RRCenc} and skips the RRC key truncation. Similarly, the new gNB 510 retains the 256-bit keys of K_{UPint} and K_{UPenc} and skips the UP key truncation.

[0153] The new gNB 510 selects the 256-bit algorithm with a highest priority from the received 5G security capabilities (based on supported 256-bit cryptographic algorithm) of the UE 104 according to the prioritized locally configured list of 256-bit algorithms (applicable to both integrity and ciphering algorithms). When the new gNB 510 selects the same security algorithms as the last serving gNB 520, then the new gNB 510 uses the selected algorithms to derive RRC integrity and RRC encryption keys to protect the RRCResume message and send to the UE 104 on SRB1 and may additionally send the "Use 256-bit AS key" indication. In some cases, if a loss of downlink (DL) user data buffered in the last serving gNB 520 is to be prevented, the last serving gNB 520 provides forwarding addresses.

[0154] In step 5, the target gNB 510 performs a path switch. The target gNB 510 sends the Path-Switch message with the 5G security capabilities (e.g., 256-bit security capabilities) of the UE 104 and received from the last serving gNB 520 to an AMF 530, such as a source AMF (e.g., an AMF associated with the last serving gNB 520).

[0155] In step 6, the AMF 530 verifies that the 5G security capabilities (e.g., 256-bit security capabilities) of the UE 104 received from the new gNB 510 are the same as the 5G security capabilities locally stored at the AMF 530.

[0156] In step 7, if there is a mismatch, the AMF 530 sends the locally stored 5G security capabilities (e.g., 256-bit security capabilities) associated with the UE 104 to the new gNB 510 in the Path-Switch Acknowledge message. The AMF 530 may support logging capabilities for this event and may take additional measures, such as raising an alarm.

[0157] In step 8, the new gNB 510 establishes the RRC security (e.g., or in step 4 or directly performs an AS Security mode command procedure in steps 11-13) and also may be the UP security. The new gNB 510 selects and applies a 256-bit cryptographic algorithm (for AS security, such as RRC integrity and ciphering protection and UP integrity and ciphering protection) when it receives UE security capabilities that support 256-bit algorithms from the last serving gNB 520 and/or when the operator configuration policy includes 256-bit algorithms in the prioritized list. When the new gNB 510 determines to

apply 256-bit cryptographic algorithm for AS (RRC and UP) security, based on the “Use 256-bit AS key” indication and following the RRC integrity and encryption key derivation (K_{RRCint} and K_{RRCenc}) and UP integrity and encryption key derivation (K_{UPint} and K_{UPenc}), the new gNB 510 retains the 256-bit keys of K_{RRCint} and K_{RRCenc} and skips the RRC key truncation. Similarly, the new gNB 510 retains the 256-bit keys of K_{UPint} and K_{UPenc} and skips the UP key truncation.

[0158] The new gNB 510 selects the 256-bit algorithm with a highest priority from the received 5G security capabilities (based on supported 256-bit cryptographic algorithm) of the UE 104 according to the prioritized locally configured list of 256-bit algorithms (applicable for both integrity and ciphering algorithms).

[0159] In step 9, the new gNB 510 keeps the UE in RRC_INACTIVE state by sending *RRCRelease* with suspend indication and the “Use 256-bit AS key” indication.

[0160] In step 10, the new gNB 510 triggers the release of the UE resources at the last serving gNB 520 (e.g., the UE Context Release).

[0161] In step 11, when the new gNB 510 does not support the received algorithms or if the new gNB 510 prefers to use different algorithms, the new gNB 510 sends an RRCSetup message on SRB0 to proceed with RRC connection establishment as if the UE 104 was in RRC_IDLE (fallback procedure) to the UE 104. The UE 104 performs NAS based RRC recovery and negotiates a suitable algorithm with the new gNB 510 via AS SMC procedure, as described herein.

[0162] In some cases, new gNB 510 may initiate a AS security mode procedure, where the new gNB 510 selects and applies a 256-bit cryptographic algorithm (for AS security, such as RRC integrity and ciphering protection and UP integrity and ciphering protection) based on the received UE security capabilities and when an operator configuration policy includes 256-bit algorithms in a prioritized list. If the new gNB 510 determines to apply 256-bit cryptographic algorithm for AS (RRC and UP) security, and follows the RRC integrity and encryption key derivation (K_{RRCint} and K_{RRCenc}) and UP integrity and encryption key derivation (K_{UPint} and K_{UPenc}), the new gNB 510 retains the 256-bit keys of

K_{RRCint} and K_{RRCenc} and skips the RRC key truncation. Similarly, the new gNB 510 retains the 256-bit keys of K_{UPint} and K_{UPenc} and skips the UP key truncation.

[0163] The new gNB 510 activates the RRC integrity protection before sending the AS Security Mode Command message. The AS security mode command message sent from the new gNB 510 to the UE 104 may contain the selected 256-bits RRC and UP encryption and integrity algorithms and may also contain the "Use 256-bit AS key" indication. The AS security mode command message may be integrity protected with a 256-bit RRC integrity key based on the new gNB 510 and using the selected 256-bits cryptographic algorithm for integrity protection (if the new gNB 510 selects and uses 256-bit integrity algorithm).

[0164] In step 12, following step 9 or 11, the UE 104 derives and retains 256-bit keys (for AS keys, such as RRC keys: K_{RRCint} , K_{RRCenc} and UP Keys: K_{UPint} and K_{UPenc}) and skips the RRC and UP key truncation based on the received selected RRC and UP algorithms (indicating 256-bit integrity and 256-bit ciphering algorithms) or based on the received "Use 256-bit key size" indication and/or "Use 256-bit security" indication from the new gNB 510. The UE 104 verifies the AS Security Mode Command message, such as by verifying the integrity protection using the indicated (256-bit) RRC integrity algorithm and the RRC integrity key.

[0165] In step 13, the AS security mode complete message sent from the UE 104 to the new gNB 510 is integrity protected with the selected (256 bits) RRC algorithm indicated in the AS security mode command message and (256 bits) RRC integrity key based on the current K_{gNB}.

[0166] In some embodiments, the UE 104 and the network can establish a same level of security during a dual connectivity mode of operation, such as when the UE 104 connects to more than one NG-RAN node (with a 5G core). Figure 6 illustrates a messaging flow 600 of a dual connectivity procedure in accordance with aspects of the present disclosure. The messaging flow 600 supports dual connectivity, where the UE 104 is connected to one gNB (or ng-eNB) that acts as a Master Node (MN) 610 and one gNB (or ng-eNB) that acts as a secondary Node (SN) 620. The MN 610 may be connected to the 5GC CN 106, while the SN 620 may be connected to the MN 610 via an Xn interface.

[0167] In step 1, the UE 104 and the MN 610 establish an RRC connection.

[0168] In step 2, the MN 610 sends a SN Addition/Modification Request to the SN 62- over the Xn-C to negotiate available resources, configuration, and algorithms at the SN 620. The MN 610 computes and delivers the K_{SN} to the SN 620 if a new key is needed. The security capabilities of the UE 104, such as 256-bit security capabilities, the "Use 256 bit AS key" indication, and the UP security policy received from an SMF may be sent to the SN 620. In case of a PDU split, UP integrity protection and ciphering activation decision from the MN 610 may be also included as described in TS 33.501 subclause 6.10.4. When the MN 610 decides to configure CPA or CPC, and if there are more than one candidate SNs, for each SN, the MN 610 derives a different KSN and delivers the KSN separately to each SN.

[0169] In step 3, the SN 620 allocates the necessary resources and the SN selects and applies a 256-bit cryptographic algorithm (for AS security, such as RRC integrity and ciphering protection and UP integrity and ciphering protection) when it received UE security capabilities to support of 256-bit algorithms and when an operator configuration policy includes 256-bit algorithms in a prioritized list. If the SN 620 determines to apply 256-bit cryptographic algorithm for AS (RRC and UP) security, based on the "Use 256-bit AS key" indication, and follows the RRC integrity and encryption key derivation (K_{RRCint} and K_{RRCenc}) and UP integrity and encryption key derivation (K_{UPint} and K_{UPenc}), the SN 620 retains the 256-bit keys of K_{RRCint} and K_{RRCenc} and skips the RRC key truncation. Similarly, the SN 620 retains the 256-bit keys of K_{UPint} and K_{UPenc} and skips the UP key truncation.

[0170] The SN 620 may select the 256-bit algorithm with a highest priority from the received 5G security capabilities (based on supported 256-bit cryptographic algorithm) of the UE 104 according to the prioritized locally configured list of 256-bit algorithms (applicable for both integrity and ciphering algorithms). If a new K_{SN} was delivered to the SN 620, then the SN 620 calculates a needed RRC. The UP keys may be derived at the same time when the RRC key derived. The SN 620 may activate the UP security policy as described in TS 33.501 subclause 6.10.4.

[0171] In step 4, the SN 620 sends the SN Addition/Modification Acknowledge to the MN 610 indicating availability of requested resources and the identifiers for the selected 256-bit algorithms for the requested DRBs and/or SRB for the UE 104 along with the "Use 256-bit AS key" indication. The UP integrity protection and encryption indications may be sent to the MN 610.

[0172] In step 5, the MN 610 sends the RRC Connection Reconfiguration Request to the UE 104 instructing the UE 104 to configure the new DRBs and/or SRB for the SN 620. The MN 610 may include a SN Counter parameter to indicate a new K_{SN} is needed and the UE 104 may compute the K_{SN} for the SN 620. The MN 610 forwards the UE configuration parameters (which contains the 256-bit algorithm identifiers received from the SN 620 in step 4), the "Use 256-bit AS key" indication, and UP integrity protection and encryption indications (received from the SN in step 4) to the UE 104 (see subclause 6.10.3.3). If the SN 620 sends more than one candidate PScell SCG configuration, the MN 610 signals to the UE 104 that all these configurations are associated with the same SN counter value.

[0173] In some cases, because a message is sent over the RRC connection between the MN 610 and the UE 104, the message is integrity protected using the K_{RRCint} of the MN 610, and the SN Counter cannot be tampered with.

[0174] In steps 6a-b, the UE 104 derives and retains 256-bit keys (for AS keys, RRC keys: K_{RRCint}, K_{RRCenc} and UP Keys: K_{UPint} and K_{UPenc}) and skips the RRC and UP key truncation based on the received selected RRC and UP algorithms (indicating 256-bit integrity and 256-bit ciphering algorithms) and/or based on the received "Use 256-bit AS key" indication in step 5. Further, the UE 104 determines to use 256-bit algorithms for ciphering and integrity protection based on the 256-bit integrity algorithm, 256-bit ciphering algorithm (step 5) received for the associated SRB and/or DRBs, respectively. This may include using the integrity protection with the indicated (256-bit) RRC integrity algorithm and the RRC integrity key for further RRC connections, in step 6b.

[0175] The UE 104 accepts the RRC Connection Reconfiguration Request after validating its integrity. The UE 104 computes the K_{SN} for the SN 620 if an SN Counter parameter was included. The UE 104 sends the RRC Reconfiguration Complete to the MN

610. The UE 104 activates the chosen encryption/decryption and integrity protection keys with the SN 620 at this point.

[0176] In steps 7a-b, the MN 610 sends the SN Reconfiguration Complete to the SN 620 over the Xn-C to inform the SN 620 of the configuration result. Upon receipt of the message, SN 620, in step 7b, may activate the 256-bit chosen encryption/decryption and integrity protection with the UE 104 and uses 256-bit keys for RRC and UP. If the SN 620 does not activate encryption/decryption and integrity protection with the UE 104 at this stage, the SN 620 activates the encryption/decryption and integrity protection upon receiving the Random Access request from the UE 104.

[0177] In step 8, the Random Access Procedure between the UE 104 and the SN 620 is complete.

[0178] Figure 7 illustrates an example of a UE 700 in accordance with aspects of the present disclosure. The UE 700 may include a processor 702, a memory 704, a controller 706, and a transceiver 708. The processor 702, the memory 704, the controller 706, or the transceiver 708, or various combinations thereof or various components thereof may be examples of means for performing various aspects of the present disclosure as described herein. These components may be coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces.

[0179] The processor 702, the memory 704, the controller 706, or the transceiver 708, or various combinations or components thereof may be implemented in hardware (e.g., circuitry). The hardware may include a processor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), or other programmable logic device, or any combination thereof configured as or otherwise supporting a means for performing the functions described in the present disclosure.

[0180] The processor 702 may include an intelligent hardware device (e.g., a general-purpose processor, a DSP, a CPU, an ASIC, an FPGA, or any combination thereof). In some implementations, the processor 702 may be configured to operate the memory 704. In some other implementations, the memory 704 may be integrated into the processor 702.

The processor 702 may be configured to execute computer-readable instructions stored in the memory 704 to cause the UE 700 to perform various functions of the present disclosure.

[0181] The memory 704 may include volatile or non-volatile memory. The memory 704 may store computer-readable, computer-executable code including instructions when executed by the processor 702 cause the UE 700 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as the memory 704 or another type of memory. 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.

[0182] In some implementations, the processor 702 and the memory 704 coupled with the processor 702 may be configured to cause the UE 700 to perform one or more of the functions described herein (e.g., executing, by the processor 702, instructions stored in the memory 704). For example, the processor 702 may support wireless communication at the UE 700 in accordance with examples as disclosed herein.

[0183] The controller 706 may manage input and output signals for the UE 700. The controller 706 may also manage peripherals not integrated into the UE 700. In some implementations, the controller 706 may utilize an operating system such as iOS®, ANDROID®, WINDOWS®, or other operating systems. In some implementations, the controller 706 may be implemented as part of the processor 702.

[0184] In some implementations, the UE 700 may include at least one transceiver 708. In some other implementations, the UE 700 may have more than one transceiver 708. The transceiver 708 may represent a wireless transceiver. The transceiver 708 may include one or more receiver chains 710, one or more transmitter chains 712, or a combination thereof.

[0185] A receiver chain 710 may be configured to receive signals (e.g., control information, data, packets) over a wireless medium. For example, the receiver chain 710 may include one or more antennas for receiving the signal over the air or wireless medium. The receiver chain 710 may include at least one amplifier (e.g., a low-noise amplifier

(LNA)) configured to amplify the received signal. The receiver chain 710 may include at least one demodulator configured to demodulate the received signal and obtain the transmitted data by reversing the modulation technique applied during transmission of the signal. The receiver chain 710 may include at least one decoder for decoding and/or processing the demodulated signal to receive the transmitted data.

[0186] A transmitter chain 712 may be configured to generate and transmit signals (e.g., control information, data, packets). The transmitter chain 712 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 transmitter chain 712 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 transmitter chain 712 may also include one or more antennas for transmitting the amplified signal into the air or wireless medium.

[0187] Figure 8 illustrates an example of a processor 800 in accordance with aspects 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, which may be, for example, an 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).

[0188] 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).

[0189] 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.

[0190] 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.

[0191] The memory 804 may include one or more caches (e.g., memory local to or included in the processor 800) or other memory, such as 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).

[0192] 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.

[0193] 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.

[0194] The processor 800 may support wireless communication in accordance with examples as disclosed herein.

[0195] Figure 9 illustrates an example of a NE 900 in accordance with aspects of the present disclosure. The NE 900 may include a processor 902, a memory 904, a controller 906, and a transceiver 908. The processor 902, the memory 904, the controller 906, or the transceiver 908, or various combinations thereof or various components thereof may be examples of means for performing various aspects of the present disclosure as described herein. These components may be coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces.

[0196] The processor 902, the memory 904, the controller 906, or the transceiver 908, or various combinations or components thereof may be implemented in hardware (e.g., circuitry). The hardware may include a processor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), or other programmable logic device, or any combination thereof configured as or otherwise supporting a means for performing the functions described in the present disclosure.

[0197] The processor 902 may include an intelligent hardware device (e.g., a general-purpose processor, a DSP, a CPU, an ASIC, an FPGA, or any combination thereof). In some implementations, the processor 902 may be configured to operate the memory 904. In some other implementations, the memory 904 may be integrated into the processor 902. The processor 902 may be configured to execute computer-readable instructions stored in the memory 904 to cause the NE 900 to perform various functions of the present disclosure.

[0198] The memory 904 may include volatile or non-volatile memory. The memory 904 may store computer-readable, computer-executable code including instructions when executed by the processor 902 cause the NE 900 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as the memory 904 or another type of memory. 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.

[0199] In some implementations, the processor 902 and the memory 904 coupled with the processor 902 may be configured to cause the NE 900 to perform one or more of the functions described herein (e.g., executing, by the processor 902, instructions stored in the memory 904). For example, the processor 902 may support wireless communication at the NE 900 in accordance with examples as disclosed herein. The NE 900 may be configured to support a means for initiating a handover procedure for a UE, determining a security capability of the UE, selecting a target base station based on the security capability of the UE, and transmitting the determined security capability of the UE to the selected target base station.

[0200] As another example, the NE 900 may be configured to support a means for initiating, for a UE, a handover procedure from the base station to a target base station, generating an STC that indicates support of 256-bit security algorithms at the UE, and transmitting the generated STC to an AMF associated with the base station that initiated the handover procedure.

[0201] As another example, the NE 900 may be configured to support a means for receiving, from a source base station during a handover procedure for a UE, an STC that indicates support of 256-bit security algorithms at the UE and transmitting the generated STC to a target base station during the handover procedure.

[0202] As another example, the NE 900 may be configured to support a means for receiving an indication that a UE served by the base station has moved out of an RNA associated with the base station, initiating an RNA update procedure for the UE to a new base station, and transmitting a 256-bit security capability of the UE to the new base station during the initiated RNA update procedure.

[0203] As another example, the NE 900 may be configured to support a means for transmitting a security capability of a UE to a secondary base station, wherein the UE is also connected to the base station, receiving, from the secondary base station, 256-bit ciphering and integrity protection algorithms selected by the secondary base station to apply 256-bit security for the UE, and transmitting the 256-bit ciphering and integrity protection algorithms selected by the secondary base station to the UE.

[0204] The controller 906 may manage input and output signals for the NE 900. The controller 906 may also manage peripherals not integrated into the NE 900. In some implementations, the controller 906 may utilize an operating system such as iOS®, ANDROID®, WINDOWS®, or other operating systems. In some implementations, the controller 906 may be implemented as part of the processor 902.

[0205] In some implementations, the NE 900 may include at least one transceiver 908. In some other implementations, the NE 900 may have more than one transceiver 908. The transceiver 908 may represent a wireless transceiver. The transceiver 908 may include one or more receiver chains 910, one or more transmitter chains 912, or a combination thereof.

[0206] A receiver chain 910 may be configured to receive signals (e.g., control information, data, packets) over a wireless medium. For example, the receiver chain 910 may include one or more antennas for receiving the signal over the air or wireless medium. The receiver chain 910 may include at least one amplifier (e.g., a low-noise amplifier (LNA)) configured to amplify the received signal. The receiver chain 910 may include at least one demodulator configured to demodulate the received signal and obtain the transmitted data by reversing the modulation technique applied during transmission of the signal. The receiver chain 910 may include at least one decoder for decoding and/or processing the demodulated signal to receive the transmitted data.

[0207] A transmitter chain 912 may be configured to generate and transmit signals (e.g., control information, data, packets). The transmitter chain 912 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 transmitter chain 912 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 transmitter chain 912 may also include one or more antennas for transmitting the amplified signal into the air or wireless medium.

[0208] Figure 10 illustrates a flowchart of a method in accordance with aspects of the present disclosure. The operations of the method may be implemented by a NE as described herein. In some implementations, the NE may execute a set of instructions to control the function elements of the NE to perform the described functions.

[0209] At 1002, the method may include initiating a handover procedure for a UE. The operations of 1002 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1002 may be performed by a NE as described with reference to Figure 9.

[0210] At 1004, the method may include determining a security capability of the UE. The operations of 1004 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1004 may be performed by a NE as described with reference to Figure 9.

[0211] At 1006, the method may include selecting a target base station based on the security capability of the UE. The operations of 1006 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1006 may be performed by a NE as described with reference to Figure 9.

[0212] At 1008, the method may include transmitting the determined security capability of the UE to the selected target base station. The operations of 1008 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1006 may be performed by a NE as described with reference to Figure 9.

[0213] It should be noted that the method described herein describes a possible implementation, and that the operations and the steps may be rearranged or otherwise modified and that other implementations are possible.

[0214] Figure 11 illustrates a flowchart of a method in accordance with aspects of the present disclosure. The operations of the method may be implemented by a NE as described herein. In some implementations, the NE may execute a set of instructions to control the function elements of the NE to perform the described functions.

[0215] At 1102, the method may include initiating, for a UE, a handover procedure from the base station to a target base station. The operations of 1102 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1102 may be performed by a NE as described with reference to Figure 9.

[0216] At 1104, the method may include generating an STC that indicates support of 256-bit security algorithms at the UE. The operations of 1104 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1104 may be performed by a NE as described with reference to Figure 9.

[0217] At 1106, the method may include transmitting the generated STC to an AMF associated with the base station that initiated the handover procedure. The operations of 1106 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1106 may be performed by a NE as described with reference to Figure 9.

[0218] It should be noted that the method described herein describes a possible implementation, and that the operations and the steps may be rearranged or otherwise modified and that other implementations are possible.

[0219] Figure 12 illustrates a flowchart of a method in accordance with aspects of the present disclosure. The operations of the method may be implemented by a NE as described herein. In some implementations, the NE may execute a set of instructions to control the function elements of the NE to perform the described functions.

[0220] At 1202, the method may include receiving, from a source base station during a handover procedure for a UE, an STC that indicates support of 256-bit security algorithms at the UE. The operations of 1202 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1202 may be performed by a NE as described with reference to Figure 9.

[0221] At 1204, the method may include transmitting the generated STC to a target base station during the handover procedure. The operations of 1204 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1204 may be performed by a NE as described with reference to Figure 9.

[0222] It should be noted that the method described herein describes a possible implementation, and that the operations and the steps may be rearranged or otherwise modified and that other implementations are possible.

[0223] Figure 13 illustrates a flowchart of a method in accordance with aspects of the present disclosure. The operations of the method may be implemented by a NE as described herein. In some implementations, the NE may execute a set of instructions to control the function elements of the NE to perform the described functions.

[0224] At 1302, the method may include receiving an indication that a UE served by the base station has moved out of an RNA associated with the base station. The operations of 1302 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1302 may be performed by a NE as described with reference to Figure 9.

[0225] At 1304, the method may include initiating an RNA update procedure for the UE to a new base station. The operations of 1304 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1304 may be performed by a NE as described with reference to Figure 9.

[0226] At 1306, the method may include transmitting a 256-bit security capability of the UE to the new base station during the initiated RNA update procedure. The operations of 1306 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1306 may be performed by a NE as described with reference to Figure 9.

[0227] It should be noted that the method described herein describes a possible implementation, and that the operations and the steps may be rearranged or otherwise modified and that other implementations are possible.

[0228] Figure 14 illustrates a flowchart of a method in accordance with aspects of the present disclosure. The operations of the method may be implemented by a NE as described herein. In some implementations, the NE may execute a set of instructions to control the function elements of the NE to perform the described functions.

[0229] At 1402, the method may include transmitting a security capability of a UE to a secondary base station, wherein the UE is also connected to the base station. The operations of 1402 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1402 may be performed by a NE as described with reference to Figure 9.

[0230] At 1404, the method may include receiving, from the secondary base station, 256-bit ciphering and integrity protection algorithms selected by the secondary base station to apply 256-bit security for the UE. The operations of 1404 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1404 may be performed by a NE as described with reference to Figure 9.

[0231] At 1406, the method may include transmitting the 256-bit ciphering and integrity protection algorithms selected by the secondary base station to the UE. The operations of 1406 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 1406 may be performed by a NE as described with reference to Figure 9.

[0232] It should be noted that the method described herein describes a possible implementation, and that the operations and the steps may be rearranged or otherwise modified and that other implementations are possible.

[0233] 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.