

TECHNIQUES FOR ENABLING LEGACY NETWORK ACCESS RESTRICTIONS

TECHNICAL FIELD

[0001] The present disclosure relates to wireless communications, and more specifically to techniques for enabling legacy network access restrictions.

5 BACKGROUND

[0002] 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)).

SUMMARY

[0003] 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.

[0004] Some implementations of the method and apparatuses described herein may receive an indication of a network access restriction enforcement capability of a UE, receive a handover request for the UE, determine network access restriction information for the UE, transmit the network access restriction information to a network entity associated with a different network, and transmit a handover command comprising the network access restriction information to a base station associated with the UE for processing the handover request according to the network access restriction information.

[0005] Some implementations of the method and apparatuses described herein may receive an indication of a network access restriction enforcement capability of a UE from a network entity, receive network access restriction information for the UE from the network entity, and apply at least one network access restriction based on the received indication of the network access restriction enforcement capability of the UE and the received network access restriction information for the UE.

[0006] Some implementations of the method and apparatuses described herein may receive network access restriction information for a UE, store the network access restriction information, and apply at least one network access restriction based on the received network access restriction information for the UE.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Figure 1 illustrates an example of a wireless communications system in accordance with aspects of the present disclosure.

[0008] Figure 2A illustrates a first part of an example procedure flow for handover from 5GS to evolved packet core (EPC) over N26 procedure in accordance with aspects of the present disclosure.

[0009] Figure 2B illustrates a second part of an example procedure flow for handover from 5GS to EPC over N26 procedure in accordance with aspects of the present disclosure.

[0010] Figure 3A illustrates a first part of an example procedure flow for tracking area update mobility from 5G to 4G in accordance with aspects of the present disclosure.

[0011] Figure 3B illustrates a second part of an example procedure flow for tracking area update mobility from 5G to 4G in accordance with aspects of the present disclosure.

[0012] Figure 4A illustrates a first part of an example procedure flow for applying 3G/2G access restriction during 5G Single Radio Voice Call Continuity (SRVCC) from new radio (NR) to Universal Terrestrial Radio Access Network (UTRAN) based on the type of access restriction requirements in accordance with aspects of the present disclosure.

[0013] Figure 4B illustrates a second part of an example procedure flow for applying 3G/2G access restriction during 5G SRVCC from NR to UTRAN based on the type of access restriction requirements in accordance with aspects of the present disclosure.

[0014] Figure 4C illustrates a third part of an example procedure flow for applying 3G/2G access restriction during 5G SRVCC from NR to UTRAN based on the type of access restriction requirements in accordance with aspects of the present disclosure.

[0015] Figure 5 illustrates an example of a UE in accordance with aspects of the present disclosure.

[0016] Figure 6 illustrates an example of a processor in accordance with aspects of the present disclosure.

[0017] Figure 7 illustrates an example of a network equipment (NE) in accordance with aspects of the present disclosure.

[0018] Figure 8 illustrates a flowchart of a method performed by an NE in accordance with aspects of the present disclosure.

[0019] Figure 9 illustrates a flowchart of a method performed by an NE in accordance with aspects of the present disclosure.

[0020] Figure 10 illustrates a flowchart of a method performed by an NE in accordance with aspects of the present disclosure.

DETAILED DESCRIPTION

[0021] In wireless communications, 2G/3G False Base Stations (FBSs) remain a serious security threat to mobile networks. In these generations, critical security features

are missing, for example, mutual authentication, integrity protection, strong security algorithms, etc. If a UE connects to a 2G/3G FBS from 4G or 5G, then it is vulnerable to bidding down attack, e.g., fraudulent SMS or phone call, which could cause significant financial losses for subscribers. If a mobile network operator has decommissioned the 2G/3G network and if the 5G to 4G handover happens, it may further allow different cases of handover from 4G to 3G/2G such as: (i) inter-radio access technology (RAT) handover from 4G to 3G, (ii) inter-RAT handover from 4G to 2G; and (iii) Routing Area Update (RAU) procedure when a UE that is registered with a mobility management entity (MME) (4G) selects a UTRAN (3G) or GSM EDGE Radio Access Network (GERAN) (2G). Currently, if a 2G/3G network is decommissioned and a UE gets a handover from 5G to 4G, to prevent 2G/3G access, there is no way to enforce 4G to 3G/2G handover restrictions.

[0022] There are several existing procedures for UEs connected to 4G/5G to establish a connection with 2G/3G base station. For instance, when the UE is in a CONNECTED state in 4G, it may use an inter-RAT handover procedure (e.g., as specified in 5.5.2 in TS 23.401, incorporated herein by reference) or circuit-switched fallback (CSFB) procedure, which includes redirection from 4G to 2G/3G (e.g., as specified in TS 23.272, incorporated herein by reference) to connect to a 2G/3G base station. When the UE is in an IDLE state in 4G, it may use a RAU procedure (e.g., as specified in 5.3.3.3 or 5.3.3.6 in TS 23.401, incorporated herein by reference) or cell selection once 4G signalling is not available to connect to a 2G/3G base station.

[0023] In another example, when the UE is in a CONNECTED state in 5G, it may use Single Radio Voice Call Continuity (SRVCC) procedure (as in TS 23.216, incorporated herein by reference) to connect to a 3G base station. When the UE is in an IDLE or INACTIVE state in 5G, it may use cell selection once 4G and 5G signaling is not available to connect to a 2G/3G base station.

[0024] It is worth noting that, as mobile network systems continuously evolve and improve, operators periodically shift focus and investment to the newest generation network and decommission older generation networks, which is happening with 2G and 3G networks. In these circumstances, it is no longer appropriate to allow a UE supporting 2G or 3G networks to continue selecting such networks. In fact, due to weaker security measures in these older generation networks, if UEs are deceived into selecting such

networks, then they will be vulnerable to many known attacks pertaining to 2G and 3G, e.g., see 3GPP SP-231789, incorporated herein by reference.

[0025] There are various cases that allow interworking from 4G to 2G/3G e.g., (i) inter-RAT handover can occur from 4G to 3G (e.g., security procedure as specified in 9.2.1 in TS 33.401 (incorporated herein by reference)), (ii) similarly inter-RAT handover from 4G to 2G (e.g., security procedure as specified in 10.3.1 in TS 33.401 (incorporated herein by reference)) can happen and (iii) Routing Area Update procedure takes place when a UE that is registered with an MME (4G) selects a UTRAN (3G) (e.g., as specified in 9.1.1 in TS 33.401 (incorporated herein by reference)) or GERAN (2G) (e.g., as specified in 10.2.1 in TS 33.401 (incorporated herein by reference)).

[0026] One existing solution for preventing bidding down attacks is directed to handover from 5GS to EPS (4G), as described in clause 8.3 of TS 33.501 (incorporated herein by reference). However, the 5GS to EPS handover procedure does not enforce 4G to legacy network (2G/3G i.e., UTRAN/GERAN) access restrictions and so there is a chance that a UE, after handover to 4G, can get further handed over to 2G/3G (e.g., 2G and 3G can be decommissioned networks).

[0027] Another existing solution for preventing bidding down attacks is directed to idle mode mobility from 5GS to EPS over N26, as specified in Clause 8.5 of TS 33.501 (incorporated herein by reference). However, the idle mode mobility from 5GS to EPS related tracking area update (TAU) procedure does not enforce 4G to legacy network (2G/3G i.e., UTRAN/GERAN) access restrictions and so there is a chance that a UE, after handover to 4G, can get further handed over to 2G/3G (e.g., 2G and 3G can be decommissioned networks).

[0028] Another existing solution is directed to a security solution for SRVCC from 5G to 3G, as described in Annex J of TS 33.501 (incorporated herein by reference). However, when the UE is handed over from 5G to 3G in the SRVCC scenario, further bidding down to 2G is not prevented. Further, even if the mobile network operator has decommissioned the 3G and 2G network, the gNB may initiate SRVCC related handover from 5G to 3G for voice continuity, thereby leading to a bidding down attack. Moreover, if the mobile network operator has decommissioned the 3G/2G network, and if 5G signaling is not available (e.g., 5G signals blocked by an attacker), 2G/3G cell selection

may occur, which causes the UE to connect to a 2G/3G network, resulting in a successful bidding down attack.

[0029] Solutions to the foregoing problems and limitations of exiting solutions are described below with reference to the figures. Aspects of the present disclosure are described in the context of a wireless communications system.

[0030] 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.

[0031] 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.

[0032] 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 112 associated with the same
5 or different radio access technologies may overlap, but the different geographic coverage areas may be associated with different NE 102.

[0033] 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,
10 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.

15 [0034] 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,
20 the communication link 114 may be referred to as a sidelink. For example, a UE 104 may support wireless communication directly with another UE 104 over a PC5 interface.

[0035] 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, N2, or network interface). In some
25 implementations, the NE 102 may communicate with each other directly. In some other implementations, the NE 102 may communicate with each other or 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
30 other access network transmission entities, which may be referred to as a radio heads, smart radio heads, or TRPs.

[0036] 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.

[0037] The CN 106 may communicate with a packet data network over one or more backhaul links (e.g., via an S1, N2, N2, 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).

[0038] 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.

[0039] One or more numerologies may be supported in the wireless communications system 100, and a numerology may include a subcarrier spacing and a cyclic prefix. A first numerology (e.g., $\mu=0$) may be associated with a first subcarrier spacing (e.g., 15 kHz) and a normal cyclic prefix. In some implementations, the first numerology (e.g., $\mu=0$) associated with the first subcarrier spacing (e.g., 15 kHz) may utilize one slot per subframe. A second numerology (e.g., $\mu=1$) may be associated with a second subcarrier spacing (e.g., 30 kHz) and a normal cyclic prefix. A third numerology (e.g., $\mu=2$) may be associated with a third subcarrier spacing (e.g., 60 kHz) and a normal cyclic prefix or an extended cyclic prefix. A fourth numerology (e.g., $\mu=3$) may be associated with a fourth subcarrier spacing (e.g., 120 kHz) and a normal cyclic prefix. A fifth numerology (e.g., $\mu=4$) may be associated with a fifth subcarrier spacing (e.g., 240 kHz) and a normal cyclic prefix.

[0040] 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.

[0041] Additionally or alternatively, a time interval of a resource (e.g., a communication resource) may be organized according to slots. For example, a subframe may include a number (e.g., quantity) of slots. The number of slots in each subframe may also depend on the one or more numerologies supported in the wireless communications system 100. For instance, the first, second, third, fourth, and fifth numerologies (i.e., $\mu=0$, $\mu=1$, $\mu=2$, $\mu=3$, $\mu=4$) associated with respective subcarrier spacings of 15 kHz, 30 kHz, 60 kHz, 120 kHz, and 240 kHz may utilize a single slot per subframe, two slots per subframe, four slots per subframe, eight slots per subframe, and 16 slots per subframe, respectively. Each slot may include a number (e.g., quantity) of symbols (e.g., OFDM symbols). In some implementations, the number (e.g., quantity) of slots for a subframe may depend on a numerology. For a normal cyclic prefix, a slot may include 14 symbols. For an extended cyclic prefix (e.g., applicable for 60 kHz subcarrier spacing), a slot may include 12 symbols. The relationship between the number of symbols per slot, the number of slots per subframe, and the number of slots per frame for a normal cyclic prefix and an

extended cyclic prefix may depend on a numerology. It should be understood that reference to a first numerology (e.g., $\mu=0$) associated with a first subcarrier spacing (e.g., 15 kHz) may be used interchangeably between subframes and slots.

[0042] 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.

[0043] FR1 may be associated with one or multiple numerologies (e.g., at least three numerologies). For example, FR1 may be associated with a first numerology (e.g., $\mu=0$), which includes 15 kHz subcarrier spacing; a second numerology (e.g., $\mu=1$), which includes 30 kHz subcarrier spacing; and a third numerology (e.g., $\mu=2$), which includes 60 kHz subcarrier spacing. FR2 may be associated with one or multiple numerologies (e.g., at least 2 numerologies). For example, FR2 may be associated with a third numerology (e.g., $\mu=2$), which includes 60 kHz subcarrier spacing; and a fourth numerology (e.g., $\mu=3$), which includes 120 kHz subcarrier spacing.

[0044] The solutions discussed herein relate to techniques for preventing bidding down attacks. In general, the subject matter disclosed herein describes features to provide the UTRAN (3G) and GERAN (2G) access restriction information from the AMF (in 5G system) to the MME (in 4G system) to avoid any further handover initiation from 4G to UTRAN (i.e., 3G network) and/or GERAN (i.e., 2G network). For the case of decommissioned 2G and/or 3G networks, the embodiments further describe determining, based on the UTRAN and GERAN access restriction information available in 5G and provided to MME in 4G, to make the MME defer from SRVCC handover to 3G for UE and to make the MME perform S1 handover.

[0045] For the case where only the 2G network is decommissioned, 5G NR provides GERAN access/handover restriction to UTRAN (e.g., via E-UTRAN i.e., 4G) to further avoid a handover initiation to GERAN (2G network) during SRVCC from 5G to 3G. Further embodiments describe the novel feature of providing the UTRAN (3G) and
5 GERAN (2G) access restriction information from the AMF (in 5G system) to the MME (in 4G system) in context response during a TAU procedure to prevent further handover of the UE to 3G/2G systems.

[0046] A first embodiment is directed to provisioning and enforcing UTRAN and GERAN access, handover, and/or mobility restrictions during 5GS to EPC over N26. IN
10 one embodiment, the mobile network operator may have decommissioned 2G and 3G networks, and it may not be desirable to allow UE connections in 5G to fall back/handover to a 2G/3G network connection. This embodiment describes how the UTRAN and GERAN access restriction information can be provided from the AMF (in 5G system) to the MME (in 4G LTE system) to prevent any further handover of the UE from E-UTRAN
15 (4G) to UTRAN/GERAN (3G/2G) network, as shown in Figures 2A – 2B. The UTRAN and GERAN access restriction information received at the MME may be stored locally in the MME and in the eNB to further enforce the related access restrictions (e.g., to determine not to initiate/allow handover or relocation from 4G E-UTRAN to a UTRAN or GERAN accordingly).

[0047] Figures 2A – 2B illustrate an example procedure flow for handover from 5GS to EPC over N26 procedure in accordance with aspects of the present disclosure. In such an embodiment, if the UE is initially registered and connected to the 5GC, the 5GC has a current security context for the UE. The current 5G security context may be a mapped 5G security context resulting from a previous mobility from EPC, or a native 5G security
25 context resulting from a primary authentication with the 5GC.

[0048] At 1a (see messaging 202), in one embodiment, the UE 201 sends an initial NAS message that includes an indication of the UE's capabilities to support GERAN and UTRAN access restrictions. In one embodiment, the UE 201 sends an initial NAS message that includes an information element (IE) that indicates support of network
30 access restriction enforcement capability. The network access restriction enforcement capability(ies) IE may contain information to indicate support of GERAN and UTRAN access restrictions.

[0049] In one embodiment, the initial NAS message to the AMF 207 in 1a may be an initial registration request message, a mobility registration update request message, or a service request message. In one embodiment, the network may initiate and run primary authentication with the UE 201 to perform mutual authentication (e.g., using EAP-AKA',
5 5G AKA, or another EAP method) (see messaging 204).

[0050] In one embodiment, if the AMF 207 is not configured with the network access restriction information, the AMF 207 may fetch subscription data from the UDM by sending a *Nudm_SubscriberDataManagement* (SDM) get request or using a *Nudm* service operation message with subscription permanent identifier (SUPI) and network
10 access restriction enforcement capability (if received in 1a).

[0051] In one embodiment, based on operator's local policy (or if the 2G/3G networks are decommissioned), the UDM/UDR manages GERAN and UTRAN access restrictions as part of the network access restriction requirements for the UE(s) in the subscription data (e.g., as part of UE access and mobility context). The UDM sends a *Nudm_SDM_Get*
15 *Response* message, which includes the network access restriction information (UTRAN access restricted/not allowed, GERAN access restricted/not allowed) along with the other subscription data.

[0052] In one embodiment, based on an operator local policy, the AMF 207 is configured with the network access restriction information. In one embodiment, the AMF
20 207 locally stores the UE's support of network access restriction enforcement capability (received in 1a) along with the network access restriction information (fetched from the UDM or locally configured in the AMF 207), in the UE context. In one embodiment, the UE 201 is connected to the network and may consume services. At a later time, a handover may be initiated by the gNB/ng-eNB 203 (e.g., due to UE mobility or signal weakness)
25 (see block 206).

[0053] At 1b (see messaging 208), in one embodiment, the gNB/ng-eNB 203 sends a Handover Required message to the AMF 207, including the UE's identity.

[0054] At 2 (see block 210), in one embodiment, when the source AMF 207 performs a handover procedure to the EPC, after checking the UE's access rights and security
30 capabilities, the source AMF 207 prepares a UE context including a mapped EPS security context for the target MME 209 and the network access restriction information (UTRAN access restricted, GERAN access restricted). To construct the mapped EPS security

context, the source AMF 207 may derive a K'_{ASME} using the K_{AMF} key and the current downlink 5G NAS COUNT of the current 5G security context, e.g., as described in clause 8.6.1 in TS 33.501 (incorporated herein by reference) and then increments its stored downlink 5G NAS COUNT value by one.

5 [0055] In one embodiment, the source AMF 207 selects the EPS NAS algorithms identifiers (e.g., it has stored) to be used in the target MME 209 at interworking handover to EPS, e.g., for encryption and integrity protection. In one embodiment, a legacy target MME 209 is expecting to receive the selected EPS NAS algorithms identifiers over N26 from the source AMF 207 as the target MME 209 believes the source AMF 207 is another
10 MME 209. The source AMF 207 has therefore provisioned the EPS NAS security algorithms identifiers to be used at interworking handover to EPS to the UE 201 in the 5G NAS security mode command (SMC) in 5G access, e.g., as described in clause 6.7.2 (incorporated herein by reference). The target MME 209 could re-select different EPS NAS algorithms thought to be used with the UE 201 by running a NAS SMC in the
15 following Tracking Area Update (TAU) procedure.

[0056] In one embodiment, the uplink and downlink EPS NAS COUNT associated with the newly derived $K_{ASME'}$ key are set. The eKSI for the newly derived $K_{ASME'}$ key may be defined as described in clause 8.6.1 TS 33.501 (incorporated herein by reference).

[0057] In one embodiment, the source AMF 207 may also derive the initial K_{eNB} key
20 from the $K_{ASME'}$ key and the uplink NAS COUNT, e.g., as specified in Annex A.3 of TS 33.401 (incorporated by reference), using $2^{32}-1$ as the value of the uplink NAS COUNT parameter.

[0058] In one embodiment, the source AMF 207 and the UE 201 uses $2^{32}-1$ as the value of the uplink NAS COUNT for the purpose of deriving K_{eNB} and do not set the
25 uplink NAS COUNT to $2^{32}-1$. The reason for choosing such a value not in the normal NAS COUNT range, e.g., $[0, 2^{24}-1]$ may be to avoid any possibility that the value may be used to derive the same K_{eNB} again.

[0059] In one embodiment, the source AMF 207 subsequently derives NH two times, e.g., as specified in clause A.4 of TS 33.401 (incorporated herein by reference). The {NH,
30 NCC=2} pair is provided to the target MME 209 as a part of UE security context in the Forward Relocation Request message.

[0060] At 3a (see messaging 212), in one embodiment, the source AMF 207 transfers the UE security context (including new K_{ASME}' , eKSI, uplink and downlink EPS NAS COUNT's, UE EPS security capabilities, UE's support of network access restriction enforcement capability, and/or selected EPS NAS algorithms identifiers), network access
5 restriction information (UTRAN access restricted, GERAN access restricted) to the target MME 209 in the Forward Relocation Request message. In one embodiment, the UE NR security capabilities may be sent by the source AMF 207.

[0061] At 3b (see block 214), in one embodiment, the target MME 209 stores the network access restriction information (UTRAN access restricted/not allowed, GERAN
10 access restricted/not allowed) and the UE's support of network access restriction enforcement capability as part of the UE context (if received from the AMF 207 in 3a).

[0062] In one embodiment, based on the received network access restriction information (UTRAN access restricted, GERAN access restricted) and the network access restriction enforcement capability (in 3a), the MME 209 performs an action including not
15 initiating an inter-RAT handover to UTRAN/GERAN, not initiating or forwarding relocation requests related to SRVCC specific handover from 5G/4G to 3G or 2G, and provisioning the network access restriction information (UTRAN access restricted/not allowed, GERAN access restricted/not allowed) to the eNB 205 and the UE 201 to enforce the UTRAN and GERAN access restrictions for the UE 201 at the eNB 205 and the UE
20 201.

[0063] In one embodiment, at 4a (see messaging 216), when the target MME 209 receives a Forward Relocation Request message from source AMF 207, then the target MME 209 derives EPS NAS keys (e.g., K_{NASenc} and K_{NASint}) from the received K_{ASME}' key with the received EPS NAS security algorithm identifiers as input, to be used in EPC,
25 e.g., as described in Annex A.7 in TS 33.401 (incorporated herein by reference). In such an embodiment, the target MME 209 includes the {NH, NCC=2} pair, the UE security capabilities, network access restriction information (UTRAN access restricted/not allowed, GERAN access restricted/not allowed) in the S1 HANDOVER REQUEST message to the target eNB 205. The UE security capabilities may include the UE EPS
30 security capabilities received from the source AMF 207 and/or the UE's support of network access restriction enforcement.

[0064] At 4b (see block 218), in one embodiment, upon receipt of the S1 HANDOVER REQUEST from the target MME 209, the eNB 205 stores the network access restriction information (UTRAN access restricted/not allowed, GERAN access restricted/not allowed), and UE's support of network access restriction enforcement capability (if received in the S1 HANDOVER REQUEST), along with the UE context. Further, in one embodiment, based on the received network access restriction information (UTRAN access restricted/not allowed, GERAN access restricted/not allowed), and the UE's support of network access restriction enforcement capability, the eNB 205 performs an action including not initiating a inter-RAT handover to UTRAN/GERAN, not initiating SRVCC from 5G/4G to 3G or 2G, and provisioning the network access restriction information (UTRAN access restricted/not allowed, GERAN access restricted/not allowed) to the UE.

[0065] At 5 (see messaging 220 in Figure 2B), in one embodiment, upon receipt of the S1 HANDOVER REQUEST from the target MME 209, the target eNB 205 selects AS security algorithms from the UE EPS security capabilities, e.g., as described in clause 7.2.4.2.3 in TS 33.401 (incorporated herein by reference) and computes the KeNB to be used with the UE 201 and proceed, e.g., as described in clause 7.2.8.4.3 in TS 33.401 (incorporated herein by reference). The target eNB 205 then sends the selected AS security algorithms in the target to source transparent container in the S1 Handover Request Ack Message to the target MME 209.

[0066] At 6 (see messaging 222), in one embodiment, the target MME 209 shall include the target to source transparent container received from the target eNB 205 in the Forward Relocation Response message sent to the source AMF 207.

[0067] At 7 (see messaging 224), in one embodiment, the source AMF 207 includes the target to source transparent container, network access restriction information (UTRAN access restricted, GERAN access restricted) (if network access restriction information is available for the UE 201), and the 8 least significant bits (LSB) of the downlink NAS COUNT value used in K_{ASME} derivation in 2, in the Handover command sent to the source gNB/ng-eNB 203.

[0068] At 8 (see messaging 226), in one embodiment, the source gNB/ng-eNB 203 includes the target to source transparent container, network access restriction information

(UTRAN access restricted/not allowed, GERAN access restricted/not allowed) and the 8 LSB of the downlink NAS COUNT value in the Handover command sent to the UE 201.

[0069] In one embodiment, the gNB/ng-eNB 203 stores the network access restriction information (UTRAN access restricted, GERAN access restricted), if received from the AMF 207, as part of the UE context, along with 5G-global unique temporary identifier (GUTI), radio network temporary identifier (RNTI), and temporary mobile subscriber identity (TMSI). Further, based on the received network access restriction information, the RAN performs an action including not initiating an inter-RAT handover to UTRAN/GERAN and not initiating SRVCC from 4G to 3G or 2G.

[0070] In one embodiment, upon the reception of the Handover Command message, the UE 201 estimates the downlink NAS COUNT value using the received 8 LSB of the downlink NAS COUNT value and its stored downlink NAS COUNT value. The UE 201 shall ensure that the estimated downlink NAS COUNT value is greater than the stored downlink NAS COUNT value. Then, the UE 201 may derive the mapped EPS security context, e.g., derive K_{ASME}' from K_{AMF} e.g., as described in clause 8.6.1 of TS 33.501 (incorporated herein by reference) using the estimated downlink 5G NAS COUNT value. After the derivation, the UE 201 may set the downlink NAS COUNT value in the 5G NAS security context to the received downlink NAS COUNT value.

[0071] At 9a (see block 228), in one embodiment, the eKSI for the newly derived K_{ASME}' key is defined, e.g., as described in clause 8.6.1 TS 33.501 (incorporated herein by reference). The UE 201 may also derive the EPS NAS keys (e.g., K_{NASenc} and K_{NASint}) as the MME 209 did in 4a using the EPS NAS security algorithms identifiers stored in the UE 201 and provisioned by the AMF 207 to the UE 201 in 5G NAS SMC in earlier 5G access. The UE 201 may also derive the initial K_{eNB} from the K_{ASME}' and the uplink NAS COUNT, e.g., as specified in Annex A.3 of TS 33.401 (incorporated herein by reference) using $2^{32}-1$ as the value of the uplink NAS COUNT parameter.

[0072] In one embodiment, the UE 201 may also derive the $\{NH, NCC=2\}$ pair, e.g., as described in A.4 of TS 33.401 (incorporated herein by reference) and further derive the K_{eNB} to be used with the UE 201 by performing the key derivation, e.g., defined in Annex A.5 in TS 33.401 (incorporated herein by reference). The UE 201 may derive the AS radio resource control (RRC) keys and the AS UP keys based on the K_{eNB} and the received AS EPS security algorithms identifiers selected by the target eNB 205, e.g., as

described in Annex A.7 in TS 33.401 (incorporated herein by reference). The uplink and downlink EPS NAS COUNT associated with the derived EPS NAS keys may be set to the values, e.g., as described in clause 8.6.1 (incorporated herein by reference). The UE 201 may immediately take into use the newly created mapped EPS security context, both
5 for NAS and AS communication.

[0073] At 9b (see block 230), in one embodiment, the UE 201 stores the network access restriction information (UTRAN access restricted/not allowed, GERAN access restricted/not allowed) if received in the handover command and determines not to select UTRAN access (3G) or GERAN access (2G), e.g., even if the 5G signal or 4G signal is
10 not available and the UE 201 waits until the 5G/4G signal is available to prevent a bidding down attack. In one embodiment, specific in this handover scenario, the UE 201 connects to 4G e.g., LTE/E-UTRAN.

[0074] At 10 (see messaging 232), in one embodiment, the UE 201 sends the Handover Complete message to the target eNB 205. The UE 201 may cipher and integrity
15 protect this message using the newly created mapped EPS security context.

[0075] At 11 (see messaging 234), in one embodiment, the target eNB 205 notifies the target MME 209 with a Handover Notify message.

[0076] In one embodiment, after successful completion of the handover procedure, the UE 201 deletes any mapped 5G security context. In further embodiments, after
20 deleting the mapped 5G security context, if the UE 201 has a full non-current native 5G NAS security context, then the UE 201 makes the non-current native 5G NAS security context the current one.

[0077] A second embodiment is directed to provisioning and enforcing UTRAN and GERAN access, handover, and/or mobility restrictions during Idle mode mobility from
25 5G to 4G. As shown in Figures 3A-3B, UTRAN and GERAN access restriction information can be provided from the AMF 307 in the 5G system to the MME 305 in the 4G/LTE system during the tracking area update when the UE 301 is in Idle mode mobility from 5G to 4G system to prevent further handover of the UE 301 from E-UTRAN (4G) to UTRAN/GERAN (3G/2G) network. The UTRAN and GERAN access restriction
30 information received at the MME 305 can be stored locally in MME 305 and in the eNB 303 to further enforce the related access restrictions (e.g., to determine not to

initiate/allow handover or relocation from 4G E-UTRAN to an UTRAN or GERAN accordingly).

[0078] Figures 3A – 3B illustrate an example procedure flow for TAU e.g., Idle mode mobility from 5G to 4G in accordance with aspects of the present disclosure. In one embodiment, the UE 301 performs either TAU or Initial Attach procedure in this scenario.

[0079] At 1 (see messaging 302), in one embodiment, the UE 301 initiates the TAU procedure by sending a TAU Request to the MME 305 with a mapped EPS GUTI derived from the 5G GUTI, its EPS security capabilities, and an indication of the UE's capabilities to support GERAN and UTRAN access restrictions. The mapped EPS GUTI contains the information of the AMF 307 that has the latest UE context in the 5G network.

[0080] In one embodiment, the UE 301 sends an initial NAS message that includes an information element (IE) that indicates support of network access restriction enforcement capability. The network access restriction enforcement capability(ies) IE may contain information to indicate support of GERAN and UTRAN access restrictions.

[0081] In one embodiment, the UE 301 integrity protects the TAU Request message using the current 5G NAS security context identified by the 5G GUTI used to derive the mapped EPS GUTI. More precisely, the UE 301 shall compute the NAS medium access control (MAC) for the TAU request as it is done for a 5G NAS message over a 3GPP access. The NAS Uplink COUNT for integrity protection of the TAU request shall use the same value as the 5G NAS Uplink COUNT. Consequently, this results in an increase of the stored NAS Uplink COUNT value in the NAS COUNT pair associated with the 3GPP access. The corresponding ngKSI value of the 5G Security context is included in the eKSI parameter of the TAU Request message.

[0082] At 2 (see block 304), in one embodiment, upon receipt of the TAU Request, the MME 305 obtains the AMF address from the mapped EPS GUTI value.

[0083] At 3 (see messaging 306), in one embodiment, the MME 305 forwards the complete TAU Request message including the eKSI, NAS-MAC, mapped EPS GUTI, and the UE's support of network access restriction enforcement capability in the Context Request message.

[0084] At 4 (see block 308), in one embodiment, the AMF 307 uses the eKSI value field to identify the 5G NAS security context and use it to verify the TAU Request

message as if it was a 5G NAS message received over 3GPP access. The AMF 307 further checks if there is any UTRAN and GERAN network access restriction information available (locally or in the UDM) for the UE in the UE context. If available, the AMF 307 fetches the UTRAN and GERAN access restriction information (e.g., GERAN not
5 allowed/restricted, UTRAN not allowed/restricted).

[0085] At 5 (see messaging 310), in one embodiment, if the verification is successful, the AMF 307 shall derive a mapped EPS NAS security context, e.g., as described in clause 8.6.1 TS 33.501 (incorporated herein by reference). The AMF 307 shall set the EPS NAS algorithms to the algorithms indicated earlier to the UE 301 in a NAS SMC as described
10 in clause 6.7.2 (incorporated herein by reference).

[0086] In one embodiment, the AMF 307 includes the mapped EPS NAS security context and the UTRAN and GERAN access not allowed indications in the Context Response message and sends it to the MME 305. In one embodiment, the AMF 307 shall never transfer 5G security parameters to an entity outside the 5G system.

15 [0087] At 6 (see block 312), in one embodiment, the UE 301 derives a mapped EPS NAS security context, e.g., as described in clause 8.6.1 TS 33.501 (incorporated herein by reference). The UE 301 shall select the EPS algorithms using the ones received in an earlier NAS SMC from the AMF 307, e.g., as described in clause 6.7.2 TS 33.501 (incorporated herein by reference). The UE 301 shall immediately activate the mapped
20 EPS security context and be ready to use it for the processing of the TAU Accept message in 7.

[0088] At 7a (see block 314), in one embodiment, the MME 305 compares the UE security algorithms to its configured list after it receives the Context Response message. If an algorithm change is required, the MME 305 selects the NAS algorithm that has the
25 highest priority from its configured list and is also present in the UE 5G security capabilities and initiates an NAS SMC to the UE 301. Otherwise, 8-10 shall be skipped.

[0089] At 7b (see block 316), in one embodiment, the MME 305 stores the network access restriction information (e.g., GERAN not allowed/restricted, UTRAN not allowed/restricted) received in 5 and the UE's support of network access restriction
30 enforcement capability as part of the UE context (if received from the AMF 307 in 1).

[0090] Further, in one embodiment, based on the received network access restriction information (e.g., GERAN not allowed/restricted, UTRAN not allowed/restricted), and the network access restriction enforcement capability, the MME 305 performs an action including not initiating an inter-RAT handover to UTRAN/GERAN, not initiating or
5 forwarding relocation requests related to an SRVCC-specific handover from 5G/4G to 3G or 2G, and provisioning the network access restriction information (GERAN not allowed/restricted, UTRAN not allowed/restricted) to the eNB 303, and the UE 301 to enforce the UTRAN and GERAN access restrictions for the UE 301 at the eNB 303 and UE 301.

10 [0091] At 8 (see messaging 318), in one embodiment, the MME 305 and the UE 301 perform a NAS SMC to derive new NAS keys with the new algorithms, e.g., as described in Clause 7.2.8.1.2 of TS 33.401 (incorporated herein by reference). The MME 305 sends, to the UE 301, the UE's support of network access restriction enforcement capability (received in 1) and UTRAN and GERAN access/handover restriction information e.g.,
15 UTRAN access restricted/not allowed, GERAN access restricted/not allowed indications) (based on UTRAN and GERAN access restriction information received from the AMF 307 in 5 and stored in 7b) in the NAS SMC message.

[0092] At 9 (see block 320), in one embodiment, the UE 301 derives a new NAS key from a selected algorithm in NAS SMC. The UE 301 verifies the NAS SMC message
20 using the NAS keys (for integrity verification).

[0093] At 10a (see messaging 322), in one embodiment, following a successful verification, the UE 301 sends the NAS security mode complete message to the MME 305.

[0094] At 10b (see block 324), in one embodiment, the UE 301 stores the network
25 access restriction information (UTRAN access restricted/not allowed, GERAN access restricted/not allowed), if received in the NAS SMC message, and determines not to select UTRAN access (3G) or GERAN access (2G), e.g., even if the 5G signal or 4G signal is not available and the UE 201 waits until the 5G/4G signal is available to prevent a bidding down attack. In one embodiment, specific in this handover scenario, the UE 201 connects
30 to 4G e.g., LTE/E-UTRAN.

[0095] At 11 (see messaging 326), in one embodiment, the MME 305 completes the procedure with a TAU Accept message. In one embodiment, the MME 305 may send the

network access restriction information (UTRAN access restricted/not allowed, GERAN access restricted/not allowed) to the UE 301 in a TAU accept message in 11 instead of in 8. The UE 301 may then store the network access restriction information (UTRAN access restricted/not allowed, GERAN access restricted/not allowed) if it is received in a TAU
5 accept message and determines not to select UTRAN access (3G) or GERAN access (2G), e.g., even if the 5G signal or 4G signal is not available and the UE 201 waits until the 5G/4G signal is available to prevent a bidding down attack. In one embodiment, specific in this handover scenario, the UE 201 connects to 4G e.g., LTE/E-UTRAN.

[0096] At 12a (see messaging 328), in one embodiment, the MME 305 sends the
10 network access restriction information (UTRAN access restricted/not allowed, GERAN access restricted/not allowed) to the eNB 303, if network access restriction information is available for the UE 301, in an S1 message.

[0097] At 12b (see block 330), in one embodiment, the eNB 303 stores the network access restriction information (UTRAN access restricted, GERAN access restricted), if it
15 is received from the MME 305, as part of the UE context along with GUTI, RNTI, and/or TMSI. Further, based on the received network access restriction information, the RAN determines to perform an action including initiating an inter-RAT handover to UTRAN/GERAN and not initiating SRVCC from 4G to 3G or 2G.

[0098] In one embodiment, after successful completion of the TAU procedure, the
20 UE 301 deletes any mapped 5G security context. After deleting the mapped 5G security context, if the UE 301 has a full non-current native 5G NAS security context, then the UE 301 makes the non-current native 5G NAS security context the current one.

[0099] A third embodiment is directed to applying UTRAN and/or GERAN access, handover, and/or mobility restrictions during SRVCC from NR considering the type of
25 access (3G and/or 2G) restrictions enforced.

[0100] In this embodiment, the AMF in 5GS can provide UTRAN and/or GERAN access restrictions information to the MME during the 5G SRVCC, to allow the MME to determine and apply either a suitable GERAN access restriction (or) both GERAN and UTRAN access restrictions while enabling an allowed handover (e.g., preventing
30 restricting handover and to establish only allowed handover for the UE).

[0101] There are two main 5G SRVCC scenarios addressed by this embodiment. The first is where 2G network is decommissioned. If a mobile network operator decommissioned only 2G network, then following a relocation request (with GERAN access restriction information) received from AMF, the MME determines to continue
5 with SRVCC to 3G e.g., UTRAN, but MME provides the GERAN access restriction information to the UTRAN so that further handover of UE to a GERAN can be prevented in the UTRAN.

[0102] The second scenario is where 2G and 3G network is decommissioned. If a mobile network operator decommissioned both 2G network and 3G network, then
10 following a relocation request (with UTRAN access restrictions and GERAN access restriction information) received from AMF, the MME determines not to initiate SRVCC to 3G/2G e.g., UTRAN/GERAN to prevent any handover to 3G/2G. Instead, the MME determines to initiate S1 handover to enable the UE to handover to the 4G network.

[0103] Figures 4A-4C illustrate an example procedure flow for applying 3G/2G
15 access restriction during 5G SRVCC from NR to E-UTRAN or UTRAN based on the type of access (3G and/or 2G) restriction requirements/enforced in accordance with aspects of the present disclosure. If the UE is initially registered and connected to the 5GC, the 5GC has a current security context for the UE. The current 5G security context may be a mapped 5G security context resulting from a previous mobility from EPC, or a
20 native 5G security context resulting from a primary authentication with the 5GC.

[0104] At 1a (see messaging 402), in one embodiment, the UE 401 sends an initial NAS message that includes an indication of the UE's capabilities to support GERAN and UTRAN access restrictions. In one embodiment, the UE 401 sends an initial NAS message that includes an information element (IE) that indicates support of network
25 access restriction enforcement capability. The network access restriction enforcement capability(ies) IE may contain information to indicate support of GERAN and UTRAN access restrictions.

[0105] In one embodiment, the initial NAS message to the AMF 407 in 1a may be an initial registration request message, a mobility registration update request message, or a
30 service request message. In one embodiment, the network may initiate and run primary authentication with the UE 401 to perform mutual authentication (e.g., using EAP-AKA', 5G AKA, or another EAP method) (see messaging 404).

[0106] In one embodiment, if the AMF 407 is not configured with the network access restriction information, the AMF 407 may fetch subscription data from the UDM by sending a *Nudm_SubscriberDataManagement* (SDM) get request or using a *Nudm* service operation message with subscription permanent identifier (SUPI) and network access restriction enforcement capability (if received in 1a).

[0107] In one embodiment, based on operator's local policy (or if the 2G/3G networks are decommissioned), the UDM/UDR manages GERAN and UTRAN access restrictions as part of the network access restriction requirements for the UE(s) in the subscription data (e.g., as part of UE access and mobility context). The UDM sends a *Nudm_SDM_Get Response* message, which includes the network access restriction information (UTRAN access restricted/not allowed, GERAN access restricted/not allowed) along with the other subscription data.

[0108] In one embodiment, based on an operator local policy, the AMF 207 is configured with the network access restriction information. In one embodiment, the AMF 407 locally stores the UE's support of network access restriction enforcement capability (received in 1a) along with the network access restriction information (fetched from the UDM or locally configured in the AMF 407), in the UE context. In one embodiment, the UE 401 is connected to the network and may consume services. At a later time, a handover may be initiated by the gNB/eNB 403, 405 (e.g., due to UE mobility or signal weakness).

[0109] At 1b (see messaging 406), in one embodiment, the gNB/eNB 403, 405 sends a Handover Required message to the AMF 407, including the UE's identity.

[0110] At 2 (see block 408), in one embodiment, the AMF 407 derives a new K_{ASME_SRVCC} key using the K_{AMF} key and the current downlink 5G NAS COUNT of the current 5G security context, e.g., as described in clause A.21 of TS 33.501 (incorporated herein by reference). The AMF 407 increases the downlink 5G NAS COUNT by one.

[0111] In one embodiment, the AMF 407 stores and manages the UE's support of network access restriction enforcement capability (received in 1a) along with the network access restriction information (fetched from UDM or locally configured in AMF), in the UE context as described in 1a. Further, if the AMF 407 has the network access restriction information (GERAN access restrictions and/or UTRAN access restrictions) for the UE 401, the AMF 407 provides the network access restriction information to the MME_SRVCC 409 to prevent subsequent handovers/mobility to the 3G or 2G network

as indicated in the network access restriction information. In one embodiment, a GERAN access restriction can indicate a GERAN access not allowed/restricted and a UTRAN access restrictions can indicate a UTRAN access not allowed/restricted.

[0112] At 3a (see messaging 410), in one embodiment, the AMF 407 assigns the value of ngKSI to the eKSI (maps ngKSI to eKSI) and transfers the new K_{ASME_SRVCC} key, UE's support of network access restriction enforcement capability, network access restriction information e.g., UTRAN access not allowed indication/restricted (if available/configured) and/or GERAN access not allowed indication/restricted (if available/ configured), and the UE security capability to the MME_SRVCC 409 via forward relocation request message.

[0113] At 3b (see block 412), in one embodiment, the MME_SRVCC 409 determines if SRVCC is allowed to the 3G/2G based on the received network access restriction information e.g., UTRAN access not allowed/restricted and/or GERAN access not allowed/restricted.

[0114] In case 1 (shown in Figure 4B), an operator may have decommissioned the 2G network and so 3b may include an indication that GERAN is not allowed/restricted. If the MME_SRVCC 409 received a GERAN access not allowed indication, then the MME_SRVCC 409 performs SRVCC to 3G e.g., UTRAN, if needed, and performs 4 to 10b.

[0115] At 4 (see block 414), in one embodiment, the MME_SRVCC 409 derives the CK_{SRVCC} , IK_{SRVCC} based on the new K_{ASME_SRVCC} key, e.g., as in clause A.12 in TS 33.401 (incorporated herein by reference) using a downlink NAS COUNT of zero.

[0116] At 5 (see messaging 416), in one embodiment, the MME_SRVCC assigns the value of eKSI to KSI_{SRVCC} (maps eKSI to KSI_{SRVCC}) and transfers CK_{SRVCC} , IK_{SRVCC} with KSI_{SRVCC} , the UE security capability, UE's support of network access restriction enforcement capability and the GERAN access not allowed/restricted indication to the mobile switching center (MSC) server 411 in packet switched (PS) to circuit switched (CS) handover (HO) request message.

[0117] At 6a (see block 418), in one embodiment, if the MSC server 411 receives the network access restriction information (e.g., GERAN access not allowed/restricted indication) from the MME_SRVCC 409, the MSC server 411 stores the network access

restriction information as part of the UE context. Further based on the received network access restriction information, the MSC server 411 performs an action such as not initiating an inter-RAT handover to GERAN and/or not initiating SRVCC related handover to 2G.

5 [0118] At 6b (see messaging 420), in one embodiment, the MSC server 411 sends the PS to CS HO response message to the MME_SRVCC 409.

[0119] At 7 (see messaging 422), in one embodiment, the MME_SRVCC 409 sends the forward relocation response message to the AMF 407.

10 [0120] At 8 (see messaging 424), in one embodiment, the AMF 407 sends the HO command to the gNB 403, in which the AMF 407 includes the 4 LSBs of the downlink NAS COUNT used to calculate K_{ASME_SRVCC} , GERAN access restriction information (e.g., GERAN access not allowed/restricted indication).

15 [0121] At 9 (see messaging 426), in one embodiment, the gNB 403 sends the HO command to the UE 401, in which the gNB 403 includes the 4 LSB of the downlink NAS COUNT and GERAN access restriction information (e.g., GERAN access not allowed/restricted indication) received from the AMF 407.

20 [0122] In one embodiment, if the gNB 403/eNB 405 receives the network access restriction information (GERAN access not allowed/restricted indication) from the AMF 407, the gNB 403/eNB 405 stores the network access restriction information as part of the UE context along with 5G-GUTI, RNTI, and TMSI. Further, based on the received network access restriction information, the RAN performs an action including not initiating an inter-RAT handover to GERAN and not initiating SRVCC from 5G to 2G.

25 [0123] At 10a (see block 428), in one embodiment, when the UE 401 receives the message, the UE 401 derives the new K_{ASME_SRVCC} key, e.g., as described in Annex A.21 of TS 33.501 (incorporated herein by reference) using the K_{AMF} key and the downlink 5G NAS COUNT estimated from the 4 LSB received from the AMF 407. The UE 401 derives CK_{SRVCC} , IK_{SRVCC} based on the new K_{ASME_SRVCC} key, e.g., as described in the clause A.12 in TS 33.401 (incorporated herein by reference) using a downlink NAS COUNT of zero. The UE 401 may identify the CK_{SRVCC} and IK_{SRVCC} from eKSI (= ngKSI) as the
30 MME_SRVCC 409 does.

[0124] In one embodiment, if the SRVCC handover is not completed successfully, the newly mapped CK_{SRVCC} , IK_{SRVCC} and KSI_{SRVCC} cannot be used. In this case, the MSC server 411, enhanced for SRVCC, deletes the newly mapped SRVCC security context for the UE 411, including CK_{SRVCC} , IK_{SRVCC} and KSI_{SRVCC} .

5 [0125] At 10b (see block 430), in one embodiment, the UE 401 stores the network access restriction information (GERAN access restricted/not allowed) if received in the handover command and determines not to select GERAN access (2G) (e.g., even if the 5G signal or 4G/3G signal is not available and the UE 401 waits until the 5G/4G/3G signal is available to prevent a bidding down attack. In this handover scenario, the UE
10 connects to 3G e.g., UTRAN).

[0126] Referring to Figure 4C, at 11 (see block 432), in one embodiment, if the MME_SRVCC 409 received both GERAN access restriction and UTRAN access restrictions in 3a, then the MME_SRVCC 409 initiates S1 handover for the UE 401 and does not perform a handover/SRVCC to 3G as well as 2G. Here as 2G and 3G are both
15 decommissioned, 12a to 19 are performed for Case 2 e.g., S1 handover.

[0127] At 12a (see messaging 434), in one embodiment, when the target MME 409 receives a Forward Relocation Request message from source AMF 407 (in 3a), then the target MME 409 initiates S1 handover as SRVCC to 3G/2G cannot be allowed as described in 11, and shall derive EPS NAS keys (e.g., K_{NASenc} and K_{NASint}) from the
20 received K_{ASME} key with the received EPS NAS security algorithm identifiers as input, to be used in EPC, e.g., as described in Annex A.7 in TS 33.401 (incorporated herein by reference). The target MME 409 includes the {NH, NCC=2} pair, the UE security capabilities, UTRAN access not allowed indication, and GERAN access not allowed indication in the S1 HANDOVER REQUEST message to the target eNB 405. The UE
25 security capabilities, in one embodiment, including the UE EPS security capabilities received from the source AMF 407 and the UE's support of network access restriction enforcement capability can be sent in this message.

[0128] At 12b (see block 436), in one embodiment, upon receipt of the S1 HANDOVER REQUEST from the target MME 409, if the eNB 405 received the UTRAN
30 access not allowed indication, the GERAN access not allowed indication, and the UE's support of network access restriction enforcement capability in the S1 HANDOVER REQUEST, the eNB 405 stores them along with the UE context. Further based on the

received UTRAN access not allowed indication and GERAN access not allowed indication and the UE's support of network access restriction enforcement capability, the eNB 405 performs an action including not initiating an inter-RAT handover to UTRAN/GERAN, not initiating SRVCC from 5G/4G to 3G or 2G, and provisioning the
5 network access restriction information (UTRAN access restricted/not allowed, GERAN access restricted/not allowed indications) to the UE 401.

[0129] At 13 (see messaging 438), in one embodiment, upon receipt of the S1 HANDOVER REQUEST from the target MME 409, the target eNB 405 selects AS security algorithms from the UE EPS security capabilities, e.g., as described in clause
10 7.2.4.2.3 in TS 33.401 (incorporated herein by reference) and computes the KeNB to be used with the UE 401 and proceed, e.g., as described in clause 7.2.8.4.3 in TS 33.401 (incorporated herein by reference). The target eNB 405 sends the selected AS security algorithms in the target to source transparent container in the S1 Handover Request Ack Message to the target MME 409.

15 [0130] At 14 (see messaging 440), in one embodiment, the target MME 409 shall include the target to source transparent container received from the target eNB 405 in the Forward Relocation Response message sent to the source AMF 407.

[0131] At 15 (see messaging 442), in one embodiment, the source AMF 407 shall include the target to source transparent container, UTRAN access restricted/not allowed
20 indication, GERAN access restricted/not allowed indication (if network access restriction information is available for the UE 401), and the 8 LSB of the downlink NAS COUNT value used in K_{ASME} derivation in 2, in the handover command sent to the source gNB 403/eNB 405.

[0132] At 16 (see messaging 444), in one embodiment, the source gNB 403/eNB 405
25 shall include the target to source transparent container, UTRAN access restricted/not allowed indication, GERAN access restricted/not allowed indication, and the 8 LSB of the downlink NAS COUNT value in the handover command sent to the UE 401.

[0133] In one embodiment, the if the source gNB 403/eNB 405 receives the network access restriction information (UTRAN access restricted, GERAN access restricted) from
30 AMF 407, it is stored in the gNB 403/eNB 405 as part of the UE context along with 5G-GUTI, RNTI, and TMSI. Further, based on the received network access restriction

information, the RAN determines to perform an action including not initiating an inter-RAT handover to UTRAN/GERAN and not initiating SRVCC from 4G to 3G or 2G.

[0134] In one embodiment, upon reception of the Handover Command message, the UE 401 estimates the downlink NAS COUNT value using the received 8 LSB of the downlink NAS COUNT value and its stored downlink NAS COUNT value. The UE 401 shall ensure that the estimated downlink NAS COUNT value is greater than the stored downlink NAS COUNT value. Then, the UE 401 shall derive the mapped EPS security context, e.g., derive K_{ASME}' from K_{AMF} e.g., as described in clause 8.6.1 of TS 33.501 (incorporated herein by reference) using the estimated downlink 5G NAS COUNT value. After the derivation, the UE 401 shall set the downlink NAS COUNT value in the 5G NAS security context to the received downlink NAS COUNT value.

[0135] At 17a (see block 446), in one embodiment, the eKSI for the newly derived K_{ASME}' key is defined, e.g., as described in clause 8.6.1 of TS 33.501 (incorporated herein by reference). The UE 401 shall also derive the EPS NAS keys (e.g., K_{NASenc} and K_{NASint}) as the MME 409 did in 4a using the EPS NAS security algorithm identifiers stored in the UE 401 and provisioned by the AMF 407 to the UE 401 in 5G NAS SMC in earlier 5G access. The UE 401 shall also derive the initial K_{eNB} from the K_{ASME}' and the uplink NAS COUNT, e.g., as specified in Annex A.3 of TS 33.401 (incorporated herein by reference) using $2^{32}-1$ as the value of the uplink NAS COUNT parameter.

[0136] In one embodiment, the UE shall also derive the $\{NH, NCC=2\}$ pair, e.g., as described in A.4 of TS 33.401 (incorporated herein by reference) and further derive the K_{eNB} to be used with the UE 401 by performing the key derivation e.g., defined in Annex A.5 in TS 33.401 (incorporated herein by reference). The UE 401 shall derive the AS RRC keys and the AS UP keys based on the K_{eNB} and the received AS EPS security algorithms identifiers selected by the target eNB 405, e.g., as described in Annex A.7 in TS 33.401 (incorporated herein by reference). The uplink and downlink EPS NAS COUNT associated with the derived EPS NAS keys are set to the values, e.g., as described in clause 8.6.1 (incorporated herein by reference). The UE 401 shall immediately use the newly created mapped EPS security context, both for NAS and AS communication.

[0137] At 17b (see block 448), in one embodiment, the UE 401 also stores the network access restriction information (UTRAN access restricted/not allowed, GERAN access restricted/not allowed) if received in the handover command and determines not

to select UTRAN access (3G) or GERAN access (2G) (e.g., even if the 5G signal or 4G signal is not available and the UE 401 waits until the 5G/4G signal is available to prevent a bidding down attack. Specific to this handover scenario, the UE connects to 4G i.e., LTE/E-UTRAN).

- 5 **[0138]** At 18 (see messaging 450), in one embodiment, the UE 401 sends the Handover Complete message to the target eNB 405. The UE 401 shall cipher and integrity protect this message using the newly created mapped EPS security context.

[0139] At 19 (see messaging 452), in one embodiment, the target eNB 405 notifies the target MME 409 with a Handover Notify message.

- 10 **[0140]** In one embodiment, after successful completion of the Handover procedure, the UE 401 shall delete any mapped 5G security context. In further embodiments, after deleting the mapped 5G security context, if the UE 401 has a full non-current native 5G NAS security context, then the UE 401 shall make the non-current native 5G NAS security context the current one.

- 15 **[0141]** Figure 5 illustrates an example of a UE 500 in accordance with aspects of the present disclosure. The UE 500 may include a processor 502, a memory 504, a controller 506, and a transceiver 508. The processor 502, the memory 504, the controller 506, or the transceiver 508, or various combinations thereof or various components thereof may be examples of means for performing various aspects of the present disclosure as described
20 herein. These components may be coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces.

- [0142]** The processor 502, the memory 504, the controller 506, or the transceiver 508, 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
25 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.

- [0143]** The processor 502 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
30 some implementations, the processor 502 may be configured to operate the memory 504. In some other implementations, the memory 504 may be integrated into the processor

502. The processor 502 may be configured to execute computer-readable instructions stored in the memory 504 to cause the UE 500 to perform various functions of the present disclosure.

[0144] The memory 504 may include volatile or non-volatile memory. The memory
5 504 may store computer-readable, computer-executable code including instructions when executed by the processor 502 cause the UE 500 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such the memory 504 or another type of memory. Computer-readable media includes both non-transitory computer storage media and communication media including any medium that
10 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.

[0145] In some implementations, the processor 502 and the memory 504 coupled with the processor 502 may be configured to cause the UE 500 to perform one or more of the
15 functions described herein (e.g., executing, by the processor 502, instructions stored in the memory 504). For example, the processor 502 may support wireless communication at the UE 500 in accordance with examples as disclosed herein.

[0146] The controller 506 may manage input and output signals for the UE 500. The controller 506 may also manage peripherals not integrated into the UE 500. In some
20 implementations, the controller 506 may utilize an operating system such as iOS®, ANDROID®, WINDOWS®, or other operating systems. In some implementations, the controller 506 may be implemented as part of the processor 502.

[0147] In some implementations, the UE 500 may include at least one transceiver 508. In some other implementations, the UE 500 may have more than one transceiver
25 508. The transceiver 508 may represent a wireless transceiver. The transceiver 508 may include one or more receiver chains 510, one or more transmitter chains 512, or a combination thereof.

[0148] A receiver chain 510 may be configured to receive signals (e.g., control information, data, packets) over a wireless medium. For example, the receiver chain 510
30 may include one or more antennas for receiving the signal over the air or wireless medium. The receiver chain 510 may include at least one amplifier (e.g., a low-noise amplifier (LNA)) configured to amplify the received signal. The receiver chain 510 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 510 may include at least one decoder for decoding and processing the demodulated signal to receive the transmitted data.

5 [0149] A transmitter chain 512 may be configured to generate and transmit signals (e.g., control information, data, packets). The transmitter chain 512 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
10 modulation (FM), or digital modulation schemes like phase-shift keying (PSK) or quadrature amplitude modulation (QAM). The transmitter chain 512 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 512 may also include one or more antennas for transmitting the amplified signal into the
15 air or wireless medium.

[0150] Figure 6 illustrates an example of a processor 600 in accordance with aspects of the present disclosure. The processor 600 may be an example of a processor configured to perform various operations in accordance with examples as described herein. The processor 600 may include a controller 602 configured to perform various operations in
20 accordance with examples as described herein. The processor 600 may optionally include at least one memory 604, which may be, for example, an L1/L2/L3 cache. Additionally, or alternatively, the processor 600 may optionally include one or more arithmetic-logic units (ALUs) 606. One or more of these components may be in electronic communication or otherwise coupled (e.g., operatively, communicatively, functionally, electronically,
25 electrically) via one or more interfaces (e.g., buses).

[0151] The processor 600 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
30 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 600) 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).

[0152] The controller 602 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 600 to cause the processor 600 to support various operations in accordance with examples as described herein. For example, the controller 602 may operate as a control unit of the processor 600, generating control signals that manage the operation of various components of the processor 600. These control signals include enabling or disabling functional units, selecting data paths, initiating memory access, and coordinating timing of operations.

[0153] The controller 602 may be configured to fetch (e.g., obtain, retrieve, receive) instructions from the memory 604 and determine subsequent instruction(s) to be executed to cause the processor 600 to support various operations in accordance with examples as described herein. The controller 602 may be configured to track memory address of instructions associated with the memory 604. The controller 602 may be configured to decode instructions to determine the operation to be performed and the operands involved. For example, the controller 602 may be configured to interpret the instruction and determine control signals to be output to other components of the processor 600 to cause the processor 600 to support various operations in accordance with examples as described herein. Additionally, or alternatively, the controller 602 may be configured to manage flow of data within the processor 600. The controller 602 may be configured to control transfer of data between registers, arithmetic logic units (ALUs), and other functional units of the processor 600.

[0154] The memory 604 may include one or more caches (e.g., memory local to or included in the processor 600 or other memory, such RAM, ROM, DRAM, SDRAM, SRAM, MRAM, flash memory, etc. In some implementations, the memory 604 may reside within or on a processor chipset (e.g., local to the processor 600). In some other implementations, the memory 604 may reside external to the processor chipset (e.g., remote to the processor 600).

[0155] The memory 604 may store computer-readable, computer-executable code including instructions that, when executed by the processor 600, cause the processor 600 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 602 and/or the processor 600 may be configured to execute computer-readable instructions stored in the memory 604 to cause the processor 600 to perform various functions. For example, the processor 600 and/or the controller 602 may be coupled with or to the memory 604, the processor 600, the controller 602, and the memory 604 may be configured to perform various functions described herein. In some examples, the processor 600 may include multiple processors and the memory 604 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.

[0156] The one or more ALUs 606 may be configured to support various operations in accordance with examples as described herein. In some implementations, the one or more ALUs 606 may reside within or on a processor chipset (e.g., the processor 600). In some other implementations, the one or more ALUs 606 may reside external to the processor chipset (e.g., the processor 600). One or more ALUs 606 may perform one or more computations such as addition, subtraction, multiplication, and division on data. For example, one or more ALUs 606 may receive input operands and an operation code, which determines an operation to be executed. One or more ALUs 606 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 606 may support logical operations such as AND, OR, exclusive-OR (XOR), not-OR (NOR), and not-AND (NAND), enabling the one or more ALUs 606 to handle conditional operations, comparisons, and bitwise operations.

[0157] The processor 600 may support wireless communication in accordance with examples as disclosed herein. The processor 600 may be configured to or operable to support a means to receive an indication of a network access restriction enforcement capability of a UE, receive a handover request for the UE, determine network access restriction information for the UE, transmit the network access restriction information to a network entity associated with a different network, and transmit a handover command comprising the network access restriction information to a base station associated with

the UE for processing the handover request according to the network access restriction information.

[0158] In one embodiment, the processor 600 may be configured to or operable to support a means to receive an indication of a network access restriction enforcement capability of a UE from a network entity, receive network access restriction information for the UE from the network entity, and apply at least one network access restriction based on the received indication of the network access restriction enforcement capability of the UE and the received network access restriction information for the UE.

[0159] In one embodiment, the processor 600 may be configured to or operable to support a means to receive network access restriction information for a UE, store the network access restriction information, and apply at least one network access restriction based on the received network access restriction information for the UE.

[0160] Figure 7 illustrates an example of a NE 700 in accordance with aspects of the present disclosure. The NE 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.

[0161] 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.

[0162] The NE 700 may be configured to support a means to receive an indication of a network access restriction enforcement capability of a UE, receive a handover request for the UE, determine network access restriction information for the UE, transmit the network access restriction information to a network entity associated with a different network, and transmit a handover command comprising the network access restriction information to a base station associated with the UE for processing the handover request according to the network access restriction information.

[0163] In one embodiment, the indication of the network access restriction enforcement capability of the UE indicates whether the UE supports GERAN access restrictions, UTRAN access restrictions, or a combination thereof.

5 [0164] In one embodiment, the NE 700 may be configured to support a means to send a relocation request comprising the network access restriction information to the network entity.

[0165] In one embodiment, the network access restriction information comprises information determining whether handover for the UE is allowed for access to a GERAN, a UTRAN, or a combination thereof.

10 [0166] In one embodiment, the network entity comprises an MME of an EPS. In one embodiment, the indication of a network access restriction enforcement capability of the UE is received from the network entity as part of a TAU request message associated with the UE.

15 [0167] In one embodiment, the NE 700 may be configured to support a means to transmit the network access restriction information to a RAN associated with the UE to enforce the network access restriction for the UE at the RAN.

[0168] In one embodiment, the NE 700 may be configured to support a means to transmit the indication of a network access restriction enforcement capability of the UE and the network access restriction information for the UE to an MME.

20 [0169] In one embodiment, the NE 700 may be configured to support a means to receive an indication of a network access restriction enforcement capability of a UE from a network entity, receive network access restriction information for the UE from the network entity, and apply at least one network access restriction based on the received indication of the network access restriction enforcement capability of the UE and the
25 received network access restriction information for the UE.

[0170] In one embodiment, the indication of the network access restriction enforcement capability of the UE indicates whether the UE supports GERAN access restrictions, UTRAN access restrictions, or a combination thereof.

30 [0171] In one embodiment, the NE 700 may be configured to support a means to store the network access restriction information for the UE as part of a UE context.

[0172] In one embodiment, the NE 700 may be configured to support a means to apply the at least one network access restriction by not initiating inter-RAT handover to GERAN, UTRAN, or a combination thereof.

5 [0173] In one embodiment, the NE 700 may be configured to support a means to apply the at least one network access restriction by not initiating or forwarding relocation requests related to SRVCC for handover to GERAN, UTRAN, or a combination thereof.

[0174] In one embodiment, the NE 700 may be configured to support a means to transmit the network access restriction information to a RAN associated with the UE to enforce the network access restriction for the UE at the RAN.

10 [0175] In one embodiment, the NE 700 may be configured to support a means to transmit the network access restriction information to an eNB base station in the RAN in an S1 message.

[0176] In one embodiment, the NE 700 may be configured to support a means to indicate to the eNB in an S1 handover request message that a GERAN and a UTRAN are
15 decommissioned to prevent handover to the GERAN and UTRAN.

[0177] In one embodiment, the NE 700 may be configured to support a means to transmit the network access restriction information to the UE in a secured NAS message.

[0178] In one embodiment, the NE 700 may be configured to support a means to transmit the network access restriction information to the UE in a TAU accept message.

20 [0179] In one embodiment, the NE 700 may be configured to support a means to transmit the network access restriction information and the indication of a network access restriction enforcement capability of the UE to an eNB.

[0180] In one embodiment, the NE 700 may be configured to support a means to receive network access restriction information for a UE, store the network access
25 restriction information, and apply at least one network access restriction based on the received network access restriction information for the UE.

[0181] In one embodiment, the network access restriction information comprises an indication of whether the UE is allowed to access a GERAN, a UTRAN, or a combination thereof.

[0182] In one embodiment, the NE 700 may be configured to support a means to apply the at least one network access restriction by not initiating inter-RAT handover to GERAN, UTRAN, or a combination thereof.

5 [0183] In one embodiment, the NE 700 may be configured to support a means to apply the at least one network access restriction by not initiating or forwarding relocation requests related to SRVCC for handover to GERAN, UTRAN, or a combination thereof.

[0184] In one embodiment, the NE 700 may be configured to support a means to receive the network access restriction information in an S1 message from an MME of an EPS.

10 [0185] In one embodiment, the NE is a base station that comprises an eNB or a gNB.

[0186] 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
15 702. The processor 702 may be configured to execute computer-readable instructions stored in the memory 704 to cause the NE 700 to perform various functions of the present disclosure.

[0187] The memory 704 may include volatile or non-volatile memory. The memory 704 may store computer-readable, computer-executable code including instructions when
20 executed by the processor 702 causes the NE 700 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such 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
25 storage medium may be any available medium that may be accessed by a general-purpose or special-purpose computer.

[0188] In some implementations, the processor 702 and the memory 704 coupled with the processor 702 may be configured to cause the NE 700 to perform one or more of the functions described herein (e.g., executing, by the processor 702, instructions stored in
30 the memory 704). For example, the processor 702 may support wireless communication at the NE 700 in accordance with examples as disclosed herein.

[0189] The controller 706 may manage input and output signals for the NE 700. The controller 706 may also manage peripherals not integrated into the NE 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
5 controller 706 may be implemented as part of the processor 702.

[0190] In some implementations, the NE 700 may include at least one transceiver 708. In some other implementations, the NE 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
10 combination thereof.

[0191] 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
15 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 processing the demodulated signal to receive the transmitted data.

[0192] 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
25 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
30 air or wireless medium.

[0193] Figure 8 illustrates a flowchart of a method in accordance with aspects of the present disclosure. The operations of the method may be implemented by an 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.

[0194] At 802, the method may receive an indication of a network access restriction enforcement capability of a UE. The operations of 802 may be performed in accordance
5 with examples as described herein. In some implementations, aspects of the operations of 802 may be performed by an NE as described with reference to Figure 7.

[0195] At 804, the method may receive a handover request for the UE. The operations of 804 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 804 may be performed by an NE as
10 described with reference to Figure 7.

[0196] At 806, the method may determine network access restriction information for the UE. The operations of 806 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 806 may be performed by an NE as described with reference to Figure 7.

[0197] At 808, the method may transmit the network access restriction information to a network entity associated with a different network. The operations of 808 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 808 may be performed by an NE as described with reference
15 to Figure 7.

[0198] At 810, the method may transmit a handover command comprising the network access restriction information to a base station associated with the UE for processing the handover request according to the network access restriction information. The operations of 810 may be performed in accordance with examples as described
20 herein. In some implementations, aspects of the operations of 810 may be performed by an NE as described with reference to Figure 7.

[0199] Figure 9 illustrates a flowchart of a method in accordance with aspects of the present disclosure. The operations of the method may be implemented by an 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.

[0200] At 902, the method may receive an indication of a network access restriction enforcement capability of a UE from a network entity. The operations of 902 may be
30

performed in accordance with examples as described herein. In some implementations, aspects of the operations of 902 may be performed by an NE as described with reference to Figure 7.

[0201] At 904, the method may receive network access restriction information for the
5 UE from the network entity. The operations of 904 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 904 may be performed by an NE as described with reference to Figure 7.

[0202] At 906, the method may apply at least one network access restriction based on
10 the received indication of the network access restriction enforcement capability of the UE and the received network access restriction information for the UE. The operations of 906 may be performed in accordance with examples as described herein. In some implementations, aspects of the operations of 906 may be performed by an NE as described with reference to Figure 7.

[0203] Figure 10 illustrates a flowchart of a method in accordance with aspects of the
15 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.

[0204] At 1002, the method may receive network access restriction information for a
20 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 7.

[0205] At 1004, the method may store the network access restriction information. The
25 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 7.

[0206] At 1006, the method may apply at least one network access restriction based
30 on the received network access restriction information for 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 7.

[0207] 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.

[0208] The description herein is provided to enable a person having ordinary skill in
5 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
10 features disclosed herein.

CLAIMS

What is claimed is:

1. A network equipment (NE) for wireless communication, comprising:
 at least one memory; and
 5 at least one processor coupled with the at least one memory and
 configured to cause the NE to:
 receive an indication of a network access restriction enforcement
 capability of a user equipment (UE);
 receive a handover request for the UE;
 10 determine network access restriction information for the UE;
 transmit the network access restriction information to a network
 entity associated with a different network; and
 transmit a handover command comprising the network access
 restriction information to a base station associated with
 15 the UE for processing the handover request according to
 the network access restriction information.
2. The NE of claim 1, wherein the indication of the network access restriction
 enforcement capability of the UE indicates whether the UE supports GSM
 EDGE Radio Access Network (GERAN) access restrictions, Universal
 20 Terrestrial Radio Access Network (UTRAN) access restrictions, or a
 combination thereof.
3. The NE of claim 1, wherein the at least one processor is configured to cause the
 NE to send a relocation request comprising the network access restriction
 information to the network entity.
- 25 4. The NE of claim 1, wherein the network access restriction information
 comprises information determining whether handover for the UE is allowed for
 access to a GSM EDGE Radio Access Network (GERAN), a Universal
 Terrestrial Radio Access Network (UTRAN), or a combination thereof.
5. The NE of claim 1, wherein the network entity comprises a mobility
 30 management entity (MME) of an evolved packet system (EPS).

6. The NE of claim 1, wherein the indication of a network access restriction enforcement capability of the UE is received from the network entity as part of a tracking area update (TAU) request message associated with the UE.
7. The NE of claim 1, wherein the at least one processor is configured to cause the NE to transmit the network access restriction information to a radio access network (RAN) associated with the UE to enforce the network access restriction for the UE at the RAN.
8. The NE of claim 1, wherein the at least one processor is configured to cause the NE to transmit the indication of a network access restriction enforcement capability of the UE and the network access restriction information for the UE to a mobility management entity (MME).
9. A processor for wireless communication, comprising:
 - at least one controller coupled with at least one memory and configured to cause the processor to:
 - receive an indication of a network access restriction enforcement capability of a user equipment (UE);
 - receive a handover request for the UE;
 - determine network access restriction information for the UE;
 - transmit the network access restriction information to a network entity associated with a different network; and
 - transmit a handover command comprising the network access restriction information to a base station associated with the UE for processing the handover request according to the network access restriction information.
10. The processor of claim 9, wherein the indication of the network access restriction enforcement capability of the UE indicates whether the UE supports GSM EDGE Radio Access Network (GERAN) access restrictions, Universal Terrestrial Radio Access Network (UTRAN) access restrictions, or a combination thereof.

11. The processor of claim 9, wherein the at least one controller is configured to cause the processor to send a relocation request comprising the network access restriction information to the network entity.
12. The processor of claim 9, wherein the network access restriction information
5 comprises information determining whether handover for the UE is allowed for access to a GSM EDGE Radio Access Network (GERAN), a Universal Terrestrial Radio Access Network (UTRAN), or a combination thereof.
13. The processor of claim 9, wherein the network entity comprises a mobility management entity (MME) of an evolved packet system (EPS).
- 10 14. A method performed by a network equipment (NE), the method comprising:
receiving an indication of a network access restriction enforcement
capability of a user equipment (UE);
receiving a handover request for the UE;
determining network access restriction information for the UE;
15 transmitting the network access restriction information to a network
entity associated with a different network; and
transmitting a handover command comprising the network access
restriction information to a base station associated with the UE
for processing the handover request according to the network
20 access restriction information.
15. A base station (BS) 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 BS to:
25 receive network access restriction information for a user
equipment (UE);
store the network access restriction information; and
apply at least one network access restriction based on the
received network access restriction information for the
30 UE.

16. The BS of claim 15, wherein the network access restriction information comprises an indication of whether the UE is allowed to access a GSM EDGE Radio Access Network (GERAN), a Universal Terrestrial Radio Access Network (UTRAN), or a combination thereof.
- 5
17. The BS of claim 15, wherein the at least one processor is configured to cause the BS to apply the at least one network access restriction by not initiating inter-radio access technology (RAT) handover to GSM EDGE Radio Access Network (GERAN), Universal Terrestrial Radio Access Network (UTRAN), or a combination thereof.
- 10
18. The BS of claim 15, wherein the at least one processor is configured to cause the BS to apply the at least one network access restriction by not initiating or forwarding relocation requests related to single radio voice call continuity (SRVCC) for handover to GSM EDGE Radio Access Network (GERAN), Universal Terrestrial Radio Access Network (UTRAN), or a combination thereof.
- 15
19. The BS of claim 15, wherein the at least one processor is configured to cause the BS to receive the network access restriction information in an S1 message from a mobility management entity (MME) of an evolved packet system (EPS).
- 20
20. The BS of claim 15, wherein the BS comprises an evolved nodeB (eNB) or a gNodeB (gNB).
- 25