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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 December 2019 (26.12.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/242545 A1

(51) International Patent Classification:
H04W 12/00 (2009.01)

(21) International Application Number:
PCT/CN2019/090860

(22) International Filing Date:
12 June 2019 (12.06.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/687,810 21 June 2018 (21.06.2018) US

(71) Applicant: **HUAWEI TECHNOLOGIES CO., LTD.** [CN/CN]; Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129 (CN).

(72) Inventors: **HU, Li**; Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129 (CN). **MUHANNA, Ahmad Shawky**; 5340 Legacy Drive, Suite 175, Plano, Texas 75024 (US). **GENG, Tingting**; Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129 (CN). **CHEN, Jing**; Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129 (CN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

(54) Title: METHOD AND APPARATUS FOR SECURITY ALGORITHM NEGOTIATION

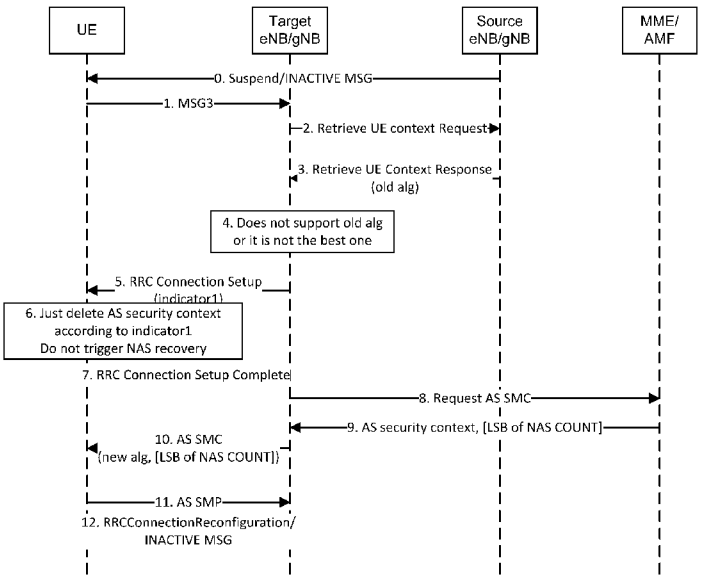

FIG. 3

(57) Abstract: A security algorithm negotiation method, a base station, and user equipment are provides. The method includes receiving indicator and algorithm identifier from a target base station, reserving a first key based on the indicator, wherein the first key is derived for a source base station, and deriving a security key based on the first key and an algorithm corresponding to the algorithm identifier. Several signaling will be reduced by using the solutions provided by the present disclosure.

[Continued on next page]

WO 2019/242545 A1

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

METHOD AND APPARATUS FOR SECURITY ALGORITHM NEGOTIATION

TECHNICAL FIELD

[0001] Embodiments of the present disclosure relate to the field of wireless communication technologies, and more specifically, to a method and apparatus for negotiating security algorithms.

BACKGROUND

[0002] For mobility network, a user equipment device or terminal device (collectively referred to as UE hereinafter) has mobility requirements. For example in long term evolution (LTE) or fourth generation (4G) communication systems, the UE may trigger a resume procedure, in the fifth generation (5G) communication systems, the UE may trigger a procedure from an INACTIVE to CONNECTED state. The UE may move from a source base station (the base station can be an eNB or a gNB) to a target base station (eNB/gNB) when triggering these procedures. Thus, the source eNB/gNB will have to send the UE's context to the target eNB/gNB. The UE's context includes old cipher and integrity protection algorithms used between the UE and the source eNB/gNB.

[0003] Different eNB/gNB may configure different algorithm priority list, or may not support the old algorithms. Thus, when the UE moves from a source eNB/gNB to a target eNB/gNB, the target eNB/gNB may not reuse the old algorithm, and should negotiate the new algorithm with the UE. However, for resume or INACTIVE to CONNECTED procedure, the message sent by the target gNB should be ciphered, that means the UE could not know the selected algorithms if the message is ciphered by the selected algorithm, because the UE could not decipher the message, and get the selected algorithm.

[0004] The current solution is to send the UE to an IDLE state, and require a NAS recovery. Referring to Fig.1, the current solution includes:

[0005] 0. Source eNB/gNB decides to suspend the UE (send the RRCConnectionRelease message with suspend cause to the UE, for 4G), or send the UE to INACTIVE (send the RRCConnectionInactive message to the UE, for 5G).

[0006] 1. The UE sends MSG3 (RRCConnectionResumeRequest message) to the target eNB/gNB to trigger resume procedure or INACTIVE to CONNECTED procedure to resume RRC connection.

[0007] 2. The target eNB/gNB sends Retrieve UE Context Request message to the source eNB/gNB to fetch UE context.

[0008] 3. The source eNB/gNB sends Retrieve UE Context Response message to the target eNB/gNB to response the message above. The Retreive UE Context Response may include UE security capability and old ciphering and integrity algorithms used between UE and source eNB/gNB.

[0009] 4. If the target eNB/gNB could not support old algorithms or if the target eNB/gNB prefers to use different algorithms,

[0010] 5. The target eNB/gNB sends RRC Connection Setup message to the UE to proceed with RRC connection establishment as if the UE was in RRC_IDLE (fallback procedure).

[0011] 6. The UE discards the stored UE AS context and indicates to upper layers that the RRC connection resume has been fallbacked.

[0012] 7. The UE sends initial NAS message (e.g. Service Request message) to the MME/AMF.

[0013] 8. The MME/AMF derives KeNB/KgNB according to current Kasme/Kamf and uplink NAS COUNT indicated by initial NAS message, and sends the KeNB/KgNB and UE security capability in Initial Context Setup Request message to the target eNB/gNB.

[0014] 9. The target eNB/gNB chooses the new ciphering and integrity algorithm which has the highest priority from its configured algorithm priority list and is also present in the UE security capability. The chosen algorithms are indicated to the UE in the access stratum security mode command (AS SMC). The target eNB/gNB derives Krrc-int according to the KeNB/KgNB and new integrity algorithm. The AS SMC is integrity protected by Krrc-int and new integrity algorithm. Note that the UE could get the new algorithms in AS SMC, because it is not ciphered.

[0015] 10. The UE derives KeNB/KgNB according to current Kasme/Kamf and uplink NAS COUNT indicated by initial NAS message, and derives Krrc-int and Krrc-enc according to

KeNB/KgNB and new integrity and ciphering algorithms indicated in AS SMC. The UE verifies AS SMC message according Krrc-int and new integrity algorithm. After successful verification, the UE may cipher and integrity protect the AS SMP message using Krrc-enc, Krrc-int, new ciphering and integrity algorithm. The UE sends the AS SMP message to the target gNB. Thus, UE and target gNB have successfully negotiate the security algorithm.

[0016] 11. The target gNB may send RRCConnectionReconfiguartion message to the UE to configurate the DRB. The target gNB may suspend the UE (send the RRCConnectionRelease message with suspend cause to the UE, for 4G), or send the UE to INACTIVE (send the RRCConnectionInactive message to the UE, for 5G).

[0017] Thus, according to figure 1, the UE will be fallback to the IDLE state. However, such a procedure costs too much signalling overhead.

SUMMARY

[0018] Embodiments of the present disclosure provide a method for negotiating security method, which can reduce the signaling overhead.

[0019] According to a first aspect, a security algorithm negotiation method is provided. The method comprises receiving, by a user equipment (UE), a first request message from a target base station; reserving, by the UE, a first key which is derived for a source base station in response to the first request message; receiving, by the UE, a second request message from a target base station, wherein the second request message comprise a identity which is used to indicate an algorithm; deriving, by the UE, a second key based on the first key and an algorithm corresponding to the identity.

[0020] It is necessary to be pointed out that if a target base station fails to support an old algorithm of the UE and the source base station, normally, the target base station will send an RRC Connection Setup message to the UE to proceed with RRC connection establishment as if the UE was in RRC_IDLE (fallback procedure), and then the steps (6-11) described in the background will be performed. Apparently, the steps (6-11) will cost several signaling. While in the present disclosure, in order to reduce the signaling, the UE will take use of the first key and an algorithm from the target base station to derive secret keys for communicating with the target base station. Because the first key was stored in the UE, so reusing the first key will achieve the goal.

[0021] Optionally, when the UE receives a first request message, the UE will send a first response message to the target base station in response to the first request message. In addition, after deriving the second key, the UE will verify the second request message, protect a second response message base on the second key and the algorithm corresponding to the identity when the second request message is verified successfully; and send the protected second response message to the target base station. Specially, the first request message can be a RRC Connection Setup message, the first response message can be a RRC Connection Setup Complete message, the second request message can be an AS SMC message, and the second response message can be an AS SMP message.

[0022] With reference to the first aspect, it should be pointed out that the first request message comprises a first indicator. The UE can delete security keys which are derived from the first key based on the first indicator and in order to reduce the signaling, the UE will not trigger Non-access stratum recovery process based on the first indicator. Optionally, in another possible manner, the UE will not trigger Non-access stratum recovery process in response to the first request message.

[0023] With reference to the first aspect, because of reusing the first key, the UE will not deriving a key for the target base station based on the second indicator included in the second request message.

[0024] With reference to the first aspect, in a first possible implementation manner of the first aspect, the performing rotation processing on a preset precoding matrix includes obtaining indication information, where the indication information is used to instruct a base station to perform the rotation processing on the preset precoding matrix; and performing the rotation processing on the preset precoding matrix according to the indication information.

[0025] According to a second aspect, a security algorithm negotiation method is provided. The method comprises: sending, by a target base station, a first request message from a user equipment (UE); wherein the first request message is used to indicate the UE to reserve a first key which is derived for a source base station; sending, by the target base station, a second request message to the UE; wherein the second request message comprises an identity which is used to indicate an algorithm; and receiving, by the target base station, a second response message from the UE.

[0026] Optionally, the target base station will receive a first response message. Specially, the first request message can be a RRC Connection Setup message, the first response message can be a RRC Connection Setup Complete message, the second request message can be an AS SMC message, and the second response message can be an AS SMP message.

[0027] Further, it is necessary to be pointed out that, in order to reduce signaling, the target base station will indicate the UE to reuse the first key (that is, just keep the first key, and no need to derive a key for the target base station). Optionally, the target base station will indicate the UE to delete security keys which are derived from the first key, optionally the target base station may indicate the UE not to trigger Non-access stratum recovery process.

[0028] According to a third aspect, the present disclosure provides a structure of user equipment including a processor, a memory, a receiver circuit, and a transmitter circuit. The processor, the memory, and the receiver circuit are connected using a bus system. The user equipment may be configured to implement steps and methods in the first aspect.

[0029] According to a fourth aspect, the present disclosure provides a structure of a base station. The base station includes a processor, a memory a receiver circuit, and a transmitter circuit. The processor, the memory, and the receiver circuit are connected using a bus system. The base station may be configured to implement steps and methods in the second aspect.

[0030] According to a fifth aspect, the present disclosure provides a memory. The memory may provide an instruction and data for a processor. When the instruction was executed, the processor will perform the method in the first aspect or in the second aspect.

[0031] In the embodiments of the present disclosure, the first key is kept and reused in the process of deriving a key for a target base station. A purpose of reducing several signaling is achieved .

BRIEF DESCRIPTION OF DRAWINGS

[0032] The following briefly describes the accompanying drawings used in describing the embodiments. The accompanying drawings in the following description show merely some embodiments of the present disclosure, and a person of ordinary skill in the art may still derive other drawings from these accompanying drawings without creative efforts.

[0033] FIG 1 is a schematic flowchart of a security algorithm negotiation method in conventional art;

[0034] FIG. 2 is a schematic flowchart of a security algorithm negotiation method according to embodiment 1 of the present disclosure;

[0035] FIG. 3 is a schematic flowchart of a security algorithm negotiation method according embodiment 2 of the present disclosure;

[0036] FIG. 4 is a schematic flowchart of a security algorithm negotiation method according embodiment 3 of the present disclosure;

[0037] FIG. 5 is a schematic flowchart of a security algorithm negotiation method according embodiment 4 of the present disclosure;

[0038] FIG. 6 is a simplified block diagram of a base station according to an embodiment of the present disclosure; and

[0039] FIG. 7 is a simplified block diagram of a user equipment device according to an embodiment of the present disclosure.

DETAILED DESCRIPTION OF EMBODIMENTS

[0040] The following describes the technical solutions in the embodiments of the present disclosure with reference to the accompanying drawings.

[0100] It should be understood that, user equipment (UE) mentioned in the embodiments of the present disclosure may be referred to as a mobile terminal (MT), mobile user equipment, and the like, and may communicate with one or more core networks using a radio access network (RAN). The user equipment may be a mobile terminal, such as a mobile phone (which is also referred to as a "cellular" phone) and a computer with a mobile terminal. For example, the user equipment may be a portable, pocket-sized, hand-held, computer built-in, or in-vehicle mobile apparatus.

[0101] A base station may be a base station (NodeB) in WCDMA, or may further be an evolved NodeB (eNB or e-NodeB for short) in LTE, or may further be a New Radio NodeB (gNodeB) in 5G. This is not limited in the present disclosure.

[0102] There are four embodiments in the present disclosure. Further, the related explanation of the words can refer to Embodiment 1.

Embodiment 1

[0103] Referring to FIG 2, in order to reduce the signaling, the target base station indicate the UE not to trigger the Non-access stratum recovery process and reuse the current KeNB/KgNB. Specially, please refer to the following steps.

[0104] 0. Source eNB/gNB decides to suspend the UE (send the RRCConnectionRelease message with suspend cause to the UE, for 4G), or send the UE to INACTIVE (send the RRCConnectionInactive message to the UE, for 5G).

[0105] It is should be understood that that source base station can be a source eNB or a source gNB.

[0106] 1. The UE sends MSG3 (RRCConnectionResumeRequest message) to the target eNB/gNB to trigger resume procedure or INACTIVE to CONNECTED procedure to resume RRC connection.

[0107] It is should be understood that that target base station can be a target eNB or a target gNB.

[0108] 2. The target eNB/gNB sends Retreive UE Context Request message to the source eNB/gNB to fetch UE context.

[0109] 3. The source eNB/gNB sends Retreive UE Context Response message to the source eNB/gNB to response the message above. The Retreive UE Context Response may include UE security capability and old ciphering and integrity algorithms used between UE and source eNB/gNB.

[0110] 4. If the target eNB/gNB could not support old algorithms or if the target eNB/gNB prefers to use different algorithms or if the old algorithm is not the best one, the target eNB/gNB send RRC Connection Setup message to the UE.

[0111] 5. RRC connection setup. There are three possible ways.

[0112] Option 1: The target eNB/gNB sends RRC Connection Setup message to the UE. The RRC Connection Setup message includes NoNASRecovery indicator.

[0113] Option 2: The target eNB/gNB sends RRC Connection Setup message to the UE. The RRC Connection Setup message includes NASRecovery indicator.

[0114] Option 3: The target eNB/gNB sends RRC Connection Setup without NAS Recovery message to the UE.

[0115] 6. There are three possible solutions.

[0116] Option 1: When the NoNASRecovery indicator is included or NoNASRecovery is set to TRUE, the UE does not indicate to upper layers that the RRC connection resume has been fallbacked. The UE also keep the current KeNB/KgNB. The UE could optionally discard the keys derived from the current KeNB/KgNB (Krrc-int, Krrc-enc, Kup-int and Kup-enc (if exists)) stored in UE AS security context. Otherwise, the UE discards the stored UE AS context and indicates to upper layers that the RRC connection resume has been fallbacked.

[0117] It is necessary to point out that the Krrc-enc is used for radio resource control (RRC) ciphering protection, the Krrc-int is used for RRC integrity protection, the Kup-int is used for user plane (UP) integrity protection and Kup-enc is used for UP ciphering protection.

[0118] Option 2: When the NASRecovery indicator is included or NASRecovery is set to TRUE, the UE discards the stored UE AS context and indicates to upper layers that the RRC connection resume has been fallbacked. Otherwise, the UE does not indicate to upper layers that the RRC connection resume has been fallbacked, the UE also keep the current KeNB/KgNB, the UE could optionally discard the Krrc-int, Krrc-enc, Kup-int (if exists), and Kup-enc (if exists) stored in UE AS security context.

[0119] Option 3: When the UE receives RRC Connection Setup without NAS Recovery message from target eNB/gNB, the UE does not indicate to upper layers that the RRC connection resume has been fallbacked. The UE also keeps the current KeNB/KgNB. The UE could optionally discard the Krrc-int, Krrc-enc, Kup-int (if exists), and Kup-enc (if exists) stored in UE AS security context.

[0120] 7. (Optional) The UE sends RRC Connection Setup Complete message to the target eNB/gNB.

[0121] 8. The target eNB/gNB chooses the new ciphering and integrity algorithm which has the highest priority from its configured algorithm priority list and is also present in the UE security capability, which can be received from source eNB/gNB. The chosen algorithms are indicated to the UE in RRC message. The target eNB/gNB derives Krrc-int according to the KeNB/KgNB and new integrity algorithm. The RRC message is integrity protected by Krrc-int and new integrity algorithm.

[0122] There are four possible manners to perform the step 8.

[0123] Option 1: the RRC message is AS SMC, and does not include any indicator.

[0124] Option 2: the RRC message is AS SMC, and includes NoRootKeyDerivation indicator.

[0125] Option 3: the RRC message is AS SMC, and includes RootKeyDerivation indicator.

[0126] Option 4: the RRC message is AS SMC without Root Key Derivation.

[0127] 9. There are four possible manner in response to the step 8.

[0128] Option 1: If NoNASRecovery indicator is included or NoNASRecovery is set to TRUE or if NASRecovery indicator is not included or NASRecovery is set to False, or if the UE receives RRC Connection Setup without NAS Recovery message, the UE does not derive a new KeNB/KgNB.

[0129] Option 2: If NoRootKeyDerivation indicator is included or NoRootKeyDerivation is set to TRUE, the UE does not derive a new KeNB/KgNB. Otherwise, the UE derives a new KeNB/KgNB.

[0130] Option 3: If RootKeyDerivation indicator is not included or RootKeyDerivation is set to FALSE, the UE does not derive a new KeNB/KgNB. Otherwise, the UE derives a new KeNB/KgNB.

[0131] Option 4: if the UE receives AS SMC without Root Key Derivation message, the UE does not derive a new KeNB/KgNB.

[0132] The UE derives Krrc-int and Krrc-enc according to current KeNB/KgNB and new integrity and ciphering algorithms indicated in AS SMC. The UE verifies AS SMC message according Krrc-int and new integrity algorithm.

[0133] 10. After successful verification, the UE may cipher and integrity protect the AS SMP message using Krrc-enc, Krrc-int, new ciphering and integrity algorithm. The UE sends the AS SMP message to the target gNB. Thus, UE and target gNB have successfully negotiate the security algorithm.

[0134] 11. The target gNB may send RRCConnectionReconfiguartion message to the UE to configurate the DRB. The target gNB may suspend the UE (send the RRCConnectionRelease message with suspend cause to the UE, for 4G), or send the UE to INACTIVE (send the RRCConnectionInactive message to the UE, for 5G).

[0135] Compared to current solution, this embodiment 1 adds new indicator in the current RRC message or involves new RRC message to tell the UE does not perform NAS recovery, and that will reduce some signaling.

Embodiment 2

[0136] Referring to FIG 3, in order to reduce the signaling, the target base station indicate the UE to reuse the AS security context (e.g. Kasme/Kamf), and derive a new key for the target base station base on the AS security context and non-access stratum (NAS) count. Specially, please refer to the following steps.

[0137] 0. Source eNB/gNB decides to suspend the UE (send the RRCConnectionRelease message with suspend cause to the UE, for 4G), or send the UE to INACTIVE (send the RRCConnectionInactive message to the UE, for 5G).

[0138] 1. The UE sends MSG3 (RRCConnectionResumeRequest message) to the target eNB/gNB to trigger resume procedure or INACTIVE to CONNECTED procedure to resume RRC connection.

[0139] 2. The target eNB/gNB sends Retreive UE Context Request message to the source eNB/gNB to fetch UE context.

[0140] 3. The source eNB/gNB sends Retreive UE Context Response message to the source eNB/gNB to response the message above. The Retreive UE Context Response may include UE security capability and old ciphering and integrity algorithms used between UE and source eNB/gNB.

[0141] 4. If the target eNB/gNB could not support old algorithms or if the target eNB/gNB prefers to use different algorithms, target eNB/gNB send a RRC Connection Setup message.

[0142] 5. There are three possible manners in sending RRC Connection Setup message.

[0143] Option 1: The target eNB/gNB sends RRC Connection Setup message to the UE. The RRC Connection Setup message includes NoNASRecovery indicator.

[0144] Option 2: The target eNB/gNB sends RRC Connection Setup message to the UE. The RRC Connection Setup message includes NASRecovery indicator.

[0145] Option 3: The target eNB/gNB sends RRC Connection Setup without NAS Recovery message to the UE.

[0146] 6. Corresponding to the step 5, there are three solutions.

[0147] Option 1: When the NoNASRecovery indicator is included or NoNASRecovery is set to TRUE, the UE does not indicate to upper layers that the RRC connection resume has been fallbacked, the UE keeps the current AS context, the UE could optionally discard the KgNB, Krrc-int, Krrc-enc, Kup-int (if exists), and Kup-enc (if exists) stored in UE AS context.

Otherwise, the UE discards the stored UE AS context and indicates to upper layers that the RRC connection resume has been fallbacked.

[0148] Option 2: When the NASRecovery indicator is included or NASRecovery is set to TRUE, the UE discards the stored UE AS context and indicates to upper layers that the RRC connection resume has been fallbacked. Otherwise, the UE does not indicate to upper layers that the RRC connection resume has been fallbacked, the UE keeps the current AS context, the UE could optionally discard the KgNB, Krrc-int, Krrc-enc, Kup-int (if exists), and Kup-enc (if exists) stored in UE AS context.

[0149] Option 3: When the UE receives RRC Connection Setup without NAS Recovery message from target eNB/gNB, the UE does not indicate to upper layers that the RRC connection resume has been fallbacked. The UE keeps the current AS context (e.g. Kasme/Kamf), the UE could optionally discard the KgNB, Krrc-int, Krrc-enc, Kup-int (if exists), and Kup-enc (if exists) stored in UE AS context.

[0150] It should be pointed out that the Kasme is a key in the 4G system, and the Kamf is a key in the 5G system.

[0151] 7. (Optional) The UE sends RRC Connection Setup Complete message to the target eNB/gNB.

[0152] 8. The target eNB/gNB decides to send S1/N2 message to the MME/AMF to request UE context.

[0153] 9. The mobility management entity (MME)/ Access and Mobility Management Function (AMF) derives KeNB/KgNB according to current Kasme/Kamf and current uplink NAS COUNT, and sends the KeNB/KgNB and UE security capability to the target eNB/gNB. Optionally, the MME/AMF may send the NAS COUNT or least significant bit (LSB) of NAS COUNT to the target eNB/gNB.

[0154] 10. The target eNB/gNB chooses the new ciphering and integrity algorithm which has the highest priority from its configured algorithm priority list and is also present in the UE security capability. The chosen algorithms are indicated to the UE in the AS SMC. The target eNB/gNB derives Krrc-int according to the KeNB/KgNB and new integrity algorithm. The AS SMC is integrity protected by Krrc-int and new integrity algorithm. Note that the UE could get the new algorithms in AS SMC, because it is not ciphered. Optionally, the target eNB/gNB may include the NAS COUNT or LSB of NAS COUNT in AS SMC.

[0155] 11. The UE derives KeNB/KgNB according to current Kasme/Kamf and current uplink NAS COUNT (Optionally, the UE may get NAS COUNT according to NAS COUNT or LSB of NAS COUNT in AS SMC), and derives Krrc-int and Krrc-enc according to KeNB/KgNB and new integrity and ciphering algorithms indicated in AS SMC. The UE verifies AS SMC message according Krrc-int and new integrity algorithm. After successful verification, the UE may cipher and integrity protect the AS SMP message using Krrc-enc, Krrc-int, new ciphering and integrity algorithm. The UE sends the AS SMP message to the target gNB. Thus, UE and target gNB have successfully negotiate the security algorithm.

[0156] 12. The target gNB may send RRCConnectionReconfiguartion message to the UE to configurate the DRB. The target gNB may suspend the UE (send the RRCConnectionRelease message with suspend cause to the UE, for 4G), or send the UE to INACTIVE (send the RRCConnectionInactive message to the UE, for 5G).

[0157] Compared to the current solution, this embodiment 2 adds new indicator in the current RRC message or involves new RRC message to tell the UE to reuse the AS context, and that will reduce NAS signaling.

Embodiment 3

[0158] Referring to FIG. 4, the method according to this embodiment of the present disclosure includes the following steps.

[0159] 0. Source eNB/gNB decides to suspend the UE (send the RRCConnectionRelease message with suspend cause to the UE, for 4G), or send the UE to INACTIVE (send the RRCConnectionInactive message to the UE, for 5G).

[0160] 1. The UE sends MSG3 (RRCConnectionResumeRequest message) to the target eNB/gNB to trigger resume procedure or INACTIVE to CONNECTED procedure to resume RRC connection.

[0161] 2. The target eNB/gNB sends Retreive UE Context Request message to the source eNB/gNB to fetch UE context.

[0162] 3. The source eNB/gNB sends Retreive UE Context Response message to the source eNB/gNB to response the message above. The Retreive UE Context Response may include UE security capability and old ciphering and integrity algorithms used between UE and source eNB/gNB.

[0163] 4. If the target eNB/gNB could not support old algorithms or if the target eNB/gNB prefers to use different algorithms, the target eNB/gNB chooses the new ciphering and integrity algorithm which has the highest priority from its configured algorithm priority list and is also present in the UE security capability.

[0164] 5. Target gNB/eNB sends RRCConnectionReject message to the UE. The message includes the new algorithms.

[0165] 6. The UE stores new algorithms, and sends MSG3 again immediately if new algorithms are included.

[0166] 7. The UE sends MSG3 to the target eNB/gNB. Optionally, the MSG3 could include new resume cause, e.g. security negotiation complete.

[0167] 8. Option 1: When target eNB/gNB sends RRCConnectionReject message to the UE, the target eNB/gNB will maintain a state for the new algorithm, e.g. 1, the target eNB/gNB start a timer, when the target eNB/gNB receives MSG3, and the timer is not expired, the target eNB/gNB uses new integrity and ciphering algorithms to protect MSG4. E.g. 2, the target eNB/gNB logs security negotiation indication in the UE context, when the target eNB/gNB receives MSG3, the target eNB/gNB uses new integrity and ciphering algorithms to protect MSG4 if there is security negotiation indicator.

[0168] Option 2: If resume cause indicates security negotiation complete, the target eNB/gNB uses new integrity and ciphering algorithms to protect MSG4.

[0169] Note that target eNB/gNB may not maintain UE context when rejecting the UE, so, the target eNB/gNB may need to perform step 2-3 again to fetch UE context. It is also possible that the target eNB/gNB maintains the UE context.

[0170] The target eNB/gNB derives Krrc-int and Krrc-enc according to the KeNB/KgNB and new integrity and ciphering algorithm. The MSG4 is integrity protected by Krrc-int and new integrity algorithm and is ciphered by Krrc-enc and new ciphering algorithm. MSG4 could be RRCConnectionResume message, RRCConnectionRelease message with suspend cause, and RRCConnectionInactive message, etc.

[0171] 9. The UE derives Krrc-int and Krrc-enc according to KeNB/KgNB and stored new integrity and ciphering algorithms indicated in RRCConnectionReject message. The UE verifies and deciphers MSG4 according Krrc-int, Krrc-enc and new integrity and ciphering algorithm.

[0172] Compared to the current solution, this embodiment 3 adds new algorithms in the RRCConnectionReject message to tell the UE the new algorithm, and that will reduce AS signalling (3 RRC), NAS signalling (1 NAS), and S1/N2 signalling (2 S1/N2).

Embodiment 4

[0173] Referring to FIG 5, the method according to this embodiment of the present disclosure includes the following steps.

[0174] 0. Source eNB/gNB decides to suspend the UE (send the RRCConnectionRelease message with suspend cause to the UE, for 4G), or send the UE to INACTIVE (send the RRCConnectionInactive message to the UE, for 5G).

[0175] 1. Optionally, the UE could compute shortResumeMAC-I according to old algorithms. Other inputs may be needed, i.e. source physical cell identifier (PCI), source cell radio network temporary identifier (C-RNTI), target cell ID.

[0176] 2. The UE sends MSG3 (RRCConnectionResumeRequest message) to the target eNB/gNB to trigger resume procedure or INACTIVE to CONNECTED procedure to resume RRC connection. The old algorithms are included in MSG3.

[0177] 3. If the target eNB/gNB could not support the old algorithms,

[0178] 4. The target eNB/gNB sends RRC Connection Setup message to the UE to proceed with RRC connection establishment as if the UE was in RRC_IDLE (fallback procedure).

[0179] 5. The UE discards the stored UE AS context and indicates to upper layers that the RRC connection resume has been fallbacked. The UE sends initial NAS message (e.g. Service Request message) to the MME/AMF.

[0180] 6. The MME/AMF derives KeNB/KgNB according to current Kasme/Kamf and uplink NAS COUNT indicated by initial NAS message, and sends the KeNB/KgNB and UE security capability in Initial Context Setup Request message to the target eNB/gNB.

[0181] 7. The target eNB/gNB chooses the new ciphering and integrity algorithm which has the highest priority from its configured algorithm priority list and is also present in the UE security capability. The chosen algorithms are indicated to the UE in the AS SMC. The target eNB/gNB derives Krrc-int according to the KeNB/KgNB and new integrity algorithm. The AS SMC is integrity protected by Krrc-int and new integrity algorithm. Note that the UE could get the new algorithms in AS SMC, because it is not ciphered.

[0182] 8. The UE derives KeNB/KgNB according to current Kasme/Kamf and uplink NAS COUNT indicated by initial NAS message, and derives Krrc-int and Krrc-enc according to KeNB/KgNB and new integrity and ciphering algorithms indicated in AS SMC. The UE verifies AS SMC message according Krrc-int and new integrity algorithm. After successful verification, the UE may cipher and integrity protect the AS SMP message using Krrc-enc, Krrc-int, new ciphering and integrity algorithm. The UE sends the AS SMP message to the target gNB. Thus, UE and target gNB have successfully negotiate the security algorithm.

[0183] 9. The target gNB may send RRCConnectionReconfiguartion message to the UE to configurate the DRB. The target gNB may suspend the UE (send the RRCConnectionRelease message with suspend cause to the UE, for 4G), or send the UE to INACTIVE (send the RRCConnectionInactive message to the UE, for 5G).

[0184] Compared to current solution, this embodiment 4 adds new IE in the MSG3 to tell the target eNB/gNB the old algorithm, if it is not supported by the target eNB/gNB, the target eNB/gNB will fallback UE to IDLE directly, and that will reduce several signaling.

[0185] FIG. 6 is a simplified block diagram of a base station according to an embodiment of the present disclosure (the structure of a target base station or a source base station that is described in any one of embodiments 1 to 4 can be referred to the FIG. 6). The base station 60 in FIG. 6 may be configured to implement steps and methods in the foregoing method embodiments (embodiments 1 to 4). The base station 60 in FIG. 6 includes a processor 61, a memory 62, a receiver circuit 63, and a transmitter circuit 64. The processor 61, the memory 62, and the receiver circuit 63 are connected using a bus system 66.

[0186] In addition, the base station 60 may further include an antenna 65, and the like. The processor 61 controls an operation of the base station 60. The memory 62 may include a read-only memory and a random access memory, and may provide an instruction and data for the processor 61. A part of the memory 62 may further include a nonvolatile random access memory (NVRAM). In a specific application, the transmitter circuit 64 and the receiver circuit 63 may be coupled to the antenna 65. All components of the base station 60 are coupled together using the bus system 66. In addition to a data bus, the bus system 66 includes a power bus, a control bus, and a status signal bus. However, for clarity of description, various buses are marked as the bus system 66 in the figure.

[0187] The processor 61 may be an integrated circuit chip and has a signal processing capability. The foregoing processor 61 may be a general-purpose processor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), a field programmable gate array (FPGA), or another programmable logic device, a discrete gate or a transistor logic device, or a discrete hardware component, which may implement or perform the methods, the steps, and the logical block diagrams disclosed in the embodiments of the present disclosure. The general-purpose processor may be a microprocessor, or the processor may be any conventional processor, or the like. The processor 61 reads information in the memory 62, and controls all parts of the base station 60 in combination with hardware of the processor 61.

[0188] FIG. 7 is a simplified block diagram of a user equipment device according to an embodiment of the present disclosure (the structure of a user equipment which is described in any one of embodiments 1 to 4 can be referred to the FIG. 7). The user equipment 70 in FIG. 10 may be configured to implement steps and methods in the foregoing method embodiments 1-4. The user equipment 70 in FIG. 10 includes a processor 71, a memory 72, a receiver circuit 73, and a transmitter circuit 74. The processor 71, the memory 72, and the receiver circuit 73 are connected using a bus system 76.

[0189] In addition, the user equipment 70 may further include an antenna 75, and the like. The processor 71 controls an operation of the user equipment 70. The memory 72 may include a read-only memory and a random access memory, and may provide an instruction and data for the processor 71. A part of the memory 72 may further include a NVRAM. In a specific application, the transmitter circuit 74 and the receiver circuit 73 may be coupled to the antenna 75. All components of the user equipment 70 are coupled together using the bus system 76. In addition to a data bus, the bus system 76 includes a power bus, a control bus, and a status signal bus. However, for clarity of description, various buses are marked as the bus system 76 in the figure.

[0190] The processor 71 may be an integrated circuit chip and has a signal processing capability. The foregoing processor 71 may be a general-purpose processor, a DSP, an ASIC, a FPGA, or another programmable logic device, a discrete gate or a transistor logic device, or a discrete hardware component, which may implement or perform the methods, the steps, and the logical block diagrams disclosed in the embodiments of the present disclosure. The general-purpose processor may be a microprocessor, or the processor may be any conventional

processor, or the like. The processor 71 reads information in the memory 72, and controls all parts of the user equipment 70 in combination with hardware of the processor 71.

[0191] It should be understood that "an embodiment" mentioned in the whole specification does not mean that particular features, structures, or features related to the embodiment are included in at least one embodiment of the present disclosure. Therefore, "in an embodiment" appearing throughout the specification does not refer to a same embodiment. In addition, these particular features, structures, or features may be combined in one or more embodiments using any appropriate manner. Sequence numbers of the foregoing processes do not mean execution sequences in various embodiments of the present disclosure. The execution sequences of the processes should be determined according to functions and internal logic of the processes, and should not be construed as any limitation on the implementation processes of the embodiments of the present disclosure.

[0192] In addition, the terms "system" and "network" may be used interchangeably in this specification. The term "and/or" in this specification describes only an association relationship for describing associated objects and represents that three relationships may exist. For example, A and/or B may represent the following three cases: Only A exists, both A and B exist, and only B exists. In addition, the character "/" in this specification generally indicates an "or" relationship between the associated objects.

[0193] It should be understood that in the embodiments of the present disclosure, "B corresponding to A" indicates that B is associated with A, and B may be determined according to A. However, it should further be understood that determining A according to B does not mean that B is determined according to A only; that is, B may also be determined according to A and/or other information.

[0194] A person of ordinary skill in the art may be aware that, in combination with the examples described in the embodiments disclosed in this specification, units and algorithm steps may be implemented by electronic hardware, computer software, or a combination thereof. To clearly describe the interchangeability between the hardware and the software, the foregoing has generally described compositions and steps of each example according to functions. Whether the functions are performed by hardware or software depends on particular applications and design constraint conditions of the technical solutions. A person skilled in the art may use different

methods to implement the described functions for each particular application, but it should not be considered that the implementation goes beyond the scope of the present disclosure.

[0195] It may be clearly understood by a person skilled in the art that, for the purpose of convenient and brief description, for a detailed working process of the foregoing system, apparatus, and unit, reference may be made to a corresponding process in the foregoing method embodiments, and details are not described herein again.

[0196] In the several embodiments provided in the present application, it should be understood that the disclosed system, apparatus, and method may be implemented in other manners. For example, the described apparatus embodiment is merely an example. For example, the unit division is merely logical function division and may be other division in actual implementation. For example, a plurality of units or components may be combined or integrated into another system, or some features may be ignored or not performed. In addition, the displayed or discussed mutual couplings or direct couplings or communication connections may be implemented through some interfaces. The indirect couplings or communication connections between the apparatuses or units may be implemented in electronic, mechanical, or other forms.

[0197] With descriptions of the foregoing embodiments, a person skilled in the art may clearly understand that the present disclosure may be implemented by hardware, firmware or a combination thereof. When the present disclosure is implemented by software, the foregoing functions may be stored in a computer-readable medium or transmitted as one or more instructions or code in the computer-readable medium. The computer-readable medium includes a computer storage medium and a communications medium, where the communications medium includes any medium that enables a computer program to be transmitted from one place to another. The storage medium may be any available medium accessible to a computer.

[0198] The following is used as an example but is not limited: The computer readable medium may include a random access memory (RAM), a read-only memory (ROM), an electrically erasable programmable read-only memory (EEPROM), a compact disc read-only memory (CD-ROM) or other optical disk storage, a disk storage medium or other disk storage, or any other medium that can be used to carry or store expected program code in a command or data structure form and can be accessed by a computer. In addition, any connection may be appropriately defined as a computer-readable medium.

[0199] For example, if software is transmitted from a website, a server or another remote source using a coaxial cable, an optical fiber/cable, a twisted pair, a digital subscriber line (DSL) or wireless technologies such as infrared ray, radio and microwave, the coaxial cable, optical fiber/cable, twisted pair, DSL or wireless technologies such as infrared ray, radio and microwave are included in fixation of a medium to which they belong.

[0200] For example, a disk and disc used by the present disclosure includes a compact disc (CD), a laser disc, an optical disc, a digital versatile disc (DVD), a floppy disk and a Blu-ray disc, where the disk generally copies data by a magnetic means, and the disc copies data optically by a laser means. The foregoing combination should also be included in the protection scope of the computer-readable medium.

[0201] In summary, what is described above is merely an example of embodiments of the technical solutions of the present disclosure, but is not intended to limit the protection scope of the present disclosure. Any modification, equivalent replacement, or improvement made without departing from the spirit and principle of the present disclosure shall fall within the protection scope of the present disclosure.

CLAIMS

What is claimed is:

1. A method for security algorithm negotiation, comprising:

receiving, by a user equipment device (UE), a first request message from a target base station;

reserving, by the UE, a first key which is derived for a source base station in response to the first request message;

receiving, by the UE, a second request message from the target base station, wherein the second request message comprise a identity which is used to indicate an algorithm; and

deriving, by the UE, a second key based on the first key and the algorithm corresponding to the identity.

2. The method according to claim 1, wherein the first request message comprises a first indicator; and the method further comprises:

deleting, by the UE, security keys which are derived from the first key based on the first indicator.

3. The method according to claim 2, further comprising:

stop triggering, by the UE, a non-access stratum recovery process based on the first indicator.

4. The method according to claim 1, further comprising:

stop triggering, by the UE, a non-access stratum recovery process in response to the first request message.

5. The method according to claim 1, wherein the second request message comprises a second indicator; and wherein the method further comprises:

stop deriving, by the UE, a key for the target base station based on the second indicator.

6. The method according to claim 1, further comprising:

sending, by the UE, a first response message to the target base station in response to the first request message.

7. The method according to claim 1, further comprising:

verifying, by the UE, the second request message;

protecting, by the UE, a second response message base on the second key and the algorithm corresponding to the identity when the second request message is verified successfully; and

sending, by the UE, the protected second response message to the target base station.

8. A method for security algorithm negotiation, comprising:

sending, by a target base station, a first request message from a user equipment device (UE), wherein the first request message instructs the UE to reserve a first key which is derived for a source base station;

sending, by the target base station, a second request message to the UE; wherein the second request message comprises an identity which is used to indicate an algorithm; and

receiving, by the target base station, a second response message from the UE.

9. The method according to claim 8, wherein the first request message comprises a first indicator; wherein the first indicator instructs the UE to delete security keys which are derived from the first key.

10. The method according to claim 9, wherein the first indicator further instructs the UE not to trigger a non-access stratum recovery process.

11. The method according to claim 8, wherein the second request message comprises a second indicator; wherein the second indicator instructs the UE not to derive a key for the target base station.

12. A user equipment device (UE), comprising a receiver and a processor;

wherein the receiver is configured to receive a first request message from a target base station; and receive a second request message from a target base station, wherein the second request message comprise a identity which is used to indicate an algorithm; and

wherein the processor is configured to reserve a first key which is derived for a source base station in response to the first request message, and deriving a second key based on the first key and an algorithm corresponding to the identity.

13. The user equipment according to claim 12, wherein the first request message comprises a first indicator; and the processor is further configured to delete security keys which are derived from the first key based on the first indicator.

14. The user equipment according to claim 13, wherein the processor is further configured to stop triggering a non-access stratum recovery process based on the first indicator.

15. The user equipment according to claim 12, wherein the processor is further configured to stop triggering a Non-access stratum recovery process in response to the first request message.

16. The user equipment according to claim 12, wherein the second request message comprises a second indicator; and the processor is further configured to stop deriving a key for the target base station based on the second indicator.

17. The user equipment according to claim 12, further comprising a transmitter coupled to the processor, wherein the transmitter is configured to send a first response message to the target base station in response to the first request message.

18. The user equipment according to claim 12, further comprising a transmitter coupled to the processor;

wherein the processor is further configured to verify the second request message; and protect a second response message base on the second key and the algorithm corresponding to the identity when the second request message is verified successfully; and

wherein the transmitter is configured to send the protected second response message to the target base station.

19. A base station, comprising a transmitter and a receiver;

wherein the transmitter is configured to:

send a first request message to a user equipment device(UE), wherein the first request message instructs the UE to reserve a first key which is derived for a source base station; and

send a second request message to the UE, wherein the second request message comprises an identity which is used to indicate an algorithm; and

wherein the receiver circuit is configured to:

receive a second response message from the UE.

20. The base station according to claim 19, wherein the first request message comprises a first indicator; wherein the first indicator instructs the UE to delete security keys which are derived from the first key.

21. The base station according to claim 20, wherein the first indicator further instructs the UE not to trigger a non-access stratum recovery process.

22. The base station according to claim 19, wherein the second request message comprises a second indicator; wherein the second indicator instructs the UE not to derive a key for the target base station.

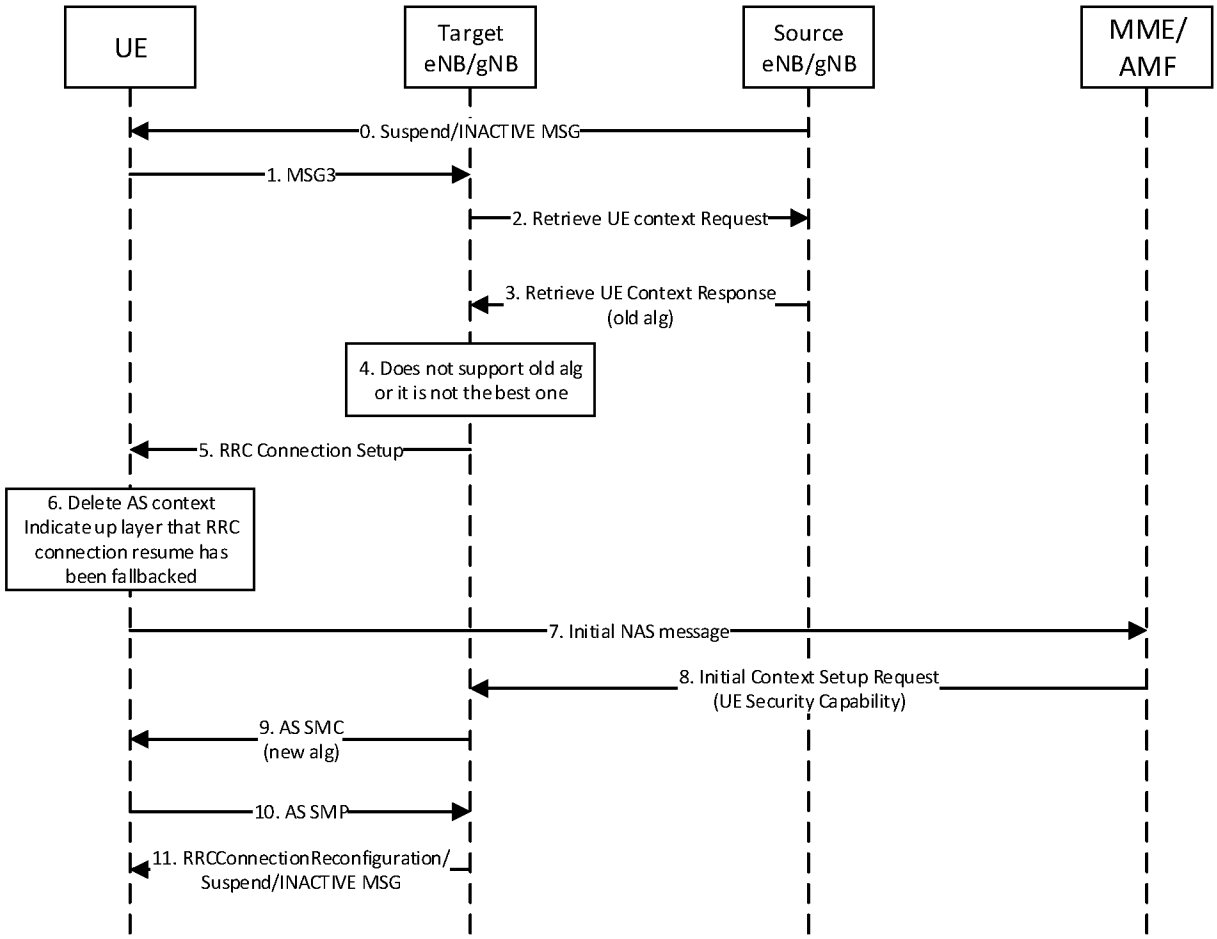
UE
Target eNB/gNB
Source eNB/gNB
MME/ AMF
0. Suspend/INACTIVE MSG
1. MSG3
2. Retrieve UE context Request
3. Retrieve UE Context Response (old alg)
4. Does not support old alg or it is not the best one
5. RRC Connection Setup
6. Delete AS context Indicate up layer that RRC connection resume has been fallbacked
7. Initial NAS message
8. Initial Context Setup Request (UE Security Capability)
9. AS SMC (new alg)
10. AS SMP
11. RRCConnectionReconfiguration/ Suspend/INACTIVE MSG

FIG. 1

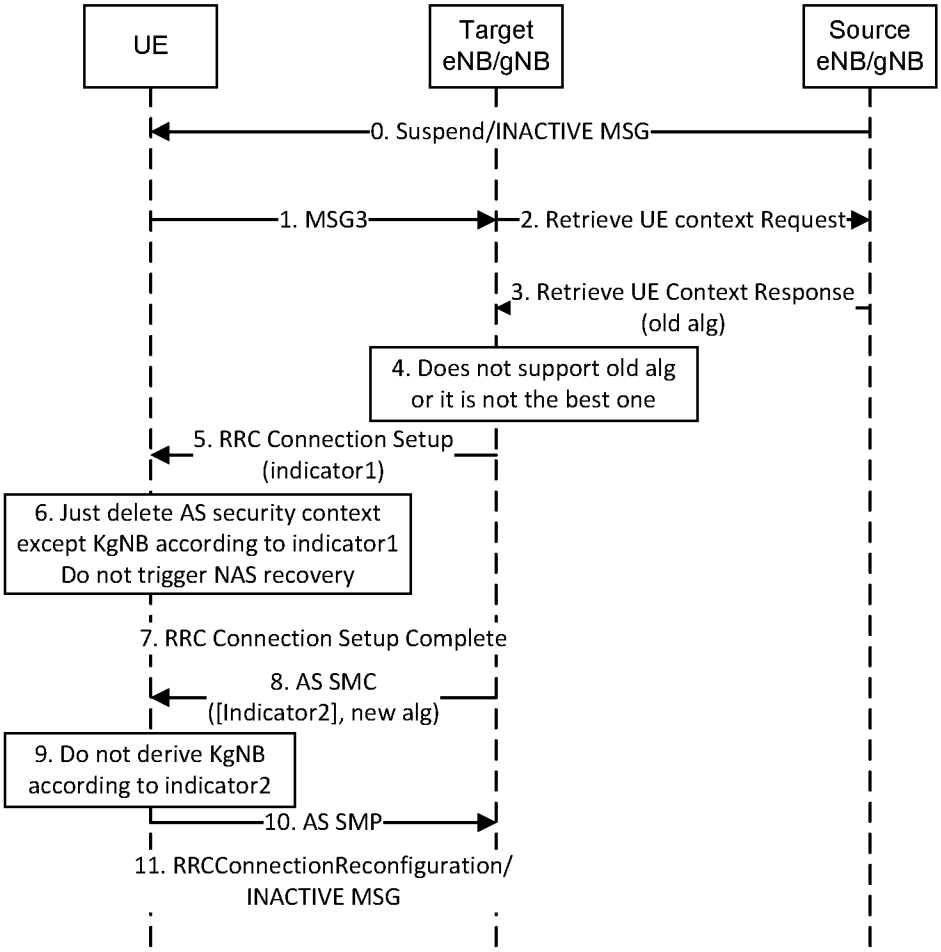
UE
Target eNB/gNB
Source eNB/gNB
0. Suspend/INACTIVE MSG
1. MSG3
2. Retrieve UE context Request
3. Retrieve UE Context Response (old alg)
4. Does not support old alg or it is not the best one
5. RRC Connection Setup (indicator1)
6. Just delete AS security context except KgNB according to indicator1 Do not trigger NAS recovery
7. RRC Connection Setup Complete
8. AS SMC ([Indicator2], new alg)
9. Do not derive KgNB according to indicator2
10. AS SMP
11. RRCConnectionReconfiguration/ INACTIVE MSG

FIG. 2

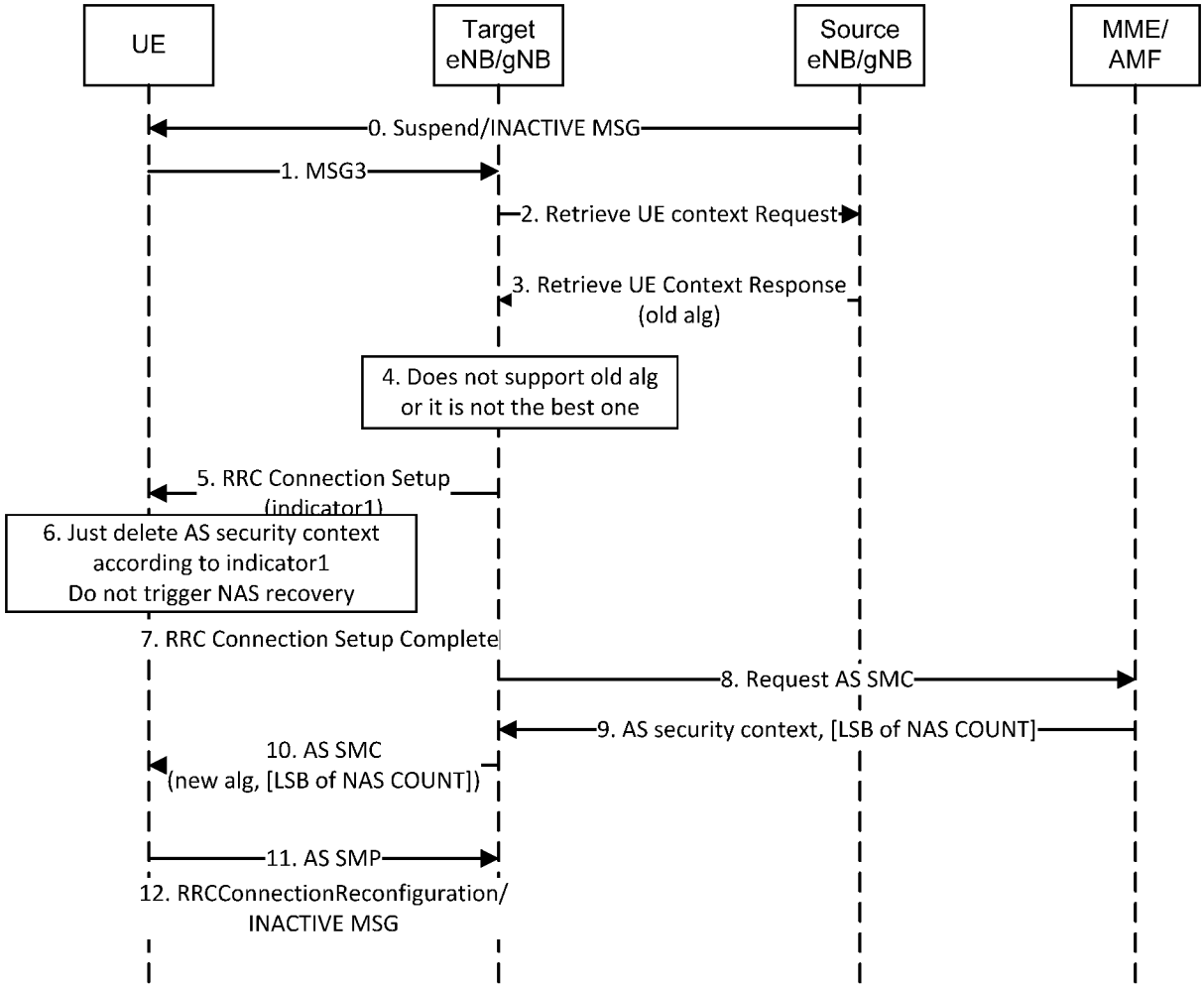
UE
Target eNB/gNB
Source eNB/gNB
MME/ AMF
0. Suspend/INACTIVE MSG
1. MSG3
2. Retrieve UE context Request
3. Retrieve UE Context Response (old alg)
4. Does not support old alg or it is not the best one
5. RRC Connection Setup (indicator1)
6. Just delete AS security context according to indicator1 Do not trigger NAS recovery
7. RRC Connection Setup Complete
8. Request AS SMC
9. AS security context, [LSB of NAS COUNT]
10. AS SMC (new alg, [LSB of NAS COUNT])
11. AS SMP
12. RRCConnectionReconfiguration/ INACTIVE MSG

FIG. 3

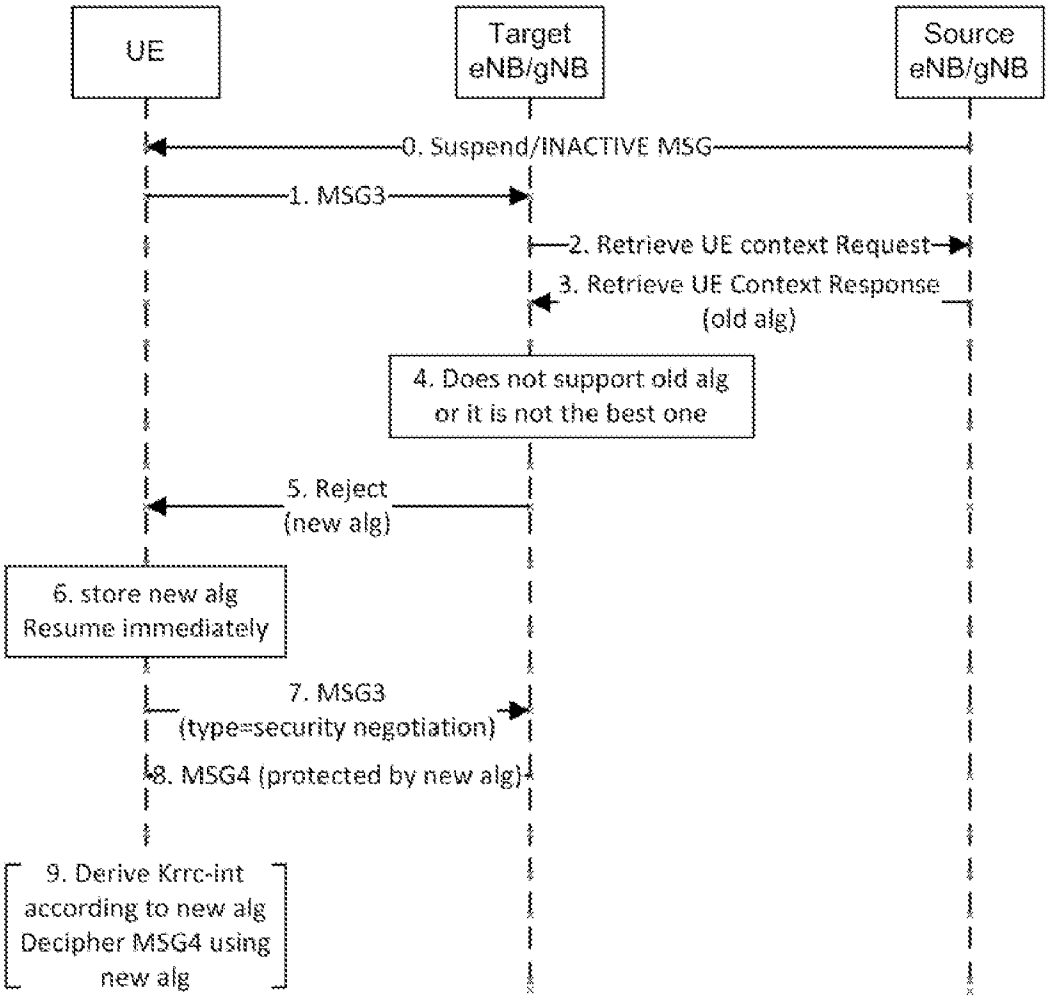
UE
Target eNB/gNB
Source eNB/gNB
0. Suspend/INACTIVE MSG
1. MSG3
2. Retrieve UE context Request
3. Retrieve UE Context Response (old alg)
4. Does not support old alg or it is not the best one
5. Reject (new alg)
6. store new alg Resume immediately
7. MSG3 (type=security negotiation)
8. MSG4 (protected by new alg)
9. Derive Krrc-int according to new alg Decipher MSG4 using new alg

FIG. 4

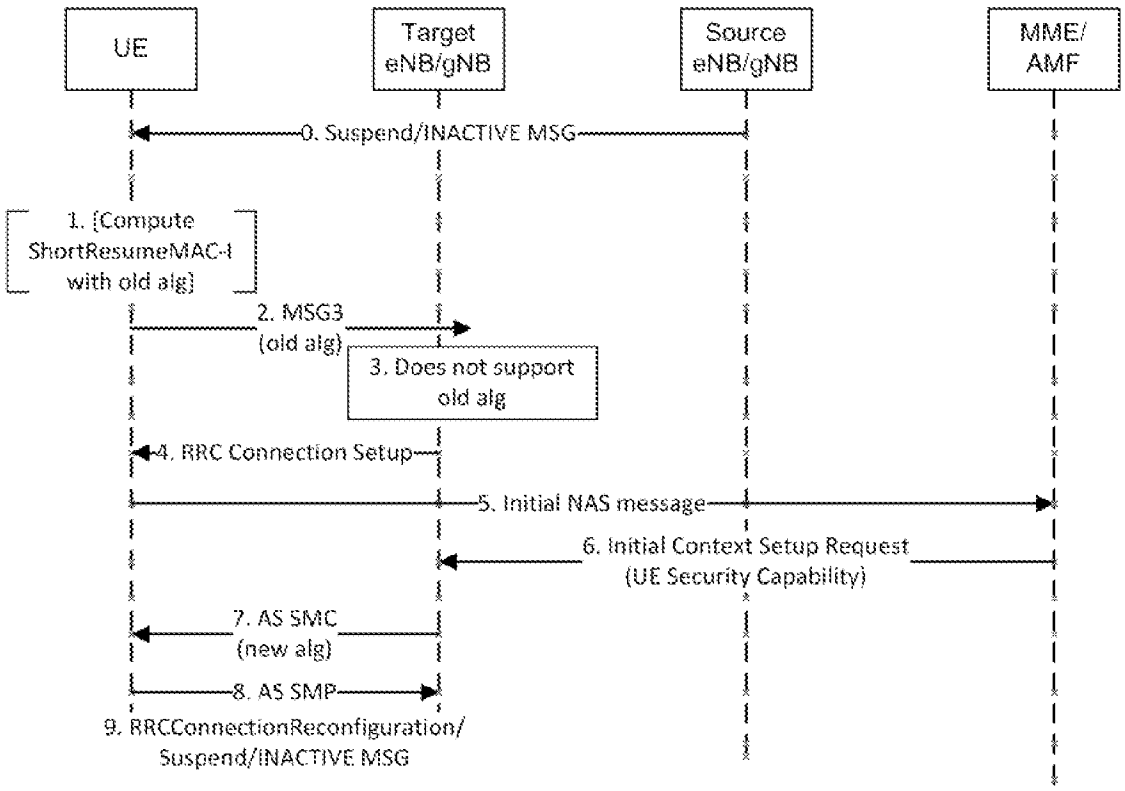
UE
Target eNB/gNB
Source eNB/gNB
MME/ AMF
0. Suspend/INACTIVE MSG
1. {Compute ShortResumeMAC-I with old alg}
2. MSG3 (old alg)
3. Does not support old alg
4. RRC Connection Setup
5. Initial NAS message
6. Initial Context Setup Request (UE Security Capability)
7. AS SMC (new alg)
8. AS SMP
9. RRCConnectionReconfiguration/ Suspend/INACTIVE MSG

FIG. 5

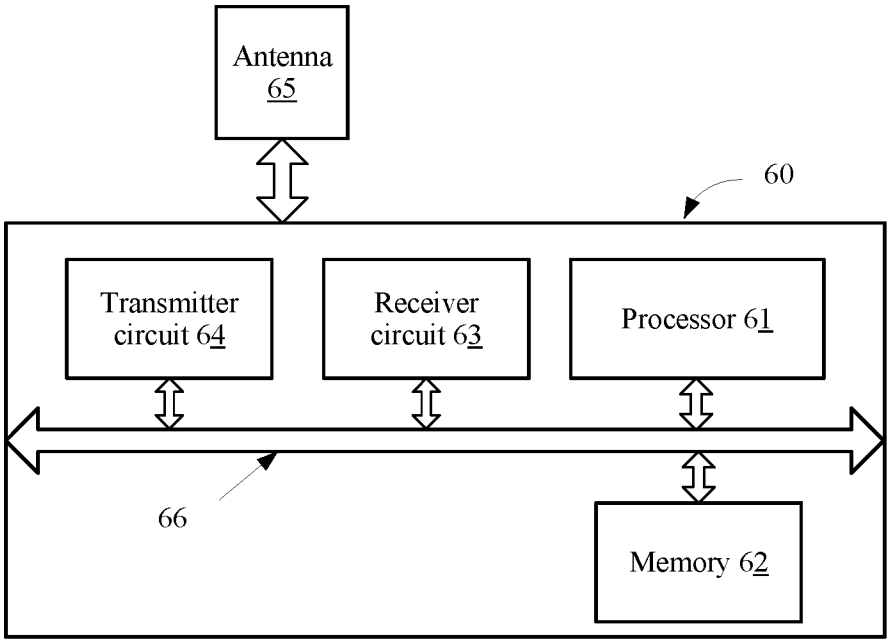
Antenna
65
60
Transmitter
circuit 64
Receiver
circuit 63
Processor 61
66
Memory 62

FIG. 6

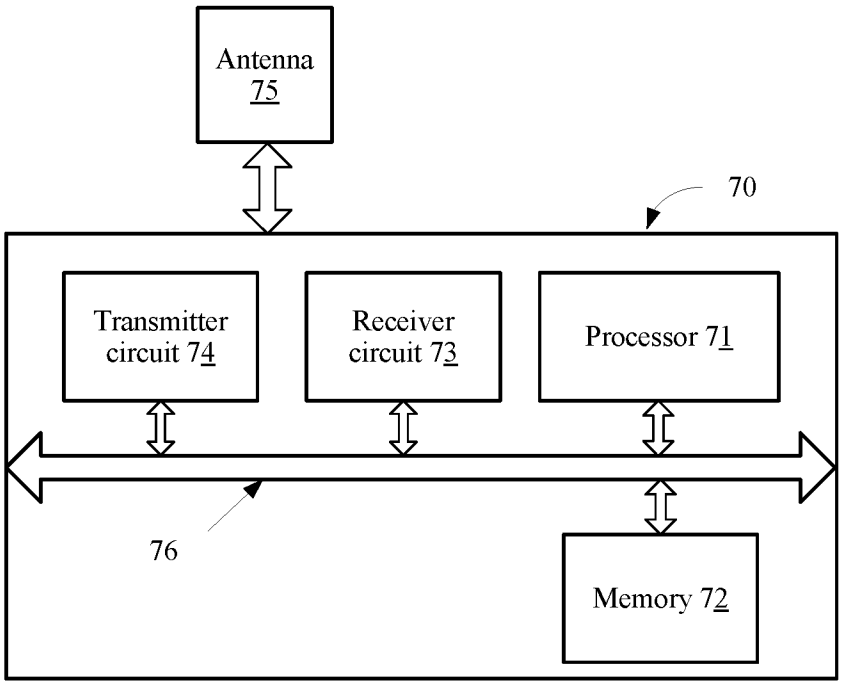
Antenna
75
70
Transmitter
circuit 74
Receiver
circuit 73
Processor 71
76
Memory 72

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/090860

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/00(2009.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; H04L

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

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

WPI; EPODOC; CNKI; CNPAT; 3GPP: KeNB, KgNB, target, source, eNB, gNB, NAS recovery, non-access stratum recovery, RRC connection setup message, indicator, algorithm, krrc-int, krrc-enc

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"3GPP TS 33.501 V15.0.0 (2018-03)" *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system(Release 15)*, 26 March 2018 (2018-03-26), section 6.7.3.1	1-22
A	CN 102238668 A (BEIJING SAMSUNG COMMUNICATION TECHNOLOGY R&D CO., LTD. ET AL.) 09 November 2011 (2011-11-09) the whole document	1-22
A	WO 2018028650 A (HUAWEI TECHNOLOGIES CO., LTD.) 15 February 2018 (2018-02-15) the whole document	1-22
A	WO 2018079692 A1 (NEC CORPORATION) 03 May 2018 (2018-05-03) the whole document	1-22

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 August 2019	**11 September 2019**

Name and mailing address of the ISA/CN	Authorized officer
National Intellectual Property Administration, PRC **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing** **100088** **China**	**LIU,Qingfeng**
Facsimile No. **(86-10)62019451**	Telephone No. **53961581**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/090860

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	102238668	A	09 November 2011	EP	2567573	A2	13 March 2013
				US	2011274086	A1	10 November 2011
				KR	20110123662	A	15 November 2011
				WO	2011139096	A2	10 November 2011
WO	2018028650	A	15 February 2018	CN	109479336	A	15 March 2019
				EP	3485694	A1	22 May 2019
				US	2018049261	A1	15 February 2018
WO	2018079692	A1	03 May 2018	None			