

(51) International Patent Classification:
H04L 29/02 (2006.01)(21) International Application Number:
PCT/CN2019/081766(22) International Filing Date:
08 April 2019 (08.04.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/655,319 10 April 2018 (10.04.2018) US
62/660,280 20 April 2018 (20.04.2018) US(71) Applicant: **MEDIATEK SINGAPORE PTE. LTD.**
[SG/SG]; #03-01 Solaris, No.1 Fusionopolis Walk, Singapore 138628 (SG).(71) Applicant (for AO only): **MEDIATEK INC.** [CN/CN];
No.1, Dusing Rd. 1st, Science-Based Industrial Park, Hsin-Chu, Taiwan 300 (CN).(72) Inventors: **MOISANEN, Matti**; Elektronikkatie 16, FI-Oulu (FI). **SITOMANIEMI, Jaakko**; Elektronikkatie 16, FI-Oulu (FI). **AKSELIN, Marko Tapani**; Elektronikkatie 16, FI-Oulu (FI). **ESKELINEN, Jarkko**; Elektronikkatie16, FI-Oulu (FI). **NIEMI, Marko**; Elektronikkatie 16, FI-Oulu (FI).(74) Agent: **BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.**; 16th Fl., Block A, Corporate Square, No.35 Jinrong Street, Beijing 100033 (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: IMPROVEMENT FOR INCORRECT KSI HANDLING IN MOBILE COMMUNICATIONS

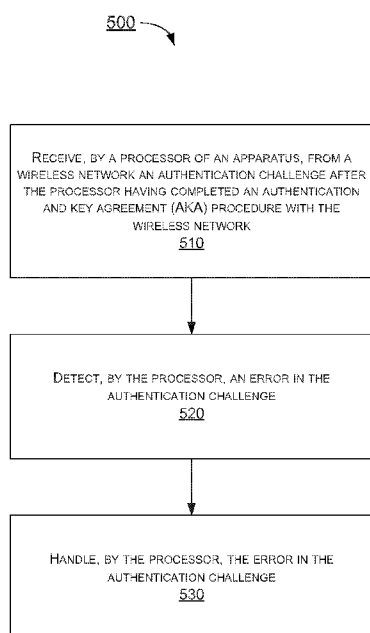


FIG. 5

(57) Abstract: Various examples pertaining to improvement for incorrect key set identifier (KSI) handling in mobile communications are described. An apparatus (e.g., user equipment) receives from a wireless network an authentication challenge after the processor having completed an authentication and key agreement (AKA) procedure with the wireless network. The apparatus detects an error in the authentication challenge and handles the error in the authentication challenge. For example, the apparatus can reject the authentication challenge responsive to detecting the error. Alternatively, the apparatus can accept the authentication challenge.

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))*

IMPROVEMENT FOR INCORRECT KSI HANDLING IN MOBILE COMMUNICATIONS

CROSS REFERENCE TO RELATED PATENT APPLICATION(S)

5 [0001]The present disclosure is part of a non-provisional application claiming the priority benefit of U.S. Patent Application Nos. 62/655,319 and 62/660,280, filed on 10 April 2018 and 20 April 2018, respectively. The contents of aforementioned applications are herein incorporated by reference in their entirety.

TECHNICAL FIELD

10 [0002]The present disclosure is generally related to mobile communications and, more particularly, to improvement for incorrect key set identifier (KSI) handling in mobile communications.

BACKGROUND

15 [0003]Unless otherwise indicated herein, approaches described in this section are not prior art to the claims listed below and are not admitted as prior art by inclusion in this section.

[0004]According to the current 3rd-Generation Partnership Project (3GPP) specification for 5th-Generation (5G) New Radio (NR) mobile communications, the 5G security context is indicated by a key set identifier for 5G (ngKSI). A user equipment (UE) and a network can have valid native or mapped 5G security context stored. This can be used to secure non-access stratum (NAS) messages when a new call-initiated (N1) NAS signaling
20 connection is established.

SUMMARY

[0005]The following summary is illustrative only and is not intended to be limiting in any way. That is, the following summary is provided to introduce concepts, highlights, benefits and advantages of the novel and
25 non-obvious techniques described herein. Select implementations are further described below in the detailed description. Thus, the following summary is not intended to identify essential features of the claimed subject matter, nor is it intended for use in determining the scope of the claimed subject matter.

[0006]In one aspect, a method may involve a processor of an apparatus receiving, from a wireless network, an authentication challenge after the processor having completed an authentication and key agreement (AKA)
30 procedure with the wireless network. The method may also involve the processor detecting an error in the authentication challenge. The method may further involve the processor rejecting the authentication challenge responsive to detecting the error.

[0007]In one aspect, a method may involve a processor of an apparatus receiving, from a wireless network, an authentication challenge after the processor having completed an authentication and key agreement (AKA)
35 procedure with the wireless network. The method may also involve the processor detecting an error in the authentication challenge. The method may further involve the processor accepting the authentication challenge.

[0008]In one aspect, a method may involve a processor of an apparatus receiving, from a wireless network, an authentication challenge after the processor having completed an authentication and key agreement (AKA) procedure with the wireless network. The method may also involve the processor detecting an error in the

authentication challenge. The method may further involve the processor handling the error in the authentication challenge.

[0009] It is noteworthy that, although description provided herein may be in the context of certain radio access technologies, networks and network topologies such as New Radio (NR) or non-3GPP access in 5G system, the proposed concepts, schemes and any variation(s)/derivative(s) thereof may be implemented in, for and by other types of radio access technologies, networks and network topologies such as, for example and without limitation, Evolved Packet System (EPS), Universal Terrestrial Radio Access Network (UTRAN), Evolved UTRAN (E-UTRAN), Global System for Mobile communications (GSM), General Packet Radio Service (GPRS)/Enhanced Data rates for Global Evolution (EDGE) Radio Access Network (GERAN), Long-Term Evolution (LTE), LTE-Advanced, LTE-Advanced Pro, Internet-of-Things (IoT) and Narrow Band Internet of Things (NB-IoT). Thus, the scope of the present disclosure is not limited to the examples described herein.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The accompanying drawings are included to provide a further understanding of the disclosure and are incorporated in and constitute a part of the present disclosure. The drawings illustrate implementations of the disclosure and, together with the description, serve to explain the principles of the disclosure. It is appreciable that the drawings are not necessarily in scale as some components may be shown to be out of proportion than the size in actual implementation in order to clearly illustrate the concept of the present disclosure.

[0011] FIG. 1 is a diagram of an example scenario in which various solutions in accordance with the present disclosure may be implemented.

[0012] FIG. 2 is a block diagram of an example communication system in accordance with an implementation of the present disclosure.

[0013] FIG. 3 is a flowchart of an example process in accordance with an implementation of the present disclosure.

[0014] FIG. 4 is a flowchart of an example process in accordance with an implementation of the present disclosure.

[0015] FIG. 5 is a flowchart of an example process in accordance with an implementation of the present disclosure.

DETAILED DESCRIPTION OF PREFERRED IMPLEMENTATIONS

[0016] Detailed embodiments and implementations of the claimed subject matters are disclosed herein. However, it shall be understood that the disclosed embodiments and implementations are merely illustrative of the claimed subject matters which may be embodied in various forms. The present disclosure may, however, be embodied in many different forms and should not be construed as limited to the exemplary embodiments and implementations set forth herein. Rather, these exemplary embodiments and implementations are provided so that description of the present disclosure is thorough and complete and will fully convey the scope of the present disclosure to those skilled in the art. In the description below, details of well-known features and techniques may be omitted to avoid unnecessarily obscuring the presented embodiments and implementations.

Overview

[0017]According to the 3GPP specification, if an ngKSI is contained in an initial NAS message during a 5G Mobility Management (5GMM) procedure, a 5G NR mobile network is to include a different ngKSI value in an authentication request message when the network initiates a 5G authentication and key agreement (AKA)-based primary authentication and key agreement procedure. Moreover, according to the 3GPP specification, if the 5G AKA-based primary authentication and key agreement procedure has been completed successfully and the related ngKSI is stored in the 5G System (5GS) security context of the network, the network is to include a different ngKSI value in the authentication request message when the network initiates a new 5G AKA-based primary authentication and key agreement procedure.

[0018]Additionally, according to the 3GPP specification, the UE can reject a 5G authentication challenge sent by the network if the UE detects authentication challenge parameters to be incorrect. That is, the UE may reject the core network due to an incorrect authentication challenge parameter such as, for example, medium access control (MAC) code failure, non-Evolved Packet System (non-EPS) authentication not accepted (e.g., incorrect “separate bit”), synchronization failure (e.g., SQN failure). However, in such cases, the UE has no means to reject the authentication if the KSI received from the network is already in use in the UE.

[0019]Besides, it has been detected in the field that in some cases, albeit rarely, the network can start an authentication challenge with a key set identifier for E-UTRAN (eKSI) that was already in use in the UE. This can happen if the network has lost the security context of the UE (e.g., due to error in location updating or network element restart). In such cases, the network has no means to know what the security context is or the eKSI used before with respect to the UE.

[0020]As can be seen, there is currently no standardized way for the UE to overcome the error caused by overlapping KSIs. Accordingly, multiple solutions and/or schemes are proposed in the present disclosure to address this issue.

[0021]FIG. 1 illustrates an example scenario 100 in which various solutions in accordance with the present disclosure may be implemented. Referring to FIG. 1, scenario 100 may involve a user equipment (UE) 110 in wireless communication with a wireless network 120 (e.g., a 5G NR mobile network) via a base station 125 (e.g., a gNB or transmit-receive point (TRP)). In scenario 100, initially UE 110 and wireless network 120 may have successfully performed and completed an authentication and key agreement (AKA) procedure 130. Subsequently, UE 110 may perform a procedure with wireless network 120 that causes or otherwise triggers wireless network 120 to transmit an authentication challenge 140 to UE 110 via base station 125. Upon receiving the authentication challenge 140 from wireless network 120, UE 110 may detect an error in the authentication challenge 140 (e.g., an incorrect KSI in authentication challenge 140 or that the KSI is already in use by UE 110). In response, UE 110 may handle the error in authentication challenge 140 based on one or more of various solutions in accordance with the present disclosure. For instance, in handling the error, UE 110 may transmit a response 150 to wireless network 120 to either reject or accept authentication challenge 140. The following description of various solutions in accordance with the present disclosure is provided with reference to FIG. 1.

[0022]Under a first proposed solution in accordance with the present disclosure, upon receiving an authentication challenge with an incorrect KSI from wireless network 120, UE 110 may reject the authentication challenge by responding with a message indicating authentication failure with a new cause value. The new cause value may indicate, for example and without limitation, that the KSI in the authentication challenge from wireless network 120 is incorrect, that the KSI is already in use by UE 110 or that a security context is invalid.

Advantageously, such indication may cause wireless network 120 to restart the authentication challenge with a different KSI value. Moreover, under the first proposed solution, upon occurrence of authentication failure, UE 110 may store received authentication parameters (e.g., with optional information elements) despite incorrect KSI. In such cases, wireless network 120 would need to transmit a new KSI while there is no need for wireless network 120 to transmit the same authentication parameters again.

[0023] Under a second proposed solution in accordance with the present disclosure, upon receiving an authentication challenge with an incorrect KSI from wireless network 120, UE 110 may transmit a response to the authentication challenge with 5GMM status. The 5GMM status may have an existing cause value or a new cause value which may indicate, for example and without limitation, that the KSI in the authentication challenge from wireless network 120 is incorrect, that the KSI is already in use by UE 110 or that a security context is invalid.

[0024] Under a third proposed solution in accordance with the present disclosure, upon receiving an authentication challenge with an incorrect KSI from wireless network 120, UE 110 may perform one or more operations. For instance, UE 110 may abort a procedure that triggered the authentication challenge. Additionally, or alternatively, UE 110 may delete a current security context. Additionally, or alternatively, UE 110 may perform either of: (a) restarting the procedure that triggered the authentication challenge; and (b) initiating a registration procedure with an indication to wireless network 120 that no key is available. In deleting the current security context (e.g., deleting an ngKSI), UE 110 may set the ngKSI to the value of “no key is available” and consider also an associated key K_{AMF} or K'_{AMF} , 5G NAS ciphering key and 5G NAS integrity key invalid. That is, the 5G security context associated with the ngKSI may be no longer considered valid.

[0025] Under a fourth proposed solution in accordance with the present disclosure, upon receiving an authentication challenge with an incorrect KSI from wireless network 120, UE 110 may accept the authentication challenge. For instance, UE 110 may clear an existing KSI and a related security context. Additionally, UE 110 may accept an overlapping KSI provided by an Access and Mobility management Function (AMF). In some cases, in accepting the authentication challenge, UE 110 may perform a security mode control (SMC) procedure with wireless network 120 with a new security context. Moreover, UE 110 may transmit an authentication response to wireless network 120.

[0026] Under a fifth proposed solution in accordance with the present disclosure, upon receiving an authentication challenge with an incorrect KSI from wireless network 120, UE 110 may accept the authentication challenge by rejecting an upcoming SMC procedure with wireless network 120. For instance, UE 110 may transmit to wireless network 120 a response with a cause value indicating rejection of the upcoming SMC procedure.

Illustrative Implementations

[0027] FIG. 2 illustrates an example system 200 having at least an example apparatus 210 and an example apparatus 220 in accordance with an implementation of the present disclosure. Each of apparatus 210 and apparatus 220 may perform various functions to implement schemes, techniques, processes and methods described herein pertaining to improvement for incorrect KSI handling in mobile communications, including the various schemes described above with respect to various proposed designs, concepts, schemes, systems and methods described above, including scenario 100, as well as processes 300, 400 and 500 described below.

[0028] Each of apparatus 210 and apparatus 220 may be a part of an electronic apparatus, which may be a

network apparatus or a UE (e.g., UE 110), such as a portable or mobile apparatus, a wearable apparatus, a wireless communication apparatus or a computing apparatus. For instance, each of apparatus 210 and apparatus 220 may be implemented in a smartphone, a smart watch, a personal digital assistant, a digital camera, or a computing equipment such as a tablet computer, a laptop computer or a notebook computer. Each of apparatus 210 and apparatus 220 may also be a part of a machine type apparatus, which may be an IoT apparatus such as an immobile or a stationary apparatus, a home apparatus, a wire communication apparatus or a computing apparatus. For instance, each of apparatus 210 and apparatus 220 may be implemented in a smart thermostat, a smart fridge, a smart door lock, a wireless speaker or a home control center. When implemented in or as a network apparatus, apparatus 210 and/or apparatus 220 may be implemented in an eNodeB in an LTE, LTE-Advanced or LTE-Advanced Pro network or in a gNB or TRP in a 5G network, an NR network or an IoT network.

[0029] In some implementations, each of apparatus 210 and apparatus 220 may be implemented in the form of one or more integrated-circuit (IC) chips such as, for example and without limitation, one or more single-core processors, one or more multi-core processors, or one or more complex-instruction-set-computing (CISC) processors. In the various schemes described above, each of apparatus 210 and apparatus 220 may be implemented in or as a network apparatus or a UE. Each of apparatus 210 and apparatus 220 may include at least some of those components shown in FIG. 2 such as a processor 212 and a processor 222, respectively, for example. Each of apparatus 210 and apparatus 220 may further include one or more other components not pertinent to the proposed scheme of the present disclosure (e.g., internal power supply, display device and/or user interface device), and, thus, such component(s) of apparatus 210 and apparatus 220 are neither shown in FIG. 2 nor described below in the interest of simplicity and brevity.

[0030] In one aspect, each of processor 212 and processor 222 may be implemented in the form of one or more single-core processors, one or more multi-core processors, or one or more CISC processors. That is, even though a singular term “a processor” is used herein to refer to processor 212 and processor 222, each of processor 212 and processor 222 may include multiple processors in some implementations and a single processor in other implementations in accordance with the present disclosure. In another aspect, each of processor 212 and processor 222 may be implemented in the form of hardware (and, optionally, firmware) with electronic components including, for example and without limitation, one or more transistors, one or more diodes, one or more capacitors, one or more resistors, one or more inductors, one or more memristors and/or one or more varactors that are configured and arranged to achieve specific purposes in accordance with the present disclosure. In other words, in at least some implementations, each of processor 212 and processor 222 is a special-purpose machine specifically designed, arranged and configured to perform specific tasks including those pertaining to improvement for incorrect KSI handling in mobile communications in accordance with various implementations of the present disclosure.

[0031] In some implementations, apparatus 210 may also include a transceiver 216 coupled to processor 212. Transceiver 216 may be capable of wirelessly transmitting and receiving data. In some implementations, transceiver 216 may be capable of wirelessly communicating with different types of wireless networks of different radio access technologies (RATs). In some implementations, transceiver 216 may be equipped with a plurality of antenna ports (not shown) such as, for example, four antenna ports. That is, transceiver 216 may be equipped with multiple transmit antennas and multiple receive antennas for multiple-input multiple-output (MIMO) wireless communications. In some implementations, apparatus 220 may also include a transceiver 226

coupled to processor 222. Transceiver 226 may include a transceiver capable of wirelessly transmitting and receiving data. In some implementations, transceiver 226 may be capable of wirelessly communicating with different types of UEs/wireless networks of different RATs. In some implementations, transceiver 226 may be equipped with a plurality of antenna ports (not shown) such as, for example, four antenna ports. That is, transceiver 226 may be equipped with multiple transmit antennas and multiple receive antennas for MIMO wireless communications.

[0032] In some implementations, apparatus 210 may further include a memory 214 coupled to processor 212 and capable of being accessed by processor 212 and storing data therein. In some implementations, apparatus 220 may further include a memory 224 coupled to processor 222 and capable of being accessed by processor 222 and storing data therein. Each of memory 214 and memory 224 may include a type of random-access memory (RAM) such as dynamic RAM (DRAM), static RAM (SRAM), thyristor RAM (T-RAM) and/or zero-capacitor RAM (Z-RAM). Alternatively, or additionally, each of memory 214 and memory 224 may include a type of read-only memory (ROM) such as mask ROM, programmable ROM (PROM), erasable programmable ROM (EPROM) and/or electrically erasable programmable ROM (EEPROM). Alternatively, or additionally, each of memory 214 and memory 224 may include a type of non-volatile random-access memory (NVRAM) such as flash memory, solid-state memory, ferroelectric RAM (FeRAM), magnetoresistive RAM (MRAM) and/or phase-change memory.

[0033] Each of apparatus 210 and apparatus 220 may be a communication entity capable of communicating with each other using various proposed schemes in accordance with the present disclosure. For illustrative purposes and without limitation, a description of capabilities of apparatus 210, as a UE, and apparatus 220, as a base station of a serving cell of a wireless network (e.g., 5G/NR mobile network), is provided below. It is noteworthy that, although the example implementations described below are provided in the context of a UE, the same may be implemented in and performed by a base station. Thus, although the following description of example implementations pertains to apparatus 210 as a UE (e.g., UE 110), the same is also applicable to apparatus 220 as a network node or base station such as a gNB, TRP or eNodeB (e.g., network node 125) of a wireless network (e.g., wireless network 120) such as a 5G NR mobile network.

[0034] Under various proposed solutions in accordance with the present disclosure, processor 212 of apparatus 210 may receive, via transceiver 216, from apparatus 220 an authentication challenge after the processor having completed an authentication and key agreement (AKA) procedure with apparatus 220. Moreover, processor 212 may detect an error in the authentication challenge. Furthermore, processor 212 may handle the error in the authentication challenge.

[0035] In some implementations, in handling the error in the authentication challenge, processor 212 may reject the authentication challenge by transmitting, via transceiver 216, to apparatus 220 a response to indicate authentication failure. In such cases, the response may include a cause value indicating that a first KSI in the authentication challenge is incorrect or that the first KSI is already in use.

[0036] In some implementations, in handling the error in the authentication challenge, processor 212 may store, in memory 214, one or more parameters associated with the authentication challenge despite the first KSI in the authentication challenge being incorrect or already in use. In some implementations, the one or more parameters may include optional information elements.

[0037] In some implementations, in handling the error in the authentication challenge, processor 212 may

perform additional operations. For instance, processor 212 may receive, via transceiver 216, from apparatus 220 a subsequent authentication challenge with a second KSI different than the first KSI. Moreover, processor 212 may perform a new AKA procedure with apparatus 220 responsive to receiving the subsequent authentication challenge with the second KSI.

5 **[0038]**In some implementations, in handling the error in the authentication challenge, processor 212 may transmit, via transceiver 216, to apparatus 220 a response to the authentication challenge with 5GMM status having an existing cause value or a new cause value indicating that a KSI in the authentication challenge is incorrect, that the KSI is already in use or that a security context is invalid.

10 **[0039]**In some implementations, in handling the error in the authentication challenge, processor 212 may perform multiple operations. For instance, processor 212 may abort a procedure that triggered the authentication challenge. Additionally, processor 212 may delete a current security context. Furthermore, processor 212 may perform either: (a) restarting the procedure that triggered the authentication challenge; or (b) initiating a registration procedure with an indication to the wireless network that no key is available.

15 **[0040]**In some implementations, in handling the error in the authentication challenge, processor 212 may accept the authentication challenge. In some implementation, in accepting the authentication challenge, processor 212 may perform multiple operations. For instance, processor 212 may clear an existing KSI and a related security context. Moreover, processor 212 may accept an overlapping KSI provided by an AMF. Furthermore, processor 212 may transmit, via transceiver 216, an authentication response to apparatus 220. In some implementations, in accepting the authentication challenge, processor 212 may also perform an SMC
20 procedure with apparatus 220 with a new security context.

[0041]In some implementations, in accepting the authentication challenge, processor 212 may reject an upcoming SMC procedure with apparatus 220 by transmitting, via transceiver 216, to apparatus 220 a response with a cause value indicating rejection of the upcoming SMC procedure.

Illustrative Processes

25 **[0042]**FIG. 3 illustrates an example process 300 in accordance with an implementation of the present disclosure. Process 300 may represent an aspect of implementing various proposed designs, concepts, schemes, systems and methods described above, whether partially or entirely, including scenario 100. More specifically, process 300 may represent an aspect of the proposed concepts and schemes pertaining to improvement for incorrect KSI handling in mobile communications. Process 300 may include one or more operations, actions,
30 or functions as illustrated by one or more of blocks 310, 320 and 330. Although illustrated as discrete blocks, various blocks of process 300 may be divided into additional blocks, combined into fewer blocks, or eliminated, depending on the desired implementation. Moreover, the blocks/sub-blocks of process 300 may be executed in the order shown in FIG. 3 or, alternatively in a different order. Furthermore, one or more of the blocks/sub-blocks of process 300 may be executed iteratively. Process 300 may be implemented by or in apparatus 210 and
35 apparatus 220 as well as any variations thereof. Solely for illustrative purposes and without limiting the scope, process 300 is described below in the context of apparatus 210 as a UE (e.g., UE 110) and apparatus 220 as a network node or base station (e.g., network node 125) of a wireless network (e.g., wireless network 120). Process 300 may begin at block 310.

40 **[0043]**At 310, process 300 may involve processor 212 of apparatus 210 receiving, via transceiver 216, from apparatus 220 an authentication challenge after the processor having completed an authentication and key

agreement (AKA) procedure with apparatus 220. Process 300 may proceed from 310 to 320.

[0044]At 320, process 300 may involve processor 212 detecting an error in the authentication challenge. Process 300 may proceed from 320 to 330.

[0045]At 330, process 300 may involve processor 212 rejecting the authentication challenge responsive to detecting the error.

[0046]In some implementations, in rejecting the authentication challenge, process 300 may involve processor 212 transmitting, via transceiver 216, to apparatus 220 a response to indicate authentication failure. In some implementations, the response may include a cause value indicating that a KSI in the authentication challenge is incorrect or that the KSI is already in use.

[0047]In some implementations, process 300 may further involve processor 212 storing, in memory 214, one or more parameters associated with the authentication challenge despite a first KSI in the authentication challenge being incorrect or already in use. In some implementations, the one or more parameters may include optional information elements.

[0048]In some implementations, process 300 may also involve processor 212 receiving, via transceiver 216, from apparatus 220 a subsequent authentication challenge with a second KSI different than the first KSI. Additionally, process 300 may involve processor 212 performing a new AKA procedure responsive to receiving the subsequent authentication challenge with the second KSI.

[0049]FIG. 4 illustrates an example process 400 in accordance with an implementation of the present disclosure. Process 400 may represent an aspect of implementing various proposed designs, concepts, schemes, systems and methods described above, whether partially or entirely, including scenario 100. More specifically, process 400 may represent an aspect of the proposed concepts and schemes pertaining to improvement for incorrect KSI handling in mobile communications. Process 400 may include one or more operations, actions, or functions as illustrated by one or more of blocks 410, 420 and 430. Although illustrated as discrete blocks, various blocks of process 400 may be divided into additional blocks, combined into fewer blocks, or eliminated, depending on the desired implementation. Moreover, the blocks/sub-blocks of process 400 may be executed in the order shown in FIG. 4 or, alternatively in a different order. Furthermore, one or more of the blocks/sub-blocks of process 400 may be executed iteratively. Process 400 may be implemented by or in apparatus 210 and apparatus 220 as well as any variations thereof. Solely for illustrative purposes and without limiting the scope, process 400 is described below in the context of apparatus 210 as a UE (e.g., UE 110) and apparatus 220 as a network node or base station (e.g., network node 125) of a wireless network (e.g., wireless network 120). Process 400 may begin at block 410.

[0050]At 410, process 400 may involve processor 212 of apparatus 210 receiving, via transceiver 216, from apparatus 220 an authentication challenge after the processor having completed an authentication and key agreement (AKA) procedure with apparatus 220. Process 400 may proceed from 410 to 420.

[0051]At 420, process 400 may involve processor 212 detecting an error in the authentication challenge. Process 400 may proceed from 420 to 430.

[0052]At 430, process 400 may involve processor 212 accepting the authentication challenge despite the error.

[0053]In some implementations, in detecting the error in the authentication challenge, process 400 may involve processor 212 detecting that a KSI in the authentication challenge is incorrect or that the KSI is already

in use.

[0054] In some implementations, in accepting the authentication challenge, process 400 may involve processor 212 performing multiple operations. For instance, process 400 may involve processor 212 clearing an existing KSI and a related security context. Additionally, process 400 may involve processor 212 accepting an overlapping KSI provided by an Access and Mobility management Function (AMF). Moreover, process 400 may involve processor 212 transmitting, via transceiver 216, an authentication response to apparatus 220.

[0055] In some implementations, in accepting the authentication challenge, process 400 may further involve processor 212 performing an SMC procedure with apparatus 220 with a new security context.

[0056] In some implementations, in accepting the authentication challenge, process 400 may involve processor 212 rejecting an upcoming SMC procedure with apparatus 220 by transmitting to apparatus 220 a response with a cause value indicating rejection of the upcoming SMC procedure.

[0057] FIG. 5 illustrates an example process 500 in accordance with an implementation of the present disclosure. Process 500 may represent an aspect of implementing various proposed designs, concepts, schemes, systems and methods described above, whether partially or entirely, including scenario 100. More specifically, process 500 may represent an aspect of the proposed concepts and schemes pertaining to improvement for incorrect KSI handling in mobile communications. Process 500 may include one or more operations, actions, or functions as illustrated by one or more of blocks 510, 520 and 530. Although illustrated as discrete blocks, various blocks of process 500 may be divided into additional blocks, combined into fewer blocks, or eliminated, depending on the desired implementation. Moreover, the blocks/sub-blocks of process 500 may be executed in the order shown in FIG. 5 or, alternatively in a different order. Furthermore, one or more of the blocks/sub-blocks of process 500 may be executed iteratively. Process 500 may be implemented by or in apparatus 210 and apparatus 220 as well as any variations thereof. Solely for illustrative purposes and without limiting the scope, process 500 is described below in the context of apparatus 210 as a UE (e.g., UE 110) and apparatus 220 as a network node or base station (e.g., network node 125) of a wireless network (e.g., wireless network 120). Process 500 may begin at block 510.

[0058] At 510, process 500 may involve processor 212 of apparatus 210 receiving, via transceiver 216, from apparatus 220 an authentication challenge after the processor having completed an authentication and key agreement (AKA) procedure with apparatus 220. Process 500 may proceed from 510 to 520.

[0059] At 520, process 500 may involve processor 212 detecting an error in the authentication challenge. Process 500 may proceed from 520 to 530.

[0060] At 530, process 500 may involve processor 212 handling the error in the authentication challenge.

[0061] In some implementations, in handling the error in the authentication challenge, process 500 may involve processor 212 rejecting the authentication challenge by transmitting, via transceiver 216, to apparatus 220 a response to indicate authentication failure. In such cases, the response may include a cause value indicating that a first KSI in the authentication challenge is incorrect or that the first KSI is already in use.

[0062] In some implementations, in handling the error in the authentication challenge, process 500 may further involve processor 212 storing, in memory 214, one or more parameters associated with the authentication challenge despite the first KSI in the authentication challenge being incorrect or already in use. In some implementations, the one or more parameters may include optional information elements.

[0063] In some implementations, in handling the error in the authentication challenge, process 500 may

involve processor 212 performing additional operations. For instance, process 500 may involve processor 212 receiving, via transceiver 216, from apparatus 220 a subsequent authentication challenge with a second KSI different than the first KSI. Moreover, process 500 may involve processor 212 performing a new AKA procedure responsive to receiving the subsequent authentication challenge with the second KSI.

5 **[0064]**In some implementations, in handling the error in the authentication challenge, process 500 may involve processor 212 transmitting, via transceiver 216, to apparatus 220 a response to the authentication challenge with 5GMM status having an existing cause value or a new cause value indicating that a KSI in the authentication challenge is incorrect, that the KSI is already in use or that a security context is invalid.

10 **[0065]**In some implementations, in handling the error in the authentication challenge, process 500 may involve processor 212 performing multiple operations. For instance, process 500 may involve processor 212 aborting a procedure that triggered the authentication challenge. Additionally, process 500 may involve processor 212 deleting a current security context. Furthermore, process 500 may involve processor 212 performing either: (a) restarting the procedure that triggered the authentication challenge; or (b) initiating a registration procedure with an indication to the wireless network that no key is available.

15 **[0066]**In some implementations, in handling the error in the authentication challenge, process 500 may involve processor 212 accepting the authentication challenge. In some implementation, in accepting the authentication challenge, process 500 may involve processor 212 performing multiple operations. For instance, process 500 may involve processor 212 clearing an existing KSI and a related security context. Moreover, process 500 may involve processor 212 accepting an overlapping KSI provided by an AMF. Furthermore, 20 process 500 may involve processor 212 transmitting, via transceiver 216, an authentication response to apparatus 220. In some implementations, in accepting the authentication challenge, process 500 may further involve processor 212 performing an SMC procedure with apparatus 220 with a new security context.

25 **[0067]**In some implementations, in accepting the authentication challenge, process 500 may involve processor 212 rejecting an upcoming SMC procedure with apparatus 220 by transmitting, via transceiver 216, to apparatus 220 a response with a cause value indicating rejection of the upcoming SMC procedure.

Additional Notes

30 **[0068]**The herein-described subject matter sometimes illustrates different components contained within, or connected with, different other components. It is to be understood that such depicted architectures are merely examples, and that in fact many other architectures can be implemented which achieve the same functionality. In a conceptual sense, any arrangement of components to achieve the same functionality is effectively "associated" such that the desired functionality is achieved. Hence, any two components herein combined to achieve a particular functionality can be seen as "associated with" each other such that the desired functionality is achieved, irrespective of architectures or intermedial components. Likewise, any two components so associated can also be viewed as being "operably connected", or "operably coupled", to each other to achieve the desired functionality, and any two components capable of being so associated can also be viewed as being "operably couplable", to each other to achieve the desired functionality. Specific examples of operably couplable include but are not limited to physically mateable and/or physically interacting components and/or wirelessly interactable and/or wirelessly interacting components and/or logically interacting and/or logically interactable components.

40 **[0069]**Further, with respect to the use of substantially any plural and/or singular terms herein, those having

skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

[0070] Moreover, it will be understood by those skilled in the art that, in general, terms used herein, and especially in the appended claims, e.g., bodies of the appended claims, are generally intended as “open” terms, e.g., the term “including” should be interpreted as “including but not limited to,” the term “having” should be interpreted as “having at least,” the term “includes” should be interpreted as “includes but is not limited to,” etc. It will be further understood by those within the art that if a specific number of an introduced claim recitation is intended, such an intent will be explicitly recited in the claim, and in the absence of such recitation no such intent is present. For example, as an aid to understanding, the following appended claims may contain usage of the introductory phrases “at least one” and “one or more” to introduce claim recitations. However, the use of such phrases should not be construed to imply that the introduction of a claim recitation by the indefinite articles “a” or “an” limits any particular claim containing such introduced claim recitation to implementations containing only one such recitation, even when the same claim includes the introductory phrases “one or more” or “at least one” and indefinite articles such as “a” or “an,” e.g., “a” and/or “an” should be interpreted to mean “at least one” or “one or more;” the same holds true for the use of definite articles used to introduce claim recitations. In addition, even if a specific number of an introduced claim recitation is explicitly recited, those skilled in the art will recognize that such recitation should be interpreted to mean at least the recited number, e.g., the bare recitation of “two recitations,” without other modifiers, means at least two recitations, or two or more recitations. Furthermore, in those instances where a convention analogous to “at least one of A, B, and C, etc.” is used, in general such a construction is intended in the sense one having skill in the art would understand the convention, e.g., “a system having at least one of A, B, and C” would include but not be limited to systems that have A alone, B alone, C alone, A and B together, A and C together, B and C together, and/or A, B, and C together, etc. In those instances where a convention analogous to “at least one of A, B, or C, etc.” is used, in general such a construction is intended in the sense one having skill in the art would understand the convention, e.g., “a system having at least one of A, B, or C” would include but not be limited to systems that have A alone, B alone, C alone, A and B together, A and C together, B and C together, and/or A, B, and C together, etc. It will be further understood by those within the art that virtually any disjunctive word and/or phrase presenting two or more alternative terms, whether in the description, claims, or drawings, should be understood to contemplate the possibilities of including one of the terms, either of the terms, or both terms. For example, the phrase “A or B” will be understood to include the possibilities of “A” or “B” or “A and B.”

[0071] From the foregoing, it will be appreciated that various implementations of the present disclosure have been described herein for purposes of illustration, and that various modifications may be made without departing from the scope and spirit of the present disclosure. Accordingly, the various implementations disclosed herein are not intended to be limiting, with the true scope and spirit being indicated by the following claims.

CLAIMS**1.** A method, comprising:

receiving, by a processor of an apparatus, from a wireless network an authentication challenge after the processor having completed an authentication and key agreement (AKA) procedure with the wireless network;

5 detecting, by the processor, an error in the authentication challenge; and

rejecting, by the processor, the authentication challenge responsive to detecting the error.

2. The method of Claim 1, wherein the rejecting of the authentication challenge comprises transmitting to the wireless network a response to indicate authentication failure.

3. The method of Claim 2, wherein the response comprises a cause value indicating that a key set identifier (KSI) in the authentication challenge is incorrect or that the KSI is already in use.

4. The method of Claim 1, further comprising:

storing, by the processor, one or more parameters associated with the authentication challenge despite a first key set identifier (KSI) in the authentication challenge being incorrect or already in use,

wherein the one or more parameters comprise optional information elements.

15 **5.** The method of Claim 4, further comprising:

receiving, by the processor, from the wireless network a subsequent authentication challenge with a second KSI different than the first KSI; and

performing, by the processor, a new AKA procedure responsive to receiving the subsequent authentication challenge with the second KSI.

20 **6.** A method, comprising:

receiving, by a processor of an apparatus, from a wireless network an authentication challenge after the processor having completed an authentication and key agreement (AKA) procedure with the wireless network;

detecting, by the processor, an error in the authentication challenge; and

accepting, by the processor, the authentication challenge.

25 **7.** The method of Claim 6, wherein the detecting of the error in the authentication challenge comprises detecting that a key set identifier (KSI) in the authentication challenge is incorrect or that the KSI is already in use.

8. The method of Claim 6, wherein the accepting of the authentication challenge comprises:

clearing an existing key set identifier (KSI) and a related security context;

30 accepting an overlapping KSI provided by an Access and Mobility management Function (AMF); and transmitting an authentication response to the wireless network.

9. The method of Claim 8, wherein the accepting of the authentication challenge further comprises performing a security mode control (SMC) procedure with the wireless network with a new security context.

10. The method of Claim 6, wherein the accepting of the authentication challenge comprises rejecting an upcoming security mode control (SMC) procedure with the wireless network by transmitting to the wireless network a response with a cause value indicating rejection of the upcoming SMC procedure.

35 **11.** A method, comprising:

receiving, by a processor of an apparatus, from a wireless network an authentication challenge after the processor having completed an authentication and key agreement (AKA) procedure with the wireless network;

40 detecting, by the processor, an error in the authentication challenge; and

handling, by the processor, the error in the authentication challenge.

12. The method of Claim 11, wherein the handling of the error in the authentication challenge comprises rejecting the authentication challenge by transmitting to the wireless network a response to indicate authentication failure, and wherein the response comprises a cause value indicating that a first key set identifier (KSI) in the authentication challenge is incorrect or that the first KSI is already in use.

13. The method of Claim 12, wherein the handling of the error in the authentication challenge further comprises:

storing one or more parameters associated with the authentication challenge despite the first KSI in the authentication challenge being incorrect or already in use,

wherein the one or more parameters comprise optional information elements.

14. The method of Claim 13, wherein the handling of the error in the authentication challenge further comprises:

receiving from the wireless network a subsequent authentication challenge with a second KSI different than the first KSI; and

performing a new AKA procedure responsive to receiving the subsequent authentication challenge with the second KSI.

15. The method of Claim 11, wherein the handling of the error in the authentication challenge comprises transmitting to the wireless network a response to the authentication challenge with 5th-Generation Mobility Management (5GMM) status having an existing cause value or a new cause value indicating that a key set identifier (KSI) in the authentication challenge is incorrect, that the KSI is already in use or that a security context is invalid.

16. The method of Claim 11, wherein the handling of the error in the authentication challenge comprises:

aborting a procedure that triggered the authentication challenge;

deleting a current security context; and

performing either:

restarting the procedure that triggered the authentication challenge; or

initiating a registration procedure with an indication to the wireless network that no key is available.

17. The method of Claim 11, wherein the handling of the error in the authentication challenge comprises accepting the authentication challenge.

18. The method of Claim 17, wherein the accepting of the authentication challenge comprises:

clearing an existing key set identifier (KSI) and a related security context;

accepting an overlapping KSI provided by an Access and Mobility management Function (AMF); and

transmitting an authentication response to the wireless network.

19. The method of Claim 18, wherein the accepting of the authentication challenge further comprises performing a security mode control (SMC) procedure with the wireless network with a new security context.

20. The method of Claim 17, wherein the accepting of the authentication challenge comprises rejecting an upcoming security mode control (SMC) procedure with the wireless network by transmitting to the wireless network a response with a cause value indicating rejection of the upcoming SMC procedure.

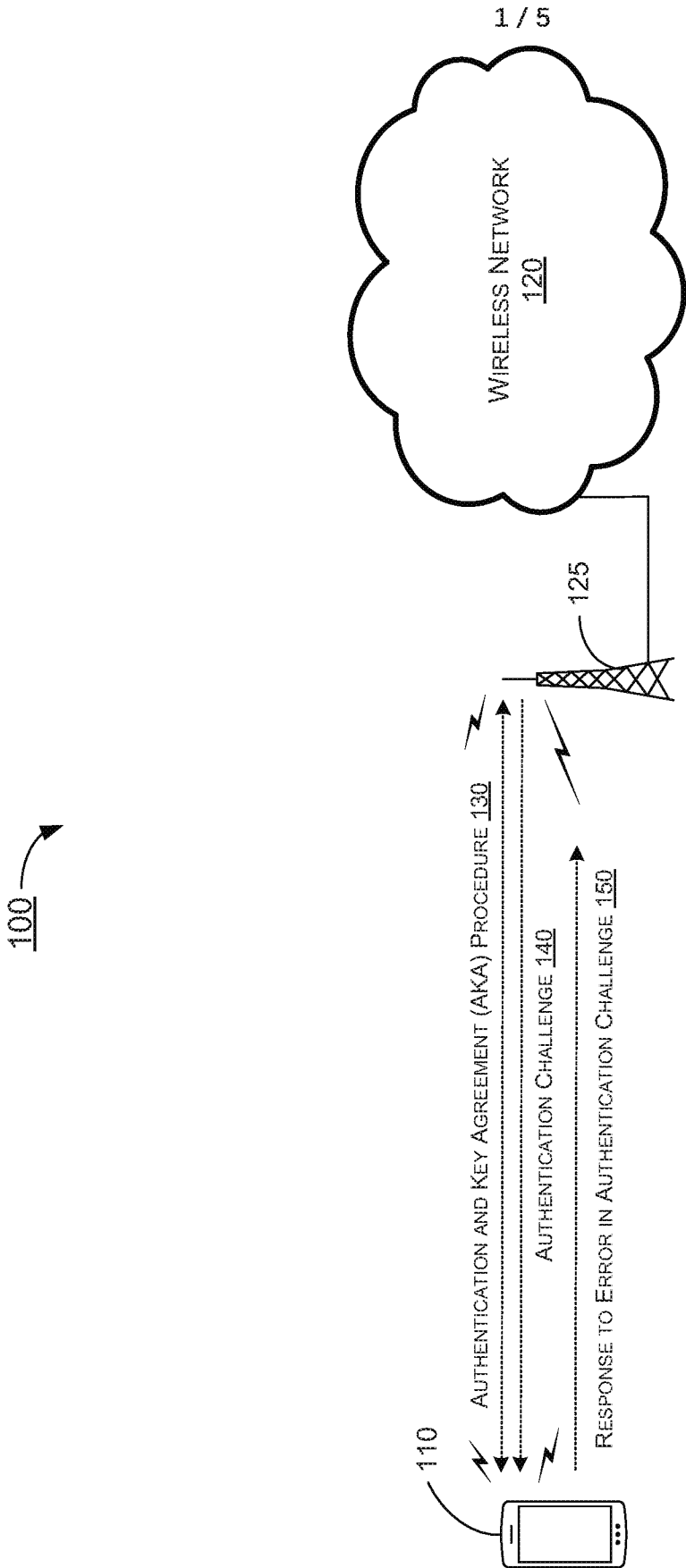


FIG. 1

200

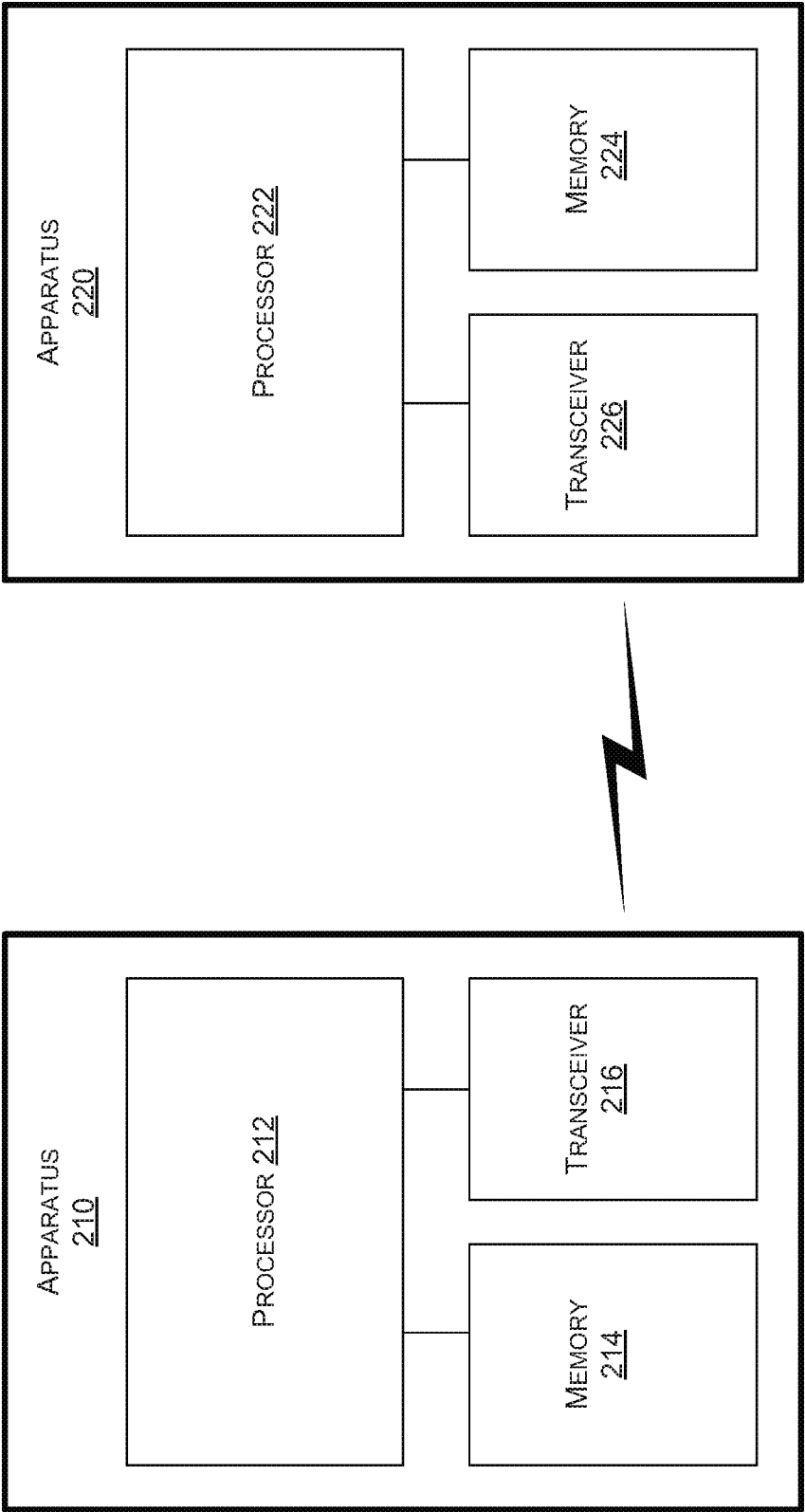


FIG. 2

3 / 5

300 →

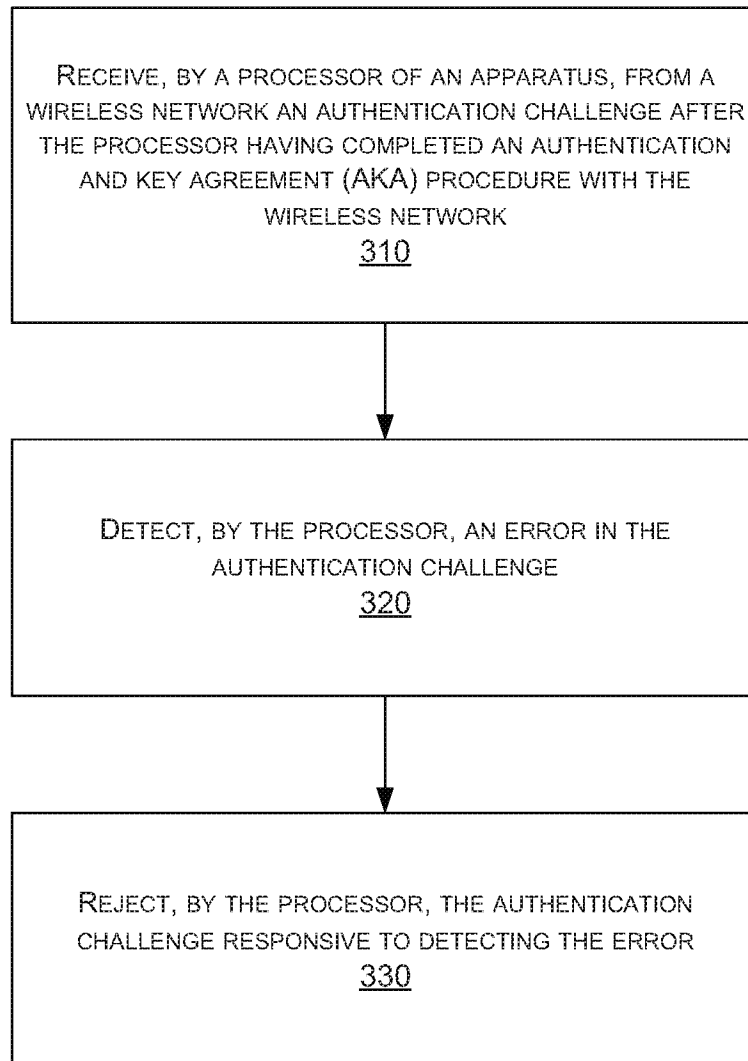


FIG. 3

4 / 5

400 →

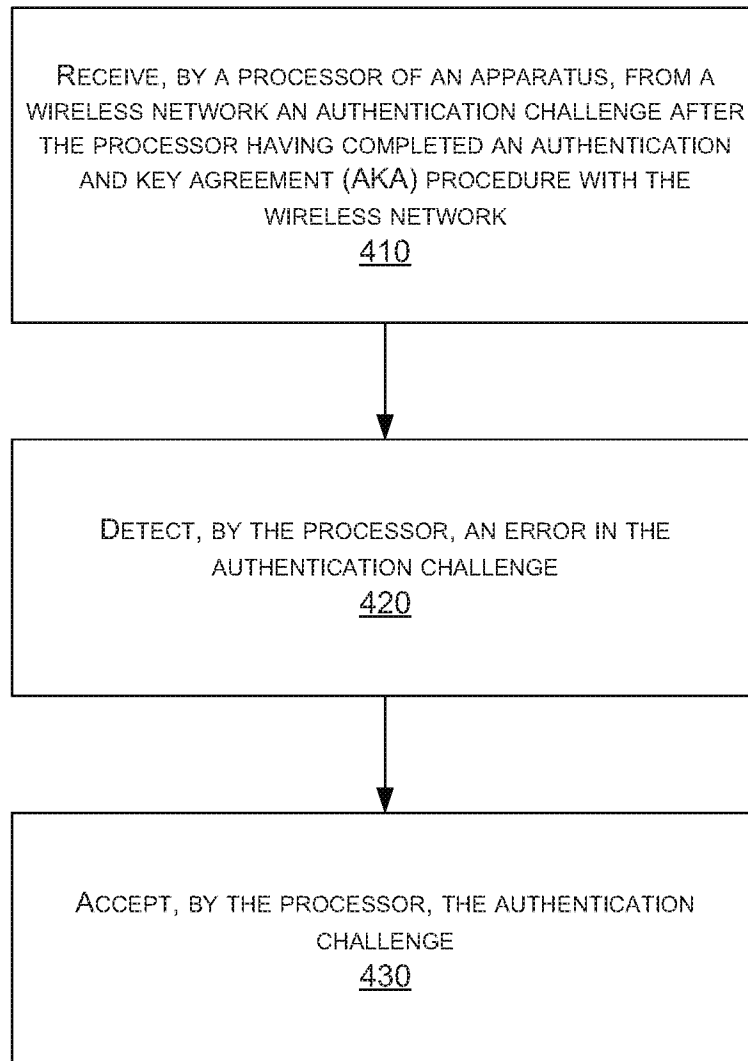


FIG. 4

5 / 5

500 →

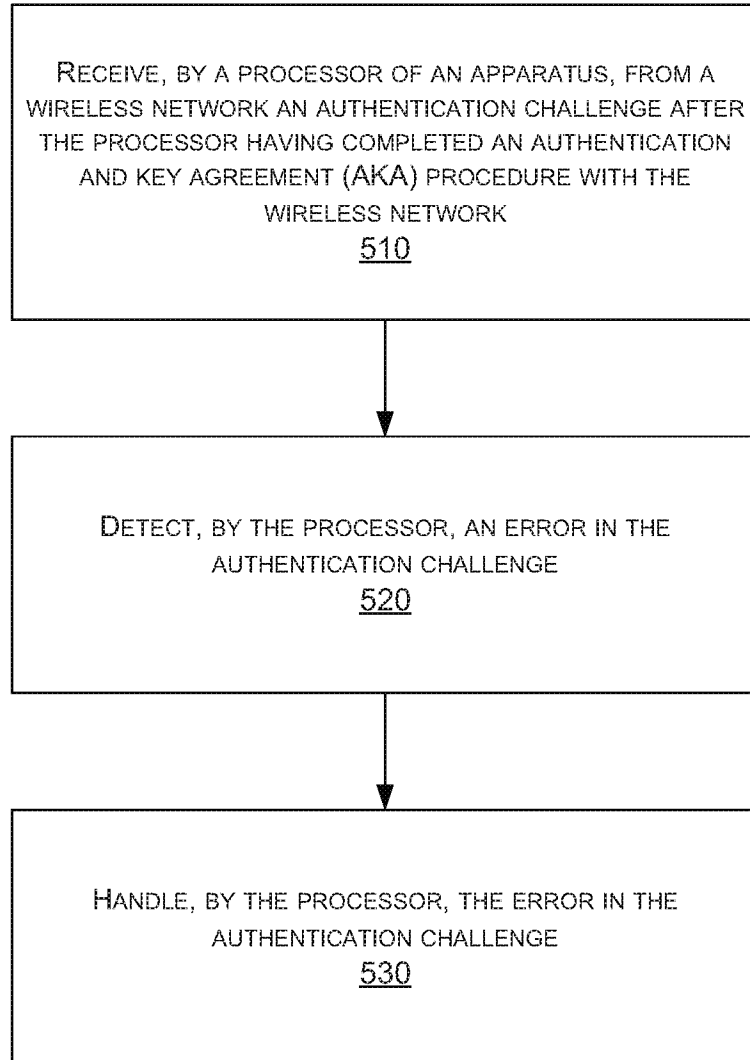


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/081766

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/02(2006.01)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)

H04L H04Q H04W

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)

CNPAT, CNKI, WPI, EPODOC:AKA KSI authentication challenge reject accept error fail

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2014113193 A1 (INTEL IP CORPORATION) 24 July 2014 (2014-07-24) description page 3, line 23 to page 11, line 3	1-20
A	CN 1870812 A (HUAWEI TECHNOLOGIES CO., LTD.) 29 November 2006 (2006-11-29) the whole document	1-20
A	CN 106304056 A (ZTE CORPORATION) 04 January 2017 (2017-01-04) the whole document	1-20
A	US 2017134444 A1 (BLACKBERRY LTD.) 11 May 2017 (2017-05-11) the whole document	1-20

☐ 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

16 June 2019

Date of mailing of the international search report

08 July 2019

Name and mailing address of the ISA/CN

National Intellectual Property Administration, PRC
6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing
100088
China

Authorized officer

FENG,Nan

Facsimile No. (86-10)62019451

Telephone No. 86-(10)-53961665

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/081766

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
WO	2014113193	A1	24 July 2014	CN	104854835	A	19 August 2015
				JP	2016510527	A	07 April 2016
				US	2018069856	A1	08 March 2018
				JP	2017184260	A	05 October 2017
				EP	2946539	A1	25 November 2015
				US	2015326572	A1	12 November 2015
CN	1870812	A	29 November 2006	EP	1755311	A1	21 February 2007
				AR	053615	A1	09 May 2007
				US	2008209532	A1	28 August 2008
				WO	2006125359	A1	30 November 2006
CN	106304056	A	04 January 2017	EP	3300405	A1	28 March 2018
				WO	2016184140	A1	24 November 2016
				US	2018160360	A1	07 June 2018
US	2017134444	A1	11 May 2017	CN	108886520	A	23 November 2018
				EP	3408993	A1	05 December 2018
				WO	2017132277	A1	03 August 2017
				CA	3011821	A1	03 August 2017
				KR	20180107776	A	02 October 2018