



(51) International Patent Classification:

H04W 76/25 (2018.01) H04W 60/04 (2009.01)
H04W 12/06 (2021.01)

(21) International Application Number:

PCT/IN2024/050928

(22) International Filing Date:

26 June 2024 (26.06.2024)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

202321044337 03 July 2023 (03.07.2023) IN

(71) Applicant: **JIO PLATFORMS LIMITED** [IN/IN]; OF-
FICE-101, SAFFRON, NR. CENTRE POINT, PANCH-
WATI 5 RASTA, AMBAWADI, GUJARAT, INDIA,
AHMEDABAD 380006 (IN).

(72) Inventors: **BHATNAGAR, Aayush**; Tower-7, 15B,
Beverly Park, Sector-14 Koper Khairane, Maharashtra,
Navi Mumbai 400701 (IN). **BISHT, Birendra**; B-2101,
Yashaskaram CHS, Plot -39, Sector -27, Kharghar, Maha-
rashtra, Navi Mumbai 410210 (IN). **SINGH, Harbinder
Pal**; Wing B1, Flat No 402, Lakhani Suncoast, Sector
15, CBD Belapur, Maharashtra, Navi Mumbai 400614

(IN). **GUPTA, Amit K**; A-606, River Retreat, Casa Rio,
Palava City, Maharastra, Dombivali East 421204 (IN).
BHATT, Naresh; E- 1402 Alpha Corp Gurgaon One, Sec-
tor- 84, Gurgaon, Haryana, Gurgaon 122004 (IN). **VED-
MA, Jayakrishna**; H.no 4-53, Kannepally, Tiryani, Kum-
ram Bheem, Telangana, Asifabad 504297 (IN).

(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, CV, CZ, DE, DJ, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG,
KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,
MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH,
TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS,
ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, CV,
GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE,

(54) Title: SYSTEM AND METHOD OF HANDLING INTEGRITY FAILURE FOR IDLE MODE NAS

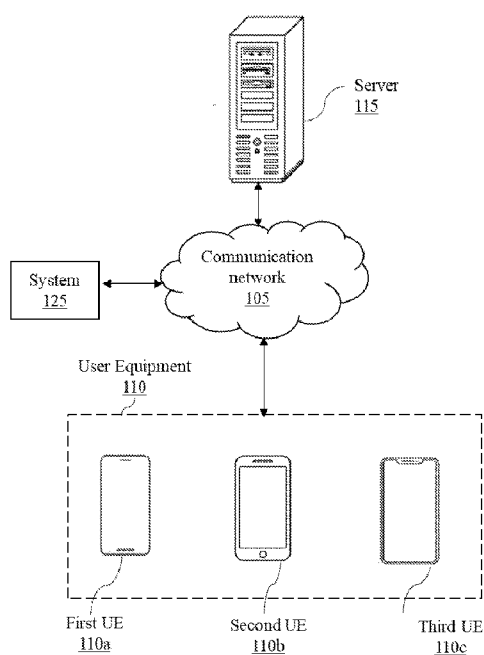


FIG. 1

(57) Abstract: SYSTEM AND METHOD OF HANDLING INTEGRITY
FAILURE FOR IDLE MODE NAS The present disclosure relates to handling
integrity failures for idle mode procedure in a communication network An AMF
receives, from a UE, a request for an idle mode procedure. The request includes
a MAC and a UE uplink SQN. The AMF determines integrity failure when a
MAC value calculated at the AMF is different from the MAC value received
from the UE. The AMF calculates a gap count by comparing the UE uplink
SQN and an AMF uplink SQN, and updates an overflow count stored at the
AMF based on comparison of the gap count and a configured gap count pre-
stored at the AMF to make the overflow count stored at the AMF equal to an
overflow count stored at the UE. The AMF performs integrity validation of the
NAS message based on the updated overflow count and the UE uplink SQN
received from the UE. Ref.

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

Declarations under Rule 4.17:

- *of inventorship (Rule 4.17(iv))*

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*
- *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

SYSTEM AND METHOD OF HANDLING INTEGRITY FAILURE FOR IDLE MODE NAS

FIELD OF THE INVENTION

[0001] The present invention relates to communication technology and, more particularly, to handling integrity failure for idle mode NAS.

BACKGROUND OF THE INVENTION

[0002] In 5G networks, Access & Mobility Management Function (AMF) is responsible for managing the mobility and access of User Equipment (UEs). When a UE is in an idle state and needs to perform certain actions like initiating a new service or responding to a paging request, it sends a request to the network. If the AMF detects an integrity failure due to packet loss, corruption, or loss in the received message, it triggers a re-authentication or re-registration process.

[0003] Re-authentication involves verifying the identity and security credentials of the UE, while re-registration involves updating the network with the UE's current location and status. These processes ensure the integrity and security of the communication between the UE and the network. By initiating re-authentication or re-registration, the AMF can mitigate potential security risks and maintain the integrity of the network connection.

[0004] However, these re-authentication or re-registration procedures performed in the idle mode can be resource consuming. Performing these procedures requires additional processing power, signaling overhead, and network resources. Further, these procedures are also time consuming, resulting in further loss and delaying of network operations.

[0005] Thus, there is a need of a solution which solves the above mentioned problems.

BRIEF SUMMARY OF THE INVENTION

[0006] One or more embodiments of the present disclosure provide a system and a method of handling integrity failures in Non-Access Stratum (NAS) message for idle mode procedure in a communication network.

[0007] In one aspect of the present invention, a system for handling integrity failures in Non-Access Stratum (NAS) message for idle mode procedure in a communication network is disclosed. The system includes a User Equipment (UE) and an Access and Mobility Management Function (AMF). The UE is configured to send a request for an idle mode procedure to the AMF. The request for the idle mode procedure includes a Message Authentication Code (MAC) and a UE uplink Sequence Number (SQN). The AMF is configured to: receive the request for the idle mode procedure from the UE; determine an integrity failure in relation to the idle mode procedure initiated by the UE when a MAC value calculated at the AMF using a NAS integrity algorithm is different from the MAC value received from the UE; calculate a gap count by comparing the UE uplink SQN received from the UE and an AMF uplink SQN stored at the AMF; update an overflow count stored at the AMF based on comparison of the gap count and a configured gap count pre-stored at the AMF to make the overflow count stored at the AMF equal to an overflow count stored at the UE; and perform integrity validation of the NAS message based on the updated overflow count and the UE uplink SQN received from the UE.

[0008] In one aspect, for performing the integrity validation, the AMF recalculates a MAC value using the UE uplink sequence number received from the UE and the updated overflow count, and determines a successful match between the overflow count stored at the AMF and the overflow count stored at the UE. The request for the idle mode procedure is received as one of a Mobility Request (MR), Periodic Request

(PR), and a Service Request (SR). The request includes one or more of a SQN and a NAS message. When the UE uplink SQN received from the UE crosses a predefined count and the AMF uplink SQN is less than or equal to the predefined count, the gap count is determined by adding a predefined number to the received UE uplink SQN and subtracting the AMF uplink SQN from a sum. When the UE uplink SQN received from the UE is less than or equal to a predefined count and the AMF uplink SQN crosses the predefined count and is greater than or equal to 0, the gap count is determined by adding a predefined number to the AMF uplink SQN and subtracting the UE uplink SQN from a sum. When the calculated gap count is less than or equal to the configured gap count pre-stored at the AMF and the UE uplink SQN received from the UE exceeds a predefined count and the AMF uplink SQN is less than or equal to the predefined count, the overflow count is incremented. Alternatively, when the calculated gap count is less than or equal to the configured gap count pre-stored at the AMF and the UE uplink SQN received from the UE is less than or equal to a predefined count and the AMF uplink SQN exceeds the predefined count, the overflow count is decremented.

[0009] In another aspect of the present invention, a method of handling integrity failures in Non-Access Stratum (NAS) message for idle mode procedure in a communication network is disclosed. The method includes the step of receiving, by an Access and Mobility Management Function (AMF), a request for an idle mode procedure from a User Equipment (UE). The request for the idle mode procedure includes a Message Authentication Code (MAC) and a UE uplink Sequence Number (SQN). The method includes the step of determining, by the AMF, an integrity failure in relation to the idle mode procedure initiated by the UE when a MAC value calculated at the AMF is different from the MAC value received from the UE. The method includes the step of calculating, by the AMF, a gap count by comparing the UE uplink SQN received from the UE and an AMF uplink SQN stored at the AMF. The method includes the step of updating, by the AMF, an overflow count stored at the AMF based on comparison of the gap count and a configured gap count pre-stored at the AMF to make the overflow count stored at the AMF equal to an overflow count

stored at the UE. The method includes the step of performing, by the AMF, integrity validation of the NAS message based on the updated overflow count and the UE uplink SQN received from the UE.

[0010] In one aspect, for performing the integrity validation, the AMF recalculates a MAC using the UE uplink SQN received from the UE and the updated overflow count, and determines a successful match between the overflow count stored at the AMF and the overflow count stored at the UE. The request for the idle mode procedure is received as one of a Mobility Request (MR), Periodic Request (PR), and a Service Request (SR). The request includes one or more of a SQN and a NAS message. When the UE uplink SQN received from the UE crosses a predefined count and the AMF uplink SQN is less than or equal to the predefined count, the gap count is determined by adding a predefined number to the received UE uplink SQN and subtracting the AMF uplink SQN from a sum. When the UE uplink SQN received from the UE is less than or equal to a predefined count and the AMF uplink SQN crosses the predefined count, the gap count is determined by adding a predefined number to the AMF uplink SQN and subtracting the UE uplink SQN from a sum. When the calculated gap count is less than or equal to the configured gap count pre-stored at the AMF and the UE uplink SQN received from the UE exceeds a predefined count and the AMF uplink SQN is less than or equal to the predefined count, the overflow count is incremented. When the calculated gap count is less than or equal to the configured gap count pre-stored at the AMF and the UE uplink SQN received from the UE is less than or equal to a predefined count and the AMF uplink SQN exceeds the predefined count, the overflow count is decremented.

[0011] In yet another aspect of the present invention, a non-transitory computer-readable medium having stored thereon computer-readable instructions is described. Upon being executed by a processor, the computer-readable instructions cause the processor to receive a request for an idle mode procedure from a User Equipment (UE). The request for the idle mode procedure includes a Message Authentication Code (MAC) value and a UE uplink Sequence Number (SQN). The computer-readable instructions further cause the processor to determine an integrity

failure in relation to the idle mode procedure initiated by the UE when a MAC value calculated at an Access and Mobility Management Function (AMF) is different from the MAC value received from the UE. The computer-readable instructions cause the processor to calculate a gap count by comparing the UE uplink SQN received from the UE and an AMF uplink SQN stored at the AMF. The computer-readable instructions cause the processor to update an overflow count stored at the AMF based on comparison of the gap count and a configured gap count pre-stored at the AMF to make the overflow count stored at the AMF equal to an overflow count stored at the UE. The computer-readable instructions cause the processor to perform integrity validation of the NAS message based on the updated overflow count and the UE uplink SQN received from the UE.

[0012] Other features and aspects of this invention will be apparent from the following description and the accompanying drawings. The features and advantages described in this summary and in the following detailed description are not all-inclusive, and particularly, many additional features and advantages will be apparent to one of ordinary skill in the relevant art, in view of the drawings, specification, and claims hereof. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes and may not have been selected to delineate or circumscribe the inventive subject matter, resort to the claims being necessary to determine such inventive subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] The accompanying drawings, which are incorporated herein, and constitute a part of this disclosure, illustrate exemplary embodiments of the disclosed methods and systems in which like reference numerals refer to the same parts throughout the different drawings. Components in the drawings are not necessarily to scale, emphasis instead being placed upon clearly illustrating the principles of the present disclosure. Some drawings may indicate the components using block diagrams and may not

represent the internal circuitry of each component. It will be appreciated by those skilled in the art that disclosure of such drawings includes disclosure of electrical components, electronic components or circuitry commonly used to implement such components.

[0014] FIG. 1 illustrates a system architecture for handling integrity failures in Non-Access Stratum (NAS) message for idle mode procedure in a communication network, according to one or more embodiments of the present subject matter;

[0015] FIG. 2 illustrates a block diagram of a system for handling integrity failures in NAS message for idle mode procedure in a communication network, according to one or more embodiments of the present subject matter;

[0016] FIG. 3 illustrates a block diagram of the system and a User Equipment communicating with each other for handling integrity failures in NAS message for idle mode procedure in a communication network, according to one or more embodiments of the present subject matter;

[0017] FIG. 4 illustrates a timing diagram of a method of connection establishment, release, and reporting integrity failure in a communication network, according to one or more embodiments of the present subject matter;

[0018] FIG. 5 illustrates a timing diagram of a method of handling integrity failures in NAS message for idle mode procedure in a communication network, according to one or more embodiments of the present subject matter; and

[0019] FIG. 6 illustrates a flow chart of a method of handling integrity failures in NAS message for idle mode procedure in a communication network, according to one or more embodiments of the present subject matter.

[0020] The foregoing shall be more apparent from the following detailed description of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0021] Some embodiments of the present disclosure, illustrating all its features, will now be discussed in detail. It must also be noted that as used herein and in the appended claims, the singular forms “a”, “an” and “the” include plural references unless the context clearly dictates otherwise.

[0022] Various modifications to the embodiment will be readily apparent to those skilled in the art and the generic principles herein may be applied to other embodiments. However, one of ordinary skill in the art will readily recognize that the present disclosure including the definitions listed here below are not intended to be limited to the embodiments illustrated but is to be accorded the widest scope consistent with the principles and features described herein.

[0023] A person of ordinary skill in the art will readily ascertain that the illustrated steps detailed in the figures and here below are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments.

[0024] Various embodiments of the present invention provide an Access and Mobility Management Function (AMF) for handling integrity failure in idle state NAS. In a preferred embodiment, the invention introduces a novel method executed by the Access and Mobility Management Function (AMF) within a communication network to effectively address integrity failures occurring in idle state responses received from User Equipment (UE). By leveraging advanced detection techniques, gap count

calculations based on uplink sequence numbers, overflow count updates, and re-performing integrity checks, the method eliminates the need for resource-consuming re-authentication and re-registration procedures.

[0025] FIG. 1 illustrates a system architecture for handling integrity failures in Non-Access Stratum (NAS) message for idle mode procedure in a communication network, in accordance with one implementation of the present embodiment. The system comprises several interconnected components that work together to handle the integrity failures.

[0026] The system architecture shows a User Equipment (UE) 110. For the purpose of description and explanation, the description will be explained with respect to one or more UEs 110, or to be more specific will be explained with respect to a first UE 110a, a second UE 110b, and a third UE 110c, and should nowhere be construed as limiting the scope of the present disclosure. In an embodiment, each of the first UE 110a, the second UE 110b, and the third UE 110c is a mobile phone or a smartphone.

[0027] Each of the first UE 110a, the second UE 110b, and the third UE 110c is configured to transmit a request for an idle mode procedure via a communication network 105 to a system 125.

[0028] The communication network 105 includes, by way of example but not limitation, one or more of a wireless network, a wired network, an internet, an intranet, a public network, a private network, a packet-switched network, a circuit-switched network, an ad hoc network, an infrastructure network, a Public-Switched Telephone Network (PSTN), a cable network, a cellular network, a satellite network, a fiber optic network, or some combination thereof. The communication network 105 may include, but is not limited to, a Third Generation (3G), a Fourth Generation (4G), a Fifth Generation (5G), a Sixth Generation (6G), a New Radio (NR), a Narrow Band Internet of Things (NB-IoT), an Open Radio Access Network (O-RAN), and the like.

[0029] Also, a server 115 is accessible via the communication network 105. The server 115 may include by way of example but not limitation, one or more of a

standalone server, a server blade, a server rack, a bank of servers, a server farm, hardware supporting a part of a cloud service or system, a home server, hardware running a virtualized server, one or more processors executing code to function as a server, one or more machines performing server-side functionality as described herein, at least a portion of any of the above, some combination thereof. In an embodiment, the entity may include, but is not limited to, a vendor, a network operator, a company, an organization, a university, a lab facility, a business enterprise, a defence facility, or any other facility that provides content.

[0030] The system **125** is configured to operate as an Access and Mobility Management Function (AMF) and hence alternatively referred as AMF. In other embodiments, the system **125** may be generic in nature and may be integrated with any application including a System Management Facility (SMF), a Business Telephony Application Server (BTAS), a Converged Telephony Application Server (CTAS), any SIP (Session Initiation Protocol) Application Server which interacts with core Internet Protocol Multimedia Subsystem (IMS) on Industrial Control System (ISC) interface as defined by Third Generation Partnership Project (3GPP) to host a wide array of cloud telephony enterprise services, a System Information Blocks (SIB)/ and a Mobility Management Entity (MME).

[0031] Operational and construction features of the system **125** will be explained in detail successively with respect to different figures. **FIG. 2** illustrates a block diagram of the system **125** for handling integrity failures in Non-Access Stratum (NAS) message for idle mode procedure in a communication network, according to one or more embodiments of the present invention. The system **125** is adapted to be embedded within the server **115** or is embedded as an individual entity. However, for the purpose of description, the system **125** is described as an integral part of the server **115**, without deviating from the scope of the present disclosure.

[0032] As per the illustrated embodiment, the system **125** includes one or more processors **205**, a memory **210**, and an input/output interface unit **215**. The one or more processor **205**, hereinafter referred to as the processor **205** may be implemented as one

or more microprocessors, microcomputers, microcontrollers, digital signal processors, central processing units, state machines, logic circuitries, single board computers, and/or any devices that manipulate signals based on operational instructions. As per the illustrated embodiment, the system **125** includes one or more processors **205**. However, it is to be noted that the system **125** may include multiple processors as per the requirement and without deviating from the scope of the present disclosure. Among other capabilities, the one or more processors **205** is configured to fetch and execute computer-readable instructions stored in the memory **210**. The memory **210** may be configured to store one or more computer-readable instructions or routines in a non-transitory computer-readable storage medium, which may be fetched and executed to create or share data packets over a network service. The memory **210** may include any non-transitory storage device including, for example, volatile memory such as RAM, or non-volatile memory such as EPROM, flash memory, and the like.

[0033] In an embodiment, the input/output (I/O) interface unit **215** includes a variety of interfaces, for example, interfaces for data input and output devices, referred to as Input/Output (I/O) devices, storage devices, and the like. The I/O interface unit **215** facilitates communication of the system **125**. In one embodiment, the I/O interface unit **215** provides a communication pathway for one or more components of the system **125**. Examples of such components include, but are not limited to, the network devices **110**, a backend database **220**, and a distributed cache **225**.

[0034] The backend database **220** is one of, but is not limited to, a centralized database, a cloud-based database, a commercial database, an open-source database, a distributed database, an end-user database, a graphical database, a No-Structured Query Language (NoSQL) database, an object-oriented database, a personal database, an in-memory database, a document-based database, a time series database, a wide column database, a key value database, a search database, a cache database, and so forth. The foregoing examples of the backend database **220** types are non-limiting and may not be mutually exclusive e.g., a database can be both commercial and cloud-based, or both relational and open-source, etc.

[0035] The distributed cache **225** is a pool of random-access memory (RAM) of multiple networked computers into a single in-memory data store for use as a data cache to provide fast access to data. The distributed cache **225** is essential for applications that need to scale across multiple servers or are distributed geographically. The distributed cache **225** ensures that data is available close to where it's needed, even if the original data source is remote or under heavy load.

[0036] Further, the one or more processors **205**, in an embodiment, may be implemented as a combination of hardware and programming (for example, programmable instructions) to implement one or more functionalities of the one or more processors **205**. In the examples described herein, such combinations of hardware and programming may be implemented in several different ways. For example, the programming for the one or more processors **205** may be processor-executable instructions stored on a non-transitory machine-readable storage medium and the hardware for one or more processors **205** may comprise a processing resource (for example, one or more processors), to execute such instructions. In the present examples, the memory **210** may store instructions that, when executed by the processing resource, implement the one or more processors **205**. In such examples, the system **125** may comprise the memory **210** storing the instructions and the processing resource to execute the instructions, or the memory **210** may be separate but accessible to the system **125** and the processing resource. In other examples, the one or more processors **205** may be implemented by electronic circuitry.

[0037] For the system **125** to handle integrity failures in NAS messages for idle mode procedure in a communication network, the processor **205** implements a request receiving module **228**, an integrity failure determining module **230**, a gap count calculation module **235**, an overflow count updating module **240**, and an integrity validation module **245** communicably coupled to each other.

[0038] The request receiving module **228** is communicably connected to each of the first UE **110a**, the second UE **110b**, and the third UE **110c** via the communication network **105**. Accordingly, the request receiving module **228** is configured to receive

a request for an idle mode procedure from a User Equipment (UE). The request for the idle mode procedure is received as a Mobility Request (MR), Periodic Request (PR), or a Service Request (SR). The request for the idle mode procedure includes a Message Authentication Code (MAC) and a UE uplink Sequence Number (SQN). In some cases, the request may include a NAS message.

[0039] MAC information element (IE) contains integrity protection information for a message. The MAC IE is included in the SECURITY PROTECTED 5GS NAS MESSAGE if a valid 5G NAS security context exists and security functions are started. The SQN consists of eight least significant bits of the NAS COUNT for a SECURITY PROTECTED 5GS NAS MESSAGE. A NAS COUNT is constructed as a NAS sequence number (8 least significant bits) concatenated with a NAS overflow counter (16 most significant bits).

[0040] The NAS message may be a plain 5GS NAS message and would include extended protocol discriminator, security header type associated with a half spare octet or PDU session identity, procedure transaction identity, message type, and other information elements, as required. Alternatively, the NAS message may be a security protected 5GS NAS message and would include extended protocol discriminator, security header type associated with a half spare octet, message authentication code, sequence number, and plain 5GS NAS message. SECURITY PROTECTED 5GS NAS MESSAGE, integrity protection shall include octet 7 to n, i.e. the SQN IE and the NAS message IE.

[0041] The one or more processors **205** further implements the integrity failure determining module **230** configured to determine an integrity failure in relation to the idle mode procedure initiated by the UE when a MAC value calculated at the AMF is different from the MAC value received from the UE.

[0042] The one or more processors **205** further implements the gap count calculation module **235** configured to calculate a gap count by comparing the UE uplink SQN received from the UE and an AMF uplink SQN stored at the AMF. In one case, when the UE uplink SQN received from the UE crosses a predefined count and the AMF

uplink SQN is less than or equal to the predefined count, the gap count is determined by adding a predefined number to the received UE uplink SQN and subtracting the AMF uplink SQN from a sum. In another case, when the UE uplink SQN received from the UE is less than or equal to a predefined count and the AMF uplink SQN crosses the predefined count, the gap count is determined by adding a predefined number to the AMF uplink SQN and subtracting the UE uplink SQN from a sum.

[0043] The one or more processors **205** further implements the overflow count updating module **240** configured to update an overflow count stored at the AMF based on comparison of the gap count and a configured gap count pre-stored at the AMF to make the overflow count stored at the AMF equal to an overflow count stored at the UE. In one case, when the calculated gap count is less than or equal to the configured gap count pre-stored at the AMF and the UE uplink SQN received from the UE exceeds a predefined count and the AMF uplink SQN is less than or equal to the predefined count, the overflow count is incremented. In another case, when the calculated gap count is less than or equal to the configured gap count pre-stored at the AMF and the UE uplink SQN received from the UE is less than or equal to a predefined count and the AMF uplink SQN exceeds the predefined count, the overflow count is decremented.

[0044] The one or more processors **205** further implements the integrity validation module **245** configured to perform integrity validation of the NAS message based on the updated overflow count and the UE uplink SQN received from the UE. To perform the integrity validation, the AMF recalculates a MAC using the UE uplink SQN received from the UE and the updated overflow count. Thereafter, the AMF determines a successful match between the overflow count stored at the AMF and the overflow count stored at the UE.

[0045] One or more parameters associated with operation of one or more of the above described modules are configurable and may be stored in one or more of the database **220** and the distributed cache **225**.

[0046] Referring to **FIG. 3** illustrating a block diagram of the system **125** and the first UE **110a** communicating with each other for handling integrity failures in NAS message for idle mode procedure in a communication network, a preferred embodiment of the system **125** is described. It is to be noted that the embodiment with respect to **FIG. 3** will be explained with respect to the first UE **110a** for the purpose of description and illustration and should nowhere be construed as limited to the scope of the present disclosure.

[0047] The first network device **110a** includes one or more primary processors **305** communicably coupled to the one or more processors **205** of the system **125**. The one or more primary processors **305** are coupled with a memory unit **310** storing instructions which are executed by the one or more primary processors **305**. Execution of the stored instructions by the one or more primary processors **305** enables the first UE **110a** to provide a request for an idle mode procedure. The first UE **110a** further includes a kernel **315** which is a core component serving as the primary interface between hardware components of the first UE **110a** and the plurality of services at the backend database **220**. The kernel **315** is configured to provide the plurality of services on the first UE **110a** to resources available in the communication network **105**. The resources include one of a Central Processing Unit (CPU), memory components such as Random Access Memory (RAM) and Read Only Memory (ROM).

[0048] In the preferred embodiment, the request receiving module **228** of the one or more processors **205** is communicably connected to the kernel **315** of the first UE **110a**. The request receiving module **228** is configured to receive a request for an idle mode procedure from a User Equipment (UE) over N1 interface. The request for the idle mode procedure includes a Message Authentication Code (MAC) and a UE uplink Sequence Number (SQN). The one or more processors **205** further include the integrity failure determining module **230** communicably connected to the request receiving module **228** to determine an integrity failure in relation to the idle mode procedure initiated by the UE when a MAC value calculated at the AMF is different from the MAC value received from the UE. The one or more processors **205** further include the

gap count calculation module **235** communicably connected to the integrity failure determining module **230** to calculate a gap count by comparing the UE uplink SQN received from the UE and an AMF uplink SQN stored at the AMF. The one or more processors **205** further include the overflow count updating module **240** communicably connected to the gap count calculation module **235** to update an overflow count stored at the AMF based on comparison of the gap count and a configured gap count pre-stored at the AMF to make the overflow count stored at the AMF equal to an overflow count stored at the UE. The one or more processors **205** further include the integrity validation module **245** communicably connected to the overflow count updating module **240** to perform integrity validation of the NAS message based on the updated overflow count and the UE uplink SQN received from the UE.

[0049] **FIG. 4** illustrates a timing diagram of a method of connection establishment, release, and reporting integrity failure in a communication network, according to one or more embodiments of the present disclosure. For the purpose of description, the method is described with the embodiments as illustrated in **FIGS. 1, 2, and 3** and should nowhere be construed as limiting the scope of the present disclosure.

[0050] At step **405**, the first UE **110a** sends a registration request to the system/AMF **125** via a Radio Access Network (RAN) **105a**, and the first UE **110a** gets connected with the system/AMF **125**. After connection establishment, the first UE **110a** sends data to the system/AMF **125**, and packet loss occurs during the communication.

[0051] At step **410**, the RAN **105a** sends a Radio Resource Control (RRC) release request to the first UE **110a**. Further, at step **415**, the RAN **105a** sends the release request to the system/AMF **125**. With this, the first UE **110a** initiates procedure to enter in idle mode.

[0052] At step 420, the system/AMF 125 sends confirmation to the RAN 105a to release the connection. At step 425, the RAN 105a sends a release completion message to the system/AMF 125, and the first UE 110a enter in the idle mode.

[0053] At step 430, the first UE 110a indicates to the system/AMF 125 about integrity failure, when the first UE 110a is operating in an uplink or Mobile Originating (MO) mode. Alternatively, when the first UE 110a is operating in a downlink or Mobile Terminating (MT) mode, the system/AMF 125 sends a paging message to the first UE 110a, at step 435. The paging message indicates to the first UE 110a that the system/AMF 125 has a message to share and the system/AMF 125 must monitor the communication channel.

[0054] FIG. 5 illustrates a timing diagram of a method of handling integrity failures in NAS message for idle mode procedure in a communication network, according to one or more embodiments of the present disclosure. For the purpose of description, the method is described with the embodiments as illustrated in FIGS. 1, 2, 3, and 4 and should nowhere be construed as limiting the scope of the present disclosure.

[0055] At step 505, the first UE 110a present in an idle state sends an idle state response i.e. a request for an idle mode procedure to a network, such as the system/AMF 125 via the RAN 105a. The RAN 105a may be a part of the communication network 105 and would be any of the following types: Distributed RAN (D-RAN), Centralized RAN (C-RAN), Virtualized RAN (vRAN), and OpenRAN (O-RAN). The first UE 110a sends the idle state response based on events like service requests or paging requests received from the system/AMF 125 via the RAN 105a. For example, the idle state response may be an MR/PR/SR response. Furthermore, the first UE 110a also transmits a MAC and a UE uplink SQN to the system/AMF 125.

[0056] At step 510, the system/AMF 125 performs an integrity check on the idle state response received from the first UE 110a. The system/AMF 125 determines

integrity failure at the system/AMF **125** when a MAC value calculated at the system/AMF **125** differs from a MAC value received from the first UE **110a**.

[0057] At step **515**, the system/AMF **125** calculates a gap count by comparing the UE uplink SQN received from the first UE **110a** with an AMF uplink SQN stored at the system/AMF **125**. In one case, when the UE uplink SQN is greater than the AMF uplink SQN, the AMF adds a predefined number, for example 255 to the UE uplink SQN and subtracts the AMF uplink SQN from the addition result to obtain the gap count. Conversely, when the UE uplink SQN is smaller than the AMF uplink SQN, the AMF adds the predefined number to the AMF uplink SQN and subtracts the UE uplink SQN to obtain the gap count.

[0058] At step **520**, the system/AMF **125** determines if the calculated gap count is less than or equal to a configured gap count pre-stored at the system/AMF **125**. The system/AMF **125** compares the gap count to update an overflow count.

[0059] At step **525**, the system/AMF **125** updates the overflow count stored at the AMF based on the comparison of the gap count. For example, the system/AMF **125** makes an overflow count stored at the system/AMF **125** equal to an overflow count stored at the first UE **110a** based on the comparison of the gap count. In one implementation, when the calculated gap count is less than or equal to the configured gap count stored at the system/AMF **125** and the UE uplink SQN is greater than the AMF uplink SQN, the system/AMF **125** increments the overflow count by a predefined value, for example 1. Conversely, if the calculated gap count is less than or equal to the configured gap count system/AMF **125** and the UE uplink SQN is smaller than the AMF uplink SQN, the system/AMF **125** decrements the overflow count by the predefined value. In this manner, updating the overflow count ensures synchronization of the overflow count between the system/AMF **125** and the first UE **110a**.

[0060] At step **530**, the system/AMF **125** re-performs the integrity check using an updated overflow count and the UE uplink SQN. By recalculating the MAC value

using these parameters, the system/AMF **125** verifies the integrity of communication. A successful integrity check eliminates the need for resource-intensive re-authentication and re-registration procedures during the idle state of the first UE **110a**. This approach optimizes network resource utilization, promotes cost-effective operations, and reduces signaling overhead.

[0061] FIG. 6 illustrates a flow chart of a method **500** of handling integrity failures in NAS message for idle mode procedure in a communication network, according to one or more embodiments of the present disclosure. For the purpose of description, the method **600** is described with the embodiments as illustrated in FIGS. 1 and 5 and should nowhere be construed as limiting the scope of the present disclosure.

[0062] When a UE is present in an idle state, the UE sends a response to the network, which may be triggered by certain events like a service request or a paging request. The response may contain important information or instructions. Furthermore, a MAC value is also received from the UE, along with a UE uplink SQN. The UE uplink SQN may be understood as a value assigned to the transmission by the UE indicating an order of the transmission. A similar value, referred as an AMF uplink SQN, is also stored at the AMF. On receiving the response from the UE, the AMF may be configured for ensuring the integrity and security of the communication between the UE and the network.

[0063] Accordingly, at step **605**, the AMF detect integrity failure by analyzing an idle state response received from the UE. An integrity failure refers to a situation where the AMF detects that a MAC value at the AMF is different than the MAC value calculated at the UE.

[0064] At step **610**, the method **600** includes the step of calculating a gap count based on an UE uplink SQN received from the UE and an AMF uplink SQN stored at the AMF, by the one or more processors **205**. By comparing the UE uplink SQN and the AMF uplink SQN, the AMF determines the difference or "gap" between the two numbers, to gain insight into transmission status. In an example, when the UE uplink

SN received from the UE is greater than the AMF uplink SN, the gap count is calculated by adding 255 to the UE uplink SN and subtracting the AMF uplink SN from the result to obtain the gap count. In another example, when the UE uplink SN received from the UE is smaller than the AMF uplink SN, the gap count is calculated by adding 255 to the AMF uplink SN and subtracting the UE uplink SN from the result to obtain the gap count.

[0065] At step **615**, the method **600** includes the step of updating an overflow count stored at the AMF, by the one or more processors **205**. The overflow count stored at the AMF is updated by the AMF based on the calculated gap count and a configured gap count pre-stored at the AMF. In an example, when the calculated gap count is less than or equal to the configured gap count that is pre-stored at the AMF and where the UE uplink sequence number received from the UE is greater than the AMF uplink sequence number, the overflow count stored at the AMF is incremented by 1. In another example, when the calculated gap count is less than or equal to the configured gap count pre-stored at the AMF and the UE uplink sequence number received from the UE is smaller than the AMF uplink sequence number, the overflow count stored at the AMF is decremented by 1. In this manner, a value of the overflow count stored at the AMF becomes equal to a value of the overflow count stored at the UE.

[0066] At step **620**, the method **600** includes the step of re-performing an integrity check, by the one or more processors **205**. The integrity check is re-performed by the AMF based on the updated overflow count and the UE uplink SN. The AMF recalculates the MAC value using the UE uplink SN and the updated overflow count. As the value of the overflow count stored at the AMF is made equal to the value of the overflow count stored at the UE, integrity check is performed successfully.

[0067] Accordingly, the need to perform resource and time consuming re-authentication and/or re-registration procedures during occurrence of integrity failure in an idle state of UE, is averted. This, in turn, facilitates optimized usage of network resources and economical operations. Further, signaling overheads are also reduced with such methodology.

[0068] The present invention further discloses a non-transitory computer-readable medium having stored thereon computer-readable instructions. The computer-readable instructions are executed by the processor 205. The processor 205 is configured to receive a request for an idle mode procedure from a User Equipment (UE). The request for the idle mode procedure includes a Message Authentication Code (MAC) and a UE uplink Sequence Number (SQN). The processor 205 is further configured to determine an integrity failure in relation to the idle mode procedure initiated by the UE when a MAC value calculated at the AMF is different from the MAC value received from the UE. The processor 205 is further configured to calculate a gap count by comparing the UE uplink SQN received from the UE and an AMF uplink SQN stored at the AMF. The processor 205 is further configured to update an overflow count stored at the AMF based on comparison of the gap count and a configured gap count pre-stored at the AMF to make the overflow count stored at the AMF equal to an overflow count stored at the UE. The processor 205 is further configured to perform integrity validation of the NAS message based on the updated overflow count and the UE uplink SQN received from the UE.

[0069] A person of ordinary skill in the art will readily ascertain that the illustrated embodiments and steps in description and drawings (FIGS.1-6) are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments.

[0070] The above described techniques of the present disclosure provide multiple advantages, including averting the need of performing re-authentication or re-registration procedure when an integrity failure occurs during idle state of UE. Averting such procedures facilitate optimized usage of network resources and economical operations. Further, implementation of techniques of the present disclosure also results in reduction of signaling overheads. Present disclosure also offers the technical advantage of checking integrity of packets to ensure no attack occurs in case when someone tries to modify or corrupt data packets.

[0071] The present invention offers multiple advantages over the prior art and the above listed are a few examples to emphasize on some of the advantageous features. The listed advantages are to be read in a non-limiting manner.

[0072] Server: A server may include or comprise, by way of example but not limitation, one or more of a standalone server, a server blade, a server rack, a bank of servers, a server farm, hardware supporting a part of a cloud service or system, a home server, hardware running a virtualized server, one or more processors executing code to function as a server, one or more machines performing server-side functionality as described herein, at least a portion of any of the above, some combination thereof. In an embodiment, the entity may include, but is not limited to, a vendor, a network operator, a company, an organization, a university, a lab facility, a business enterprise, a defence facility, or any other facility that provides content.

[0073] Network: A network may include, by way of example but not limitation, at least a portion of one or more networks having one or more nodes that transmit, receive, forward, generate, buffer, store, route, switch, process, or a combination thereof, etc. one or more messages, packets, signals, waves, voltage or current levels, some combination thereof, or so forth. The network may also include, by way of example but not limitation, one or more of a wireless network, a wired network, an internet, an intranet, a public network, a private network, a packet-switched network, a circuit-switched network, an ad hoc network, an infrastructure network, a Public-

Switched Telephone Network (PSTN), a cable network, a cellular network, a satellite network, a fiber optic network, or some combination thereof.

[0074] UE/ Wireless Device: A wireless device or a user equipment (UE) may include, but are not limited to, a handheld wireless communication device (e.g., a mobile phone, a smart phone, a phablet device, and so on), a wearable computer device (e.g., a head-mounted display computer device, a head-mounted camera device, a wristwatch computer device, and so on), a Global Positioning System (GPS) device, a laptop computer, a tablet computer, or another type of portable computer, a media playing device, a portable gaming system, and/or any other type of computer device with wireless communication capabilities, and the like. In an embodiment, the UEs may communicate with the system via set of executable instructions residing on any operating system. In an embodiment, the UEs may include, but are not limited to, any electrical, electronic, electro-mechanical or an equipment or a combination of one or more of the above devices such as virtual reality (VR) devices, augmented reality (AR) devices, laptop, a general-purpose computer, desktop, personal digital assistant, tablet computer, mainframe computer, or any other computing device, wherein the computing device may include one or more in-built or externally coupled accessories including, but not limited to, a visual aid device such as camera, audio aid, a microphone, a keyboard, input devices for receiving input from a user such as touch pad, touch enabled screen, electronic pen and the like. It may be appreciated that the UEs may not be restricted to the mentioned devices and various other devices may be used.

[0075] System (for example, computing system): A system may include one or more processors coupled with a memory, wherein the memory may store instructions which when executed by the one or more processors may cause the system to perform offloading/onloading of broadcasting or multicasting content in networks. An exemplary representation of the system for such purpose, in accordance with embodiments of the present disclosure. In an embodiment, the system may include one or more processor(s). The one or more processor(s) may be implemented as one or

more microprocessors, microcomputers, microcontrollers, edge or fog microcontrollers, digital signal processors, central processing units, logic circuitries, and/or any devices that process data based on operational instructions. Among other capabilities, the one or more processor(s) may be configured to fetch and execute computer-readable instructions stored in a memory of the system. The memory may be configured to store one or more computer-readable instructions or routines in a non-transitory computer readable storage medium, which may be fetched and executed to create or share data packets over a network service. The memory may comprise any non-transitory storage device including, for example, volatile memory such as Random-Access Memory (RAM), or non-volatile memory such as Electrically Erasable Programmable Read-only Memory (EPROM), flash memory, and the like. In an embodiment, the system may include an interface(s). The interface(s) may comprise a variety of interfaces, for example, interfaces for data input and output devices, referred to as input/output (I/O) devices, storage devices, and the like. The interface(s) may facilitate communication for the system. The interface(s) may also provide a communication pathway for one or more components of the system. Examples of such components include, but are not limited to, processing unit/engine(s) and a database. The processing unit/engine(s) may be implemented as a combination of hardware and programming (for example, programmable instructions) to implement one or more functionalities of the processing engine(s). In examples described herein, such combinations of hardware and programming may be implemented in several different ways. For example, the programming for the processing engine(s) may be processor executable instructions stored on a non-transitory machine-readable storage medium and the hardware for the processing engine(s) may comprise a processing resource (for example, one or more processors), to execute such instructions. In the present examples, the machine-readable storage medium may store instructions that, when executed by the processing resource, implement the processing engine(s). In such examples, the system may include the machine-readable storage medium storing the instructions and the processing resource to execute the instructions, or the machine-readable storage medium may be separate but accessible to the system and the

processing resource. In other examples, the processing engine(s) may be implemented by electronic circuitry. In an aspect, the database may comprise data that may be either stored or generated as a result of functionalities implemented by any of the components of the processor or the processing engines.

[0076] Computer System: A computer system may include an external storage device, a bus, a main memory, a read-only memory, a mass storage device, communication port(s), and a processor. A person skilled in the art will appreciate that the computer system may include more than one processor and communication ports. The communication port(s) may be any of an RS-232 port for use with a modem-based dialup connection, a 10/100 Ethernet port, a Gigabit or 10 Gigabit port using copper or fiber, a serial port, a parallel port, or other existing or future ports. The communication port(s) may be chosen depending on a network, such a Local Area Network (LAN), Wide Area Network (WAN), or any network to which the computer system connects. The main memory may be random access memory (RAM), or any other dynamic storage device commonly known in the art. The read-only memory may be any static storage device(s) including, but not limited to, a Programmable Read Only Memory (PROM) chips for storing static information e.g., start-up or basic input/output system (BIOS) instructions for the processor. The mass storage device may be any current or future mass storage solution, which may be used to store information and/or instructions. The bus communicatively couples the processor with the other memory, storage, and communication blocks. The bus can be, e.g. a Peripheral Component Interconnect (PCI) / PCI Extended (PCI-X) bus, Small Computer System Interface (SCSI), universal serial bus (USB), or the like, for connecting expansion cards, drives, and other subsystems as well as other buses, such a front side bus (FSB), which connects the processor to the computer system. Optionally, operator and administrative interfaces, e.g. a display, keyboard, and a cursor control device, may also be coupled to the bus to support direct operator interaction with the computer system. Other operator and administrative interfaces may be provided through network connections connected through the communication

port(s). In no way should the aforementioned exemplary computer system limit the scope of the present disclosure.

REFERENCE NUMERALS

- [0077] Communication network - 105;
- [0078] Radio Access Network (RAN) – 105a;
- [0079] User Equipment - 110;
- [0080] Server - 115;
- [0081] System - 125;
- [0082] One or more processors -205;
- [0083] Memory – 210;
- [0084] Input/output interface unit – 215;
- [0085] Database – 220;
- [0086] Distributed cache – 225;
- [0087] Request receiving module – 228;
- [0088] Integrity failure determining module – 230;
- [0089] Gap count calculation module – 235;
- [0090] Overflow count updating module – 240;
- [0091] Integrity validation module - 245;
- [0092] First UE – 110a;
- [0093] Primary processor of first UE - 305;
- [0094] Memory unit of first UE – 310; and
- [0095] Kernel – 315.

We Claim:

1. A method of handling integrity failures in Non-Access Stratum (NAS) message for idle mode procedure in a communication network, the method comprising:

receiving, by an Access and Mobility Management Function (AMF), a request for an idle mode procedure from a User Equipment (UE), wherein the request for the idle mode procedure includes a Message Authentication Code (MAC) and a UE uplink Sequence Number (SQN);

determining, by the AMF, an integrity failure in relation to the idle mode procedure initiated by the UE when a MAC value calculated at the AMF is different from the MAC value received from the UE;

calculating, by the AMF, a gap count by comparing the UE uplink SQN received from the UE and an AMF uplink SQN stored at the AMF;

updating, by the AMF, an overflow count stored at the AMF based on comparison of the gap count and a configured gap count pre-stored at the AMF to make the overflow count stored at the AMF equal to an overflow count stored at the UE; and

performing, by the AMF, integrity validation of the NAS message based on the updated overflow count and the UE uplink SQN received from the UE.

2. The method as claimed in claim 1, wherein for performing the integrity validation, the AMF:

recalculates a MAC using the UE uplink SQN received from the UE and the updated overflow count; and

determines a successful match between the overflow count stored at the AMF and the overflow count stored at the UE.

3. The method as claimed in claim 1, wherein the request for the idle mode procedure is received as one of a Mobility Request (MR), Periodic Request (PR), and a Service Request (SR).

4. The method as claimed in claim 3, wherein the request includes one or more of a SQN and a NAS message.
5. The method as claimed in claim 1, wherein when the UE uplink SQN received from the UE crosses a predefined count and the AMF uplink SQN is less than or equal to the predefined count, the gap count is determined by adding a predefined number to the received UE uplink SQN and subtracting the AMF uplink SQN from a sum.
6. The method as claimed in claim 1, wherein when the UE uplink SQN received from the UE is less than or equal to a predefined count and the AMF uplink SQN crosses the predefined count, the gap count is determined by adding a predefined number to the AMF uplink SQN and subtracting the UE uplink SQN from a sum.
7. The method as claimed in claim 1, wherein when the calculated gap count is less than or equal to the configured gap count pre-stored at the AMF and the UE uplink SQN received from the UE exceeds a predefined count and the AMF uplink SQN is less than or equal to the predefined count, the overflow count is incremented.
8. The method as claimed in claim 1, wherein when the calculated gap count is less than or equal to the configured gap count pre-stored at the AMF and the UE uplink SQN received from the UE is less than or equal to a predefined count and the AMF uplink SQN exceeds the predefined count, the overflow count is decremented.
9. A system for handling integrity failures in Non-Access Stratum (NAS) message for idle mode procedure in a communication network, the system comprising:
 - a User Equipment (UE); and
 - an Access and Mobility Management Function (AMF),

wherein the UE is configured to send a request for an idle mode procedure to the AMF, and the request for the idle mode procedure includes a Message Authentication Code (MAC) and a UE uplink Sequence Number (SQN), and

the AMF is configured to:

receive the request for the idle mode procedure from the UE;

determine an integrity failure in relation to the idle mode procedure initiated by the UE when a MAC value calculated at the AMF is different from the MAC value received from the UE;

calculate a gap count by comparing the UE uplink SQN received from the UE and an AMF uplink SQN stored at the AMF;

update an overflow count stored at the AMF based on comparison of the gap count and a configured gap count pre-stored at the AMF to make the overflow count stored at the AMF equal to an overflow count stored at the UE; and

perform integrity validation of the NAS message based on the updated overflow count and the UE uplink SQN received from the UE.

10. The system as claimed in claim 9, wherein for performing the integrity validation, the AMF:

recalculates a MAC value using the UE uplink sequence number received from the UE and the updated overflow count; and

determines a successful match between the overflow count stored at the AMF and the overflow count stored at the UE.

11. The system as claimed in claim 9, wherein the request for the idle mode procedure is received as one of a Mobility Request (MR), Periodic Request (PR), and a Service Request (SR).

12. The system as claimed in claim 11, wherein the request includes one or more of a SQN and a NAS message.

13. The system as claimed in claim 9, wherein when the UE uplink SQN received from the UE crosses a predefined count and the AMF uplink SQN is less than or equal to the predefined count, the gap count is determined by adding a predefined number to the received UE uplink SQN and subtracting the AMF uplink SQN from a sum.

14. The system as claimed in claim 9, wherein when the UE uplink SQN received from the UE is less than or equal to a predefined count and the AMF uplink SQN crosses the predefined count and is greater than or equal to 0, the gap count is determined by adding a predefined number to the AMF uplink SQN and subtracting the UE uplink SQN from a sum.

15. The system as claimed in claim 9, wherein when the calculated gap count is less than or equal to the configured gap count pre-stored at the AMF and the UE uplink SQN received from the UE exceeds a predefined count and the AMF uplink SQN is less than or equal to the predefined count, the overflow count is incremented.

16. The system as claimed in claim 9, wherein when the calculated gap count is less than or equal to the configured gap count pre-stored at the AMF and the UE uplink SQN received from the UE is less than or equal to a predefined count and the AMF uplink SQN exceeds the predefined count, the overflow count is decremented.

17. A non-transitory computer-readable medium having stored thereon computer-readable instructions that, when executed by a processor, cause the processor to:

receive a request for an idle mode procedure from a User Equipment (UE), wherein the request for the idle mode procedure includes a Message Authentication Code (MAC) value and a UE uplink Sequence Number (SQN);

determine an integrity failure in relation to the idle mode procedure initiated by the UE when a MAC value calculated at an Access and Mobility Management Function (AMF) is different from the MAC value received from the UE;

calculate a gap count by comparing the UE uplink SQN received from the UE and an AMF uplink SQN stored at the AMF;

update an overflow count stored at the AMF based on comparison of the gap count and a configured gap count pre-stored at the AMF to make the overflow count stored at the AMF equal to an overflow count stored at the UE; and

perform integrity validation of the NAS message based on the updated overflow count and the UE uplink SQN received from the UE.

18. A User Equipment (UE) comprising:

a processor coupled with a memory, wherein said memory stores instructions which when executed by the processor causes the UE to:

send a request for an idle mode procedure to an Access and Mobility Management Function (AMF), wherein the request for the idle mode procedure includes a Message Authentication Code (MAC) and a UE uplink Sequence Number (SQN),

wherein the AMF is configured to perform the steps as claimed in claim 1.

1/6

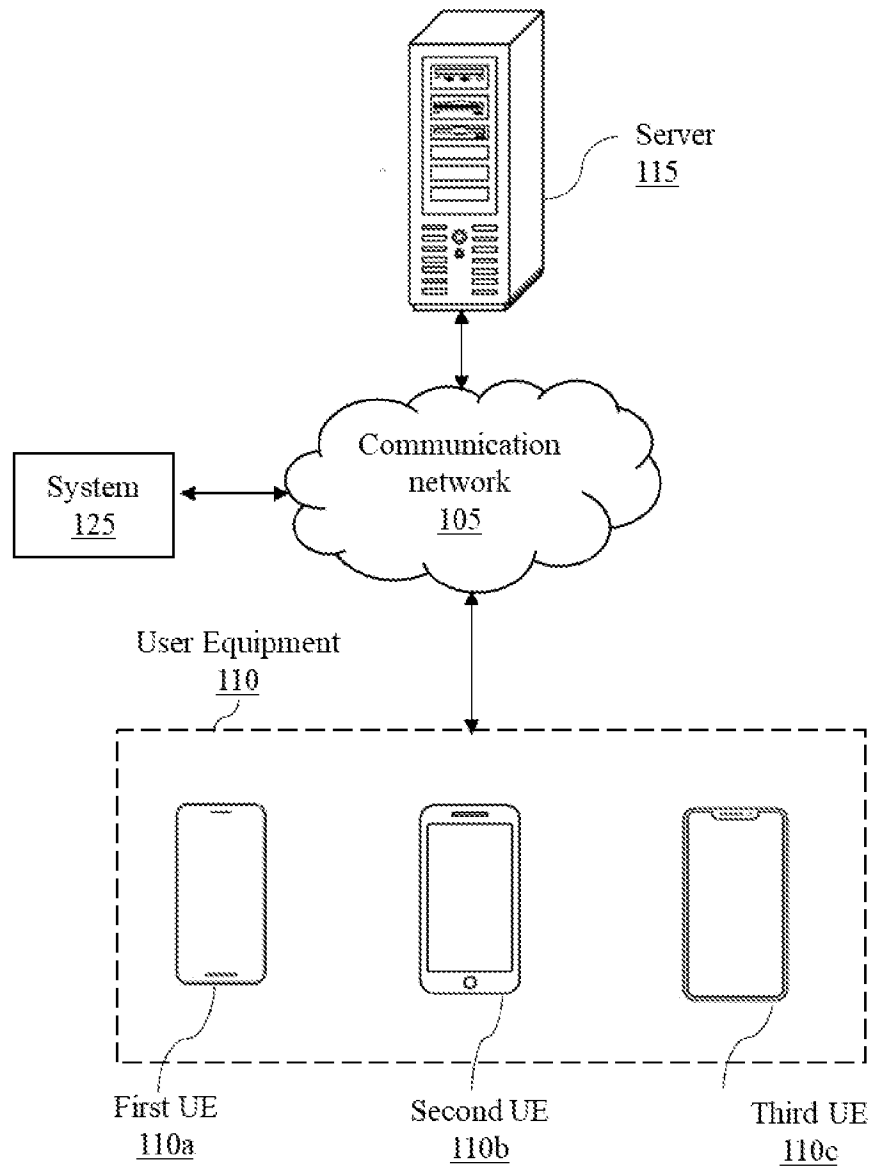


FIG. 1

2/6

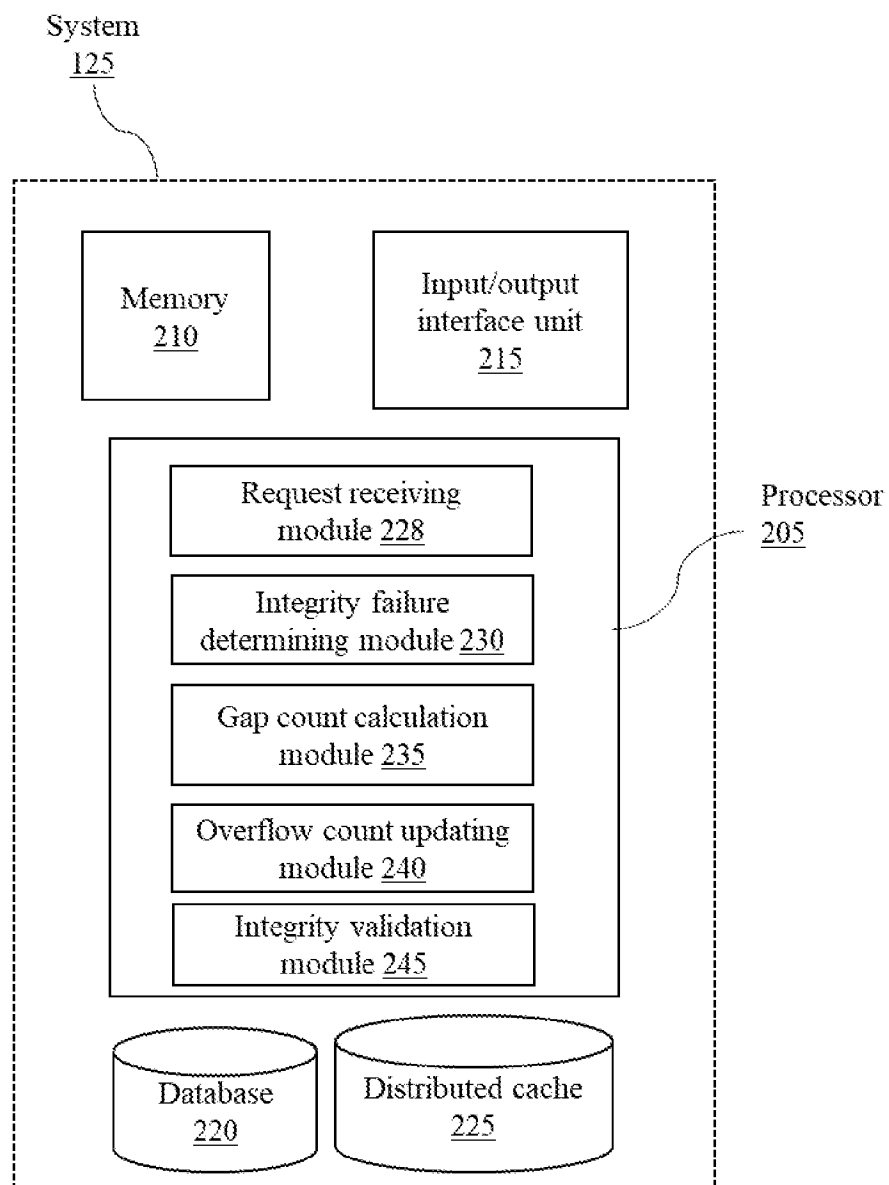


FIG. 2

3/6

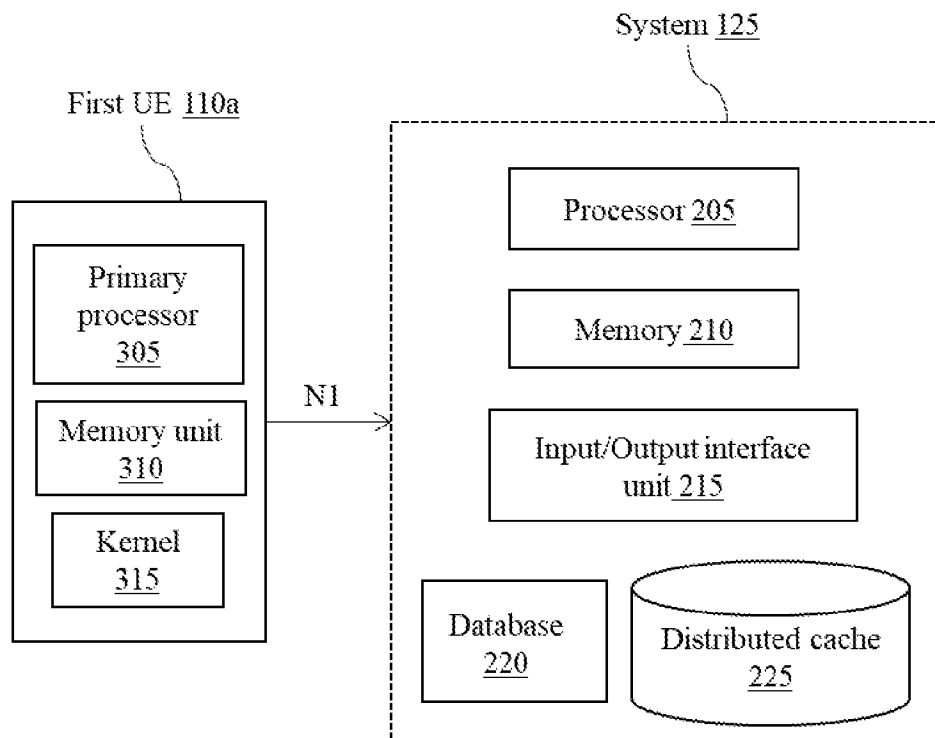


FIG. 3

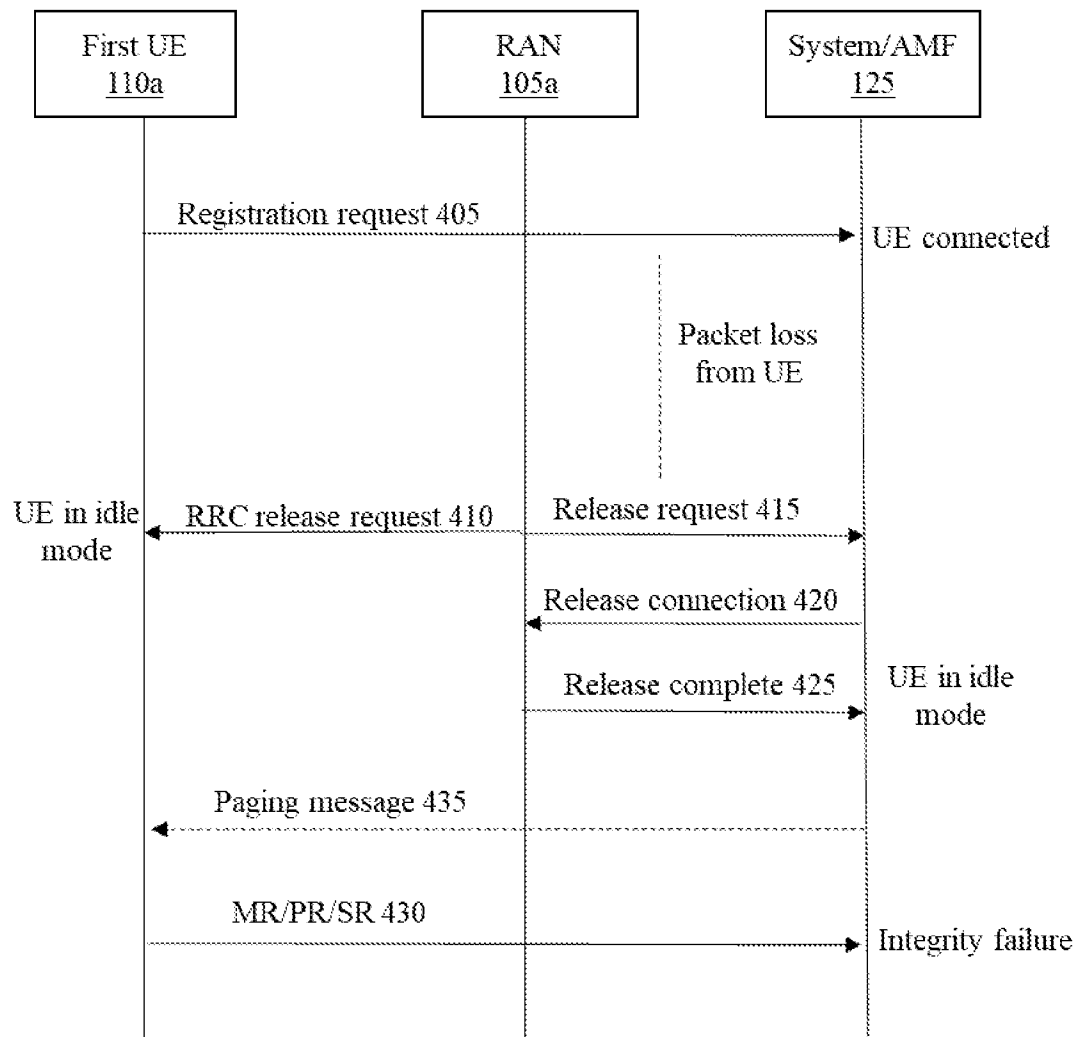


FIG. 4

5/6

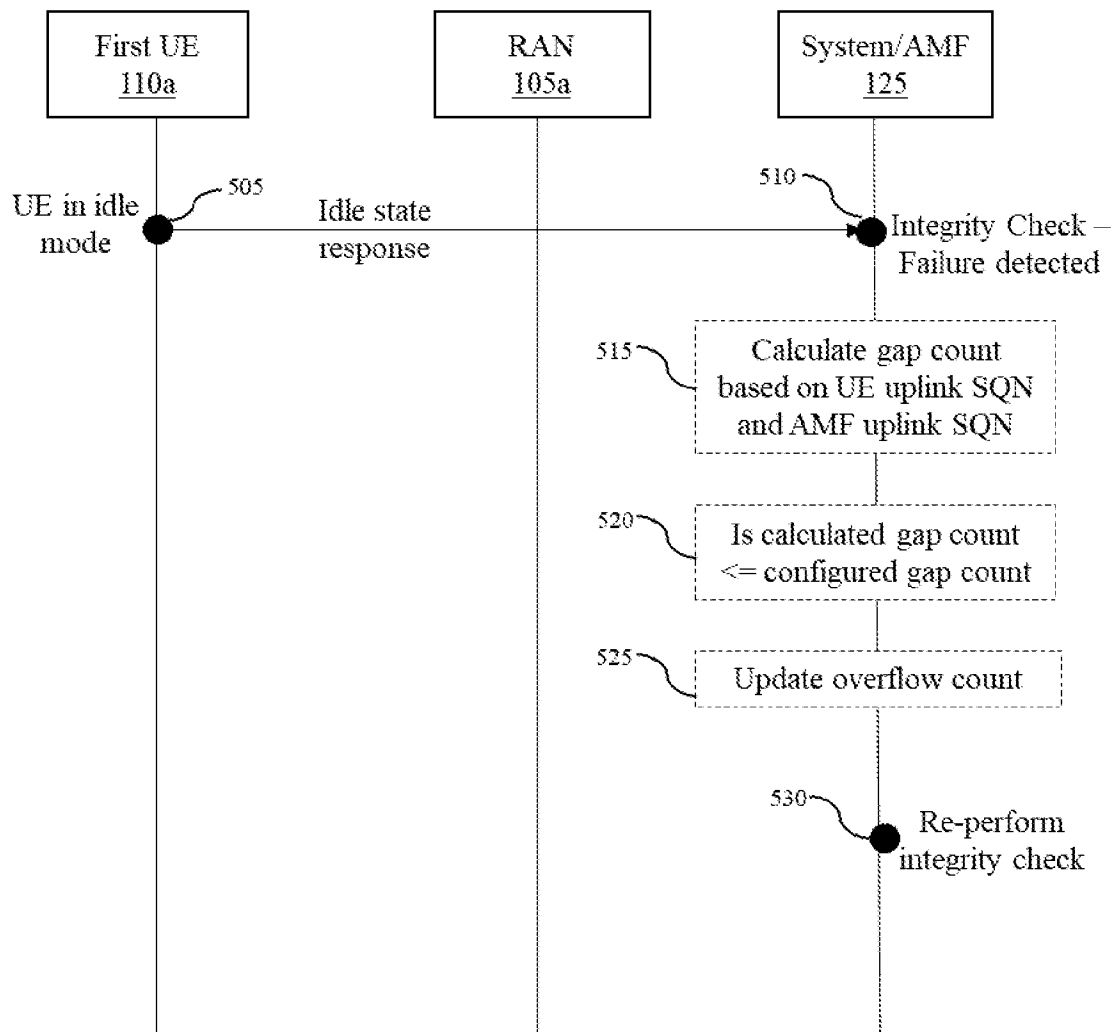


FIG. 5

6/6

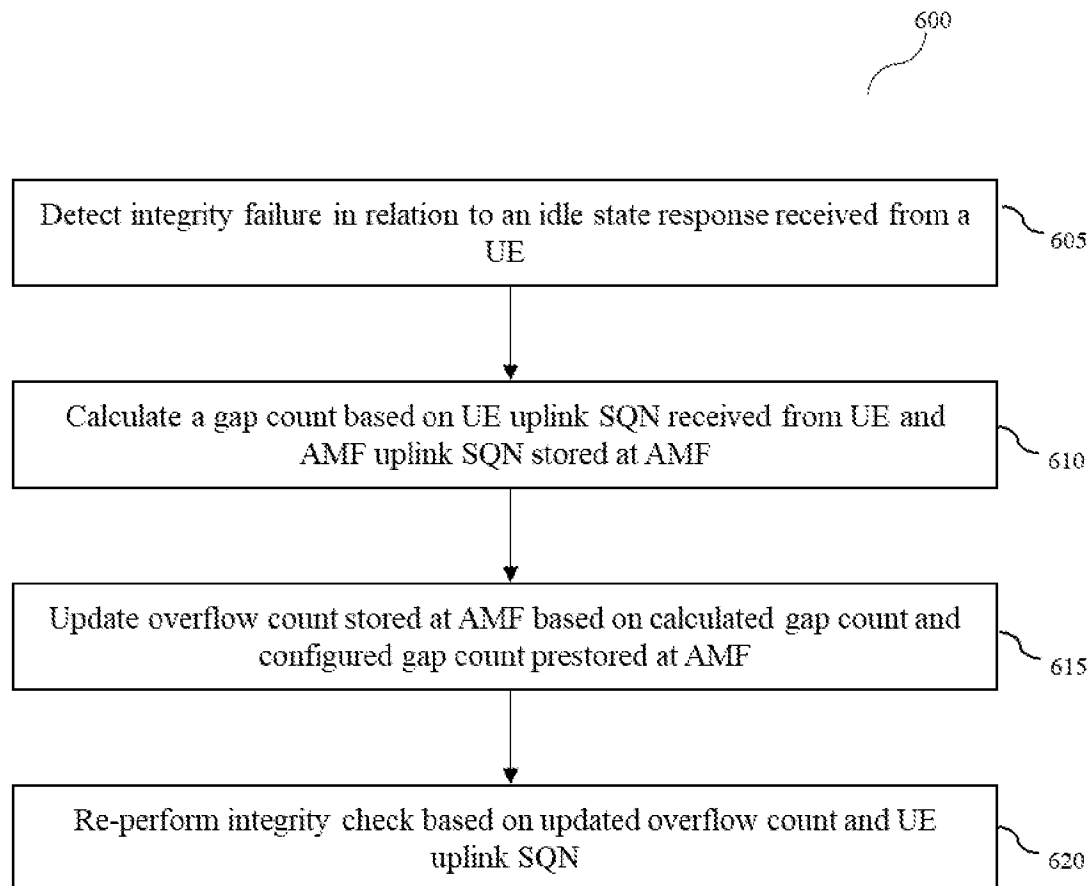


FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IN2024/050928

A. CLASSIFICATION OF SUBJECT MATTER

H04W76/25, H04W12/06, H04W60/04 Version=2024.01

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

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

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

Databases: Patseer, Google search, IPO internal database

Keywords: Access and Mobility Management Function, MAC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO2020207401A1 (MEDIATEK SINGAPORE PTE LTD) 15 October 2020 (15-10-2020) (Whole Document)	1-18
Y	US20220007182A1 (APPLE INC) 06 January 2022 (06-01-2022) (Abstract, Paragraphs [0003], [0015]-[0020], [0024]-[0028], [0034]-[0037], [0040], [0052], [0056], [0077])	1-18

☐ 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

"D" document cited by the applicant in the international application

"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

"I" 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

29-10-2024

Date of mailing of the international search report

29-10-2024

Name and mailing address of the ISA/

Indian Patent Office

Plot No.32, Sector 14, Dwarka, New Delhi-110075

Facsimile No.

Authorized officer

Sourabh Sharma

Telephone No. +91-1125300200

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IN2024/050928

Citation	Pub.Date	Family	Pub.Date
WO 2020207401 A1	15-10-2020	US 2020323017 A1	08-10-2020
		TW 202038675 A	16-10-2020
		CN 112055984 A	08-12-2020
US 20220007182 A1	06-01-2022	CN 113016202 A	22-06-2021
		WO 2020092542 A1	07-05-2020