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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 March 2020 (26.03.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/060245 A1

(51) International Patent Classification:
*H04L 9/08* (2006.01) *H04L 29/08* (2006.01)
*H04W 12/04* (2009.01)

(21) International Application Number:
PCT/KR2019/012173

(22) International Filing Date:
19 September 2019 (19.09.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2018-0112498 19 September 2018 (19.09.2018) KR
10-2018-0127036 23 October 2018 (23.10.2018) KR

(71) Applicant: **SAMSUNG ELECTRONICS CO., LTD.** [KR/KR]; 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 16677 (KR).

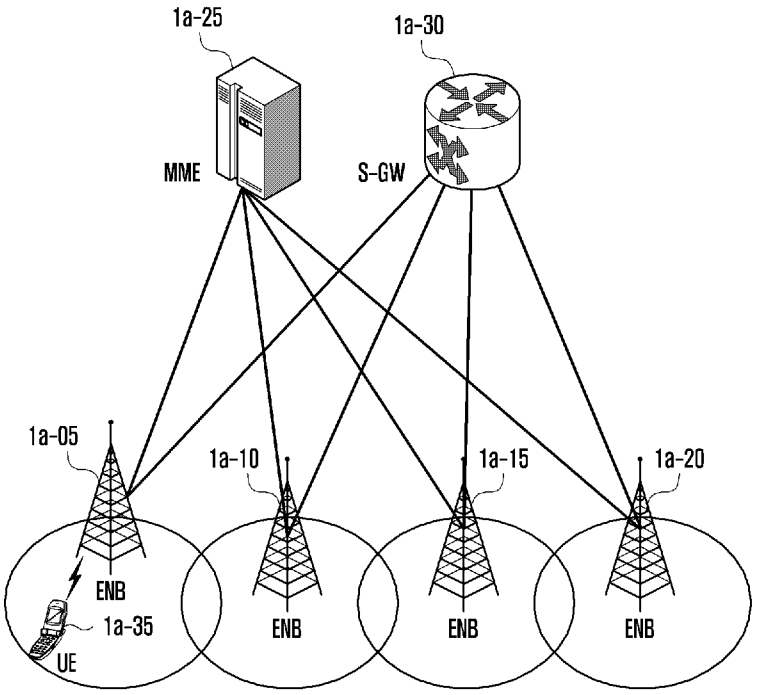
(72) Inventors: **KIM, Donggun**; 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 16677 (KR). **KIM, Soenghun**; 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 16677 (KR).

(74) Agent: **YOON & LEE INTERNATIONAL PATENT & LAW FIRM**; 3rd Fl, Ace Highend Tower-5, 226, Gasan Digital 1-ro, Geumcheon-gu, Seoul 08502 (KR).

(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, 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,

(54) Title: METHOD AND APPARATUS FOR IDENTIFYING SECURITY KEY IN NEXT GENERATION MOBILE COMMUNICATION SYSTEM




(57) Abstract: The disclosure relates to a communication scheme and system for converging a 5th generation (5G) communication system for supporting a data rate higher than that of a 4th generation (4G) system with an internet of things (IoT) technology. The disclosure is applicable to intelligent services (e.g., smart home, smart building, smart city, smart car or connected car, health care, digital education, retail, and security and safety-related services) based on the 5G communication technology and the IoT-related technology. The disclosure relates to a method and apparatus for allowing a base station to identify a ciphering key (COUNT value) for security enhancement.

[Continued on next page]

WO 2020/060245 A1

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, 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))*

# Description

# Title of Invention: METHOD AND APPARATUS FOR IDENTIFYING SECURITY KEY IN NEXT GENERATION MOBILE COMMUNICATION SYSTEM

## Technical Field

[1] The disclosure relates to operations of a terminal and a base station in a mobile communication system and, in particular, to a ciphering key (COUNT value) identification method and apparatus of the base station for security enhancement in a next generation mobile communication system. The disclosure also relates to a method and apparatus for configuring and supporting device-to-device communication in the next generation mobile communication system.

## Background Art

[2] To meet the increased demand for wireless data traffic since the deployment of 4G communication systems, efforts have been made to develop an improved 5G or pre-5G communication system. Therefore, the 5G or pre-5G communication system is also called a "Beyond 4G Network" or a "Post LTE System".

[3] Implementation of the 5G communication system in higher frequency (mmWave) bands, e.g., 60 GHz bands, is being considered in order to accomplish higher data rates. To decrease propagation loss of radio waves and increase the transmission distance, beamforming, massive multiple-input multiple-output (MIMO), Full Dimensional MIMO (FD-MIMO), array antenna, analog beam forming, and large scale antenna techniques are being discussed for the 5G communication system.

[4] In addition, in the 5G communication system, there are developments under way for system network improvement based on advanced small cells, cloud Radio Access Networks (RANs), ultra-dense networks, device-to-device (D2D) communication, wireless backhaul, moving network, cooperative communication, Coordinated Multi-Points (CoMP), reception-end interference cancellation, and the like. In the 5G system, Hybrid FSK and QAM Modulation (FQAM) and sliding window superposition coding (SWSC) as advanced coding modulation (ACM) and filter bank multi carrier (FBMC), non-orthogonal multiple access (NOMA), and sparse code multiple access (SCMA) as advanced access technology have been developed.

[5] The 5G systems will support more diverse services in comparison with the legacy 4G systems. Examples of representative services may include enhanced mobile broadband (eMBB) services, ultra-reliable and low latency communication (URLLC) services, massive machine type communication (mMTC) services, and evolved multimedia broadcast/multicast services (eMBMS). A system supporting the URLLC

services may be called URLLC system, and a system supporting the eMBB services may be called eMBB system. The terms "service" and "system" may be interchangeably used.

[6] Among these services, the URLLC service is newly considered for the 5G system, while not being considered for 4G systems, and has requirements of ultra-reliability (e.g., packet error rate of about 10-5) and low latency (e.g., about 0.5 msec). In order to meet such demanding requirements, the URLLC service may be provided with a transmission time interval shorter than that of the eMBB service in consideration of various operation schemes.

[7] Meanwhile, the Internet is evolving from a human-centric communication network in which information is generated and consumed by humans to the Internet of things (IoT) in which distributed things or components exchange and process information. The combination of the cloud server-based Big data processing technology and the IoT begets Internet of everything (IoE) technology. In order to secure the sensing technology, wired/wireless communication and network infrastructure, service interface technology, and security technology required for implementing the IoT, recent research has focused on sensor network, machine-to-machine (M2M), and machine-type communication (MTC) technologies. In the IoT environment, it is possible to provide an intelligent Internet Technology that is capable of collecting and analyzing data generated from connected things to create new values for human life. The IoT can be applied to various fields such as smart home, smart building, smart city, smart car or connected car, smart grid, health care, smart appliance, and smart medical service through legacy information technology (IT) and convergence of various industries.

[8] There are various attempts to apply the IoT to the 5G communication system. For example, the sensor network, Machine to Machine (M2M), and Machine Type Communication (MTC) technologies are implemented by means of the 5G communication technologies such as beamforming, MIMO, and array antenna. The application of the aforementioned cloud RAN as a big data processing technology is an example of convergence between the 5G and IoT technologies.

## Disclosure of Invention

## Technical Problem

[9] In a next generation mobile communication system, terminals and base stations cipher and decipher data to be transmitted and received. Typically, a ciphering and deciphering algorithm is used to cipher and decipher data with an ciphering key (or security key). The ciphering key includes ciphering keys (e.g., KgNB and K_RRCenc) agreed between a terminal and a base station and security keys (e.g., COUNT values)

varying with data. Because the COUNT value consists of a PDCP sequence number and a hyper frame number (HFN), it is necessary to acquire synchronization of a PDCP sequence number between a transmitting PDCP entity and a receiving PDCP entity. Given that the PDCP sequence number increases from 0 to 2^(PDCP sequence number length)-1 and, if reaching its maximum value, it goes back to 0 and the HFN number increases by 1; if the PDCP sequence number restarts from 0 after it reaches its maximum value, the COUNT value in use for data ciphering by the transmitting PDCP entity and the COUNT value in use for data description by the receiving PDCP entity may differ from each other, which leads to a decoding failure and HFN desynchronization problem.

[10] Such decoding failure and HFN desynchronization problem may be caused by a large amount of data loss or unexpected data invasion by a hacker. Accordingly, in case of necessity, e.g., if suspected of decoding failure or HFN desynchronization problem or data invasion by a hacker, it is necessary for the base station to verify whether the COUNT value is well synchronized between the transmitting PDCP entity and the receiving PDCP entity.

[11] Meanwhile, the next generation mobile communication system may be deployed for controlling a large number of wireless devices, which facilitates factory automation. In order to guarantee errorless operations of the wireless devices in an automated factory, the communication system has to support low-latency high-liability data transmission among the wireless devices (Industrial IoT devices).

[12] The objects of the disclosure are not limited to the aforesaid, and other objects not described herein will be clearly understood by those skilled in the art from the descriptions below.

## Solution to Problem

[13] In accordance with an aspect of the present disclosure, a method of a terminal in a wireless communication system is provided. The method comprises receiving, from a base station, a first message including a first list associated with count values of the base station, the first list includes at least one bearer identity, at least one first downlink count value of the base station associated to each bearer, and at least one first uplink count value of the base station associated to each bearer; determining whether a first bearer is configured with a new radio (NR) packet data convergence protocol (PDCP); in case that the first bearer is configured with the NR PDCP, and at least one of a second downlink count value of the terminal associated to the first bearer is different from the first downlink count value associated to the first bearer or a second uplink count value of the terminal associated to the first bearer is different from the first uplink count value associated to the first bearer, generating a second list as-

sociated with count values of the terminal including a first bearer identity of the first bearer, the second downlink count value of the terminal associated to the first bearer, and the second uplink count value of the terminal associated to the first bearer; and transmitting, to the base station, a second message including the second list as a response to the first message, wherein the second downlink count value of the terminal associated to the first bearer is a count value of a next PDCP service data unit (SDU) expected to be received - 1, and the second uplink count value of the terminal associated to the first bearer is a count value of a next PDCP SDU to be transmitted - 1.

[14] In one embodiment, the generating the second list further comprises in case that the first bearer is not configured with the NR PDCP, and at least one of a third downlink count value of the terminal associated to the first bearer is different from the first downlink count value associated to the first bearer or a third uplink count value of the terminal associated to the first bearer is different from the first uplink count value associated to the first bearer, generating the second list including the first bearer identity, the third downlink count value of the terminal associated to the first bearer, and the third uplink count value of the terminal associated to the first bearer.

[15] In one embodiment, the method further comprises in case that the first bearer is unidirectional bearer, determining that at least one of the second downlink count value of the terminal associated to the first bearer or the second uplink count value of the terminal associated to the first bearer is to be 0 for an unused direction.

[16] In one embodiment, the generating the second list further comprises in case that a second bearer identity of a second bearer established on the terminal is not included in the first list, generating the second list including the second bearer identity of the second bearer, a fourth downlink count value of the terminal associated to the second bearer, and a fourth uplink count value of the terminal associated to the second bearer, and the fourth downlink count value of the terminal associated to the second bearer is a count value of a next PDCP SDU expected to be received - 1 and the fourth uplink count value of the terminal associated to the second bearer is a count value of a next PDCP SDU to be transmitted - 1.

[17] In one embodiment, the method further comprises in case that a third bearer included in the first list is not established on the terminal, generating the second list including a third identity of the third bearer, a fifth downlink count value of the terminal associated to the third bearer, and a fifth uplink count value of the terminal associated to the third bearer with most significant bits set identical to a first downlink count value associated to the third bearer and a first uplink count value associated to the third bearer and least significant bits set to 0.

[18] The present disclosure also provides a method of a base station in a wireless communication system. The method comprises transmitting, to a terminal, a first message

including a first list associated with count values of the base station, the first list includes at least one bearer identity, at least one first downlink count value of the base station associated to each bearer, and at least one first uplink count value of the base station associated to each bearer; and receiving, from the terminal, a second message including a second list associated with count values of the terminal including a first bearer identity of a first bearer, a second downlink count value of the terminal associated to the first bearer, and a second uplink count value of the terminal associated to the first bearer, as a response to the first message, in case that the first bearer is configured with the NR PDCP, and at least one of the second downlink count value of the terminal associated to the first bearer is different from the first downlink count value associated to the first bearer or the second uplink count value of the terminal associated to the first bearer is different from the first uplink count value associated to the first bearer, wherein the second downlink count value of the terminal associated to the first bearer is a count value of a next PDCP service data unit (SDU) expected to be received - 1, and the second uplink count value of the terminal associated to the first bearer is a count value of a next PDCP SDU to be transmitted - 1.

[19] In one embodiment, in case that the first bearer is not configured with the NR PDCP, and at least one of a third downlink count value of the terminal associated to the first bearer is different from the first downlink count value associated to the first bearer or a third uplink count value of the terminal associated to the first bearer is different from the first uplink count value associated to the first bearer, the second list includes the first bearer identity, the third downlink count value of the terminal associated to the first bearer, and the third uplink count value of the terminal associated to the first bearer.

[20] In one embodiment, in case that the first bearer is uni-directional bearer, at least one of the second downlink count value of the terminal associated to the first bearer or the second uplink count value of the terminal associated to the first bearer is to be 0 for an unused direction.

[21] In one embodiment, in case that a second bearer identity of a second bearer established on the terminal is not included in the first list, the second list includes the second bearer identity of the second bearer, a fourth downlink count value of the terminal associated to the second bearer, and a fourth uplink count value of the terminal associated to the second bearer, and the fourth downlink count value of the terminal associated to the second bearer is a count value of a next PDCP SDU expected to be received - 1 and the fourth uplink count value of the terminal associated to the second bearer is a count value of a next PDCP SDU to be transmitted - 1

[22] In one embodiment, in case that a third bearer included in the first list is not established on the terminal, the second list includes a third identity of the third bearer, a

fifth downlink count value of the terminal associated to the third bearer, and a fifth uplink count value of the terminal associated to the third bearer with most significant bits set identical to a first downlink count value associated to the third bearer and a first uplink count value associated to the third bearer and least significant bits set to 0.

[23] The present disclosure also provides a terminal in a wireless communication system. The terminal comprises a transceiver; and a controller configured to: control the transceiver to receive, from a base station, a first message including a first list associated with count values of the base station, the first list includes at least one bearer identity, at least one first downlink count value of the base station associated to each bearer, and at least one first uplink count value of the base station associated to each bearer, determine whether a first bearer is configured with a new radio (NR) packet data convergence protocol (PDCP), in case that the first bearer is configured with the NR PDCP, and at least one of a second downlink count value of the terminal associated to the first bearer is different from the first downlink count value associated to the first bearer or a second uplink count value of the terminal associated to the first bearer is different from the first uplink count value associated to the first bearer, generate a second list associated with count values of the terminal including a first bearer identity of the first bearer, the second downlink count value of the terminal associated to the first bearer, and the second uplink count value of the terminal associated to the first bearer, and control the transceiver to transmit, to the base station, a second message including the second list as a response to the first message, wherein the second downlink count value of the terminal associated to the first bearer is a count value of a next PDCP service data unit (SDU) expected to be received - 1, and the second uplink count value of the terminal associated to the first bearer is a count value of a next PDCP SDU to be transmitted - 1.

[24] The present disclosure also provides a base station in a wireless communication system. The base station comprises a transceiver; and a controller configured to: control the transceiver to transmit, to a terminal, a first message including a first list associated with count values of the base station, the first list includes at least one bearer identity, at least one first downlink count value of the base station associated to each bearer, and at least one first uplink count value of the base station associated to each bearer, and control the transceiver to receive, from the terminal, a second message including a second list associated with count values of the terminal including a first bearer identity of a first bearer, a second downlink count value of the terminal associated to the first bearer, and a second uplink count value of the terminal associated to the first bearer, as a response to the first message, in case that the first bearer is configured with the NR PDCP, and at least one of the second downlink count value of the terminal associated to the first bearer is different from the first downlink count

value associated to the first bearer or the second uplink count value of the terminal associated to the first bearer is different from the first uplink count value associated to the first bearer, wherein the second downlink count value of the terminal associated to the first bearer is a count value of a next PDCP service data unit (SDU) expected to be received - 1, and the second uplink count value of the terminal associated to the first bearer is a count value of a next PDCP SDU to be transmitted - 1.

## Advantageous Effects of Invention

[25] As described above, the method and apparatus according to a disclosed embodiment is advantageous in terms of being able to solve a decoding failure and HFN desynchronization problem that may arise during data communication by allowing for a transmitter (e.g., base station) to verify whether a COUNT value is well synchronized between a transmitting PDCP entity and a receiving PDCP entity in case of necessity, e.g., if suspected of decoding failure or HFN desynchronization problem or data invasion by a hacker.

[26] The method and apparatus according to a disclosed embodiment is advantageous in terms of supporting a wireless network in a factory to facilitate configuration of reliable point-to-point wireless links for continuous low-latency data communication by deploying a next generation mobile communication system in an automized factory facility supporting a wired time sensitive network (TSN) guaranteeing low-latency and high-reliability.

[27] The advantages of the disclosure are not limited to the aforesaid, and other advantages not described herein may be clearly understood by those skilled in the art from the descriptions below.

## Brief Description of Drawings

[28] FIG. 1a illustrates a diagram of architecture of an LTE system to which the disclosure is applied;

[29] FIG. 1b illustrates a diagram of a protocol stack of an LTE system to which the disclosure is applied;

[30] FIG. 1c illustrates a diagram of architecture of a next generation mobile communication system to which the disclosure is applied;

[31] FIG. 1d illustrates a diagram of a protocol stack of a next generation mobile communication system to which the disclosure is applied;

[32] FIG. 1e illustrates a signal flow diagram of an RRC connection configuration procedure between a UE and a base station for establishing a connection to a network in a next generation mobile communication system according to some embodiments of the disclosure;

[33] FIG. 1f illustrates a diagram for explaining an operation of a receiving PDCP entity

according to a proposed embodiment;

[34] FIG. 1g illustrates a diagram of a format of a COUNT value for use in a next generation mobile communication system according to an embodiment of the disclosure;

[35] FIG. 1h illustrates a diagram for explaining a ciphering procedure of a PDCP entity, using a COUNT value, according to an embodiment of the disclosure;

[36] FIG. 1i illustrates a signal flow diagram of a COUNT CHECK procedure proposed in an embodiment of the disclosure;

[37] FIG. 1j illustrates a diagram for explaining a method for reducing a size of MSBs of a COUNT value indicated in a proposed Counter check procedure according to an embodiment of the disclosure;

[38] FIG. 1k illustrates a flowchart of an operation of a UE in a proposed Counter check procedure according to an embodiment of the disclosure;

[39] FIG. 1l illustrates a block diagram of a configuration of a UE according to an embodiment of the disclosure;

[40] FIG. 1m illustrates a block diagram of a configuration of a base station in a wireless communication according to an embodiment of the disclosure;

[41] FIG. 2a illustrates a diagram of architecture of an LTE system to which the disclosure is applied;

[42] FIG. 2b illustrates a diagram of a protocol stack of an LTE system to which the disclosure is applied;

[43] FIG. 2c illustrates a diagram of architecture of a next generation mobile communication system to which the disclosure is applied;

[44] FIG. 2d illustrates a diagram of a protocol stack of a next generation mobile communication system to which the disclosure is applied;

[45] FIG. 2e illustrates a signal flow diagram of a procedure for transitioning a UE from an RRC connected mode to an RRC idle mode based on connection release triggered by a base station and transitioning the UE from the RRC idle mode to the RRC connected mode based on connection establishment triggered by the UE according to an embodiment of the disclosure;

[46] FIG. 2f illustrates a signal flow diagram of a procedure for establishing a point-to-point link between wireless devices for data communication according to an embodiment of the disclosure;

[47] FIG. 2g illustrates a flowchart of an operation of a wireless device for configuring a point-to-point direct wireless link according to an embodiment of the disclosure;

[48] FIG. 2h illustrates a diagram of a configuration of a UE or a wireless node according to an embodiment of the disclosure; and

[49] FIG. 2i illustrates a block diagram of a configuration of a base station or a wireless

node in a wireless communication system according to an embodiment of the disclosure.

## Mode for the Invention

[50] Before undertaking the DETAILED DESCRIPTION below, it may be advantageous to set forth definitions of certain words and phrases used throughout this patent document: the terms "include" and "comprise," as well as derivatives thereof, mean inclusion without limitation; the term "or," is inclusive, meaning and/or; the phrases "associated with" and "associated therewith," as well as derivatives thereof, may mean to include, be included within, interconnect with, contain, be contained within, connect to or with, couple to or with, be communicable with, cooperate with, interleave, juxtapose, be proximate to, be bound to or with, have, have a property of, or the like; and the term "controller" means any device, system or part thereof that controls at least one operation, such a device may be implemented in hardware, firmware or software, or some combination of at least two of the same. It should be noted that the functionality associated with any particular controller may be centralized or distributed, whether locally or remotely.

[51] Moreover, various functions described below can be implemented or supported by one or more computer programs, each of which is formed from computer readable program code and embodied in a computer readable medium. The terms "application" and "program" refer to one or more computer programs, software components, sets of instructions, procedures, functions, objects, classes, instances, related data, or a portion thereof adapted for implementation in a suitable computer readable program code. The phrase "computer readable program code" includes any type of computer code, including source code, object code, and executable code. The phrase "computer readable medium" includes any type of medium capable of being accessed by a computer, such as read only memory (ROM), random access memory (RAM), a hard disk drive, a compact disc (CD), a digital video disc (DVD), or any other type of memory. A "non-transitory" computer readable medium excludes wired, wireless, optical, or other communication links that transport transitory electrical or other signals. A non-transitory computer readable medium includes media where data can be permanently stored and media where data can be stored and later overwritten, such as a rewritable optical disc or an erasable memory device.

[52] Definitions for certain words and phrases are provided throughout this patent document, those of ordinary skill in the art should understand that in many, if not most instances, such definitions apply to prior, as well as future uses of such defined words and phrases.

[53] FIGS. 1a through 2i, discussed below, and the various embodiments used to describe

the principles of the present disclosure in this patent document are by way of illustration only and should not be construed in any way to limit the scope of the disclosure. Those skilled in the art will understand that the principles of the present disclosure may be implemented in any suitably arranged system or device.

[54] The operation principle of the disclosure is described in detail with reference to the accompanying drawings. Detailed descriptions of well-known functions and structures incorporated herein may be omitted to avoid obscuring the subject matter of the disclosure. Further, the following terms are defined in consideration of the functionality in the disclosure, and they may vary according to the intention of a user or an operator, usage, etc. Therefore, the definition should be made on the basis of the overall content of the present specification.

[55] Detailed descriptions of well-known functions and structures incorporated herein may be omitted to avoid obscuring the subject matter of the disclosure. Exemplary embodiments of the disclosure are described hereinafter in detail with reference to the accompanying drawings.

[56] The terms used, in the following description, for indicating access nodes, network entities, messages, interfaces between network entities, and diverse identity informations are provided for convenience of explanation. Accordingly, the terms used in the following description are not limited to specific meanings but may be replaced by other terms equivalent in technical meanings.

[57] In the following description, the terms and definitions given in the 3rd Generation Partnership Project Long Term Evolution (3GPP LTE) standard are used. However, the disclosure is not limited by the terms and definitions but can be applied to other standard communication systems. In the following description, the terms "eNB" and "gNB" are interchangeably used for convenience of explanation. That is, a base station prementioned as eNB may be referred to as gNB. In the following description, the term "terminal" may be used to refer to any of hand-held phones, NB-IoT devices, sensors, and other wireless communication devices.

[58]

[59] Embodiment A

[60] In a next generation mobile communication system, terminals and base stations cipher and decipher data to be transmitted and received. Typically, an ciphering and deciphering algorithm is used to cipher and decrypt data with an ciphering key (or security key). The ciphering key includes ciphering keys (e.g., KgNB and K_RRCenc) agreed between a terminal and a base station and security keys (e.g., COUNT values) varying with data. Because the COUNT value consists of a PDCP sequence number and a hyper frame number (HFN), it is necessary to acquire synchronization of a PDCP sequence number between a transmitting PDCP entity and a receiving PDCP entity.

Given that the PDCP sequence number increases from 0 to 2^(PDCP sequence number length)-1 and, if reaching its maximum value, it goes back to 0 and the HFN number increases by 1; if the PDCP sequence number restarts from 0 after it reaches its maximum value, the COUNT value in use for data ciphering by the transmitting PDCP entity and the COUNT value in use for data description by the receiving PDCP entity may differ from each other, which leads to a decoding failure and HFN desynchronization problem.

[61] Such decoding failure and HFN desynchronization problem may be caused by a large amount of data loss or unexpected data invasion by a hacker. Accordingly, in case of necessity, e.g., if suspected of decoding failure or HFN desynchronization problem or data invasion by a hacker, it is necessary for the base station to verify whether the COUNT value is well synchronized between the transmitting PDCP entity and the receiving PDCP entity.

[62] The disclosure discloses a method and apparatus for solving a decoding failure and HFN desynchronization problem that may arise during data communication by allowing for a transmitter (e.g., base station) to verify whether a COUNT value is well synchronized between a transmitting PDCP entity and a receiving PDCP entity in case of necessity, e.g., if suspected of decoding failure or HFN desynchronization problem or data invasion by a hacker.

[63] FIG. 1a illustrates a diagram of architecture of an LTE system to which the disclosure is applied.

[64] In reference to FIG. 1a, a radio access network of the LTE system includes evolved Node Bs (hereinafter, interchangeably referred to as eNB, node B, and base station) 1a-05, 1a-10, 1a-15, and 1a-20; a mobility management entity (MME) 1a-25; and a serving gateway (S-GW) 1a-30. A user terminal (hereinafter, interchangeably referred to as user equipment (UE) and terminal) 1a-35 connects to an external network via the eNBs 1a-05, 1a-10, 1a-15, and 1a-20 and the S-GW 1a-30.

[65] The eNBs 1a-05, 1a-10, 1a-15, and 1a-20 correspond to the legacy node Bs of the universal mobile telecommunications system (UMTS). The UE 1a-35 connects to one of the eNBs via a radio channel, and the eNB has more complex functions than the legacy node B. In the LTE system where all user traffic including real time services such as Voice over IP (VoIP) is served through shared channels, there is a need of an entity for collecting UE-specific status information (such as buffer status, power headroom status, and channel status) and scheduling the UEs based on the collected information, and the eNB takes charge of such functions. Typically, one eNB hosts multiple cells. For example, the LTE system adopts Orthogonal Frequency Division Multiplexing (OFDM) as a radio access technology to secure a data rate of up to 100 Mbps in a bandwidth of 20 MHz. The LTE system also adopts Adaptive Modulation

and Coding (AMC) to determine the modulation scheme and channel coding rate in adaptation to the channel condition of the UE. The S-GW 1a-30 handles data bearer functions to establish and release data bearer under the control of the MME 1a-25. The MME 1a-25 handles various control functions for the UE as well as the mobile management function and has connections with the eNBs 1a-05, 1a-10, 1a-15, and 1a-20.

[66] FIG. 1b illustrates a diagram of a protocol stack of an LTE system to which the disclosure is applied.

[67] As shown in FIG. 1b, the protocol stack of the interface between the UE 1b-50 and the eNB 1b-60 in the LTE system includes Packet Data Convergence Protocol (PDCP) 1b-05 and 1b-40, Radio Link Control (RLC) 1b-10 and 1b-35, and Medium Access Control (MAC) 1b-15 and 1b-30. The PDCP 1b-05 and 1b-40 takes charge of compressing/decompressing an IP header. The main functions of the PDCP 1b-05 and 1b-40 can be summarized as follows

[68] - Header compression and decompression: ROHC only

[69] - Transfer of user data

[70] - In-sequence delivery of upper layer PDUs at PDCP re-establishment procedure for RLC AM

[71] - For split bearers in DC (only support for RLC AM): PDCP PDU routing for transmission and PDCP PDU reordering for reception

[72] - Duplicate detection of lower layer SDUs at PDCP re-establishment procedure for RLC AM

[73] - Retransmission of PDCP SDUs at handover and, for split bearers in DC, of PDCP PDUs at PDCP data-recovery procedure, for RLC AM

[74] - Ciphering and deciphering

[75] - Timer-based SDU discard in uplink

[76] The RLC 1b-10 and 1b-35 takes charge of reformatting PDCP PDUs in order to fit them into the size for ARQ operation. The main functions of the RLC layer can be summarized as follows:

[77] - Transfer of upper layer PDUs

[78] - Error Correction through ARQ (only for AM data transfer)

[79] - Concatenation, segmentation and reassembly of RLC SDUs (only for UM and AM data transfer)

[80] - Re-segmentation of RLC data PDUs (only for AM data transfer)

[81] - Reordering of RLC data PDUs (only for UM and AM data transfer)

[82] - Duplicate detection (only for UM and AM data transfer)

[83] - Protocol error detection (only for AM data transfer)

[84] - RLC SDU discard (only for UM and AM data transfer)

[85] - RLC re-establishment

[86] The MAC 1b-15 and 1b-30 allows for connection of multiple RLC entities established for one UE and takes charge of multiplexing RLC PDUs from the RLC layer into a MAC PDU and demultiplexing a MAC PDU into RLC PDUs. The main functions of the MAC layer can be summarized as follows:

[87] - Mapping between logical channels and transport channels

[88] - Multiplexing/demultiplexing of MAC SDUs belonging to one or different logical channels into/from transport blocks (TB) delivered to/from the physical layer on transport channels

[89] - Scheduling information reporting

[90] - Error correction through HARQ

[91] - Priority handling between logical channels of one UE

[92] - Priority handling between UEs by means of dynamic scheduling

[93] - MBMS service identification

[94] - Transport format selection

[95] - Padding

[96] The PHY 1b-20 and 1b-25 takes charge of channel-coding and modulation on higher layer data to generate and transmit OFDM symbols over a radio channel, and demodulating and channel-decoding on OFDM symbols received over the radio channel to deliver the decoded data to the higher layers.

[97] FIG. 1c illustrates a diagram of architecture of a next generation mobile communication system to which the disclosure is applied.

[98] As shown in FIG. 1c, the next generation mobile communication system includes a radio access network with a next generation base station (New Radio Node B (NR gNB)) 1c-10 and a new radio core network (NR CN) 1c-05. A new radio user equipment (NR UE) 1c-15 connects to an external network via the NR gNB 1c-10 and the NR CN 1c-05.

[99] In FIG. 1c, the NR gNB 1c-10 corresponds to an evolved Node B (eNB) of the legacy LTE. The NR gNB 1c-10 to which the NR UE 1c-15 connects through a radio channel is capable of providing superior services in comparison with the legacy eNB. In the next generation mobile communication system where all user traffic is served through shared channels, it is necessary to schedule the NR UEs based on scheduling information such as buffer status, power headroom status, and channel status collected by the NR UEs, and the NR gNB 1c-10 takes charge of this function. Typically, one NR gNB hosts multiple cells. In order to achieve a data rate higher than the peak data rate of legacy LTE systems, the next generation mobile communication system may adopt a beamforming technique along with orthogonal frequency division multiple access (OFDMA) as a radio access technology. The next generation mobile commu-

nication system may also adopt an adaptive modulation and coding (AMC) to determine the modulation scheme and channel coding rate in adaptation to the channel condition of the NR UE. The NR CN 1c-05 takes charge of mobility support, bearer setup, and QoS configuration. The NR CN 1c-05 may take charge of a NR UE mobility management function, and a plurality of NR gNBs may connect to the NR CN 1c-05. The next generation mobile communication system may also interoperate with a legacy LTE system and, in this case, the NR CN 1c-05 connects to an MME 1c-25 through a network interface. The MME 1c-25 communicates with the eNB 1c-40 as a legacy base station.

[100] FIG. 1d illustrates a diagram of a protocol stack of a next generation mobile communication system to which the disclosure is applied.

[101] As shown in FIG. 1d, the protocol stack of the interface between an UE 1d-50 and an NR gNB 1d-60 in a next generation mobile communication system includes NR service data adaptation protocol (NR SDAP) 1d-01 and 1d-45, NR PDCP 1d-05 and 1d-40, NR RLC 1d-10 and 1d-35, NR MAC 1d-15 and 1d-30.

[102] The main functions of the NR SDAP 1d-01 and 1d-45 may include some of the following functions

[103] - Transfer of user plane data

[104] - Mapping between a QoS flow and a DRB for both DL and UL)

[105] - Marking QoS flow ID in both DL and UL packets

[106] - Reflective QoS flow to DRB mapping for the UL SDAP PDUs).

[107] The UE 1d-50 may receive an RRC message for configuring an SDAP layer entity 1d-01 so as to determine whether to use PDCP entity-specific, bearer-specific, or logical channel-specific SDAP header and whether to use SDAP layer function via an RRC message and, if configured to use a specific PDAP header, receive a 1-bit NAS reflective QoS indicator and an AS reflective QoS indicator in the SDAP header indicative of instructing the UE 1d-50 to update or reconfigure uplink and downlink QoS flow-data bearer mappings. The SDAP header may include QoS flow ID indicating a QoS. The QoS information may be used as data processing priority and scheduling information for guaranteeing service reliability.

[108] The main functions of the NR PDCP 1d-05 and 1d-40 may include some of the following functions:

[109] - Header compression and decompression: ROHC only

[110] - Transfer of user data

[111] - In-sequence delivery of upper layer PDUs

[112] - Out-of-sequence delivery of upper layer PDUs

[113] - PDCP PDU reordering for reception

[114] - Duplicate detection of lower layer SDUs

[115] - Retransmission of PDCP SDUs

[116] - Ciphering and deciphering

[117] - Timer-based SDU discard in uplink

[118] The PDCP PDU reordering function of an NR PDCP entity 1d-05 and 1d-40 is to reorder the PDCP PDUs delivered from a lower layer based on the PDCP sequence number (PDCP SN) and may include delivering the reordered data to an upper layer, recording the missing PDCP PDUs among the reordered PDCP PDUs, transmitting a status report indicating the missing PDCP PDUs to the sender, and requesting for re-transmission of the missing PDCP PDUs.

[119] The main functions of the NR RLC 1d-10 and 1d-35 may include some of the following functions.

[120] Transfer of upper layer PDUs

[121] - In-sequence delivery of upper layer PDUs

[122] - Out-of-sequence delivery of upper layer PDUs

[123] - Error Correction through ARQ

[124] - Concatenation, segmentation and reassembly of RLC SDUs

[125] - Re-segmentation of RLC data PDUs

[126] - Reordering of RLC data PDUs

[127] - Duplicate detection

[128] - Protocol error detection

[129] - RLC SDU discard

[130] - RLC re-establishment

[131] The in-sequence delivery function of an NR RLC entity 1d-10 and 1d-35 is to deliver the RLC SDUs received from the lower layer to the upper layer and may include re-assembling, when multiple segmented RLC SDUs constituting an original RLC SDU are received, the RLC SDUs and delivering the reassembled RLC SDU to the upper layer; reordering the received RLC PDUs based on the RLC sequence number(SN) or PDCP SN; recording the missing RLC PDUs among the reordered RLC PDUs; transmitting a status report indicating the missing RLC PDUs to the sender; requesting for retransmission of the missing RLC PDUs; and delivering, when there is a missing RLC PDU, the RLC PDUs before the missing RLC PDU in sequence, delivering, if a predetermined timer expires even when there is any missing RLC SDU, all RLC SDUs received before the start of the timer to the upper layer in sequence, or delivering, if a predetermined timer expires even when there is any missing RLC SDU, all RLC SDUs received until then to the upper layer in sequence. It may also be possible to process the RLC PDUs in the receiving sequence (in the order of arrival regardless of sequence number) and deliver the RLC PDUs to the PDCP entity out of order (out-of-sequence delivery) and, if an RLC PDU is transmitted in the form of segments, to store the

received segments, or wait until all segments constituting the RLC PDU are received and reassemble the segments into the original RLC PDU, which is delivered to the PDCP entity. The NR RLC layer 1d-10 and 1d-35 may have no concatenation function and, in this case, the concatenation function may be performed in the NR MAC layer 1d-15 and 1d-30 or replaced by the multiplexing function of the NR MAC layer 1d-15 and 1d-30.

[132] The out-of-sequence delivery function of an NR RLC entity 1d-10 and 1d-35 is to deliver the RLC SDUs received from the lower layer to the upper layer out of order and may include reassembling, when multiple segmented RLC SDUs constituting an original RLC SDU are received, the segmented RLC SDUs, delivering the reassembled RLC SDUs to the upper layer, arranging the received RLC PDUs based on the RLC SN or PDCP SN, and recording the SN of the missing RLC PDUs.

[133] The NR MAC 1d-15 and 1d-30 may be connected to multiple NR RLC entities, and the main functions of the NR MAC 1d-15 and 1d-30 may include some of the following functions:

[134] - Mapping between logical channels and transport channels

[135] - Multiplexing/demultiplexing of MAC SDUs

[136] - Scheduling information reporting

[137] - Error correction through HARQ

[138] - Priority handling between logical channels of one UE

[139] - Priority handling between UEs by means of dynamic scheduling

[140] - MBMS service identification

[141] - Transport format selection

[142] - Padding

[143] The NR PHY layer 1-20 and 1d-25 takes charge of channel-coding and modulation on upper layer data to generate and transmit OFDM symbols over a radio channel and demodulating and channel-decoding on OFDM symbols received over the radio channel to deliver the decoded data to the upper layers.

[144] FIG. 1e illustrates a signal flow diagram of an RRC connection configuration procedure between a UE and a base station for establishing a connection to a network in a next generation mobile communication system according to some embodiments of the disclosure.

[145] In reference to FIG. 1e, if there is no data transmission/reception to/from the UE 1e-90 in an RRC connected mode for any reason or during a predetermined period, the base station 1e-91 may transmit an RRCConnectionRelease message to the UE 1e-90 at step 1e-01 to transition the UE 1e-90 to an RRC idle mode. If data to be transmitted are produced at the UE 1e-90 with no currently established connection (hereinafter, referred to as idle mode UE), the UE 1e-90 performs an RRC connection establishment

procedure with the base station 1e-91.

[146] The UE 1e-90 acquires uplink transmission synchronization with the base station 1e-91 through a random access procedure and transmits an RRCConnectionRequest message to the base station 1e-91 at step 1e-05. The RRCConnectionRequest message may include an identifier of the UE 1e-90 and a connection establishment cause (establishmentCause).

[147] The base station 1e-91 transmits an RRCConnectionSetup message to the 1e-90 at step 1e-10 for RRC connection setup. The RRCConnectionSetup message may include at least one of per-logical channel configuration information, per-bearer configuration information, PDCP entity configuration information, RLC entity configuration information, or MAC entity configuration information.

[148] The RRCConnectionSetup message may be used to assign per-bearer identifiers (e.g., signaling radio bearers (SRB) identifier and data radio bearer (DRB) identifiers) and configure per-bearer PDCP, RLC, MAC entity, and PHY entities. The RRCConnectionSetup message may also be used to configure per-bearer PDCP sequence number lengths for use by the PDCP entities (e.g., 12 bits and 18 bits) and RLC sequence number lengths for sue by the RLC entities (e.g., 6 bits, 12 bits, and 18 bits). The RRCConnectionSetup message may also be used to indicate whether a header compression/decompression protocol is used and an integrity protection or verification procedure is used in uplink or downlink for PDCP entities per bearer. The RRCConnectionSetup message may also be used to indicate to the UE 1e-90 whether the out-of-order delivery is performed at the PDCP entities.

[149] After completing RRC connection setup, the UE 1e-90 may transmit an RRCConnectionSetupComplete message to the base station 1e-91 at step 1e-15. The RRCConnectionSetupComplete message may include a control message called SERVICE REQUEST for requesting to an AMF 1e-92 or an MME 1e-92 for establishing a bearer for a certain service. At step 1e-20, the base station 1e-91 transmits the SERVICE REQUEST message included in the RRCConnectionSetupComplete message to the AMF 1e-92 or the MME 1e-92. The AMF 1e-92 or the MME 1e-92 may determine whether to provide the service requested by the UE 1e-90.

[150] If it is determined to provide the service requested by the UE 1e-90, the AMF/MME 1e-92 transmit an INITIAL CONTEXT SETUP REQUEST message to the base station 1e-91 at step 1e-25. The INITIAL CONTEXT SETUP REQUEST message may include quality of service (QoS) information to be applied in configuring a DRB and security information (e.g., Security Key and Security Algorithm) to be applied to the DRB.

[151] For security configuration, the base station 1e-91 transmits a SecurityModeCommand message to the UE 1e-90 at step 1e-30, and the UE 1e-90 transmits a Secu-

rityModeComplete message to the base station 1e-91 at step 1e-35. After completing security configuration, the base station 1e-91 transmits an RRCConnectionReconfiguration message to the UE 1e-90 at step 1e-40.

[152] The RRCConnectionReconfiguration message may be used to assign per-bear identifier (e.g., SRB identifier or DRB identifier) and configure per-bearer PDCP, RLC, MAC, and PHY entities. The RRCConnectionSetup message may also be used to configure per-bearer PDCP sequence number lengths for use by the PDCP entities (e.g., 12 bits and 18 bits) and RLC sequence number lengths for sue by the RLC entities (e.g., 6 bits, 12 bits, and 18 bits). The RRCConnectionSetup message may also be used to indicate whether a header compression/decompression protocol is used and an integrity protection or verification procedure is used in uplink or downlink for PDCP entities per bearer. The RRCConnectionSetup message may also be used to indicate to the UE 1e-90 whether the out-of-order delivery is performed at the PDCP entities.

[153] The RRCConnectionReconfiguration message may include configuration information of a DRB on which user data are processed, and the UE 1e-90 configures a DRB based on the configuration information and transmits an RRCConnectionReconfigurationComplete message to the base station 1e-91 at step 1e-45. After configuring the DRB bearer with the UE 1e-90, the base station 1e-91 may transmit an INITIAL CONTEXT SETUP COMPLETE message the AMF/MME 1e-92 at step 1e-50 to complete establishment of a connection.

[154] After completing the above procedure, the UE 1e-90 and the base station 1e-92 may communicate date via a core network 1e-93 at steps 1e-33 and 1e-60. According to some embodiments, the data transfer procedure may consist of three phases: RRC connection configuration, security configuration, and DRB configuration. The base station 1e-91 may transmit an RRCConnectionReconfiguration message to the UE 1e-90 at step 1e-65 for updating, adding, or modifying the configuration.

[155] The RRCConnectionReconfiguration message may be used to assign per-bear identifier (e.g., SRB identifier or DRB identifier) and configure per-bearer PDCP, RLC, MAC, and PHY entities. The RRCConnectionSetup message may also be used to configure per-bearer PDCP sequence number lengths for use by the PDCP entities (e.g., 12 bits and 18 bits) and RLC sequence number lengths for sue by the RLC entities (e.g., 6 bits, 12 bits, and 18 bits). The RRCConnectionSetup message may also be used to indicate whether a header compression/decompression protocol is used and an integrity protection or verification procedure is used in uplink or downlink for PDCP entities per bearer. The RRCConnectionSetup message may also be used to indicate to the UE 1e-90 whether the out-of-order delivery is performed at the PDCP entities.

[156] The above-described connection configuration procedure between the UE 1e-90 and the base station 1e-91 may be applied either between a UE and an LTE eNB or between a UE and an NR gNB.

[157] In the disclosed embodiments, the term "bearer" may be used to include SRB (signaling radio bearer) and DRB (data radio bearer). Meanwhile, a UM DRB denotes a DRB in use by an RRC entity operating in an unacknowledged mode (UM), and an AM DRB denotes a DRB in use by an RRC entity operating in an acknowledged mode (AM).

[158] The following disclosure discloses a method and apparatus for solving a decoding failure and HFN desynchronization problem that may arise during data communication by allowing for a transmitter (e.g., base station) to verify whether a COUNT value is well synchronized between a transmitting PDCP entity and a receiving PDCP entity in case of necessity, e.g., if suspected of decoding failure or HFN desynchronization problem or data invasion by a hacker.

[159] Before undertaking the detailed description of the method and apparatus for checking the COUNT value, a brief description is made of the operations of transmit and receive PDCP entities.

[160] In the disclosed embodiments, a transmitting PDCP entity operates as follows. The transmitting PDCP entity uses a first COUNT variable, called TX-NEXT, for maintaining a COUNT value to be allocated for transmitting next data in processing data.

[161] The operations of the transmitting PDCP entity that are proposed in the disclosed embodiments are as follows.

[162] - If data (e.g., PDCP SDU) arrives from the upper layer, the transmitting PDCP entity starts a PDCP data discard timer and, if the timer expires, discards the data.

[163] - Next, the transmitting PDCP entity assigns (allocates) a COUNT value corresponding to TX_NEXT to the data arrived from the upper layer. The TX_NEXT may be set to an initial value of 0 and maintain the COUNT value of the next data (PDCP SDU) to be transmitted.

[164] - If a header compression protocol is configured to the transmitting PDCP entity, the transmitting PDCP entity performs header compression of the data.

[165] - If an integrity protection is configured to the transmitting PDCP entity, the transmitting PDCP entity generates a PDCP header and perform integrity protection of the PDCP header and data using a security key and the COUNT value of the TX_NEXT assigned to the data.

[166] - Next, the transmitting PDCP entity performs a ciphering procedure using the security key for the data and the COUNT value of the TX_NEXT assigned to the data. Next, the transmitting PDCP entity sets least significant bits (LSBs) equal in length to

a PDCP sequence number in the COUNT value of the TX_NEXT variable as the PDCP sequence number.

[167] - Next, the transmitting PDCP entity increments the COUNT value of the TX_NEXT variable by 1 and sends the processed data prefixed with a PDCP header to the lower layers.

[168] FIG. 1f illustrates a diagram for explaining an operation of a receiving PDCP entity according to a proposed embodiment.

[169] In a disclosed embodiment, the receiving PDCP entity operates as follows. The receiving PDCP entity maintains and manages 4 COUNT variables in processing received data. When processing the received data, the receiving PDCP entity uses a second COUNT variable maintaining the COUNT value of the next data (e.g., PDCP SDU) expected to be received, the second COUNT variable being referred to as RX_NEXT. When processing the received data, the receiving PDCP entity uses a third COUNT variable maintaining the COUNT value of the first data (e.g., PDCP SDU) that has not been delivered to the upper layers, the third COUNT variable being referred to as RX_DELIV. When processing the received data, the receiving PDCP entity uses a fourth COUNT variable maintaining the COUNT value of the data (e.g., PDCP SDU) that has triggered a PDCP reordering timer (t-Reordering), the fourth COUNT variable being referred to as RX_REORD. When processing the received data, the receiving PDCP entity may uses a fifth COUNT variable maintaining the COUNT value of the currently received data (e.g., PDCP SDU), the fifth COUNT variable being referred to as RCVE_COUNT. The PDCP reordering timer may be set to a timer value or period configured via an RRC message in the upper layer (RRC layer) as described in FIG. 1e and it is used for detecting lost PDCP PDUs, and only one timer can run at one timer.

[170] Following variables are defined and used for the operations of the receiving PDCP entity of a UE.

[171] - HFN: The Hyper Frame Number (HFN) part of the window state variable

[172] - SN: The Sequence Number (SN) part of the window state variable

[173] - RCVD_SN: The PDCP SN of the received PDCP PDU, included in PDU header

[174] - RCVD_HFN: The HFN value of the received PDCP PDU, calculated by the receiving PDCP entity

[175] In a disclosed embodiment, the receiving PDCP entity operates as follows.

[176] When a PDCP PDU is received from the lower layers, the receiving PDCP entity determines a COUNT value of the received PDCP PDU.

[177] - If RCVD_SN <= SN(RX_DELIV) - Window_Size,

[178] ■ update RCVD_HFN to RCVD_HFN = HFN(RX_DELIV) + 1,

[179] - else if RCVD_SN > SN(RX_DELIV) + Window_Size,

[180] ■ update RCVD_HFN to RCVD_HFN = HFN(RX_DELIV) - 1,

[181] - else,

[182] ■ update RCVD_HFN to RCVD_HFN = HFN(RX_DELIV).

[183] - The RCVD_COUNT is determined as RCVD_COUNT = [RCVD_HFN, RCVD_SN].

[184] After determining the COUNT value of the received PDCP PDU, the receiving PDCP entity updates the window state variables and processes the PDCP PDU as follows.

[185] - The receiving PDCP entity performs deciphering and integrity verification of the PDCP PDU using the RCVD_COUNT value.

[186] ■ If integrity verification fails,

[187] ■ the receiving PDCP entity indicate the integrity verification failure to upper layers and discard the received PDCP PDU (data part of the PDCP PDU).

[188] - If RCVD_COUNT < RX_DELIV or if the PDCP PDU with the RCVD_COUNT value has been received before (packet expired, outdated, or out of window, or duplicated packet),

[189] ■ the receiving PDCP entity discards the received PDCP Data PDU (data part of PDCP PDU).

[190] If the received PDCP PDU is not discarded, the receiving PDCP entity operates as follows.

[191] - The receiving PDCP entity stores the processed PDCP SDU in the reception buffer.

[192] - if RCVD_COUNT >= RX_NEXT,

[193] ■ the receiving PDCP entity updates RX_NEXT to RCVD_COUNT + 1.

[194] - If out-of-date delivery indicator (outOfOrderDelivery) is configured (if out-of-date delivery operation is indicated),

[195] ■ the receiving PDCP entity delivers the PDCP SDU to upper layers.

[196] - If RCVD_COUNT = RX_DELIV,

[197] ■ the receiving PDCP entity performs head compression, if not decompressed before, and delivers to upper layers in an order of the COUNT value.

[198] ◆ The receiving PDCP entity delivers all stored PDCP SDUs with consecutive COUNT values starting from COUNT = RX_DELIV to the upper layer.

[199] ■ The receiving PDCP entity updates RX_DELIV value to the COUNT value of the first PDCP SDU that is equal to or greater than the current RX_DELIV and has not been delivered to the upper layers.

[200] - If the timer t-Reordering is running and if the RX_DELIV value is equal to or greater than RX_REORD,

[201] ■ the receiving PDCP entity stops and resets the timer t-Reordering.

[202] - If the timer t-Reordering is not running (includes the case where t-Reordering is

stopped under the above condition) and if RX_DELIV is less than RX_NEXT,

[203] ■ the receiving PDCP entity updates RX_REORD value to RX_NEXT, and

[204] ■ starts the timer t-Reordering.

[205] When the PDCP reordering timer (t-Reordering) expires, the receiving PDCP entity may operate as follows.

[206] - The receiving PDCP entity performs header decompression, if not decompressed before, and deliver to upper layers in an order of the COUNT values.

[207] ■ The receiving PDCP entity delivers all PDCP SDUs with COUNT values greater than the RX_REORD value.

[208] ■ The receiving PDCP entity delivers all PDCP SDUs with consecutive COUNT values starting from the RX_REORD value.

[209] - The receiving PDCP entity updates the RX_DELIV value to the COUNT value of the first PDCP SDU which has not been delivered to upper layers and of which the COUNT value is equal to or greater than the RX_REORD.

[210] - If the RX_DELIV value is less than the RX_NEXT value,

[211] ■ the receiving PDCP entity updates the RX_REORD value to the RX_NEXT value, and

[212] ■ starts timer t-Reordering.

[213] FIG. 1g illustrates a diagram of a format of a COUNT value for use in a next generation mobile communication system according to an embodiment of the disclosure.

[214] A PDCP entity maintains the COUNT value for ciphering and integrity protection between the UE and the base station and use the COUNT value as a parameter of a preconfigured ciphering and integrity protection algorithm in performing ciphering and integrity protection on a PDCP packet. The detailed description thereof is made with reference to FIG. 1g.

[215] All PDCP packets (data packets and control message packets) have a PDCP sequence number (SN), which increments by 1 for every packet. If reaching a preconfigured PDCP SN size, the SN is recounted from 0 and HFN increases by 1. In this case, an SN that has been used before may be assigned to the current PDCP packet. If a hacker intercepts a PDCP SN value and attempts hacking into the communication between a UE and a base station using this previously used PDCP SN value, the PDCP data transmitted by the hacker may continuously increase the PDCP SN, resulting in HFY desynchronization problem between the transmitter and the receiver. Even if there is no hacking invasion, if a large amount of data are lost, this is likely to cause the HFN desynchronization problem and decoding failure of the received data.

[216] The COUNT value has a length of 32 bits and consists of the HFN 1g-05 and the PDCP SN 1g-10. A UE and a base station maintain the COUNT value for use in

ciphering and integrity protection. In actual data transmission, the PDCP packet (PDCP PDU) includes only the PDCP SN. Accordingly, it is difficult for a hacker to acquire an accurate COUNT value only with the PDCP SN communicating over a radio channel. The base station transmits to the UE an RRC message including PDCP configuration information indicative of a PDCP SN length set to 12 or 18 bits, and the PDCP SN length determines the HFN length in the COUNT value (32 bits - PDCP SN length).

[217] FIG. 1h illustrates a diagram for explaining a ciphering procedure of a PDCP entity, using a COUNT value, according to an embodiment of the disclosure.

[218] In reference to FIG. 1h, the transmitting PDCP entity performs ciphering on the data received from the upper layers, and the receiving PDCP entity performs deciphering on the data. In the next generation mobile communication system, all packets are transmitted/received without being ciphered before the AS security is activated; if the AS security is activated, all traffic (control data (CP) and user data (UP)) are ciphered before being transmitted. That is, as described with reference to FIG. 1e, after the securing configuration has been completed between the base station and the UE by exchanging the SecurityModeCommand and SecurityModeComplete messages, the RRC messages being exchanged between the base station and the terminal are ciphered and integrity-protected, and the corresponding IP packets are secured.

[219] After AS security setup, if data arrive from upper layers at step 1h-05, the transmitting PDCP entity performs an exclusive operation on a key stream block acquired through a key generation algorithm (EPS Encryption Algorithm (EEA) for ciphering at the UE and a pure data block at step 1h-20 to generate a ciphered user packet. Here, the key stream block for use in ciphering may be acquired through a key generation algorithm with the input of parameters such as a key (K_UPenc 1h-10) for user plane ciphering that is obtained from K_gNB, COUNT (32-bit uplink NAS COUNT value), Bearer ID, Direction (message transmission direction 0 for uplink and 1 for downlink), and Length (key stream block length). If the user data packet encrypted by the transmitting PDCP entity is received, the receiving PDCP entity generates the same key stream block used for encryption by applying the same key generation algorithm applied by the UE and performs the exclusive operation thereon at step 1h-35. As in the terminal, the key stream block for use in deciphering, at the base station, may be acquired through a key generation algorithm with the input of parameters such as a key (K_UPenc 1h-10) for user plane ciphering that is obtained from K_gNB, COUNT (32-bit uplink NAS COUNT value), Bearer ID, Direction (message transmission direction 0 for uplink and 1 for downlink), and Length (key stream block length). The receiver may perform a deciphering procedure in the reverse order of the ciphering procedure of the transmitter.

[220] In order to perform the ciphering and deciphering procedures precisely, the COUNT value stored in the UE and the base station should be accurate. That is, it is necessary to check whether the COUNT value is accurate to apply an accurate ciphering key to the PDCP packet to be ciphered. In order to accomplish this object, a disclosed embodiment proposes a method for a base station to instruct a UE to perform a COUNT CHECK operation in a next generation mobile communication system. That is, the UE verifies the validity of a COUNT value in response to a request from the base station and transmits, if the validity is verified, the current COUNT value to the base station.

[221] FIG. 1i illustrates a signal flow diagram of a COUNT CHECK procedure proposed in an embodiment of the disclosure.

[222] FIG. 1i shows the entire operation for a gNB 1i-02 to check for the COUNT value of the UE 1i-01, and the gNB 1e-02 may verify whether a COUNT value configured per bearer is valid and whether to synchronize the COUNT value through the proposed procedure.

[223] In reference to FIG. 1i, the UE 1i-01 may establish an RRC connection with the gNB 1i-02 at step 1i-05. If necessary, e.g., if suspected of decoding failure or HFN desynchronization problem or data invasion by a hacker, the gNB 1i-02 transmits a CounterCheck RRC message to the UE 1i-01, at step 1i-10, to request for per-bearer COUNT check and report so as to determine whether the COUNT value is well synchronized between the transmitting PDCP entity and the receiving PDCP entity. This message may be carried by an RRCConnectionReconfiguration or RRCConnectionReestablishment message being transmitted on a dedicated common control channel (DCCH). The CounterCheck message may include a list of bearers (e.g., DRB or SRB) for per-bearer COUNT check, drb-CountMSB-InfoList, which contains DRB identifier, countMSB-Uplink(25bit), and countMSB-Downlink(25bit). That is, the list includes per-bearer identifiers of the bearers for which the COUNT check is required and 25 most significant bits (MSBs) of each of the uplink and downlink COUNT values of the gNB 1i-02 on the corresponding bearers.

[224] Upon receipt of this message, the UE 1i-01 may compare the 25 MSBs of the uplink COUNT value (countMSB-Uplink) for the bearer identified by the bearer identifier included in the drb-CountMSB-InfoList of the message with the 25 MSBs of the uplink COUNT value stored in the UE 1i-01. The UE 1i-01 may also compare the 25 MSBs of the downlink COUNT value (countMSB-Uplink) for the bearer identified by the bearer identifier included in the drb-CountMSB-InfoList of the message with the 25 MSBs of the downlink COUNT value stored in the UE 1i-01. If it is determined that the two values, in downlink or uplink, are different from each other, the UE 1i-01 configures, at step 1i-15, a drb-CountInfoList for reporting 32-bit full COUNT values (full COUNT 32 bits) for the corresponding bearers and generates a Counter Check

Response message including the identifiers of the bearers for which the compared values are different from each other and the 32-bit full COUNT values (full COUNT 32 bits). If it is determined that the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink) indicated by the eNB 1i-02 are all identical with those of the COUNT value stored in the UE 1i-01 in both the uplink and downlink, the corresponding values are not included in the reporting list.

[225] At step 1i-15, the UE 1i-01 also configures a reporting list (drb-CountInfoList) for reporting the 32-bit full COUNT values (full COUNT 32 bits) for the bearers that are not indicated by the bearer identifiers in the drb-CountMSB-InfoList of the Count Check message received from the eNB 1i-02 and generates the Counter Check Response message including the 32-bit full COUNT values (full COUNT 32 bits) along with the identifiers of the non-indicated bearers.

[226] After the per-bearer COUNT value comparison and report determination, the UE 1i-01 transmits, at step 1i-20, a CounterCheckResponse message including the reporting list configured at the previous step to the eNB 1i-02.

[227] Hereinafter, a description is made of the operation of the UE 1i-01 for determining the COUNT values to compare and apply in comparing 25 MSBs of the COUNT values (countMSB-Uplink or countMSB-Downlink) indicated per bearer by the eNB 1i-02 in the COUNT CHECK procedure proposed in the embodiment of FIG. 1i.

[228] According to a first embodiment, when the eNB 1i-02 transmits the Counter Check message indicating use of the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink), the UE 1i-01 determines COUNT values to be compared and reported as follows.

[229] In the first embodiment, the UE 1i-01 uses, for uplink, the TX_NEXT value as the first COUNT variable maintaining the COUNT value of the next data to be transmitted by the transmitting PDCP entity for the case of comparing the countMSB-Uplink and the 25 MSBs and, for downlink, the second COUNT variable (RX_NEXT) maintaining the COUNT value of the next data (e.g., PDCP SDU) expected to be received among 4 COUNT variables (i.e., the first COUNT variable (RX_NEXT), the third COUNT variable (RX_DELIV), the fourth COUNT variable (RX_REORD), and the fifth COUNT variable (RCVD_COUNT)) in use by the receiving PDCP entity for the case of comparing the countMSB-Downlink and the 25 MSBs and reporting the COUNT values via the Counter Check Response message.

[230] In the first embodiment, when the Counter Check message is received, the UE 1i-01 operates as follows.

[231] - For each established bearer (e.g., DRB),

[232] ■ if there is no COUNT value for a given direction (uplink or downlink) because the bearer is a unidirectional bearer configured only in an opposite direction,

[233] ◆ the UE 1i-01 assumes that the COUNT value is 0 for the direction not in use.

[234] ■ If the drb-CountMSB-InfoList does not include a bearer identifier of any bearer of the UE,

[235] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to TX_NEXT and RX_NEXT in the drb-CountInfoList of the Counter Check Response message.

[236] ■ (if the drb-CountMSB-InfoList includes a bearer identifier of a bearer of the UE) if the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink) indicated in the drb-CountMSB-InfoList for at least one direction differs from the COUNT value (TX_NEXT or RX_NEXT) for the bearer of the UE,

[237] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to TX_NEXT and RX_NEXT in the drb-CountInfoList of the Counter Check Response message.

[238] - For each bearer (e.g., DRB) indicated in the drb-CountMSB-InfoList of the Counter Check message but not established,

[239] ■ the UE includes the bearer identifier of the bearer and count-Uplink 25 MSBs of the countMSB-Uplink and countMSB-Downlink set respectively to be equal to the 25 MSBs of the countMSB-Uplink or countMSB-Downlink indicated in the drb-CountMSB-InfoList along with the 7 least significant bits (LSBs) set to 0 in the drb-CountInfoList of the Counter Check response message.

[240] - The Counter Check Response message configured as above is sent to low layers for transmission.

[241] According to a second embodiment, when the eNB 1i-02 transmits the Counter Check message indicating use of the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink), the UE i1-01 determines COUNT values to be compared and reported as follows.

[242] In the second embodiment, the UE 1i-01 uses, for uplink, a value obtained by subtracting 1 from the TX_NEXT value as the first COUNT variable maintaining the COUNT value of the next data to be transmitted by the transmitting PDCP entity for the case of comparing the countMSB-Uplink and the 25 MSBs and, for downlink, a value obtained subtracting 1 from the second COUNT variable (RX_NEXT) maintaining the COUNT value of the next data (e.g., PDCP SDU) expected to be received among 4 COUNT variables (i.e., the first COUNT variable (RX_NEXT), the third COUNT variable (RX_DELIV), the fourth COUNT variable (RX_REORD), and the fifth COUNT variable (RCVD_COUNT)) in use by the receiving PDCP entity for the case of comparing the countMSB-Downlink and the 25 MSBs and reporting the COUNT values via the Counter Check Response message. Because the COUNT variables (TX_NEXT and RX_NEXT) indicate the COUNT values of the next data to

be received or delivered, they should be subtracted by 1 to indicate the current COUNT value.

[243] In the second embodiment, when the Counter Check message is received, the UE 1i-01 operates as follows.

[244] - For each established bearer (e.g., DRB),

[245] ■ if there is no COUNT value for a given direction (uplink or downlink) because the bearer is a unidirectional bearer configured only in an opposite direction,

[246] ◆ the UE 1i-01 assumes that the COUNT value is 0 for the direction not in use.

[247] ■ If the drb-CountMSB-InfoList does not include a bearer identifier of any bearer of the UE,

[248] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to TX_NEXT-1 and RX_NEXT-1 in the drb-CountInfoList of the Counter Check Response message.

[249] ■ (if the drb-CountMSB-InfoList includes a bearer identifier of a bearer of the UE) if the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink) indicated in the drb-CountMSB-InfoList for at least one direction differs from the COUNT value (TX_NEXT-1 or RX_NEXT-1) for the bearer of the UE,

[250] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to TX_NEXT-1 and RX_NEXT-1 in the drb-CountInfoList of the Counter Check Response message.

[251] - For each bearer (e.g., DRB) indicated in the drb-CountMSB-InfoList of the Counter Check message but not established,

[252] ■ the UE includes the bearer identifier of the bearer and count-Uplink 25 MSBs of the countMSB-Uplink and countMSB-Downlink set respectively to be equal to the 25 MSBs of the countMSB-Uplink or countMSB-Downlink indicated in the drb-CountMSB-InfoList along with the 7 least significant bits (LSBs) set to 0 in the drb-CountInfoList of the Counter Check response message.

[253] - The Counter Check Response message configured as above is sent to low layers for transmission.

[254] According to a third embodiment, when the eNB 1i-02 transmits the Counter Check message indicating use of the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink), the UE i1-01 determines COUNT values to be compared and reported as follows.

[255] In the third embodiment, the UE 1i-01 uses, for uplink, the TX_NEXT value as the first COUNT variable maintaining the COUNT value of the next data to be transmitted by the transmitting PDCP entity for the case of comparing the countMSB-Uplink and the 25 MSBs and, for downlink, the third COUNT variable (RX_DELIV) maintaining the COUNT value of the first data (e.g., PDCP SDU) that has not been delivered to the

upper layers among 4 COUNT variables (i.e., the first COUNT variable (RX_NEXT), the third COUNT variable (RX_DELIV), the fourth COUNT variable (RX_REORD), and the fifth COUNT variable (RCVD_COUNT)) in use by the receiving PDCP entity for the case of comparing the countMSB-Downlink and the 25 MSBs and reporting the COUNT values via the Counter Check Response message.

[256] In the third embodiment, when the Counter check message is received, the UE 1i-01 operates as follows.

[257] - For each established bearer (e.g., DRB),

[258] ■ if there is no COUNT value for a given direction (uplink or downlink) because the bearer is a unidirectional bearer configured only in an opposite direction,

[259] ◆ the UE 1i-01 assumes that the COUNT value is 0 for the direction not in use.

[260] ■ If the drb-CountMSB-InfoList does not include a bearer identifier of any bearer of the UE,

[261] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to TX_NEXT and RX_DELIV in the drb-CountInfoList of the Counter Check Response message.

[262] ■ (if the drb-CountMSB-InfoList includes a bearer identifier of a bearer of the UE) if the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink) indicated in the drb-CountMSB-InfoList for at least one direction differs from the COUNT value (TX_NEXT or RX_DELIV) for the bearer of the UE,

[263] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to TX_NEXT and RX_DELIV in the drb-CountInfoList of the Counter Check Response message.

[264] - For each bearer (e.g., DRB) indicated in the drb-CountMSB-InfoList of the Counter Check message but not established,

[265] ■ the UE includes the bearer identifier of the bearer and count-Uplink 25 MSBs of the countMSB-Uplink and countMSB-Downlink set respectively to be equal to the 25 MSBs of the countMSB-Uplink or countMSB-Downlink indicated in the drb-CountMSB-InfoList along with the 7 least significant bits (LSBs) set to 0 in the drb-CountInfoList of the Counter Check response message.

[266] - The Counter Check Response message configured as above is sent to low layers for transmission.

[267] According to a fourth embodiment, when the eNB 1i-02 transmits the Counter Check message indicating use of the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink), the UE i1-01 determines COUNT values to be compared and reported as follows.

[268] In the fourth embodiment, the UE 1i-01 uses, for uplink, a value obtained by 1 from the TX_NEXT value as the first COUNT variable maintaining the COUNT value of

the next data to be transmitted by the transmitting PDCP entity for the case of comparing the countMSB-Uplink and the 25 MSBs and, for downlink, a value obtained by subtracting 1 from the third COUNT variable (RX_DELIV) maintaining the COUNT value of the first data (e.g., PDCP SDU) that has not been delivered to the upper layers among 4 COUNT variables (i.e., the first COUNT variable (RX_NEXT), the third COUNT variable (RX_DELIV), the fourth COUNT variable (RX_REORD), and the fifth COUNT variable (RCVD_COUNT)) in use by the receiving PDCP entity for the case of comparing the countMSB-Downlink and the 25 MSBs and reporting the COUNT values via the Counter Check Response message. Because the COUNT variables (TX_NEXT and RX_DELIV) indicate the COUNT values of the next data to be received or delivered, they should be subtracted by 1 to indicate the current COUNT value.

[269] In the fourth embodiment, when the Counter check message is received, the UE 1i-01 operates as follows.

[270] - For each established bearer (e.g., DRB),

[271] ■ if there is no COUNT value for a given direction (uplink or downlink) because the bearer is a unidirectional bearer configured only in an opposite direction,

[272] ◆ the UE 1i-01 assumes that the COUNT value is 0 for the direction not in use.

[273] ■ If the drb-CountMSB-InfoList does not include a bearer identifier of any bearer of the UE,

[274] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to TX_NEXT-1 and RX_DELIV-1 in the drb-CountInfoList of the Counter Check Response message.

[275] ■ (if the drb-CountMSB-InfoList includes a bearer identifier of a bearer of the UE) if the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink) indicated in the drb-CountMSB-InfoList for at least one direction differs from the COUNT value (TX_NEXT-1 or RX_DELIV-1) for the bearer of the UE,

[276] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to TX_NEXT-1 and RX_DELIV-1 in the drb-CountInfoList of the Counter Check Response message.

[277] - For each bearer (e.g., DRB) indicated in the drb-CountMSB-InfoList of the Counter Check message but not established,

[278] ■ the UE includes the bearer identifier of the bearer and count-Uplink 25 MSBs of the countMSB-Uplink and countMSB-Downlink set respectively to be equal to the 25 MSBs of the countMSB-Uplink or countMSB-Downlink indicated in the drb-CountMSB-InfoList along with the 7 least significant bits (LSBs) set to 0 in the drb-CountInfoList of the Counter Check response message.

[279] - The Counter Check Response message configured as above is sent to low layers for

transmission.

[280] According to a fifth embodiment, when the eNB 1i-02 transmits the Counter Check message indicating use of the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink), the UE i1-01 determines COUNT values to be compared and reported as follows.

[281] In the fifth embodiment, the UE 1i-01 uses, for uplink, the TX_NEXT value as the first COUNT variable maintaining the COUNT value of the next data to be transmitted by the transmitting PDCP entity for the case of comparing the countMSB-Uplink and the 25 MSBs and, for downlink, the fifth COUNT variable (RCVD_COUNT) maintaining the currently received COUNT among 4 COUNT variables (i.e., the first COUNT variable (RX_NEXT), the third COUNT variable (RX_DELIV), the fourth COUNT variable (RX_REORD), and the fifth COUNT variable (RCVD_COUNT)) in use by the receiving PDCP entity for the case of comparing the countMSB-Downlink and the 25 MSBs and reporting the COUNT values via the Counter Check Response message.

[282] In the fifth embodiment, when the Counter check message is received, the UE 1i-01 operates as follows.

[283] - For each established bearer (e.g., DRB),

[284] ■ if there is no COUNT value for a given direction (uplink or downlink) because the bearer is a unidirectional bearer configured only in an opposite direction,

[285] ◆ the UE 1i-01 assumes that the COUNT value is 0 for the direction not in use.

[286] ■ If the drb-CountMSB-InfoList does not include a bearer identifier of any bearer of the UE,

[287] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to TX_NEXT and RCVD_COUNT in the drb-CountInfoList of the Counter Check Response message.

[288] ■ (if the drb-CountMSB-InfoList includes a bearer identifier of a bearer of the UE) if the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink) indicated in the drb-CountMSB-InfoList for at least one direction differs from the COUNT value (TX_NEXT or RCVD_COUNT) for the bearer of the UE,

[289] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to TX_NEXT and RCVD_COUNT in the drb-CountInfoList of the Counter Check Response message.

[290] - For each bearer (e.g., DRB) indicated in the drb-CountMSB-InfoList of the Counter Check message but not established,

[291] ■ the UE includes the bearer identifier of the bearer and count-Uplink 25 MSBs of the countMSB-Uplink and countMSB-Downlink set respectively to be equal to the 25 MSBs of the countMSB-Uplink or countMSB-Downlink indicated in the drb-

CountMSB-InfoList along with the 7 least significant bits (LSBs) set to 0 in the drb-CountInfoList of the Counter Check response message.

[292] - The Counter Check Response message configured as above is sent to low layers for transmission.

[293] According to a sixth embodiment, when the eNB 1i-02 transmits the Counter Check message indicating use of the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink), the UE i1-01 determines COUNT values to be compared and reported as follows.

[294] In the sixth embodiment, the UE 1i-01 uses, for uplink, a value acquired by subtracting 1 from the TX_NEXT value as the first COUNT variable maintaining the COUNT value of the next data to be transmitted by the transmitting PDCP entity for the case of comparing the countMSB-Uplink and the 25 MSBs and, for downlink, a value acquired by subtracting 1 from the fifth COUNT variable (RCVD_COUNT) maintaining the currently received COUNT among 4 COUNT variables (i.e., the first COUNT variable (RX_NEXT), the third COUNT variable (RX_DELIV), the fourth COUNT variable (RX_REORD), and the fifth COUNT variable (RCVD_COUNT)) in use by the receiving PDCP entity for the case of comparing the countMSB-Downlink and the 25 MSBs and reporting the COUNT values via the Counter Check Response message. Because the COUNT variables (TX_NEXT and RCVD_COUNT) indicate the COUNT values of the next data to be received or delivered, they should be subtracted by 1 to indicate the current COUNT value.

[295] In the sixth embodiment, when the Counter check message is received, the UE 1i-01 operates as follows.

[296] - For each established bearer (e.g., DRB),

[297] ■ if there is no COUNT value for a given direction (uplink or downlink) because the bearer is a unidirectional bearer configured only in an opposite direction,

[298] ◆ the UE 1i-01 assumes that the COUNT value is 0 for the direction not in use.

[299] ■ If the drb-CountMSB-InfoList does not include a bearer identifier of any bearer of the UE,

[300] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to TX_NEXT-1 and RCVD_COUNT-1 in the drb-CountInfoList of the Counter Check Response message.

[301] ■ (if the drb-CountMSB-InfoList includes a bearer identifier of a bearer of the UE) if the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink) indicated in the drb-CountMSB-InfoList for at least one direction differs from the COUNT value (TX_NEXT-1 or RCVD_COUNT-1) for the bearer of the UE,

[302] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to TX_NEXT-1 and RCVD_COUNT-1 in the drb-

CountInfoList of the Counter Check Response message.

[303] - For each bearer (e.g., DRB) indicated in the drb-CountMSB-InfoList of the Counter Check message but not established,

[304] ■ the UE includes the bearer identifier of the bearer and count-Uplink 25 MSBs of the countMSB-Uplink and countMSB-Downlink set respectively to be equal to the 25 MSBs of the countMSB-Uplink or countMSB-Downlink indicated in the drb-CountMSB-InfoList along with the 7 least significant bits (LSBs) set to 0 in the drb-CountInfoList of the Counter Check response message.

[305] - The Counter Check Response message configured as above is sent to low layers for transmission.

[306] The first to sixth embodiments of the disclosure are directed to the COUNT check procedures in which an NR PDCP entity is established per data bearer in the UE 1i-01. However, the UE 1i-01 accessible to both the LTE eNB and NR gNB may be configured to have an NR PDCP entity or an LTE PDCP entity per data bearer with the version change of the PDCP entity. In this case, the method for selecting the COUNT values to be compared and reported in the counter check procedure may vary according to whether the PDCP entity configured for each bearer (DRB) is the NR PDCP entity or the LTE PDCP entity.

[307] Hereinafter, a description is made of the method for selecting a COUNT value to be compared and reported differently according to whether the PDCP entity configured for each bearer (e.g., DRB) is an NR PDCP entity or an LTE PDCP entity.

[308] According to a seventh embodiment, when the eNB 1i-02 transmits the Counter Check message indicating use of the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink), the UE i1-01 determines COUNT values to be compared and reported according to whether the PDCP entity configured per bearer is an LTE PDCP entity or an NR PDCP entity as follows.

[309] In the seventh embodiment, if an NR PDCP entity is configured for a bearer, the UE 1i-01 uses, for uplink, a value acquired by subtracting 1 form the TX_NEXT value as the first COUNT variable maintaining the COUNT value of the next data to be transmitted by the transmitting PDCP entity for the case of comparing the countMSB-Uplink and the 25 MSBs and, for downlink, a value acquired by subtracting 1 from the second COUNT variable (RX_NEXT) maintaining the COUNT value of the next data (e.g., PDCP SDU) expected to be received among 4 COUNT variables (i.e., the first COUNT variable (RX_NEXT), the third COUNT variable (RX_DELIV), the fourth COUNT variable (RX_REORD), and the fifth COUNT variable (RCVD_COUNT)) in use by the receiving PDCP entity for the case of comparing the countMSB-Downlink and the 25 MSBs and reporting the COUNT values via the Counter Check Response message. Because the COUNT variables (TX_NEXT and RX_NEXT) indicate the

COUNT values of the next data to be received or delivered, they should be subtracted by 1 to indicate the current COUNT value.

[310] In the seventh embodiment, if an NR PDCP entity is configured for a bearer, the UE 1i-01 uses, for uplink, a value acquired by subtracting 1 from the Next_PDCP_TX_SN value as the first window variable maintaining the PDCP SN of the next data to be transmitted by the transmitting PDCP entity and a COUNT value generated based on the TX_HFN variable maintaining the HFN value of the transmitter for the case of comparing the countMSB-Uplink and the 25 MSBs and, for downlink, a value acquired by subtracting 1 from the second window variable (Next_PDCP_RX_SN) maintaining the PDCP SN value of the next data (e.g., PDCP SDU) expected to be received among 3 window variables (i.e., the second window variable (Next_PDCP_RX_SN indicating the PDCP SN of the next data expected to be received), the third window variable (Last_Submitted_PDCP_RX_SN indicating PDCP SN of last data delivered to upper layers), and the fourth window variable (Reordering_PDCP_RX_COUNT indicating COUNT value triggering a timer)) in use by the receiving PDCP entity and a COUNT value generated based on the RX_HFN variable maintaining the HFN value of the receiver for the case of comparing the countMSB-Downlink and the 25 MSBs and reporting the COUNT values via the Counter Check Response message. Because the window variables (Next_PDCP_TX_SN and Next_PDCP_RX_SN) indicate the PDCP SN values of the next data to be received or delivered, they should be subtracted by 1 to indicate the current PDCP SN value.

[311] In the seventh embodiment, when the Counter check message is received, the UE 1i-01 operates as follows.

[312] - For each established bearer (e.g., DRB),

[313] ■ if there is no COUNT value for a given direction (uplink or downlink) because the bearer is a unidirectional bearer configured only in an opposite direction,

[314] ◆ the UE 1i-01 assumes that the COUNT value is 0 for the direction not in use.

[315] ■ If the drb-CountMSB-InfoList does not include a bearer identifier of any bearer of the UE and if an LTE PDCP entity is configured for the bearer identified by the bearer identifier,

[316] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to the COUNT value based on the TX_HFN and Next_PDCP_TX_SN -1 and the COUNT value based on the RX_HFN and Next_PDCP_RX_SN-1 in the drb-CountInfoList of the Counter Check Response message.

[317] ■ (if the drb-CountMSB-InfoList includes a bearer identifier of a bearer of the UE) if the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink)

indicated in the drb-CountMSB-InfoList for at least one direction differs from the COUNT value (TX_NEXT-1 or RX_NEXT-1) for the bearer of the UE and if an LTE PDCP entity is configured for the bearer,

[318] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to the COUNT value based on the TX_HFN and Next_PDCP_TX_SN -1 and the COUNT value based on the RX_HFN and Next_PDCP_RX_SN-1 in the drb-CountInfoList of the Counter Check Response message.

[319] ■ If the drb-CountMSB-InfoList does not include a bearer identifier of any bearer of the UE and if an NR PDCP entity is configured for the bearer identified by the bearer identifier,

[320] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to TX_NEXT-1 and RX_NEXT-1.

[321] ■ (if the drb-CountMSB-InfoList includes a bearer identifier of a bearer of the UE) if the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink) indicated in the drb-CountMSB-InfoList for at least one direction differs from the COUNT value (TX_NEXT-1 or RX_NEXT-1) for the bearer of the UE and if an NR PDCP entity is configured for the bearer,

[322] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to TX_NEXT-1 and RX_NEXT-1 in the drb-CountInfoList of the Counter Check Response message.

[323] - For each bearer (e.g., DRB) indicated in the drb-CountMSB-InfoList of the Counter Check message but not established,

[324] ■ the UE includes the bearer identifier of the bearer and count-Uplink 25 MSBs of the countMSB-Uplink and countMSB-Downlink set respectively to be equal to the 25 MSBs of the countMSB-Uplink or countMSB-Downlink indicated in the drb-CountMSB-InfoList along with the 7 least significant bits (LSBs) set to 0 in the drb-CountInfoList of the Counter Check response message.

[325] - The Counter Check Response message configured as above is sent to low layers for transmission.

[326] Hereinafter, a description is made of the method for selecting a COUNT value to be compared and reported regardless of whether the PDCP entity configured per bearer (e.g., DRB) is an NR PDCP entity or an LTE PDCP entity .

[327] According to an eighth embodiment, when the eNB 1i-02 transmits the Counter Check message indicating use of the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink), the UE i1-01 determines COUNT values to be compared and reported regardless of whether the PDCP entity configured per bearer is an LTE PDCP entity or an NR PDCP entity as follows.

[328] In the eighth embodiment, the UE 1i-01 uses, for uplink, a COUNT value corresponding to the data with the highest (or largest) PDCP SN among the data (e.g., PDCP SDUs or PDCP PDUs) transmitted by the transmitting PDCP entity until then for the case of comparing the countMSB-Uplink and the 25 MSBs and, for downlink, a COUNT value corresponding to the data with the highest (or largest) PDCP SN among the data (e.g., PDCP SDUs or PDCP PDUs) received by the receiving PDCP entity until then for the case of comparing the countMSB-Downlink and the 25 MSBs and reporting the COUNT values via the Counter Check Response message.

[329] In the eighth embodiment, when the Counter check message is received, the UE 1i-01 operates as follows.

[330] - For each established bearer (e.g., DRB),

[331] ■ if there is no COUNT value for a given direction (uplink or downlink) because the bearer is a unidirectional bearer configured only in an opposite direction,

[332] ◆ the UE 1i-01 assumes that the COUNT value is 0 for the direction not in use.

[333] ■ If the drb-CountMSB-InfoList does not include a bearer identifier of any bearer of the UE and if an LTE PDCP entity is configured for the bearer identified by the bearer identifier,

[334] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to the COUNT value corresponding to the data with the highest (or largest) PDCP SN among the data (e.g., PDCP SDUs or PDCP PDUs) transmitted until then and the COUNT value corresponding to the data with the highest (or largest) PDCP SN among the data (e.g., PDCP SDUs or PDCP PDUs) received until then in the drb-CountInfoList of the Counter Check Response message.

[335] ■ (if the drb-CountMSB-InfoList includes a bearer identifier of a bearer of the UE) if the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink) indicated in the drb-CountMSB-InfoList for at least one direction differs from the COUNT value (TX_NEXT-1 or RX_NEXT-1) for the bearer of the UE and if an LTE PDCP entity is configured for the bearer,

[336] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to the COUNT value corresponding to the data with the highest (or largest) PDCP SN among the data (e.g., PDCP SDUs or PDCP PDUs) transmitted until then and the COUNT value corresponding to the data with the highest (or largest) PDCP SN among the data (e.g., PDCP SDUs or PDCP PDUs) received until then in the drb-CountInfoList of the Counter Check Response message.

[337] - For each bearer (e.g., DRB) indicated in the drb-CountMSB-InfoList of the Counter Check message but not established,

[338] ■ the UE includes the bearer identifier of the bearer and count-Uplink 25 MSBs of the countMSB-Uplink and countMSB-Downlink set respectively to be equal to the 25

MSBs of the countMSB-Uplink or countMSB-Downlink indicated in the drb-CountMSB-InfoList along with the 7 least significant bits (LSBs) set to 0 in the drb-CountInfoList of the Counter Check response message.

[339] - The Counter Check Response message configured as above is sent to low layers for transmission.

[340] Hereinafter, a description is made of the Counter check procedure for the terminal 1i-01 accessible only to the LTE eNB. That is, a method for the UE 1i-01 allowed for establishing only per-bearer (e.g., DRB) LTE PDCP entities to select and report COUNT values.

[341] According to a ninth embodiment, when the eNB 1i-02 transmits the Counter Check message indicating use of the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink), the UE i1-01 configured with an LTE PDCP entity per bearer determines COUNT values to be compared and reported as follows.

[342] In the ninth embodiment, because an LTE PDCP entity is configured per bearer, the UE 1i-01 uses, for uplink, a value acquired by subtracting 1 from the Next_PDCP_TX_SN value as the first window variable maintaining the PDCP SN of the next data to be transmitted by the transmitting PDCP entity and a COUNT value generated based on the TX_HFN variable maintaining the HFN value of the transmitter for the case of comparing the countMSB-Uplink and the 25 MSBs and, for downlink, a value acquired by subtracting 1 from the second window variable (Next_PDCP_RX_SN) maintaining the PDCP SN value of the next data (e.g., PDCP SDU) expected to be received among 3 window variables (i.e., the second window variable (Next_PDCP_RX_SN indicating the PDCP SN of the next data expected to be received), the third window variable (Last_Submitted_PDCP_RX_SN indicating PDCP SN of last data delivered to upper layers), and the fourth window variable (Reordering_PDCP_RX_COUNT indicating COUNT value triggering a timer)) in use by the receiving PDCP entity and a COUNT value generated based on the RX_HFN variable maintaining the HFN value of the receiver for the case of comparing the countMSB-Downlink and the 25 MSBs and reporting the COUNT values via the Counter Check Response message. Because the window variables (Next_PDCP_TX_SN and Next_PDCP_RX_SN) indicate the PDCP SN values of the next data to be received or delivered, they should be subtracted by 1 to indicate the current PDCP SN value.

[343] In the ninth embodiment, when the Counter check message is received, the UE 1i-01 operates as follows.

[344] - For each established bearer (e.g., DRB),

[345] ■ if there is no COUNT value for a given direction (uplink or downlink) because the bearer is a unidirectional bearer configured only in an opposite direction,

[346] ◆ the UE 1i-01 assumes that the COUNT value is 0 for the direction not in use.

[347] ■ If the drb-CountMSB-InfoList does not include a bearer identifier of any bearer of the UE,

[348] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to the COUNT value based on the TX_HFN and Next_PDCP_TX_SN -1 and the COUNT value based on the RX_HFN and Next_PDCP_RX_SN-1 in the drb-CountInfoList of the Counter Check Response message.

[349] ■ (if the drb-CountMSB-InfoList includes a bearer identifier of a bearer of the UE) if the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink) indicated in the drb-CountMSB-InfoList for at least one direction differs from the COUNT value (TX_NEXT-1 or RX_NEXT-1) for the bearer of the UE,

[350] ◆ the UE includes the bearer identifier of the bearer and the count-Uplink and count-Downlink values set respectively to the COUNT value based on the TX_HFN and Next_PDCP_TX_SN -1 and the COUNT value based on the RX_HFN and Next_PDCP_RX_SN-1 in the drb-CountInfoList of the Counter Check Response message.

[351] - For each bearer (e.g., DRB) indicated in the drb-CountMSB-InfoList of the Counter Check message but not established,

[352] ■ the UE includes the bearer identifier of the bearer and count-Uplink 25 MSBs of the countMSB-Uplink and countMSB-Downlink set respectively to be equal to the 25 MSBs of the countMSB-Uplink or countMSB-Downlink indicated in the drb-CountMSB-InfoList along with the 7 least significant bits (LSBs) set to 0 in the drb-CountInfoList of the Counter Check response message.

[353] - The Counter Check Response message configured as above is sent to low layers for transmission.

[354] FIG. 1j illustrates a diagram for explaining a method for reducing a size of MSBs of a COUNT value indicated in a proposed Counter check procedure according to an embodiment of the disclosure.

[355] The proposed Counter check procedure aims to check for the HFN value of per-bearer COUNT value. Accordingly, the size of the MSBs of the COUNT value indicated by the gNB 1i-02 may be dramatically reduced according to the length of a configurable PDCP SN. As aforementioned, in the next generation mobile communication system, the length of the PDCP SN may be set to 12 bits in the case as denoted by reference number 1j-05 or 18 bits in the case as denoted by reference number 1j-10. For all bearers, 20 MSBs of the COUNT value are enough even when comparing HFN values as denoted by reference number 1j-15. Instead of using 25 MSBs of the COUNT value as described in the above Count check procedures, if 20

MSBs of the COUNT value is used, it is possible to reduce overhead by 5 bits x number of bearers. It may also be possible to further reduce the header overhead by setting the number of MSBs to (32 bits - PDCP SN length per bearer).

[356] Given that an RLC entity supports 6-bit RLC SN, if a new PDCP SN length of 6 bits is introduced for reducing the header overhead, the HFN occupying the 25 MSBs of the COUNT may be extended to 26 bits in the above Count check procedure for comparison accuracy.

[357] The proposed Counter check procedure may be applied when a Counter check message transmitted on SRB1 in use by the gNB 1i-02 corresponding to a master cell group (MCG).

[358] Hereinafter, a description is made of the operation of a UE when the UE receives a Counter check message transmitted on SRB3 in use by the gNB 1i-02 corresponding to a secondary cell group (SCG) rather than an MCG. The description is made with reference to FIG. 1i. The UE operations of determining the COUNT values to be compared and reported upon receipt of the Counter Check message indicating use of 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink) from the eNB 1i-02 according to the first to sixth embodiments are applicable to the Count check procedure in which the Counter check message is transmitted on SRB3 in use by an SCG. The method for reducing overhead of MSBs of the COUNT value, as described with reference to FIG. 1j, may also be applicable to the Count check procedure in which the Counter check message is transmitted on SRB3 in use by an SCG.

[359] In the case where an RRC connection is established between the UE 1i-01 and the gNB 1i-02, the gNB 1i-02 transmits a CounterCheck RRC message to the UE 1i-01 at step 1i-10 to request for per-DRB COUNT check and report. This message may be carried by an RRCConnectionReconfiguration or RRCConnectionReestablishment message being transmitted on a dedicated common control channel (DCCH). The CounterCheck message may include a list of bearers (e.g., DRB or SRB) for per-bearer COUNT check, drb-CountMSB-InfoList, which contains DRB identifier, countMSB-Uplink(25bit), and countMSB-Downlink(25bit). That is, the list includes per-bearer identifiers of the bearers for which the COUNT check is required and 25 most significant bits (MSBs) of each of the uplink and downlink COUNT values of the gNB 1i-02 on the corresponding bearers. Meanwhile, the gNB 1i-02 may transmit the CounterCheck message on SRB1 or SRB3. That is, the COUNT CHECK request may be made through an MCG SRB (e.g., SRB1) for the case where the UE 1i-01 is connected to the MCG or through an SCG SRB (e.g., SRB3) for the case where the UE 1i-01 is connected to the SCG. The COUNT CHECK request may also be made simultaneously through both SRB1 and SRB3.

[360] The UE 1i-01 determines whether the CounterCheck message has been received on SRB1 or SRB3 and performs a subsequent operation at step 1i-15 as follows.

[361] Receipt on SRB1 (first operation): The UE generates a COUNT CHECK RESPONSE message including full COUNTs of the first and third DRB groups.

[362] Receipt on SRB3 (second operation): The UE generate a COUNT CHECK RESPONSE message including full COUNTs of the second DRB and third DRB groups.

[363] The DRB groups for use in the first and second operations are defined as follows.

[364] First DRB group: A set of DRBs that are not included in drb-CountMSB-InfoList among MCG bearers (or MCG terminated bearers, i.e., bearers for which a PDCP entity exists in MCG) and MCG split bearers.

[365] Second DRB group: A set of DRBs that are not included in drb-CountMSB-InfoList among SCG bearers (or SCG terminated bearers, i.e., bearers for which a PDCP entity exists in SCG) and SCG split bearers.

[366] Third DRB group: A set of DRBs with 25 MSBs that are not matched among DRBs included in drb-CountMSB-InfoList.

[367] For example, if the CounterCheck message is received through SRB1, the UE 1i-01 includes full COUNT values for the DRBs that are not included in the configured DRB list among the MCG bearers and MCG split bearers and for the DRBs with non-matching result of comparison between the 25 MSBs for the DRBs configured in the received CounterCheck message and the 25 MSBs (in both countMSB-Uplink for uplink and countMSB-Downlink for downlink) stored in the UE 1i-01. If the COUNT value transmitted by the gNB 1i-02 matches the COUNT value calculated by the UE 1i-01, the corresponding COUNT value is not included in the reporting list.

[368] Here, it is necessary to select a PDCP SDU of which COUNT value is to be compared with a value (countMSB-Uplink (25 bits) or countMSB-Downlink (25bits)) configured in the CounterCheck message. The UE 1i-01 may use one of two methods as follows:

[369] selecting the PDCP SDU with the highest COUNT (NEXT_RX_COUNT-1) among the PDCP SDUs received until then; and

[370] selecting PDCP SDU with the highest COUNT among PDCP SDUs reordered until then.

[371] It is also necessary to select a PDCP SDU of which COUNT value is reported. The UE 1i-01 may use one of three methods as follows:

[372] selecting the PDCP SDU with a matching result of COUNT value comparison;

[373] selecting the PDCP SDU with the highest COUNT value at reporting time point; and

[374] selecting the PDCP SDU with the highest COUNT value among PDCP SDUs reordered at reporting time point.

[375] After generating the CountCheck result information as above, the UE 1i-01 transmits, at step 1i-20, an RRC message (CounterCheckResponse) including the corresponding information to the gNB 1i-01.

[376] FIG. 1k illustrates a flowchart of an operation of a UE in a proposed Counter check procedure according to an embodiment of the disclosure.

[377] In FIG. 1k, the UE receives an RRC message, i.e., a Counter check message, at step 1k-05; upon receipt of this message, the UE determines at step 1k-10 whether the drb-CountMSB-InfoList includes a bearer identifier per bearer (e.g., DRB) established for the UE. If it is determined that the drb-CountMSB-InfoList does not include a bearer identifier of any bearer for the UE, the UE selects count-Uplink and count-Downlink values at step 1k-15 according to one of the first to sixth embodiments and includes the bearer identifiers of the corresponding bearers and the selected uplink and downlink COUNT values in the drb-CountInfoList of a Counter Check Response message at step 1k-20.

[378] If it is determined that the drb-CountMSB-InfoList includes a bearer identifier of any bearer for the UE, the UE selects the uplink and downlink COUNT values at step 1k-25 according to one of the first to sixth embodiments and compares, at step 1k-30, the selected COUNT values with MSBs of the COUNT value that is indicated by the base station.

[379] If the 25 MSBs of the COUNT value (countMSB-Uplink or countMSB-Downlink) differs from the COUNT value (uplink or downlink COUNT value) for the bearer that is selected by the UE in at least one direction, the UE includes the bearer identifier of the corresponding bearer and the selected uplink and downlink COUNT values in the drb-CountInfoList of the Counter Check Response message at step 1k-35.

[380] FIG. 1l illustrates a block diagram of a configuration of a UE according to an embodiment of the disclosure.

[381] In reference to FIG. 1l, the UE includes a radio frequency (RF) processor 1l-10, a baseband processor 1l-20, a storage unit 1l-30, and a controller 1l-40.

[382] The RF processor 1l-10 has a function for transmitting/receiving a signal over a radio channel such as band conversion and amplification of the signal. That is, the RF processing unit 1l-10 up-converts a baseband signal from the baseband processor 1l-20 to an RF band signal and transmits the RF signal via an antenna and down-converts the RF signal received via the antenna to a baseband signal. For example, the RF processor 1l-10 may include a transmission filter, a reception filter, an amplifier, a mixer, an oscillator, a digital-to-analog converter (DAC), and an analog-to-digital converter (ADC). Although one antenna is depicted in the drawing, the UE may be provided with a plurality of antennas. The RF processor 1l-10 may also include a plurality of RF chains. The RF processor 1l-10 may perform beamforming. For beamforming, the RF

processor 11-10 may adjust the phase and size of a signal to be transmitted/received by means of the antennas or antenna elements. The RF processor 11-10 may be configured to support a MIMO scheme with which the UE can receive multiple layers simultaneously. The RF processor 11-10 may configure the plurality of antennas or antenna elements appropriately, under the control of the controller 11-40, to perform beam sweeping and adjust the beam direction and beam width to achieve an alignment of the reception and transmission beam.

[383] The baseband processor 11-20 has a baseband signal-bit string conversion function according to a physical layer standard of the system. For example, in a data transmission mode, the baseband processor 11-20 performs encoding and modulation on the transmission bit string to generate complex symbols. In a data reception mode, the baseband processor 11-20 performs demodulation and decoding on the baseband signal from the RF processor 11-10 to recover the transmitted bit string. In the case of using an OFDM scheme for data transmission, the baseband processor 11-20 performs encoding and modulation on the transmission bit string to generate complex symbols, maps the complex symbols to subcarriers, performs inverse fast Fourier transform (IFFT) on the symbols, and inserts a cyclic prefix (CP) into the symbols to generate OFDM symbols. In the data reception mode, the baseband processor 11-20 splits the baseband signal from the RF processor 11-10 into OFDM symbols, perform fast Fourier transform (FFT) on the OFDM symbols to recover the signals mapped to the subcarriers, and performs demodulation and decoding on the signals to recover the transmitted bit string.

[384] The baseband processor 11-20 and the RF processor 11-10 process the transmission and reception signals as described above. Accordingly, the baseband processor 11-20 and the RF processor 11-10 may be referred to as a transmitter, a receiver, a transceiver, or a communication unit/circuit. At least one of the baseband processor 11-20 and the RF processor 11-10 may include a plurality of communication modules for supporting different radio access technologies. At least one of the baseband processor 11-20 and the RF processor 11-10 may also include multiple communication modules for processing the signals in different frequency bands. For example, the different radio access technologies may include a wireless local area network (WLAN) (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.11) and a cellular network (e.g., LTE). The different frequency bands may include a super high frequency (SHF) band (e.g., 2.2 GHz and 2 GHz bands) and an mmWave band (e.g., 60 GHz).

[385] The storage unit 11-30 stores data such as basic programs for operation of the UE, application programs, and setting information. The storage unit 11-30 provides the stored information in response to a request from the controller 11-40.

[386] The controller 11-40 controls overall operations of the UE. For example, the controller 11-40 controls the baseband processor 11-20 and the RF processor 11-10 for transmitting and receiving signals. The controller 11-40 writes and reads data to and from the storage unit 11-40. For this purpose, the controller 11-40 may include at least one processor. For example, the controller 11-40 may include a communication processor (CP) for controlling communications and an application processor (AP) for controlling higher layer programs such as applications. The controller 11-40 may be electrically connected to the transceiver.

[387] FIG. 1m illustrates a block diagram of a configuration of a base station in a wireless communication according to an embodiment of the disclosure.

[388] In reference to FIG. 1m, the base station includes an RF processor 1m-10, a baseband processor 1m-20, a backhaul communication unit 1m-30, a storage unit 1m-40, and a controller 1m-50.

[389] The RF processor 1m-10 has a function for transmitting/receiving a signal over a radio channel such as band conversion and amplification of the signal. That is, the RF processing unit 1m-10 up-converts a baseband signal from the baseband processor 1m-20 to an RF band signal and transmits the RF signal via an antenna and down-converts the RF signal received via the antenna to a baseband signal. For example, the RF processor 1m-10 may include a transmission filter, a reception filter, an amplifier, a mixer, an oscillator, a DAC, and an ADC. Although one antenna is depicted in the drawing, the base station may be provided with a plurality of antennas. The RF processor 1m-10 may also include a plurality of RF chains. The RF processor 1i-10 may perform beamforming. For beamforming, the RF processor 1m-10 may adjust the phase and size of a signal to be transmitted/received by means of the antennas or antenna elements. The RF processor 1m-10 may be configured to transmit one or more layers for a downlink MIMO operation.

[390] The baseband processor 1m-20 has a baseband signal-bit string conversion function according to a physical layer standard of the system. For example, in a data transmission mode, the baseband processor 1m-20 performs encoding and modulation on the transmission bit string to generate complex symbols. In a data reception mode, the baseband processor 1m-20 performs demodulation and decoding on the baseband signal from the RF processor 1m-10 to recover the transmitted bit string. In the case of using an OFDM scheme for data transmission, the baseband processor 1m-20 performs encoding and modulation on the transmission bit string to generate complex symbols, maps the complex symbols to subcarriers, performs inverse fast Fourier transform (IFFT) on the symbols, and inserts a cyclic prefix (CP) into the symbols to generate OFDM symbols. In the data reception mode, the baseband processor 1m-20 splits the baseband signal from the RF processor 1m-10 into OFDM symbols, performs fast

Fourier transform (FFT) on the OFDM symbols to recover the signals mapped to the subcarriers, and performs demodulation and decoding on the signals to recover the transmitted bit string. The baseband processor 1m-20 and the RF processor 1m-10 process the transmission and reception signals as described above. Accordingly, the baseband processor 1m-20 and the RF processor 1m-10 may be referred to as a transmitter, a receiver, a transceiver, or a communication unit.

[391] The communication unit 1m-30 provides an interface for communication with other nodes in the network.

[392] The storage unit 1m-40 stores data such as basic programs for operation of the base station, application programs, and setting information. The storage unit 1m-40 may also store the information on the bearers established for UEs and measurement results reported by the connected UEs. The storage unit 1m-40 may also store the information for use by a UE in determining whether to enable or disable multi-connectivity. The storage unit 1m-40 may provide the stored data in reference to a request from the controller 1m-50.

[393] The controller 1m-50 controls overall operations of the base station. For example, the controller 1m-50 controls the baseband processor 1m-20, the RF processor 1m-10, and the backhaul communication unit 1m-30 for transmitting and receiving signals. The controller 1m-50 writes and reads data to and from the storage unit 1m-40. For this purpose, the controller 1m-50 may include at least one processor. The controller may be electrically connected to the transceiver.

[394] Embodiment B

[395] The disclosure proposes a bearer management and data processing method of wireless nodes in a next generation mobile communication system supporting wireless backhaul and a method for recovering lost data caused by radio link breakage or congestion at the wireless nodes.

[396] In detail, the disclosure proposes a PDCP status report-based lost data retransmission method and procedure between PDCP entities of two wireless end nodes in a wireless backhaul network.

[397] Detailed descriptions of the proposed methods are made hereinafter in various disclosed embodiments hereinafter.

[398] FIG. 2a illustrates a diagram of architecture of an LTE system to which the disclosure is applied.

[399] In reference to FIG. 2a, a radio access network of the LTE system includes evolved Node Bs (hereinafter, interchangeably referred to as eNB, node B, and base station) 2a-05, 2a-10, 2a-15, and 2a-20; a mobility management entity (MME) 2a-25; and a serving gateway (S-GW) 2a-30. A user terminal (hereinafter, interchangeably referred to as user equipment (UE) and terminal) 2a-35 connects to an external network via the

eNBs 2a-05, 2a-10, 2a-15, and 2a-20 and the S-GW 2a-30.

[400] The eNBs 2a-05, 2a-10, 2a-15, and 2a-20 correspond to the legacy node Bs of the universal mobile telecommunications system (UMTS). The UE 2a-35 connects to one of the eNBs via a radio channel, and the eNB has more complex functions than the legacy node B. In the LTE system where all user traffic including real time services such as Voice over IP (VoIP) is served through shared channels, there is a need of an entity for collecting UE-specific status information (such as buffer status, power headroom status, and channel status) and scheduling the UEs based on the collected information, and the eNB takes charge of such functions. Typically, one eNB hosts multiple cells. For example, the LTE system adopts Orthogonal Frequency Division Multiplexing (OFDM) as a radio access technology to secure a data rate of up to 100 Mbps in a bandwidth of 20 MHz. The LTE system also adopts Adaptive Modulation and Coding (AMC) to determine the modulation scheme and channel coding rate in adaptation to the channel condition of the UE. The S-GW 2a-30 handles data bearer functions to establish and release data bearer under the control of the MME 2a-25. The MME 2a-25 handles various control functions for the UE as well as the mobile management function and has connections with the eNBs 2a-05, 2a-10, 2a-15, and 2a-20.

[401] FIG. 2b illustrates a diagram of a protocol stack of an LTE system to which the disclosure is applied.

[402] As shown in FIG. 2b, the protocol stack of the interface between the UE 2b-50 and the eNB 2b-60 in the LTE system includes Packet Data Convergence Protocol (PDCP) 2b-05 and 2b-40, Radio Link Control (RLC) 2b-10 and 2b-35, and Medium Access Control (MAC) 2b-15 and 2b-30. The PDCP 2b-05 and 2b-40 takes charge of compressing/decompressing an IP header. The main functions of the PDCP 2b-05 and 2b-40 can be summarized as follows:

[403] - Header compression and decompression: ROHC only

[404] - Transfer of user data

[405] - In-sequence delivery of upper layer PDUs at PDCP re-establishment procedure for RLC AM

[406] - For split bearers in DC (only support for RLC AM): PDCP PDU routing for transmission and PDCP PDU reordering for reception

[407] - Duplicate detection of lower layer SDUs at PDCP re-establishment procedure for RLC AM

[408] - Retransmission of PDCP SDUs at handover and, for split bearers in DC, of PDCP PDUs at PDCP data-recovery procedure, for RLC AM

[409] - Ciphering and deciphering

[410] - Timer-based SDU discard in uplink

[411] The RLC 2b-10 and 2b-35 takes charge of reformatting PDCP PDUs in order to fit them into the size for ARQ operation. The main functions of the RLC layer can be summarized as follows:

[412] - Transfer of upper layer PDUs)

[413] - Error Correction through ARQ (only for AM data transfer)

[414] - Concatenation, segmentation and reassembly of RLC SDUs (only for UM and AM data transfer)

[415] - Re-segmentation of RLC data PDUs (only for AM data transfer)

[416] - Reordering of RLC data PDUs (only for UM and AM data transfer

[417] - Duplicate detection (only for UM and AM data transfer)

[418] - Protocol error detection (only for AM data transfer)

[419] - RLC SDU discard (only for UM and AM data transfer)

[420] - RLC re-establishment

[421] The MAC 2b-15 and 2b-30 allows for connection of multiple RLC entities established for one UE and takes charge of multiplexing RLC PDUs from the RLC layer into a MAC PDU and demultiplexing a MAC PDU into RLC PDUs. The main functions of the MAC layer can be summarized as follows:

[422] - Mapping between logical channels and transport channels

[423] - Multiplexing/demultiplexing of MAC SDUs belonging to one or different logical channels into/from transport blocks (TB) delivered to/from the physical layer on transport channels

[424] - Scheduling information reporting

[425] - Error correction through HARQ

[426] - Priority handling between logical channels of one UE

[427] - Priority handling between UEs by means of dynamic scheduling

[428] - MBMS service identification

[429] - Transport format selection

[430] - Padding

[431] The PHY layer 2b-20 and 2b-25 takes charge of channel-coding and modulation on higher layer data to generate and transmit OFDM symbols over a radio channel, and demodulating and channel-decoding on OFDM symbols received over the radio channel to deliver the decoded data to the higher layers.

[432] FIG. 2c illustrates a diagram of architecture of a next generation mobile communication system to which the disclosure is applied.

[433] As shown in FIG. 2c, the next generation mobile communication system includes a radio access network with a next generation base station (New Radio Node B (NR gNB)) 2c-10 and a new radio core network (NR CN) 2c-05. A new radio user equipment (NR UE) 2c-15 connects to an external network via the NR gNB 2c-10 and

the NR CN 2c-05.

[434] In FIG. 2c, the NR gNB 2c-10 corresponds to an evolved Node B (eNB) of the legacy LTE. The NR gNB 2c-10 to which the NR UE 2c-15 connects through a radio channel is capable of providing superior services in comparison with the legacy eNB. In the next generation mobile communication system where all user traffic is served through shared channels, it is necessary to schedule the NR UEs based on scheduling information such as buffer status, power headroom status, and channel status collected by the NR UEs, and the NR gNB 2c-10 takes charge of this function. Typically, one NR gNB hosts multiple cells. In order to achieve a data rate higher than the peak data rate of legacy LTE systems, the next generation mobile communication system may adopt a beamforming technique along with orthogonal frequency division multiple access (OFDMA) as a radio access technology. The next generation mobile communication system may also adopt an adaptive modulation and coding (AMC) to determine the modulation scheme and channel coding rate in adaptation to the channel condition of the NR UE. The NR CN 2c-05 takes charge of mobility support, bearer setup, and QoS configuration. The NR CN 2c-05 may take charge of a NR UE mobility management function, and a plurality of NR gNBs may connect to the NR CN 2c-05. The next generation mobile communication system may also interoperate with a legacy LTE system and, in this case, the NR CN 2c-05 connects to an MME 2c-25 through a network interface. The MME 2c-25 communicates with the eNB 2c-40 as a legacy base station.

[435] FIG. 2d illustrates a diagram of a protocol stack of a next generation mobile communication system to which the disclosure is applied.

[436] As shown in FIG. 2d, the protocol stack of the interface between an NR UE 2d-50 and an NR gNB 2d-60 in a next generation mobile communication system includes NR service data adaptation protocol (NR SDAP) 2d-01 and 2d-45, NR PDCP 2d-05 and 2d-40, NR RLC 2d-10 and 2d-35, and NR MAC 2d-15 and 2d-30.

[437] The main functions of the NR SDAP 2d-01 and 2d-45 may include some of the following functions:

[438] - transfer of user plane data

[439] - mapping between a QoS flow and a DRB for both DL and UL

[440] - marking QoS flow ID in both DL and UL packets)

[441] - reflective QoS flow to DRB mapping for the UL SDAP PDUs

[442] The UE 2d-50 may receive an RRC message for configuring an SDAP entity 2d-01 so as to determine whether to use PDCP entity-specific, bearer-specific, or logical channel-specific SDAP header and whether to use SDAP layer function via an RRC message and, if configured to use a specific PDAP header, receive a 1-bit NAS reflective QoS indicator and an AS reflective QoS indicator in the SDAP header in-

dicative of instructing the UE 2d-50 to update or reconfigure uplink and downlink QoS flow-data bearer mappings. The SDAP header may include QoS flow ID indicating a QoS. The QoS information may be used as data processing priority and scheduling information for guaranteeing service reliability.

[443] The main functions of the NR PDCP 2d-05 and 2d-40 may include some of the following functions:

[444] - Header compression and decompression: ROHC only

[445] - Transfer of user data

[446] - In-sequence delivery of upper layer PDUs

[447] - Out-of-sequence delivery of upper layer PDUs

[448] - PDCP PDU reordering for reception

[449] - Duplicate detection of lower layer SDUs

[450] - Retransmission of PDCP SDUs

[451] - Ciphering and deciphering

[452] - Timer-based SDU discard in uplink

[453] The PDCP PDU reordering function of an NR PDCP entity 2d-05 and 2d-40 is to reorder the PDCP PDUs delivered from a lower layer based on the PDCP sequence number (PDCP SN) and may include delivering the reordered data to an upper layer, recording the missing PDCP PDUs among the reordered PDCP PDUs, transmitting a status report indicating the missing PDCP PDUs to the sender, and requesting for retransmission of the missing PDCP PDUs.

[454] The main functions of the NR RLC 2d-10 and 2d-35 may include some of the following functions.

[455] - Transfer of upper layer PDUs)

[456] - In-sequence delivery of upper layer PDUs

[457] - Out-of-sequence delivery of upper layer PDUs

[458] - Error Correction through ARQ

[459] - Concatenation, segmentation and reassembly of RLC SDUs

[460] - Re-segmentation of RLC data PDUs

[461] - Reordering of RLC data PDUs

[462] - Duplicate detection

[463] - Protocol error detection

[464] - RLC SDU discard

[465] - RLC re-establishment

[466] The in-sequence delivery function of an NR RLC entity 2d-10 and 2d-35 is to deliver the RLC SDUs received from the lower layer to the upper layer and may include reassembling, when multiple segmented RLC SDUs constituting an original RLC SDU are received, the RLC SDUs and delivering the reassembled RLC SDU to the upper

layer; reordering the received RLC PDUs based on the RLC sequence number(SN) or PDCP SN; recording the missing RLC PDUs among the reordered RLC PDUs; transmitting a status report indicating the missing RLC PDUs to the sender; requesting for retransmission of the missing RLC PDUs; and delivering, when there is a missing RLC PDU, the RLC PDUs before the missing RLC PDU in sequence, delivering, if a predetermined timer expires even when there is any missing RLC SDU, all RLC SDUs received before the start of the timer to the upper layer in sequence, or delivering, if a predetermined timer expires even when there is any missing RLC SDU, all RLC SDUs received until then to the upper layer in sequence. It may also be possible to process the RLC PDUs in the receiving sequence (in the order of arrival regardless of sequence number) and deliver the RLC PDUs to the PDCP entity out of order (out-of-sequence delivery) and, if an RLC PDU is transmitted in the form of segments, to store the received segments, or wait until all segments constituting the RLC PDU are received and reassemble the segments into the original RLC PDU, which is delivered to the PDCP entity. The NR RLC layer 2d-10 and 2d-35 may have no concatenation function and, in this case, the concatenation function may be performed in the NR MAC layer 2d-15 and 2d-30 or replaced by the multiplexing function of the NR MAC layer 2d-15 and 2d-30.

[467] The out-of-sequence delivery function of an NR RLC entity 2d-10 and 2d-35 is to deliver the RLC SDUs received from the lower layer to the upper layer out of order and may include reassembling, when multiple segmented RLC SDUs constituting an original RLC SDU are received, the segmented RLC SDUs, delivering the reassembled RLC SDUs to the upper layer, arranging the received RLC PDUs based on the RLC SN or PDCP SN, and recording the SN of the missing RLC PDUs.

[468] The NR MAC 2d-15 and 2d-30 may be connected to multiple NR RLC entities, and the main functions of the NR MAC 2d-15 and 2d-30 may include some of the following functions:

[469] - Mapping between logical channels and transport channels

[470] - Multiplexing/demultiplexing of MAC SDUs

[471] - Scheduling information reporting

[472] - Error correction through HARQ

[473] - Priority handling between logical channels of one UE

[474] - Priority handling between UEs by means of dynamic scheduling

[475] - MBMS service identification

[476] - Transport format selection

[477] - Padding

[478] The NR PHY layer 2d-20 and 2d-25 takes charge of channel-coding and modulation on upper layer data to generate and transmit OFDM symbols over a radio channel and

demodulating and channel-decoding on OFDM symbols received over the radio channel to deliver the decoded data to the upper layers.

[479] FIG. 2e illustrates a signal flow diagram of a procedure for transitioning a UE from an RRC connected mode to an RRC idle mode based on connection release triggered by a base station and transitioning the UE from the RRC idle mode to the RRC connected mode based on connection establishment triggered by the UE according to an embodiment of the disclosure.

[480] In reference to FIG. 2e, if there is no data transmission/reception to/from the UE 2e-90 in the RRC connected mode for any reason or during a predetermined period, the base station 2e-91 may transmit an RRCConnectionRelease message to the UE 2e-90 at step 2e-01 to transition the UE 2e-90 to an RRC idle mode. If data to be transmitted are produced at the UE 2e-90 with no currently established connection (hereinafter, referred to as idle mode UE), the UE 2e-90 performs an RRC connection establishment procedure with the base station 2e-91.

[481] The UE 2e-90 acquires uplink transmission synchronization with the base station 2e-91 through a random access procedure and transmits an RRCConnectionRequest message to the base station 2e-91 at step 2e-05. The RRCConnectionRequest message may include an identifier of the UE 2e-90 and a connection establishment cause (establishmentCause).

[482] The base station 2e-91 transmits an RRCConnectionSetup message to the 2e-90 at step 2e-10 for RRC connection setup.

[483] The RRCConnectionSetup message includes RRC connection configuration information. The RRCConnectionSetup message may also include a UE identifier for use in identifying the UE 2e-90 connected to the base station 2e-91. The RRCConnectionSetup message may also include a list of identifiers of other UEs that are currently connected to the base station 2e-91. The list of the identifiers of other UEs that are currently connected to the base station 2e-91 may be periodically updated based on the system information broadcast by the base station 2e-91 in order for the UEs located within coverage of the base station 2e-91 to identify other UEs available for communication. When a wireless device are installed in a factory, the identifiers of other wireless devices available for communication may preset. The UE identifier may be a cell radio network temporary identifier (C-RNTI), part of the C-RNTI, or part of a NAS layer identifier (e.g., globally unique temporary identifier (GUTI)).

[484] An RRC connection may be referred to as signaling radio bearer and used for communicating RRC messages as control messages between the UE 23-90 and the base station 2e-91. After establishing the RRC connection, the UE 2e-90 transmits an RRCConnectionSetupComplete message to the base station 2e-91 at step 2e-15. The RRCConnectionSetupComplete message includes a control message called SERVICE

REQUEST for requesting to an MME 2e-92 for establishing a bearer for a certain service. At step 2e-20, the base station 2e-91 transmits the SERVICE REQUEST message included in the RRCConnectionSetupComplete message to the MME 2e-92, and the MME 2e-92 determines whether provide the service requested by the UE 2e-90.

[485] If it is determined to provide the service requested by the UE 2e-90, the MME 2e-92 transmit an INITIAL CONTEXT SETUP REQUEST message to the base station 2e-91 at step 2e-25. The this message includes quality of service (QoS) information to be applied in configuring a DRB and security information (e.g., Security Key and Security Algorithm) to be applied to the DRB.

[486] For security configuration, the base station 2e-91 transmits a SecurityModeCommand message to the UE 2e-90 at step 2e-30, and the UE 2e-90 transmits a SecurityModeComplete message to the base station 2e-91 at step 2e-35. After completing security configuration, the base station 2e-91 transmits an RRCConnectionReconfiguration message to the UE 2e-90 at step 2e-40.

[487] The RRCConnectionReconfiguration message may include UE identifier for use in identifying the UE 2e-90 within coverage of the base station 2e-91. This message may also include a list of identifiers of other UEs that are currently connected to the base station 2e-91. The list of the identifiers of other UEs that are currently connected to the base station 2e-91 may be periodically updated based on the system information broadcast by the base station 2e-91 in order for the UEs located within coverage of the base station 2e-91 to identify other UEs available for communication. When a wireless device are installed in a factory, the identifiers of other wireless devices available for communication may preset. The UE identifier may be a cell radio network temporary identifier (C-RNTI), part of the C-RNTI, or part of a NAS layer identifier (e.g., globally unique temporary identifier (GUTI)).

[488] The RRCConnectionReconfiguration message include DRB configuration information for processing user data, and the UE 2e-90 configures a DRB based on this configuration information and transmits an RRCConnectionReconfigurationComplete message to the base station 2e-91 at step 2e-45. After completing DRB configuration with the UE 2e-90, the base station 2e-91 transmits an INITIAL CONTEXT SETUP COMPLETE message to the MME 2e-92 at step 2e-50; upon receipt of the INITIAL CONTEXT SETUP COMPLETE message, the MME 2e-92 configures a S1 bearer with an S-GW 2e-93 by transmitting an S1 BEARER SETUP message to the S-GW 2e-93 at step 2e-55 and receiving an S1 BEARER SETUP RESPONSE message from the S-GW 2e-93 at step 2e-60. The S1 bearer is a connection for data transfer between the S-GW 2e-93 and the base station 2e-91 and mapped to the DRB 1 one to one. After completing the above procedure, the UE 2e-90 performs data communication via base

station 2e-91 and S-GW 2e-93 at steps 2e-65 and 2e-70. This typical data communication procedure consists of three phases: RRC connection configuration, security configuration, and DRB configuration. The base station 2e-91 may transmit an RRCConnectionReconfiguration message to the UE 2e-90 at step 2e-75 for updating, adding, or modifying the configuration.

[489] Hereinafter, a description is made of the low latency data communication procedure between wireless devices.

[490] FIG. 2f illustrates a signal flow diagram of a procedure for establishing a point-to-point link between wireless devices for data communication according to an embodiment of the disclosure. The one-to-one link denotes a link established for direct data communication between the wireless devices without intervention of the base station.

[491] The proposed procedure of configuring a point-to-point communication link between wireless devices may be divided into four steps: wireless device discovery, inter-device point-to-point wireless link or direct link assessment and measurement, inter-device direct wireless link establishment, and data communication through the inter-device direct link; the procedure is characterized by one or more of the following:

[492] 1. A gNB 2f-03 may share and manage UE identifiers of wireless devices within its coverage for supporting wireless data communication.

[493] 2. The gNB 2f-03 may configure the wireless devices within its coverage for supporting wireless data communication to always remain in an RRC connected mode or an RRC deactivated mode.

[494] 3. A wireless device transmits a transmission resource request message including an identifier of a destination device or a source device to the gNB 2f-03 to request for allocation of transmission resources for point-to-point communication.

[495] 4. The gNB 2f-03, upon being requested by the wireless device to allocate transmission resources for point-to-point communication, performs a procedure for discovering the destination wireless device (e.g., transmitting paging message) using the identifier of the destination wireless device. If the gNB 2f-03 fails to discover the destination wireless device or if the destination wireless device is not located within the coverage of the gNB 2f-03, the gNB 2f-03 allocates uplink transmission resources to the source wireless device and relays data between the source and destination wireless devices.

[496] 5. The gNB 2f-03 may allocate part of normal uplink transmission resources of the UE as transmission resources for point-to-point communication.

[497] 6. The gNB 2f-03, when allocating transmission resources for point-to-point communication to wireless devices, may inform the wireless devices of a source wireless device identifier or a destination wireless device identifier, send frequency con-

figuration information for point-to-point wireless link to the wireless devices, and instruct the wireless devices to perform frequency measurement or transmit a reference signal.

[498] 7. The wireless devices allocated the transmission resources for point-to-point communication performs frequency measurement on point-to-point wireless links for point-to-point communication and report frequency measurement results to the gNB 2f-30.

[499] 8. The gNB 2f-03 may receive the frequency measurement results from the source and destination wireless devices and instruct the source wireless device to perform data transmission based on the frequency measurement results using a newly defined L1 signal (e.g., DCI) or L2 signal (e.g., MAC CE) and the destination wireless device to perform data transmission based on the frequency measurement results using the newly defined L1 signal (e.g., DCI) or L2 signal (e.g., MAC CE).

[500] 9. The wireless device that is instructed to perform data transmission through the newly defined L1 signal (e.g., DCI) or L2 signal (e.g., MAC CE) starts data transmission.

[501] The proposed procedure for establishing a point-to-point wireless link between wireless devices is described in more detail hereinafter.

[502] The gNB 2f-03 may share and manage UE identifiers of wireless devices within its coverage for supporting wireless data communication. The gNB 2f-03 may configure the wireless devices 2f-01 or 2f-03 within its coverage for supporting wireless data communication to always remain in an RRC connected mode or an RRC deactivated mode to maintain low transmission latency.

[503] At step 2f-05, the wireless device 2f-01 may transmit a transmission resource request message including an identifier of a destination device 2f-02 or the source device 2f-01 to the gNB 2f-03 to request for allocation of transmission resources for point-to-point communication. The point-to-point transmission resource request message may include QoS requirements. For example, the resource request message being transmitted from the wireless device 2f-01 to the 2f-03 may include an average packet size, a transmission bit rate, a transmission delay requirement, a reliability, and an error rate.

[504] Upon being requested by the (source) wireless device 2f-01 to allocate transmission resources, the 2f-03 may perform, at step 2f-10, a procedure for discovering the destination wireless device 2f-02 (e.g., transmitting paging message) using the identifier of the destination wireless device 2f-02. If the gNB 2f-03 fails to discover the destination wireless device 2f-02 or if the destination wireless device 2f-02 is not located within the coverage of the gNB 2f-03, the gNB 2f-03 allocates uplink transmission resources to the source wireless device 2f-01 and relays data in such a way of receiving the data from the source wireless device 2f-01 and transmit the data to a network. The

paging message may include the identifier of the source wireless device 2f-01 or the destination wireless device 2f-02.

[505] If the destination wireless device 2f-02 receives the paging message, it establishes a connection with the gNB 2f-03 at step 2f-15. Then, the gNB 2f-03 may transmit a point-to-point response message to the source wireless device 2f-01 at step 2f-20, in response to the request for allocation of transmission resources for point-to-point communication, and a point-to-point configuration message to the destination wireless device 2f-02 at step 2f-25. The gNB 2f-03 may allocate part of normal uplink transmission resources of the UE as transmission resources for point-to-point communication. The allocated transmission resources may be transmission resources being allocated repetitively at a predetermined interval. In this case, once the transmission resources are configured, the wireless devices 2f-01 and 2f-02 may perform point-to-point communication continuously with the transmission resources without intervention of the gNB 2f-03. Such transmission resources may be allocated via system information broadcasted by the gNB 2f-03 rather than a dedicated signaling, and the gNB 2f-03 may inform the wireless device 2f-01 and 2f-02 of the resources for use in point-to-point communication among the transmission resources indicated in the system information. If the wireless device 2f-01 and 2f-02 is allocated transmission resources by the gNB 2f-03 via both the system information and dedicated signaling, it may prioritize the transmission resources allocated by the gNB 2f-03 via the dedicated signaling. When allocating transmission resources for point-to-point communication to wireless devices, the gNB 2f-03 may inform the wireless devices 2f-01 and 2f-02 of the identifiers of the source and destination wireless devices 2f-01 and 2f-02, send frequency configuration information for point-to-point wireless link to the wireless devices, and instruct the wireless devices to perform frequency measurement or transmit a reference signal.

[506] The transmission resources for point-to-point communication may include time resources, frequency resources, code resources, the identifier of the source wireless device 2f-01 or the identifier of the destination wireless device 2f-02, modulation or demodulation coding information (MCS), a transport block (TB) size, an identifier for activating the wireless information (e.g., RNTI).

[507] The source and destination wireless devices 2f-01 and 2f-02 that have been allocated the transmission resources for point-to-point communication may transmit a reference signal on the transmission resources, perform frequency measurement on the point-to-point wireless link, at step 2f-30, for point-to-point communication, and report frequency measurement results to the gNB 2f-03 at steps 2f-35 and 2f-40.

[508] Upon receipt of the frequency measurement results from the source and destination wireless devices 2f-01 and 2f-02, the gNB 2f-03 may instruct, at step 2f-45, the source

wireless device 2f-01 to perform data transmission based on the frequency measurement results using a newly defined L1 signal (e.g., DCI) or L2 signal (e.g., MAC CE) and, at step 2f-50, the destination wireless device 2f-02 to perform data transmission based on the frequency measurement results using the newly defined L1 signal (e.g., DCI) or L2 signal (e.g., MAC CE).

[509] Upon being instructed by the gNB 2f-03, via the newly defined L1 signal (e.g., DCI) or L2 signal (e.g., MAC CE), to perform data transmission, the source wireless device 2f-01 or the destination wireless device 2f-02 may perform data transmission, at step 2f-55, on the transmission resources allocated for point-to-point communication.

[510] In the above procedure, the source and destination wireless devices 2f-01 and 2f-02 may perform reliability measurement on the data being transmitted/received or frequency measurement on the reference signal on the direct wireless link periodically to request to the gNB 2f-03, if the measurement result is equal to or less than a level predetermined or preconfigured for the configured point-to-point link, for update of the point-to-point link or a new point-to-point link as at step 2f-05. When perform reliability measurement on the data being transmitted/received, the source and destination wireless devices 2f-01 and 2f-02 may check sequence numbers of the data to identify a number, size, or amount of lost data to assess the quality of the direct wireless link.

[511] When requesting to the gNB 2f-03 for update of the point-to-point wireless link, the source wireless device 2f-01 or the destination wireless device 2f-02 may report the reliability, transmission latency, or error assessed or experienced on the currently configured direct wireless link.

[512] FIG. 2g illustrates a flowchart of an operation of a wireless device for configuring a point-to-point direct wireless link according to an embodiment of the disclosure.

[513] At step 2g-05, the source wireless device may transmit a direct wireless link resource request message including an identifier of a destination wireless device or an identifier of the source wireless device to a base station to request for allocation of transmission resources for point-to-point communication. Upon being requested by the source wireless device to allocate transmission resources for point-to-point communication, the base station may perform a procedure for discovering the destination wireless device (e.g., transmitting a paging message) with the identifier of the destination wireless device. If the destination wireless device receives the paging message, it establishes a connection with the base station. Then the base station may transmit a response message indicating the transmission resources for point-to-point communication to the source wireless device in reply to the direct wireless link resource request message and a point-to-point configuration message to the destination wireless device to allocate transmission resources; the wireless devices receive the response

message at step 2g-10. When allocating the transmission resources for point-to-point communication to the wireless devices, the base station may notify the wireless devices of the identifier of the source or destination wireless device, configure a frequency of the point-to-point link to the wireless devices, instruct the wireless devices to perform frequency measurement, and/or configure and instruct the wireless devices to transmit reference signals.

[514] After being allocated the transmission resources for point-to-pit communication, the source and destination wireless devices may transmit reference signals on the transmission resources, perform frequency measurement on a point-to-point link for point-to-point communication, and report frequency measurement results to the base station at step 2g-15.

[515] Upon receipt of the frequency measurement results from the source and destination wireless devices, the base station may instruct the source wireless device to perform data transmission based on the frequency measurement results using a newly defined L1 signal (e.g., DCI with an identifier) or L2 signal (e.g., MAC CE) and the destination wireless device to perform data transmission based on the frequency measurement results using the newly defined L1 signal (e.g., DCI) or L2 signal (e.g., MAC CE); the wireless devices activate a direct link and receive the data transmission instruction at step 2g-20.

[516] Upon receipt of the instruction for instructing to perform data transmission through the newly defined L1 signal (e.g., DCI with an identifier) or L2 signal (e.g., MAC CE), the source or destination wireless device may perform data transmission on the transmission resources at step 2g-25.

[517] FIG. 2h illustrates a diagram of a configuration of a UE or a wireless node according to an embodiment of the disclosure.

[518] In reference to FIG. 2h, the UE includes a radio frequency (RF) processor 2h-10, a baseband processor 2h-20, a storage unit 2h-30, and a controller 2h-40.

[519] The RF processor 2h-10 has a function for transmitting/receiving a signal over a radio channel such as band conversion and amplification of the signal. That is, the RF processing unit 2h-10 up-converts a baseband signal from the baseband processor 2h-20 to an RF band signal and transmits the RF signal via an antenna and down-converts the RF signal received via the antenna to a baseband signal. For example, the RF processor 2h-10 may include a transmission filter, a reception filter, an amplifier, a mixer, an oscillator, a digital-to-analog converter (DAC), and an analog-to-digital converter (ADC). Although one antenna is depicted in the drawing, the UE may be provided with a plurality of antennas. The RF processor 2h-10 may also include a plurality of RF chains. The RF processor 2h-10 may perform beamforming. For beamforming, the RF processor 2h-10 may adjust the phase and size of a signal to be

transmitted/received by means of the antennas or antenna elements. The RF processor 2h-10 may be configured to support a MIMO scheme with which the UE can receive multiple layers simultaneously. The RF processor 2h-10 may configure the plurality of antennas or antenna elements appropriately, under the control of the controller 2h-40, to perform beam sweeping and adjust the beam direction and beam width to achieve an alignment of the reception and transmission beam.

[520] The baseband processor 2h-20 has a baseband signal-bit string conversion function according to a physical layer standard of the system. For example, in a data transmission mode, the baseband processor 2h-20 performs encoding and modulation on the transmission bit string to generate complex symbols. In a data reception mode, the baseband processor 2h-20 performs demodulation and decoding on the baseband signal from the RF processor 2h-10 to recover the transmitted bit string. In the case of using an OFDM scheme for data transmission, the baseband processor 2h-20 performs encoding and modulation on the transmission bit string to generate complex symbols, maps the complex symbols to subcarriers, performs inverse fast Fourier transform (IFFT) on the symbols, and inserts a cyclic prefix (CP) into the symbols to generate OFDM symbols. In the data reception mode, the baseband processor 2h-20 splits the baseband signal from the RF processor 2h-10 into OFDM symbols, perform fast Fourier transform (FFT) on the OFDM symbols to recover the signals mapped to the subcarriers, and performs demodulation and decoding on the signals to recover the transmitted bit string.

[521] The baseband processor 2h-20 and the RF processor 2h-10 process the transmission and reception signals as described above. Accordingly, the baseband processor 2h-20 and the RF processor 2h-10 may be referred to as a transmitter, a receiver, a transceiver, or a communication unit/circuit. At least one of the baseband processor 2h-20 and the RF processor 2h-10 may include a plurality of communication modules for supporting different radio access technologies. At least one of the baseband processor 2h-20 and the RF processor 2h-10 may also include multiple communication modules for processing the signals in different frequency bands. For example, the different radio access technologies may include a wireless local area network (WLAN) (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.11) and a cellular network (e.g., LTE). The different frequency bands may include a super high frequency (SHF) band (e.g., 2.2 GHz and 2 GHz bands) and an mmWave band (e.g., 60 GHz).

[522] The storage unit 2h-30 stores data such as basic programs for operation of the UE, application programs, and setting information. The storage unit 2h-30 provides the stored information in response to a request from the controller 2h-40.

[523] The controller 2h-40 controls overall operations of the UE. For example, the

controller 2h-40 controls the baseband processor 2h-20 and the RF processor 2h-10 for transmitting and receiving signals. The controller 2h-40 writes and reads data to and from the storage unit 2h-40. For this purpose, the controller 2h-40 may include at least one processor. For example, the controller 2h-40 may include a communication processor (CP) for controlling communications and an application processor (AP) for controlling higher layer programs such as applications. The controller 2h-40 may be electrically connected to the transceiver.

[524] FIG. 2i illustrates a block diagram of a configuration of a base station or a wireless node in a wireless communication system according to an embodiment of the disclosure.

[525] In reference to FIG. 2i, the base station includes an RF processor 2i-10, a baseband processor 2i-20, a backhaul communication unit 2i-30, a storage unit 2i-40, and a controller 2i-50.

[526] The RF processor 2i-10 has a function for transmitting/receiving a signal over a radio channel such as band conversion and amplification of the signal. That is, the RF processing unit 2i-10 up-converts a baseband signal from the baseband processor 2i-20 to an RF band signal and transmits the RF signal via an antenna and down-converts the RF signal received via the antenna to a baseband signal. For example, the RF processor 2i-10 may include a transmission filter, a reception filter, an amplifier, a mixer, an oscillator, a DAC, and an ADC. Although one antenna is depicted in the drawing, the base station may be provided with a plurality of antennas. The RF processor 2i-10 may also include a plurality of RF chains. The RF processor 1i-10 may perform beamforming. For beamforming, the RF processor 2i-10 may adjust the phase and size of a signal to be transmitted/received by means of the antennas or antenna elements. The RF processor 2i-10 may be configured to transmit one or more layers for a downlink MIMO operation.

[527] The baseband processor 2i-20 has a baseband signal-bit string conversion function according to a physical layer standard of the system. For example, in a data transmission mode, the baseband processor 2i-20 performs encoding and modulation on the transmission bit string to generate complex symbols. In a data reception mode, the baseband processor 2i-20 performs demodulation and decoding on the baseband signal from the RF processor 2i-10 to recover the transmitted bit string. In the case of using an OFDM scheme for data transmission, the baseband processor 2i-20 performs encoding and modulation on the transmission bit string to generate complex symbols, maps the complex symbols to subcarriers, performs inverse fast Fourier transform (IFFT) on the symbols, and inserts a cyclic prefix (CP) into the symbols to generate OFDM symbols. In the data reception mode, the baseband processor 2i-20 splits the baseband signal from the RF processor 2i-10 into OFDM symbols, performs fast

Fourier transform (FFT) on the OFDM symbols to recover the signals mapped to the subcarriers, and performs demodulation and decoding on the signals to recover the transmitted bit string. The baseband processor 2i-20 and the RF processor 2i-10 process the transmission and reception signals as described above. Accordingly, the baseband processor 2i-20 and the RF processor 2i-10 may be referred to as a transmitter, a receiver, a transceiver, or a communication unit.

[528] The communication unit 2i-30 provides an interface for communication with other nodes in the network.

[529] The storage unit 2i-40 stores data such as basic programs for operation of the base station, application programs, and setting information. The storage unit 2i-40 may also store the information on the bearers established for UEs and measurement results reported by the connected UEs. The storage unit 2i-40 may also store the information for use by a UE in determining whether to enable or disable multi-connectivity. The storage unit 2i-40 may provide the stored data in reference to a request from the controller 2i-50.

[530] The controller 2i-50 controls overall operations of the base station. For example, the controller 2i-50 controls the baseband processor 2i-20, the RF processor 2i-10, and the backhaul communication unit 2i-30 for transmitting and receiving signals. The controller 2i-50 writes and reads data to and from the storage unit 2i-40. For this purpose, the controller 2i-50 may include at least one processor. The controller may be electrically connected to the transceiver.

[531] Although the description has been made with reference to particular embodiments, the disclosure can be implemented with various modifications without departing from the scope of the disclosure. Thus, the disclosure is not limited to the particular embodiments disclosed but will include the following claims and their equivalents.

[532] Although the present disclosure has been described with various embodiments, various changes and modifications may be suggested to one skilled in the art. It is intended that the present disclosure encompass such changes and modifications as fall within the scope of the appended claims.

# Claims

[Claim 1] A method of a terminal in a wireless communication system, the method comprising:
receiving, from a base station, a first message including a first list associated with count values of the base station, the first list including at least one bearer identity, at least one first downlink count value of the base station associated to each bearer, and at least one first uplink count value of the base station associated to each bearer;
determining whether a first bearer is configured with a new radio (NR) packet data convergence protocol (PDCP);
in case that the first bearer is configured with the NR PDCP, and at least one of a second downlink count value of the terminal associated to the first bearer is different from the first downlink count value associated to the first bearer or a second uplink count value of the terminal associated to the first bearer is different from the first uplink count value associated to the first bearer, generating a second list associated with count values of the terminal including a first bearer identity of the first bearer, the second downlink count value of the terminal associated to the first bearer, and the second uplink count value of the terminal associated to the first bearer; and
transmitting, to the base station, a second message including the second list as a response to the first message,
wherein the second downlink count value of the terminal associated to the first bearer is a count value of a next PDCP service data unit (SDU) expected to be received - 1, and the second uplink count value of the terminal associated to the first bearer is a count value of a next PDCP SDU to be transmitted - 1.

[Claim 2] The method of claim 1, wherein the generating the second list further comprises:
in case that the first bearer is not configured with the NR PDCP, and at least one of a third downlink count value of the terminal associated to the first bearer is different from the first downlink count value associated to the first bearer or a third uplink count value of the terminal associated to the first bearer is different from the first uplink count value associated to the first bearer, generating the second list including the first bearer identity, the third downlink count value of the terminal associated to the first bearer, and the third uplink count value of the

terminal associated to the first bearer.

[Claim 3] The method of claim 1, further comprising:

in case that the first bearer is a uni-directional bearer, determining that at least one of the second downlink count value of the terminal associated to the first bearer or the second uplink count value of the terminal associated to the first bearer is to be 0 for an unused direction, and

in case that a third bearer included in the first list is not established on the terminal, generating the second list including a third identity of the third bearer, a fifth downlink count value of the terminal associated to the third bearer, and a fifth uplink count value of the terminal associated to the third bearer with most significant bits set identical to a first downlink count value associated to the third bearer and a first uplink count value associated to the third bearer and least significant bits set to 0.

[Claim 4] The method of claim 1, wherein the generating the second list further comprises:

in case that a second bearer identity of a second bearer established on the terminal is not included in the first list, generating the second list including the second bearer identity of the second bearer, a fourth downlink count value of the terminal associated to the second bearer, and a fourth uplink count value of the terminal associated to the second bearer, and

wherein the fourth downlink count value of the terminal associated to the second bearer is a count value of a next PDCP SDU expected to be received - 1 and the fourth uplink count value of the terminal associated to the second bearer is a count value of a next PDCP SDU to be transmitted - 1.

[Claim 5] A method of a base station in a wireless communication system, the method comprising:

transmitting, to a terminal, a first message including a first list associated with count values of the base station, the first list including at least one bearer identity, at least one first downlink count value of the base station associated to each bearer, and at least one first uplink count value of the base station associated to each bearer; and

receiving, from the terminal, a second message including a second list associated with count values of the terminal including a first bearer identity of a first bearer, a second downlink count value of the terminal

associated to the first bearer, and a second uplink count value of the terminal associated to the first bearer, as a response to the first message, in case that the first bearer is configured with a new radio (NR) packet data convergence protocol (PDCP), and at least one of the second downlink count value of the terminal associated to the first bearer is different from the first downlink count value associated to the first bearer or the second uplink count value of the terminal associated to the first bearer is different from the first uplink count value associated to the first bearer,

wherein the second downlink count value of the terminal associated to the first bearer is a count value of a next PDCP service data unit (SDU) expected to be received - 1, and the second uplink count value of the terminal associated to the first bearer is a count value of a next PDCP SDU to be transmitted - 1.

[Claim 6] The method of claim 5,

wherein, in case that the first bearer is not configured with the NR PDCP, and at least one of a third downlink count value of the terminal associated to the first bearer is different from the first downlink count value associated to the first bearer or a third uplink count value of the terminal associated to the first bearer is different from the first uplink count value associated to the first bearer, the second list includes the first bearer identity, the third downlink count value of the terminal associated to the first bearer, and the third uplink count value of the terminal associated to the first bearer, and

wherein, in case that a third bearer included in the first list is not established on the terminal, the second list includes a third identity of the third bearer, a fifth downlink count value of the terminal associated to the third bearer, and a fifth uplink count value of the terminal associated to the third bearer with most significant bits set identical to a first downlink count value associated to the third bearer and a first uplink count value associated to the third bearer and least significant bits set to 0.

[Claim 7] The method of claim 5,

wherein, in case that the first bearer is a uni-directional bearer, at least one of the second downlink count value of the terminal associated to the first bearer or the second uplink count value of the terminal associated to the first bearer is to be 0 for an unused direction.

[Claim 8] The method of claim 5,

wherein, in case that a second bearer identity of a second bearer established on the terminal is not included in the first list, the second list includes the second bearer identity of the second bearer, a fourth downlink count value of the terminal associated to the second bearer, and a fourth uplink count value of the terminal associated to the second bearer, and

wherein the fourth downlink count value of the terminal associated to the second bearer is a count value of a next PDCP SDU expected to be received - 1 and the fourth uplink count value of the terminal associated to the second bearer is a count value of a next PDCP SDU to be transmitted - 1.

[Claim 9] A terminal in a wireless communication system, the terminal comprising:

a transceiver; and

a controller configured to:

control the transceiver to receive, from a base station, a first message including a first list associated with count values of the base station, the first list including at least one bearer identity, at least one first downlink count value of the base station associated to each bearer, and at least one first uplink count value of the base station associated to each bearer,

determine whether a first bearer is configured with a new radio (NR) packet data convergence protocol (PDCP),

in case that the first bearer is configured with the NR PDCP, and at least one of a second downlink count value of the terminal associated to the first bearer is different from the first downlink count value associated to the first bearer or a second uplink count value of the terminal associated to the first bearer is different from the first uplink count value associated to the first bearer, generate a second list associated with count values of the terminal including a first bearer identity of the first bearer, the second downlink count value of the terminal associated to the first bearer, and the second uplink count value of the terminal associated to the first bearer, and

control the transceiver to transmit, to the base station, a second message including the second list as a response to the first message,

wherein the second downlink count value of the terminal associated to the first bearer is a count value of a next PDCP service data unit (SDU) expected to be received - 1, and the second uplink count value of the

terminal associated to the first bearer is a count value of a next PDCP SDU to be transmitted - 1.

[Claim 10] The terminal of claim 9, wherein the controller is further configured to:
in case that the first bearer is not configured with the NR PDCP, and at least one of a third downlink count value of the terminal associated to the first bearer is different from the first downlink count value associated to the first bearer or a third uplink count value of the terminal associated to the first bearer is different from the first uplink count value associated to the first bearer, generate the second list including the first bearer identity, the third downlink count value of the terminal associated to the first bearer, and the third uplink count value of the terminal associated to the first bearer, and
in case that a third bearer included in the first list is not established on the terminal, generate the second list including a third identity of the third bearer, a fifth downlink count value of the terminal associated to the third bearer, and a fifth uplink count value of the terminal associated to the third bearer with most significant bits set identical to a first downlink count value associated to the third bearer and a first uplink count value associated to the third bearer and least significant bits set to 0.

[Claim 11] The terminal of claim 9, wherein the controller is further configured to:
in case that the first bearer is a uni-directional bearer, determine that at least one of the second downlink count value of the terminal associated to the first bearer or the second uplink count value of the terminal associated to the first bearer is to be 0 for an unused direction.

[Claim 12] The terminal of claim 9, wherein the controller is further configured to:
in case that a second bearer identity of a second bearer established on the terminal is not included in the first list, generate the second list including the second bearer identity of the second bearer, a fourth downlink count value of the terminal associated to the second bearer, and a fourth uplink count value of the terminal associated to the second bearer, and
wherein the fourth downlink count value of the terminal associated to the second bearer is a count value of a next PDCP SDU expected to be received - 1 and the fourth uplink count value of the terminal associated to the second bearer is a count value of a next PDCP SDU to be transmitted - 1.

[Claim 13] A base station in a wireless communication system, the base station

comprising:
a transceiver; and
a controller configured to:
control the transceiver to transmit, to a terminal, a first message including a first list associated with count values of the base station, the first list including at least one bearer identity, at least one first downlink count value of the base station associated to each bearer, and at least one first uplink count value of the base station associated to each bearer, and
control the transceiver to receive, from the terminal, a second message including a second list associated with count values of the terminal including a first bearer identity of a first bearer, a second downlink count value of the terminal associated to the first bearer, and a second uplink count value of the terminal associated to the first bearer, as a response to the first message, in case that the first bearer is configured with a new radio (NR) packet data convergence protocol (PDCP), and at least one of the second downlink count value of the terminal associated to the first bearer is different from the first downlink count value associated to the first bearer or the second uplink count value of the terminal associated to the first bearer is different from the first uplink count value associated to the first bearer,
wherein the second downlink count value of the terminal associated to the first bearer is a count value of a next PDCP service data unit (SDU) expected to be received - 1, and the second uplink count value of the terminal associated to the first bearer is a count value of a next PDCP SDU to be transmitted - 1.

[Claim 14] The base station of claim 13,
wherein, in case that the first bearer is not configured with the NR PDCP, and at least one of a third downlink count value of the terminal associated to the first bearer is different from the first downlink count value associated to the first bearer or a third uplink count value of the terminal associated to the first bearer is different from the first uplink count value associated to the first bearer, the second list includes the first bearer identity, the third downlink count value of the terminal associated to the first bearer, and the third uplink count value of the terminal associated to the first bearer, and
wherein, in case that a third bearer included in the first list is not established on the terminal, the second list includes a third identity of the

third bearer, a fifth downlink count value of the terminal associated to the third bearer, and a fifth uplink count value of the terminal associated to the third bearer with most significant bits set identical to a first downlink count value associated to the third bearer and a first uplink count value associated to the third bearer and least significant bits set to 0.

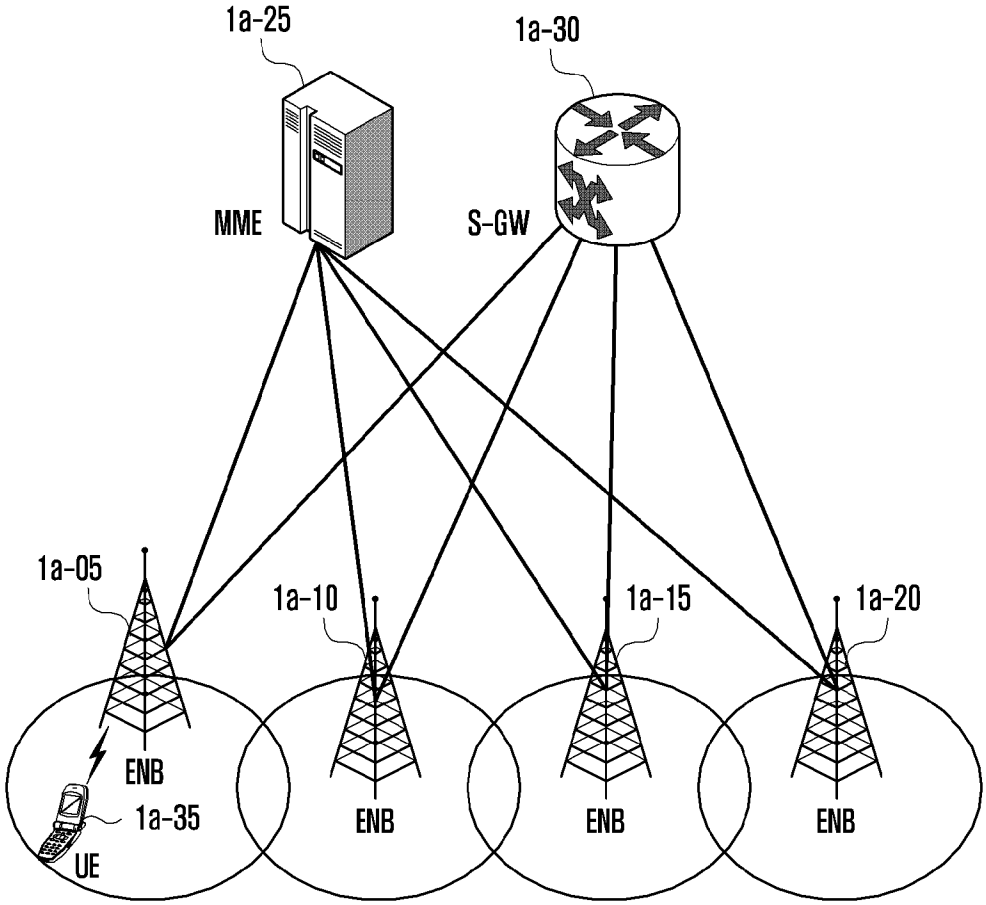
[Claim 15] The base station of claim 13,

wherein, in case that the first bearer is a uni-directional bearer, at least one of the second downlink count value of the terminal associated to the first bearer or the second uplink count value of the terminal associated to the first bearer is to be 0 for an unused direction,

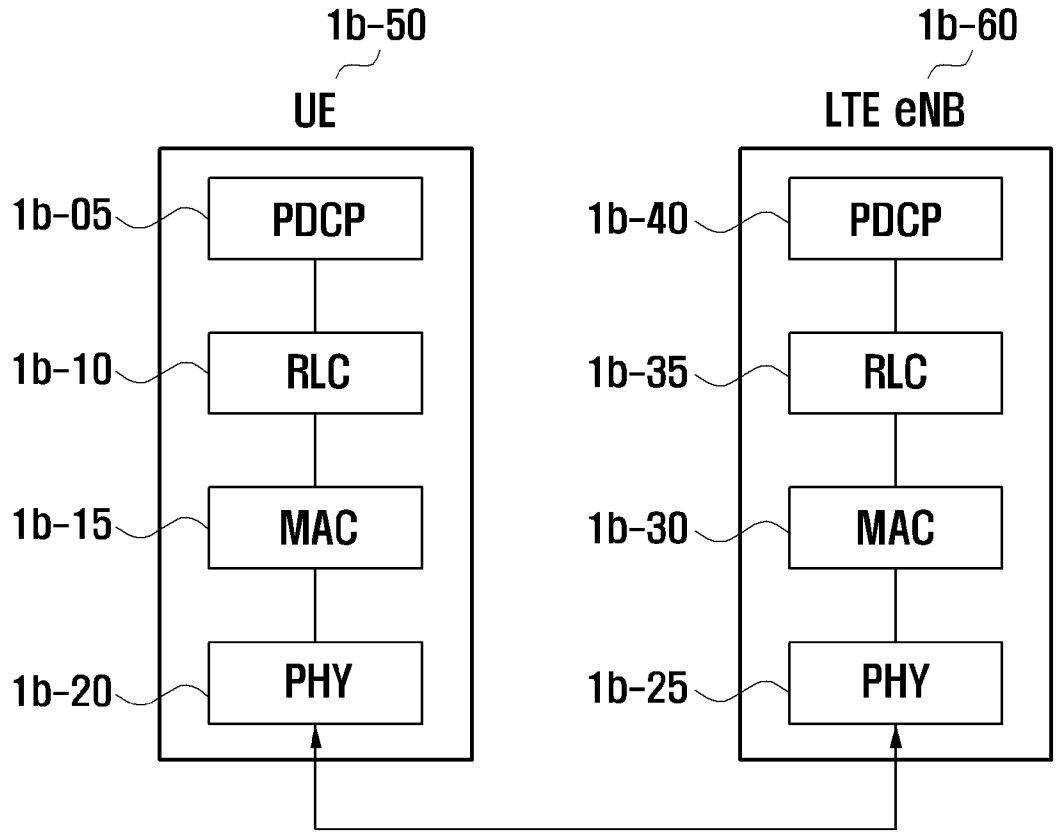
wherein, in case that a second bearer identity of a second bearer established on the terminal is not included in the first list, the second list includes the second bearer identity of the second bearer, a fourth downlink count value of the terminal associated to the second bearer, and a fourth uplink count value of the terminal associated to the second bearer, and

wherein the fourth downlink count value of the terminal associated to the second bearer is a count value of a next PDCP SDU expected to be received - 1 and the fourth uplink count value of the terminal associated to the second bearer is a count value of a next PDCP SDU to be transmitted - 1.

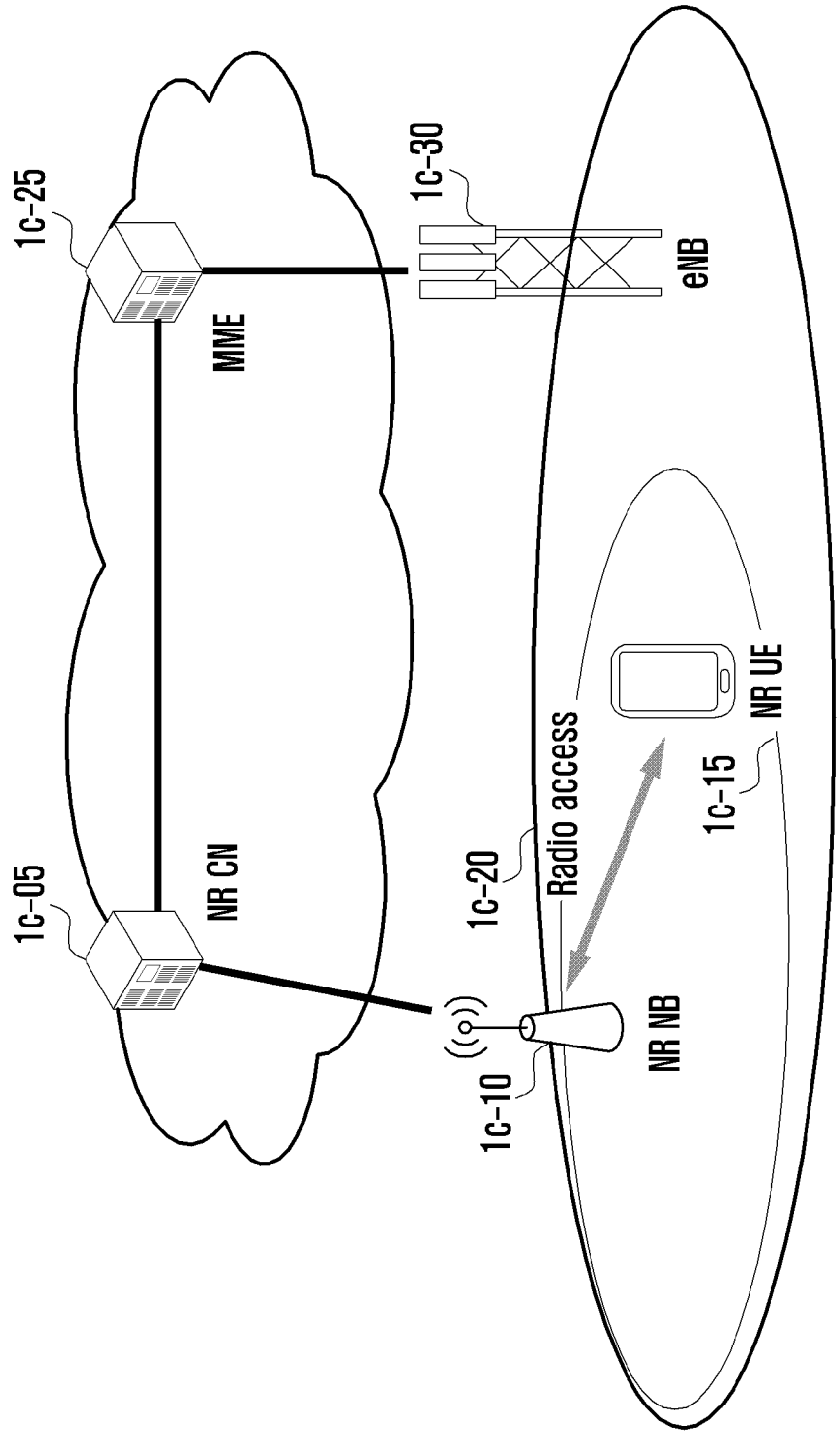
[Fig. 1a]


1a-25
1a-30
MME
S-GW
1a-05
1a-10
1a-15
1a-20
ENB
1a-35
UE
ENB
ENB
ENB

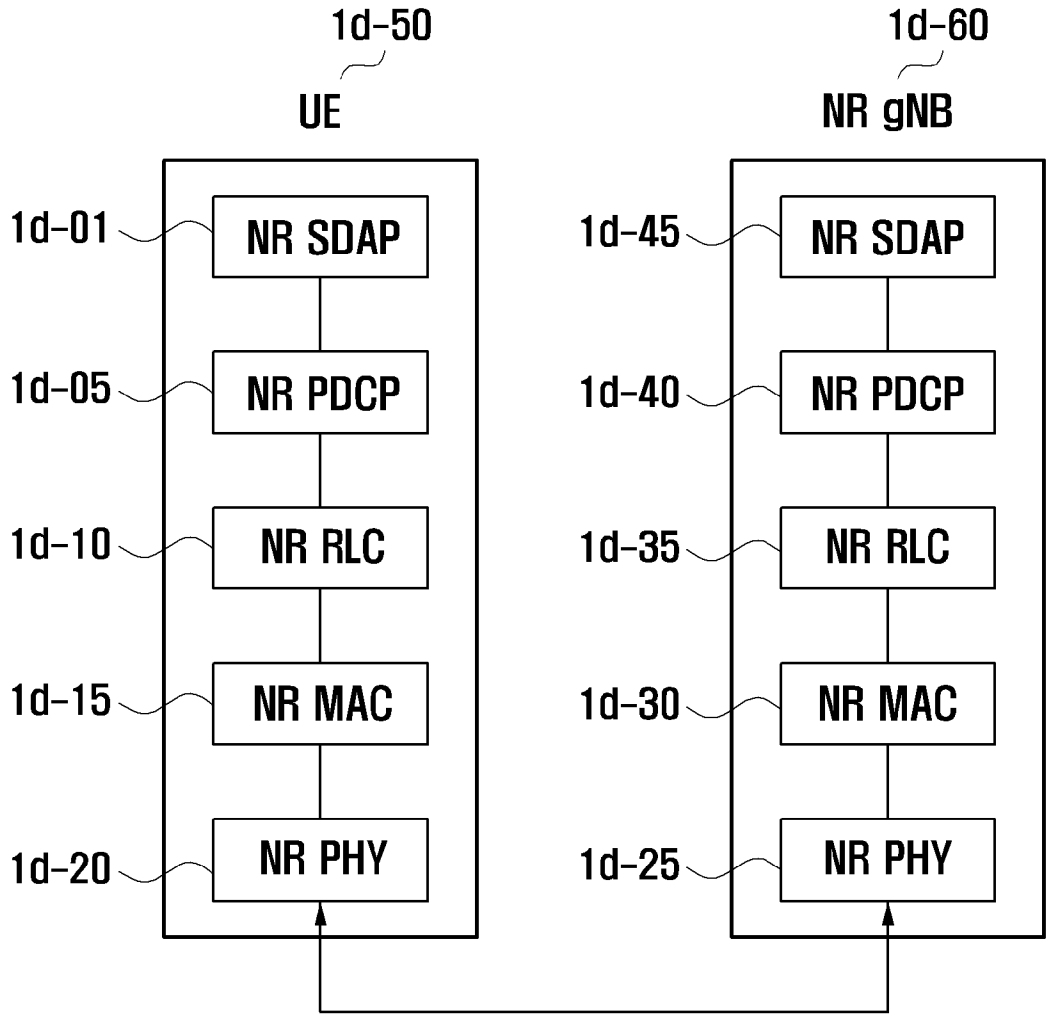
[Fig. 1b]


1b-50
UE
1b-60
LTE eNB
1b-05
PDCP
1b-40
PDCP
1b-10
RLC
1b-35
RLC
1b-15
MAC
1b-30
MAC
1b-20
PHY
1b-25
PHY

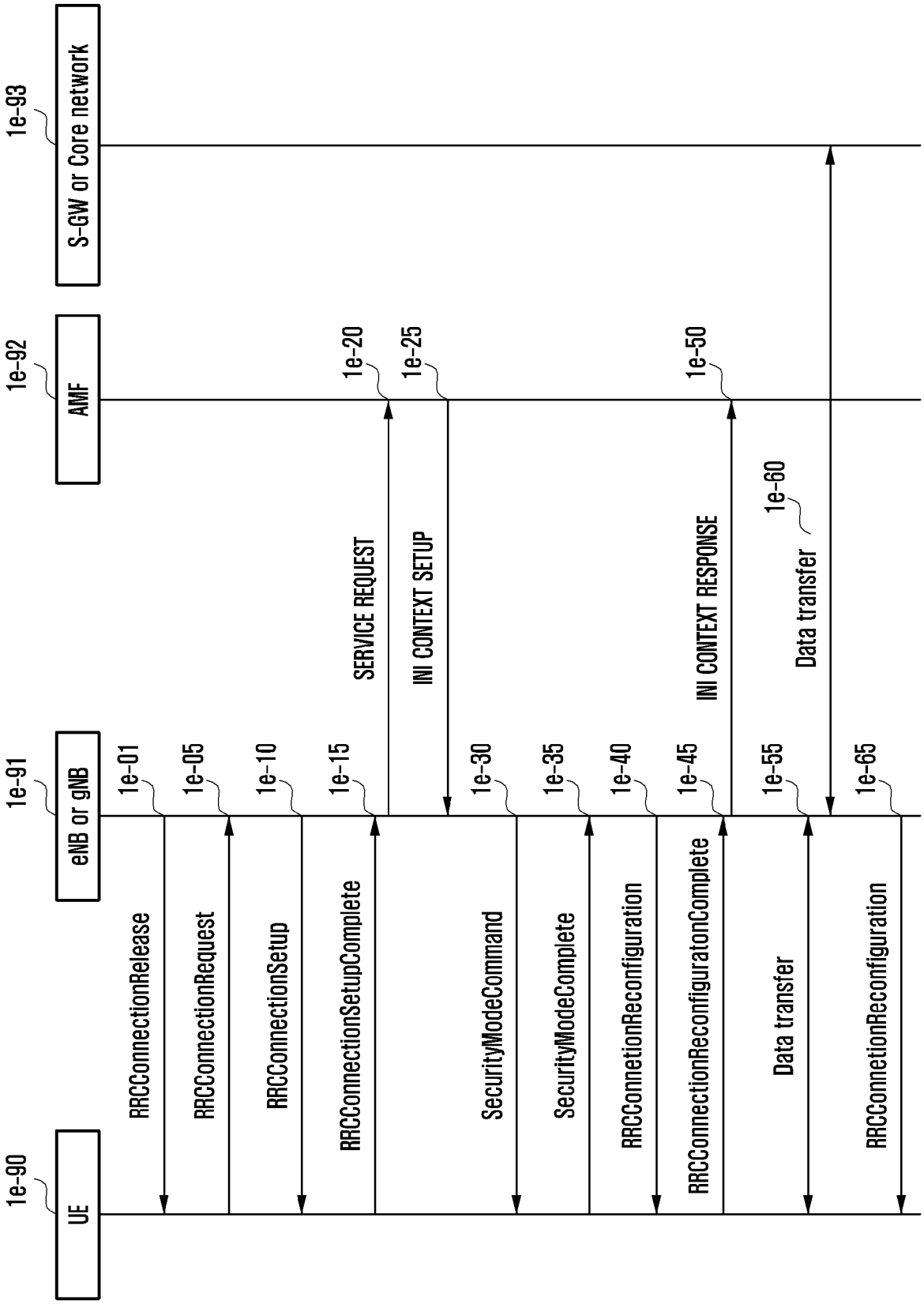
[Fig. 1c]


1c-25
MME
1c-30
eNB
NR CN
1c-05
1c-20
Radio access
1c-15
NR UE
NR NB
1c-10

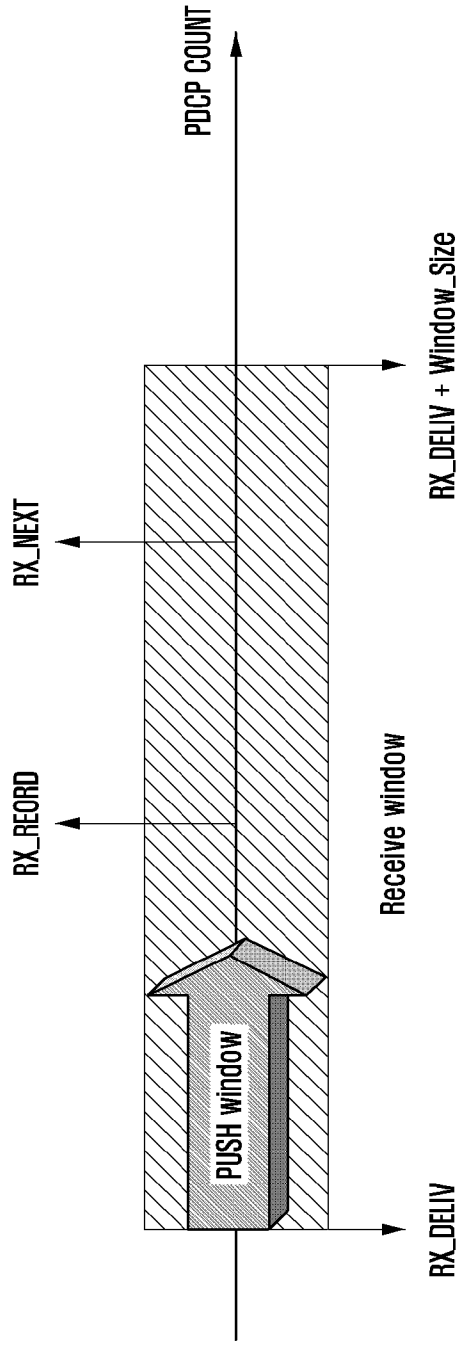
[Fig. 1d]


1d-50
UE
1d-60
NR gNB
1d-01
NR SDAP
1d-05
NR PDCP
1d-10
NR RLC
1d-15
NR MAC
1d-20
NR PHY
1d-45
NR SDAP
1d-40
NR PDCP
1d-35
NR RLC
1d-30
NR MAC
1d-25
NR PHY

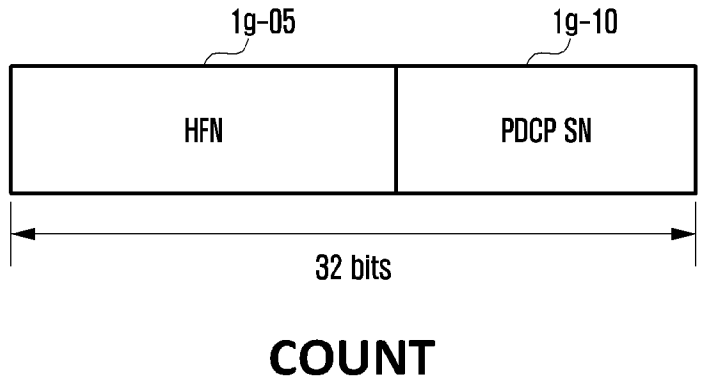
[Fig. 1e]


1e-90
UE
1e-91
eNB or gNB
1e-92
AMF
1e-93
S-GW or Core network
1e-01
RRCConnectionRelease
1e-05
RRCConnectionRequest
1e-10
RRCConnectionSetup
1e-15
RRCConnectionSetupComplete
1e-20
SERVICE REQUEST
1e-25
INI CONTEXT SETUP
1e-30
SecurityModeCommand
1e-35
SecurityModeComplete
1e-40
RRCConnetionReconfiguration
1e-45
RRCConnectionReconfiguratonComplete
1e-50
INI CONTEXT RESPONSE
1e-55
Data transfer
1e-60
Data transfer
1e-65
RRCConnetionReconfiguration

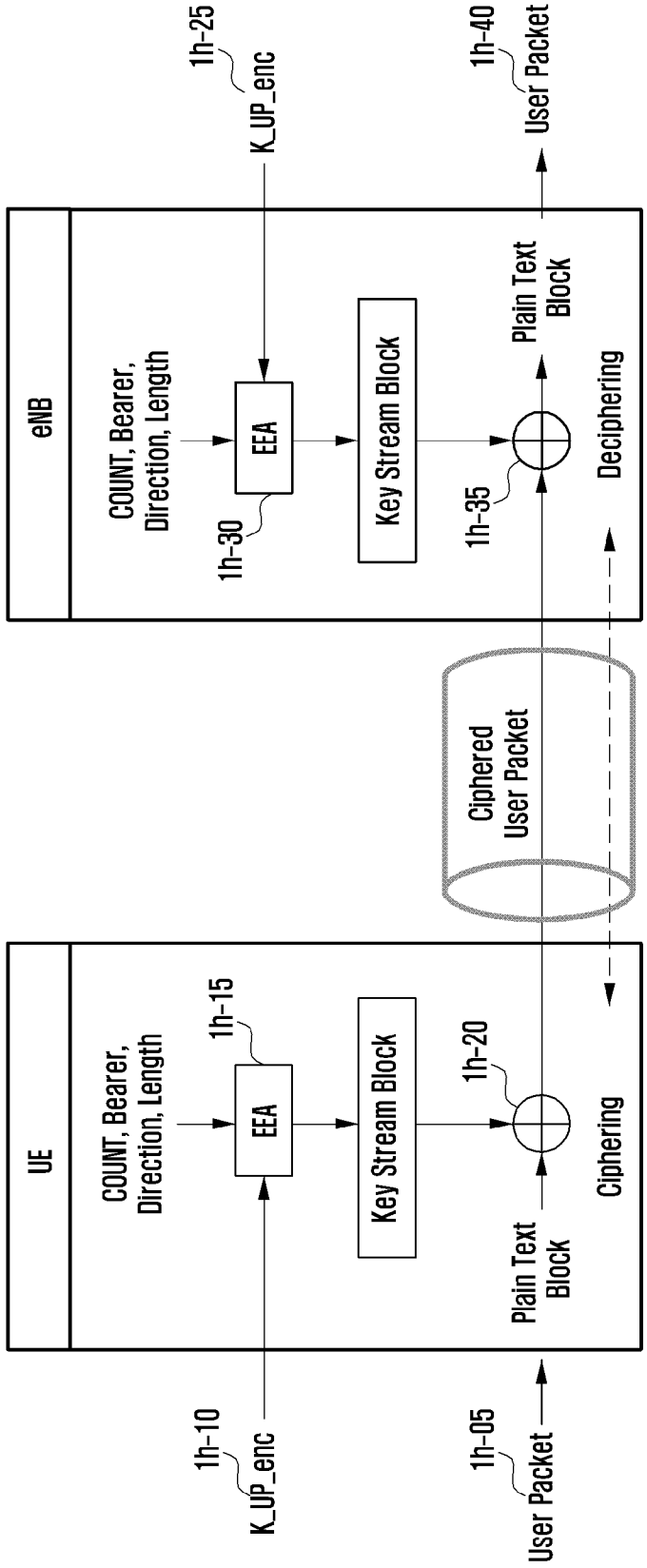
[Fig. 1f]


PDCP COUNT
RX_DELIV + Window_Size
RX_NEXT
RX_REORD
Receive window
PUSH window
RX_DELIV

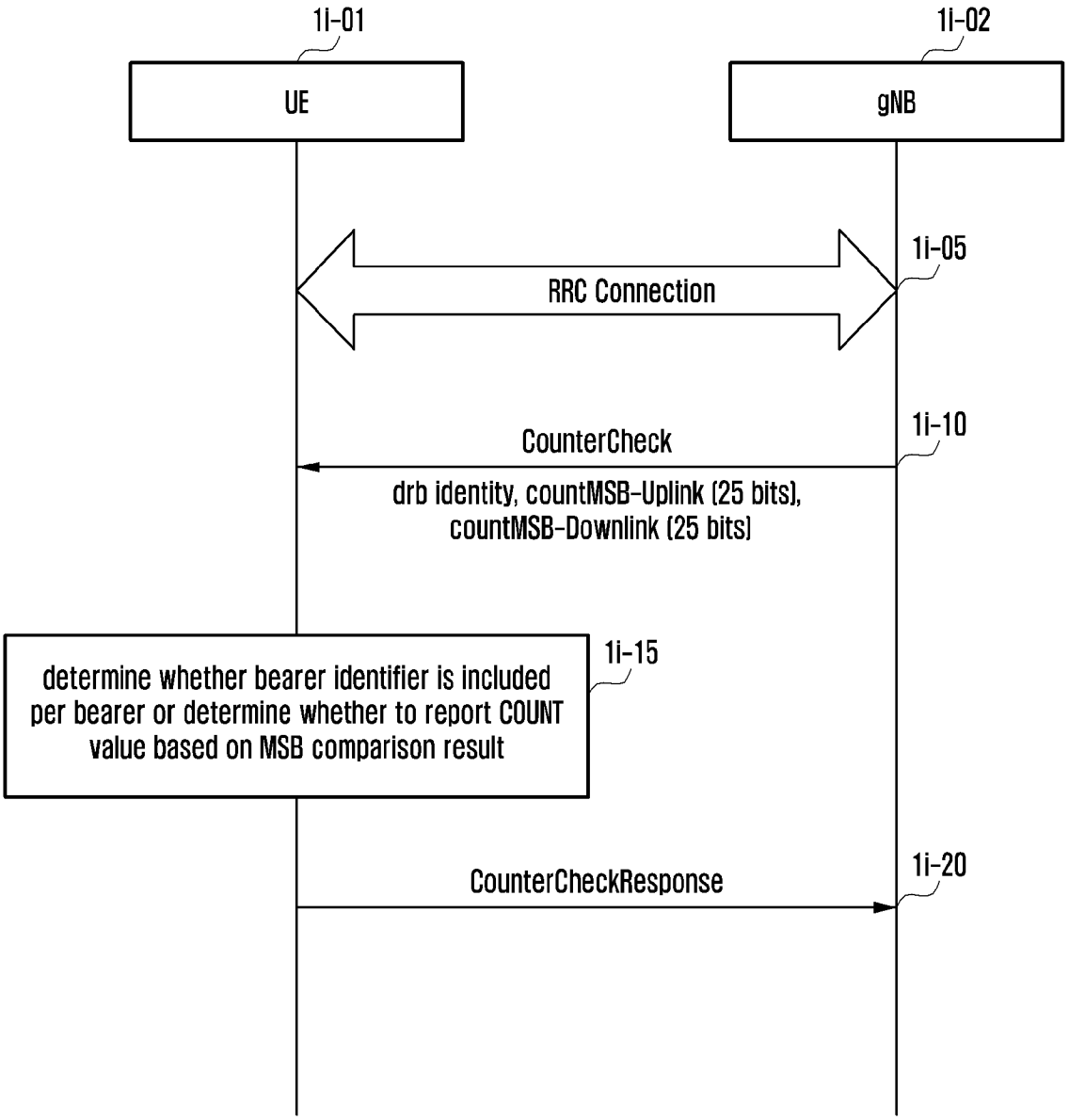
[Fig. 1g]


1g-05
1g-10
HFN
PDCP SN
32 bits
COUNT

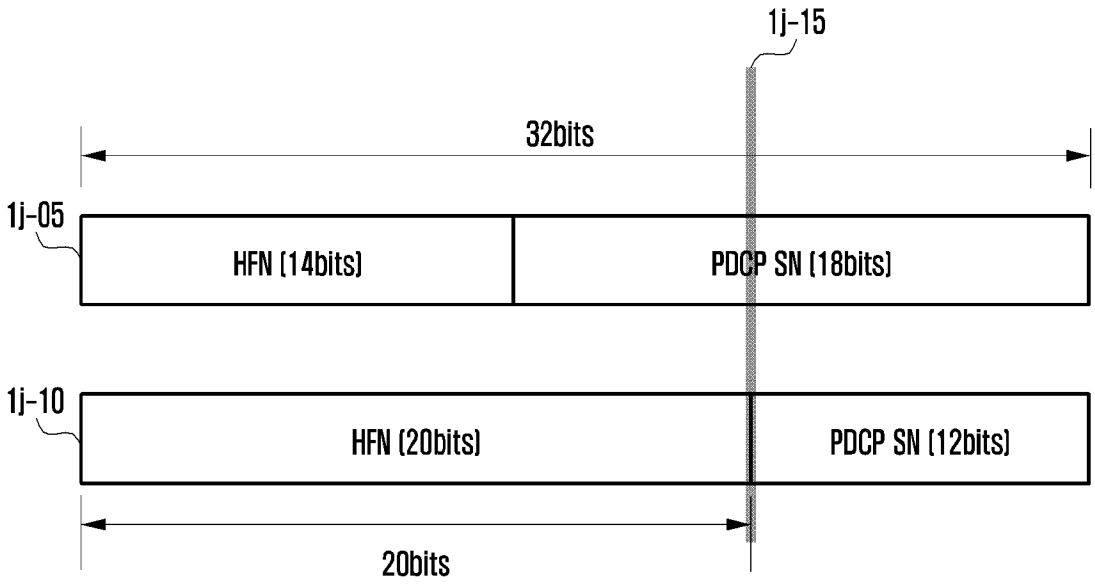
[Fig. 1h]


1h-25
K_UP_enc
1h-40
User Packet
eNB
COUNT, Bearer, Direction, Length
EEA
1h-30
Key Stream Block
Plain Text Block
1h-35
Deciphering
Ciphered User Packet
UE
COUNT, Bearer, Direction, Length
1h-15
EEA
Key Stream Block
1h-20
Plain Text Block
Ciphering
1h-10
K_UP_enc
1h-05
User Packet

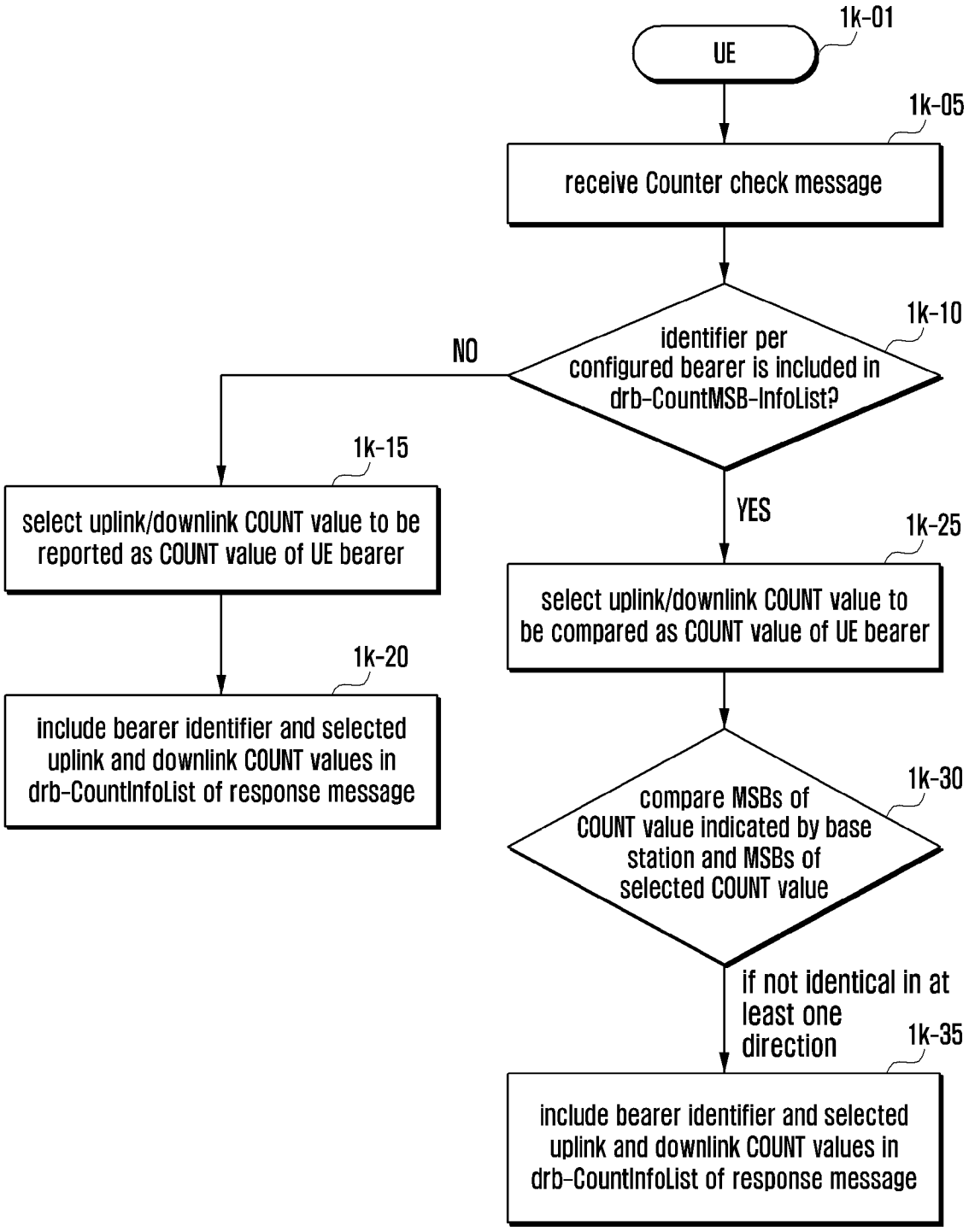
[Fig. 1i]


1i-01
UE
1i-02
gNB
RRC Connection
1i-05
CounterCheck
1i-10
drb identity, countMSB-Uplink (25 bits),
countMSB-Downlink (25 bits)
determine whether bearer identifier is included per bearer or determine whether to report COUNT value based on MSB comparison result
1i-15
CounterCheckResponse
1i-20

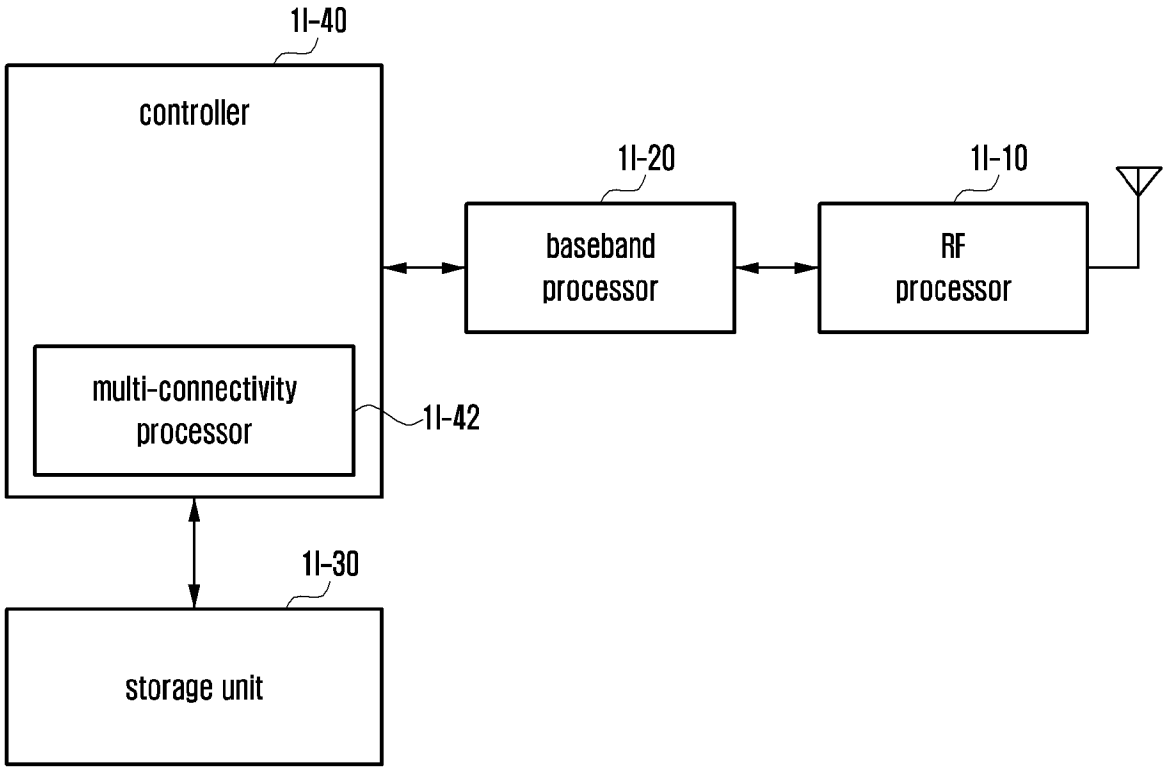
[Fig. 1j]


1j-15
32bits
1j-05
HFN (14bits)
PDCP SN (18bits)
1j-10
HFN (20bits)
PDCP SN (12bits)
20bits

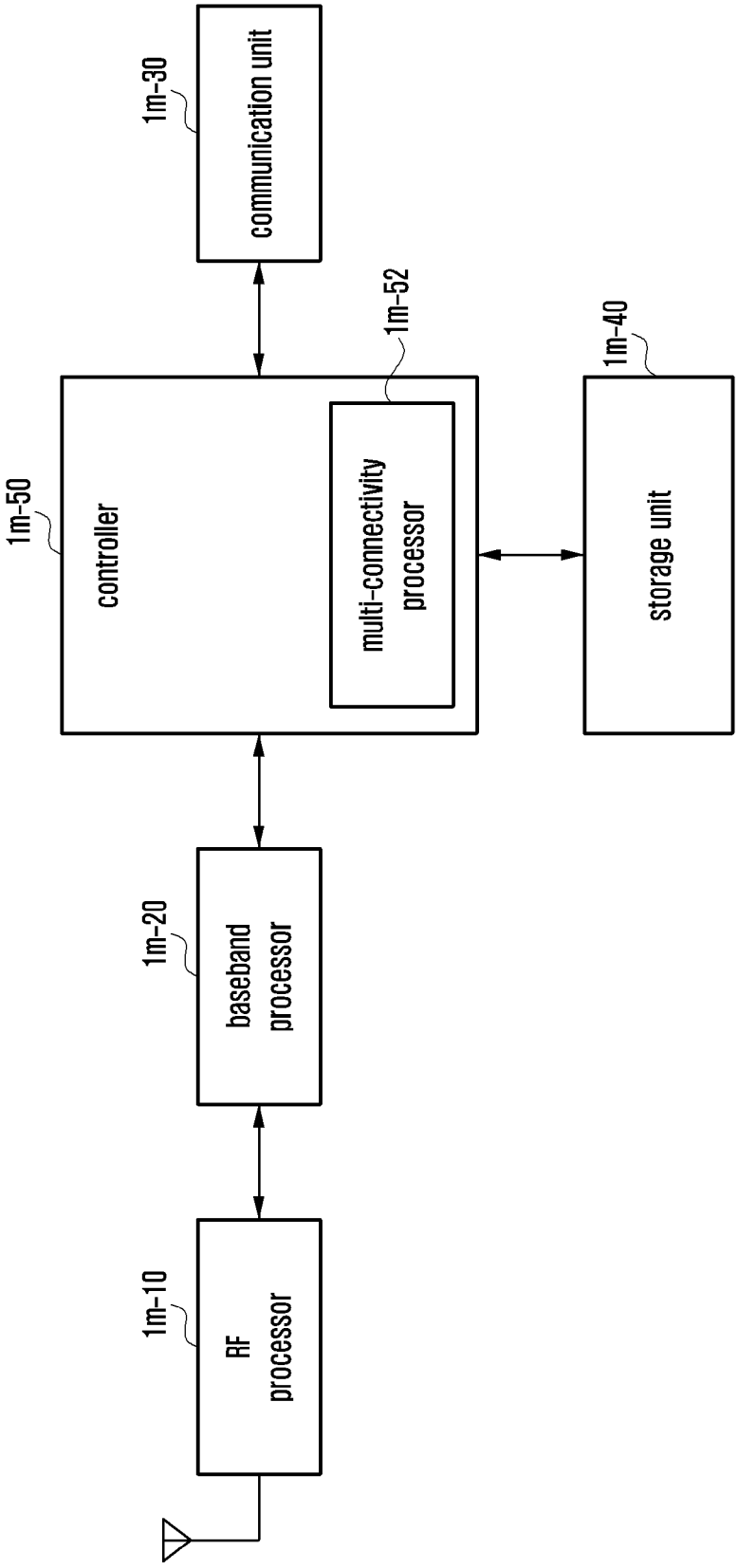
[Fig. 1k]


1k-01
UE
1k-05
receive Counter check message
1k-10
identifier per configured bearer is included in drb-CountMSB-InfoList?
NO
YES
1k-15
select uplink/downlink COUNT value to be reported as COUNT value of UE bearer
1k-20
include bearer identifier and selected uplink and downlink COUNT values in drb-CountInfoList of response message
1k-25
select uplink/downlink COUNT value to be compared as COUNT value of UE bearer
1k-30
compare MSBs of COUNT value indicated by base station and MSBs of selected COUNT value
if not identical in at least one direction
1k-35
include bearer identifier and selected uplink and downlink COUNT values in drb-CountInfoList of response message

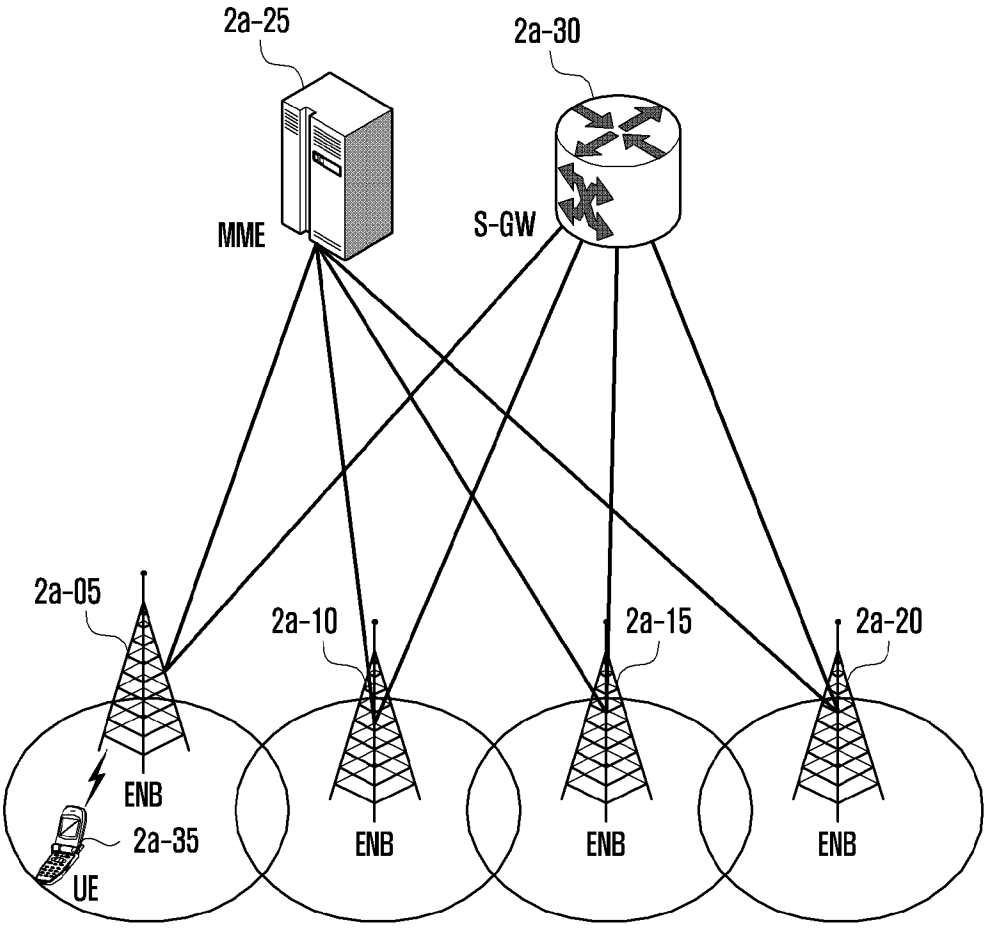
[Fig. 1l]


1l-40
controller
1l-20
baseband processor
1l-10
RF processor
multi-connectivity processor
1l-42
1l-30
storage unit

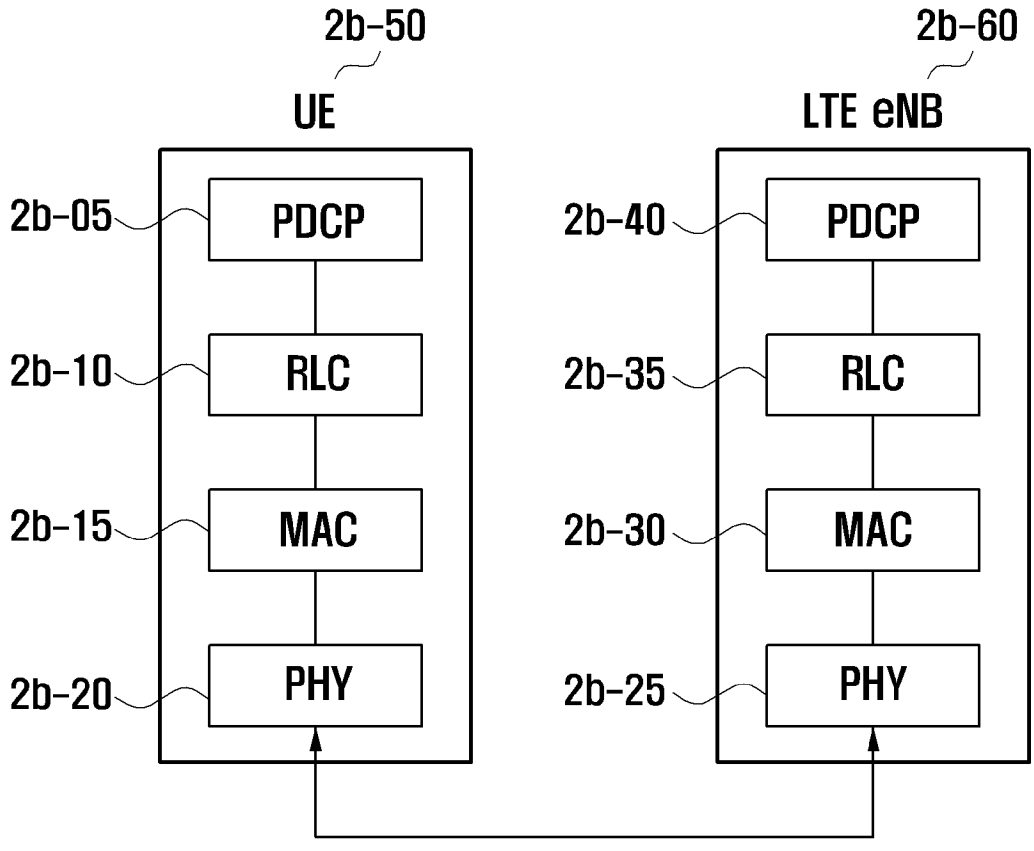
[Fig. 1m]


1m-30
communication unit
1m-52
1m-40
1m-50
controller
multi-connectivity processor
storage unit
1m-20
baseband processor
1m-10
RF processor

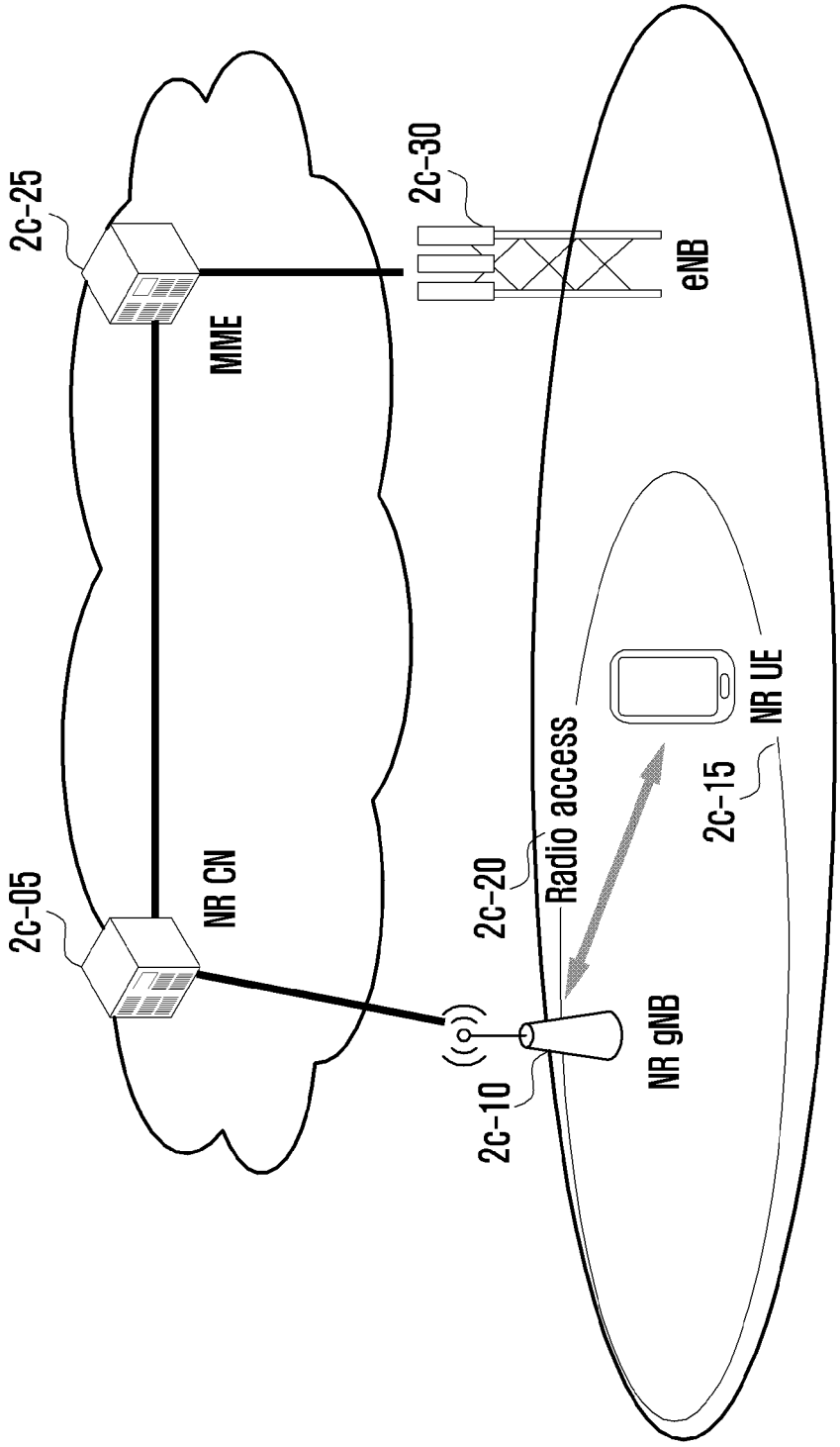
[Fig. 2a]


2a-25
2a-30
MME
S-GW
2a-05
2a-10
2a-15
2a-20
ENB
ENB
ENB
ENB
2a-35
UE

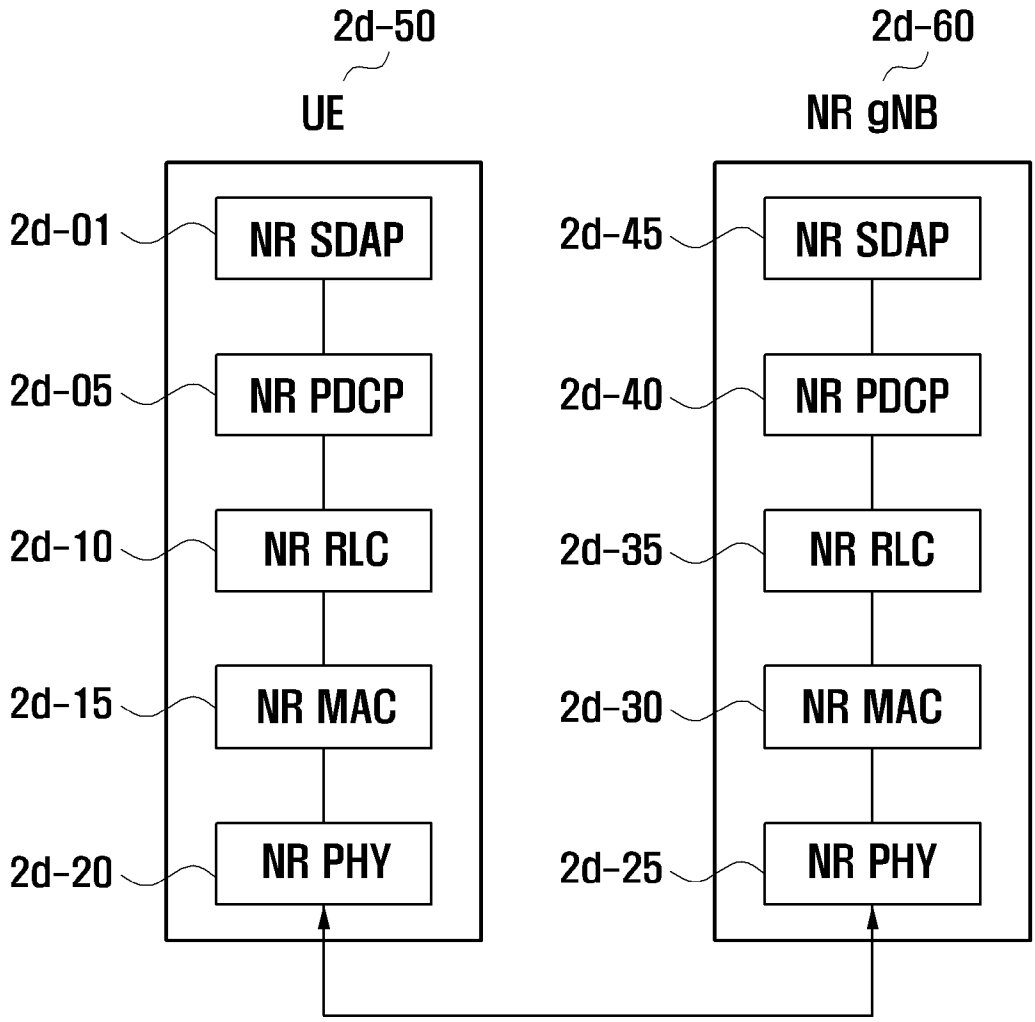
[Fig. 2b]


2b-50
UE
2b-60
LTE eNB
2b-05
PDCP
2b-40
PDCP
2b-10
RLC
2b-35
RLC
2b-15
MAC
2b-30
MAC
2b-20
PHY
2b-25
PHY

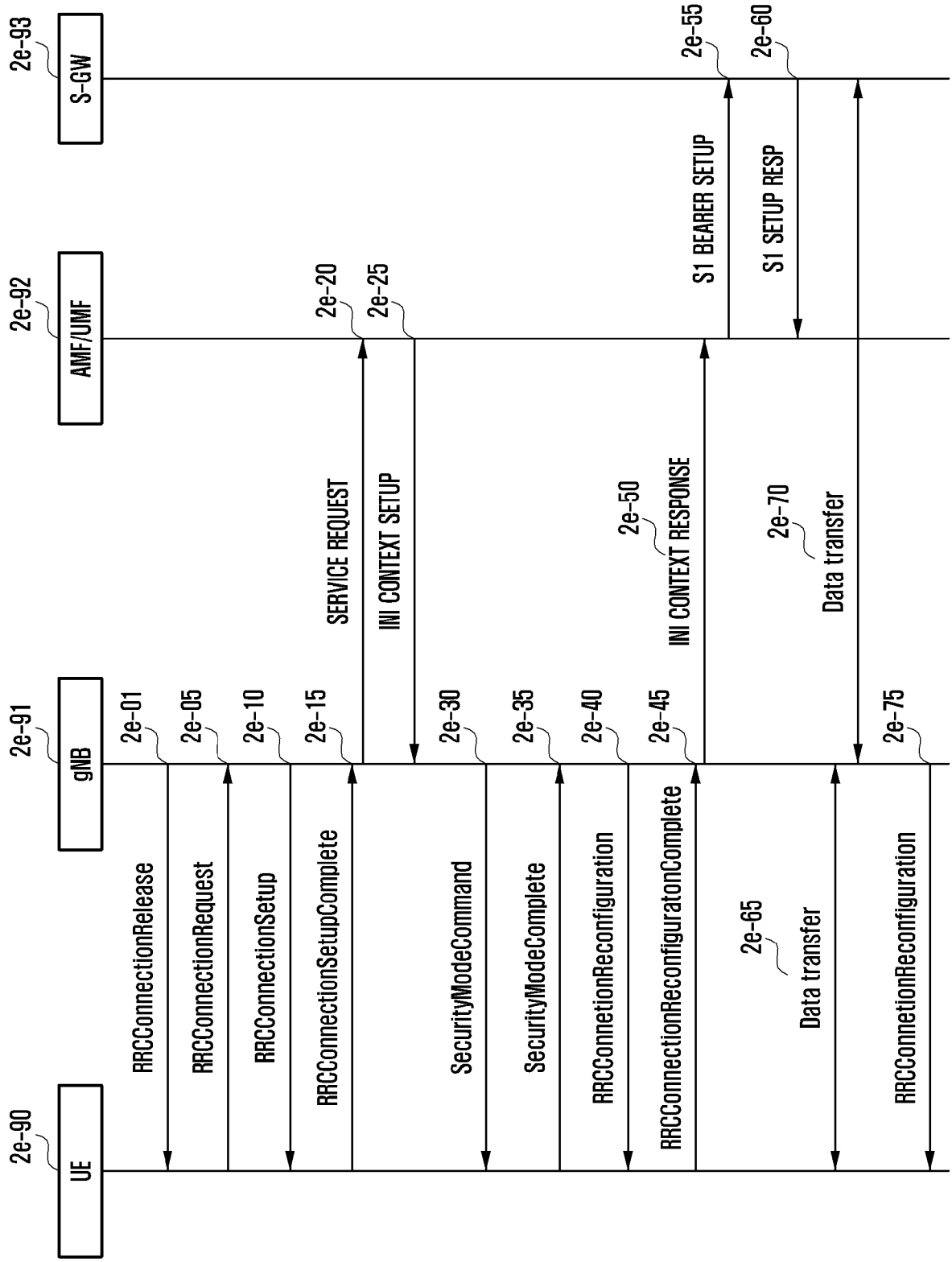
[Fig. 2c]


2c-25
MME
2c-30
eNB
NR CN
2c-05
Radio access
2c-20
NR UE
2c-15
NR gNB
2c-10

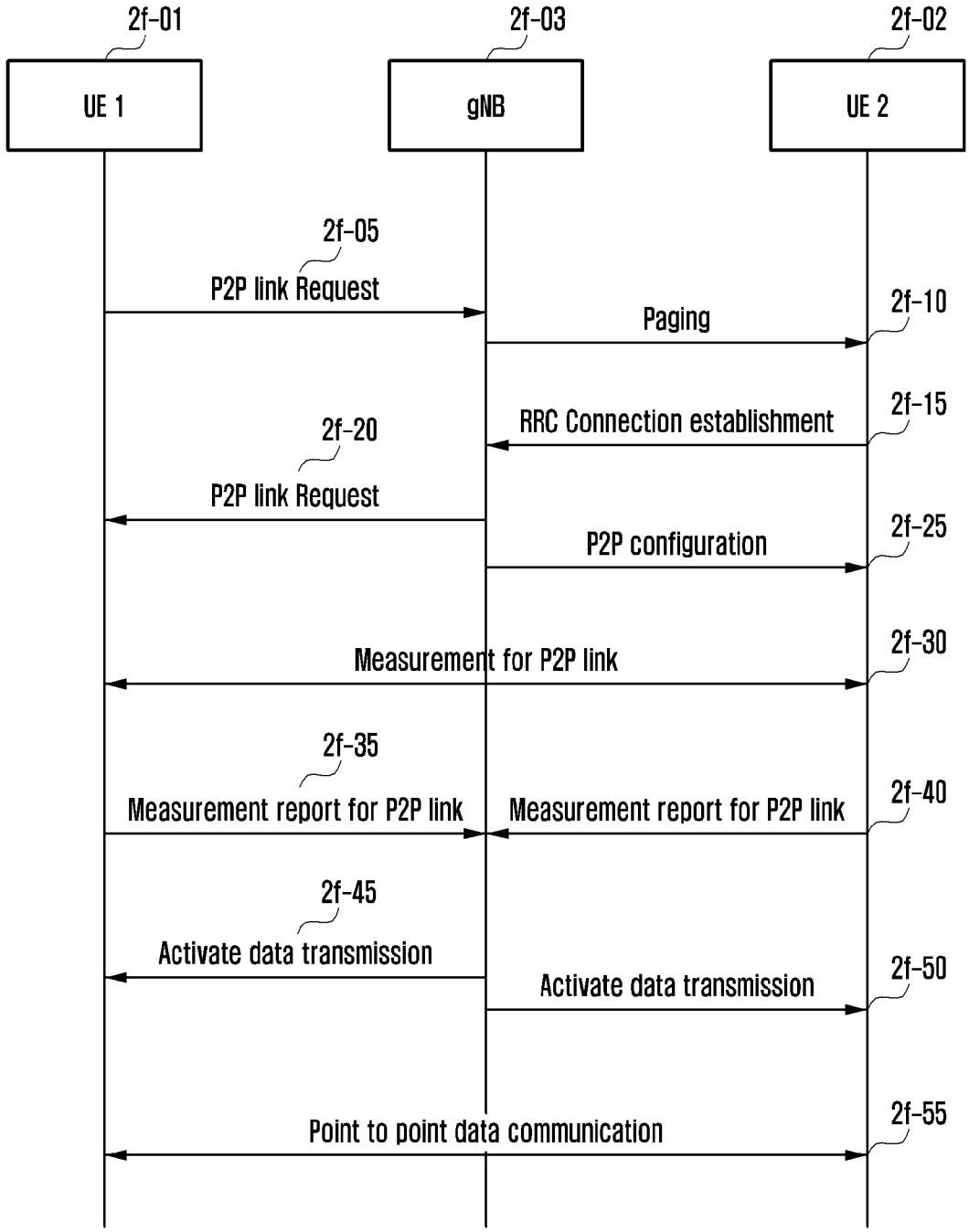
[Fig. 2d]


2d-50
UE
2d-60
NR gNB
2d-01
NR SDAP
2d-05
NR PDCP
2d-10
NR RLC
2d-15
NR MAC
2d-20
NR PHY
2d-45
NR SDAP
2d-40
NR PDCP
2d-35
NR RLC
2d-30
NR MAC
2d-25
NR PHY

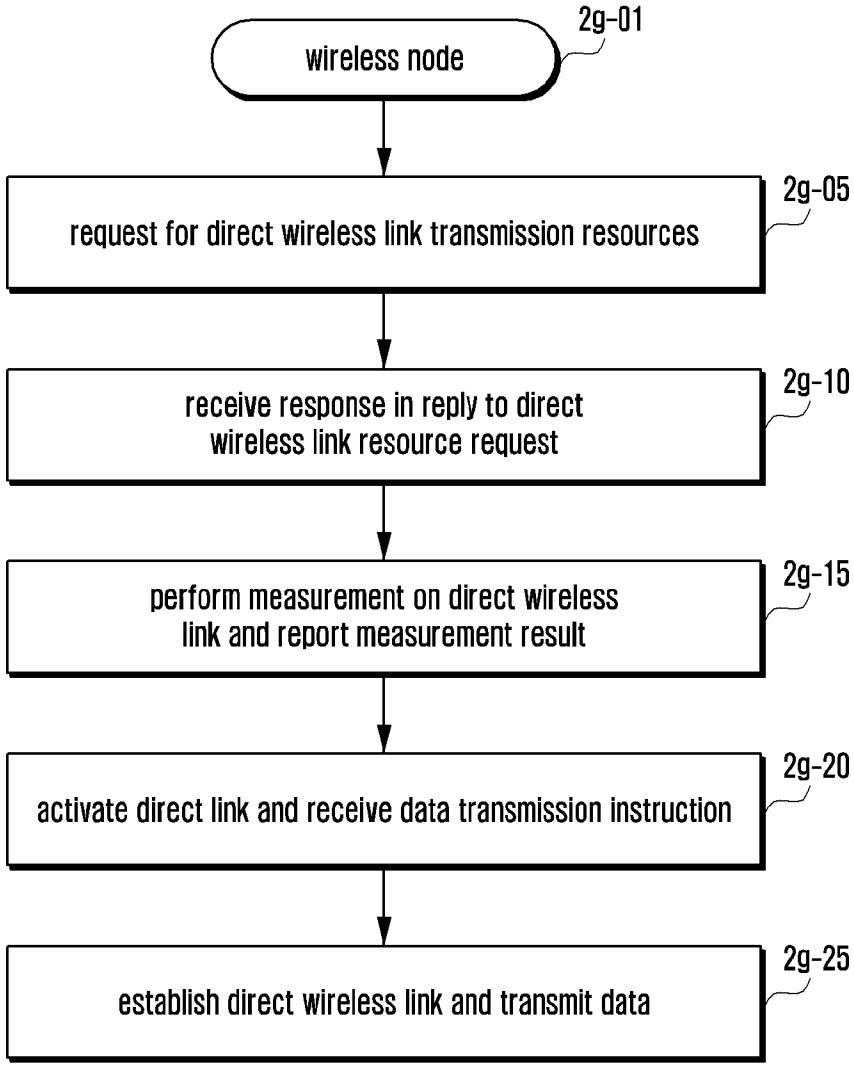
[Fig. 2e]


2e-90
UE
2e-91
gNB
2e-92
AMF/UMF
2e-93
S-GW
2e-01
RRCConnectionRelease
2e-05
RRCConnectionRequest
2e-10
RRCConnectionSetup
2e-15
RRCConnectionSetupComplete
SERVICE REQUEST
2e-20
INI CONTEXT SETUP
2e-25
2e-30
SecurityModeCommand
2e-35
SecurityModeComplete
2e-40
RRCConnetionReconfiguration
2e-45
RRCConnectionReconfiguratonComplete
2e-50
INI CONTEXT RESPONSE
S1 BEARER SETUP
2e-55
S1 SETUP RESP
2e-60
2e-65
Data transfer
2e-70
Data transfer
2e-75
RRCConnetionReconfiguration

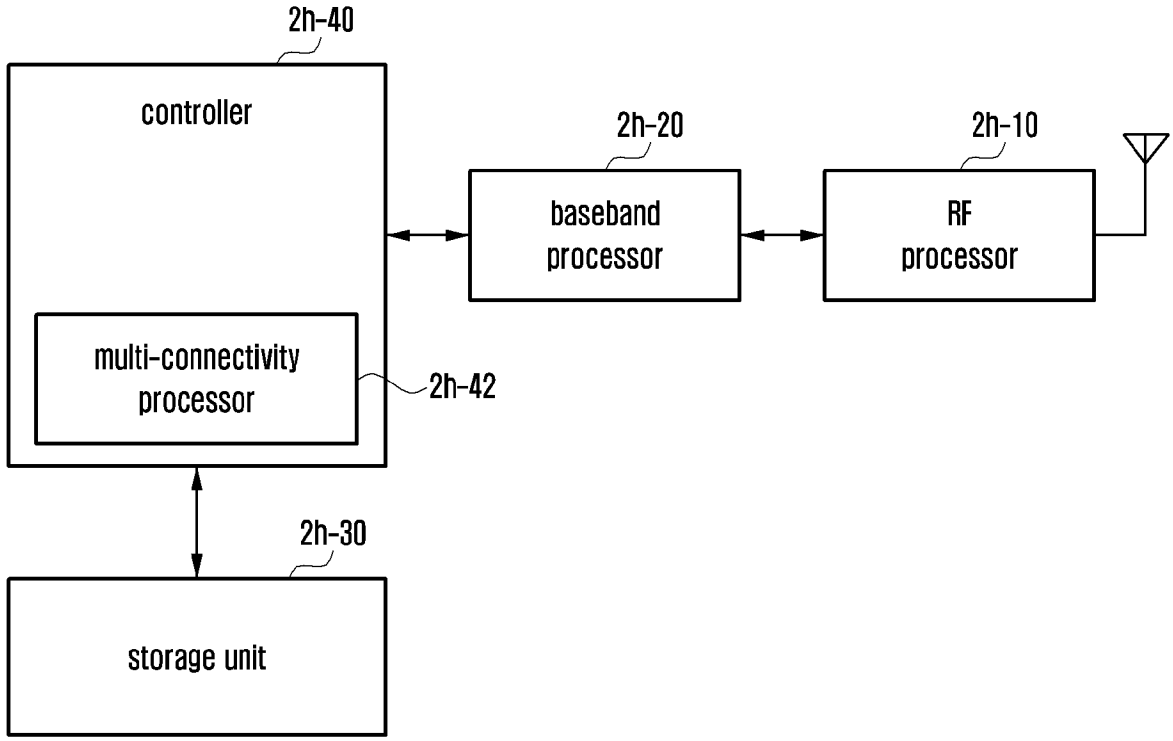
[Fig. 2f]


2f-01
UE 1
2f-03
gNB
2f-02
UE 2
2f-05
P2P link Request
Paging
2f-10
RRC Connection establishment
2f-15
2f-20
P2P link Request
P2P configuration
2f-25
Measurement for P2P link
2f-30
2f-35
Measurement report for P2P link
Measurement report for P2P link
2f-40
2f-45
Activate data transmission
Activate data transmission
2f-50
Point to point data communication
2f-55

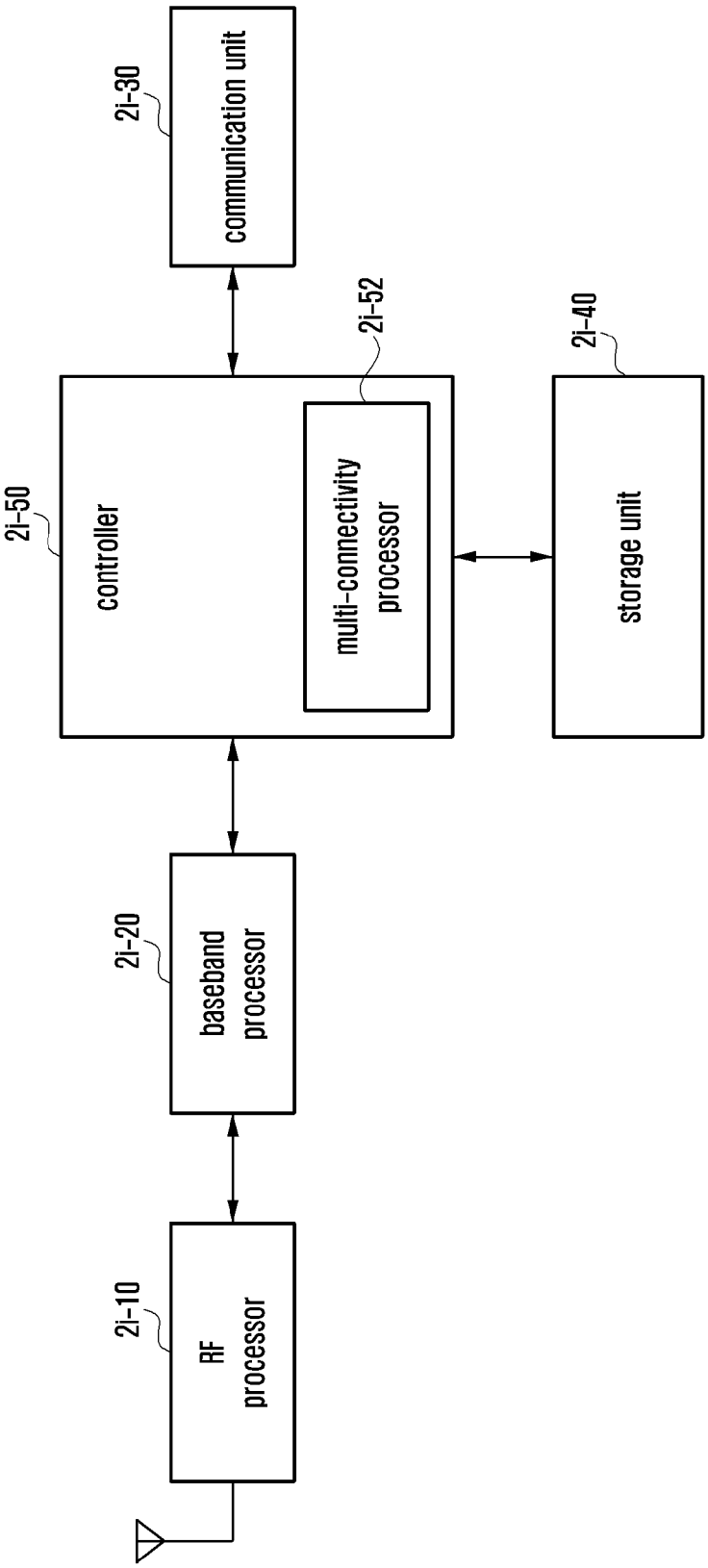
[Fig. 2g]


wireless node
2g-01
request for direct wireless link transmission resources
2g-05
receive response in reply to direct wireless link resource request
2g-10
perform measurement on direct wireless link and report measurement result
2g-15
activate direct link and receive data transmission instruction
2g-20
establish direct wireless link and transmit data
2g-25

[Fig. 2h]


2h-40
controller
2h-20
baseband processor
2h-10
RF processor
multi-connectivity processor
2h-42
2h-30
storage unit

[Fig. 2i]


2i-30
communication unit
2i-52
2i-40
2i-50
controller
multi-connectivity processor
storage unit
2i-20
baseband processor
2i-10
RF processor

**INTERNATIONAL SEARCH REPORT**

International application No.
**PCT/KR2019/012173**

**A. CLASSIFICATION OF SUBJECT MATTER**

**H04L 9/08(2006.01)i, H04W 12/04(2009.01)i, H04L 29/08(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 9/08; H04B 7/06; H04L 5/00; H04M 3/42; H04W 12/04; H04W 28/02; H04W 28/08; H04W 72/04; H04L 29/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: terminal, base station, bearer identity, uplink count value, downlink count value, new radio (NR) packet data convergence protocol (PDCP), first list, second list

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | US 2015-0341786 A1 (SAMSUNG ELECTRONICS CO., LTD.) 26 November 2015<br>See paragraphs [0007], [0114]-[0119]; and figure 8. | 1-15 |
| A | US 2015-0133135 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 14 May 2015<br>See paragraphs [0147]-[0149]; and figure 9. | 1-15 |
| A | US 2018-0083688 A1 (SAMSUNG ELECTRONICS CO., LTD.) 22 March 2018<br>See paragraphs [0186]-[0190]; and figure 5A. | 1-15 |
| A | `3GPP; TSG SA; 3GPP System Architecture Evolution (SAE); Security architecture (Release 15)`, 3GPP TS 33.401 V15.4.0, 21 June 2018<br>See section 9. | 1-15 |
| A | KR 10-2018-0035809 A (QUALCOMM INC.) 06 April 2018<br>See paragraph [0089]; and figure 5. | 1-15 |

☐ 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
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 27 December 2019 (27.12.2019) | **27 December 2019 (27.12.2019)** |


Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
BYUN, Sung Cheal
Telephone No. +82-42-481-8262

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.

**PCT/KR2019/012173**

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2015-0341786 A1 | 26/11/2015 | CN 103906049 A | 02/07/2014 |
| | | CN 103906049 B | 24/09/2019 |
| | | EP 2939481 A1 | 04/11/2015 |
| | | EP 2939481 A4 | 17/08/2016 |
| | | KR 10-2015-0103063 A | 09/09/2015 |
| | | US 10129742 B2 | 13/11/2018 |
| | | US 2017-0347261 A1 | 30/11/2017 |
| | | US 9736687 B2 | 15/08/2017 |
| | | WO 2014-104853 A1 | 03/07/2014 |
| US 2015-0133135 A1 | 14/05/2015 | CN 103703717 A | 02/04/2014 |
| | | CN 103703717 B | 14/07/2017 |
| | | CN 106992875 A | 28/07/2017 |
| | | CN 107360000 A | 17/11/2017 |
| | | CN 107484159 A | 15/12/2017 |
| | | EP 2876839 A1 | 27/05/2015 |
| | | EP 2876839 A4 | 02/09/2015 |
| | | EP 2876839 B1 | 28/12/2016 |
| | | EP 3197125 A1 | 26/07/2017 |
| | | ES 2618934 T3 | 22/06/2017 |
| | | JP 2015-530782 A | 15/10/2015 |
| | | JP 6061110 B2 | 18/01/2017 |
| | | KR 10-1713285 B1 | 07/03/2017 |
| | | KR 10-1832840 B1 | 27/02/2018 |
| | | KR 10-1941670 B1 | 23/01/2019 |
| | | KR 10-2015-0036729 A | 07/04/2015 |
| | | KR 10-2017-0027876 A | 10/03/2017 |
| | | KR 10-2019-0008449 A | 23/01/2019 |
| | | KR 10-2037115 B1 | 28/10/2019 |
| | | US 2016-0080339 A1 | 17/03/2016 |
| | | US 2017-0295153 A1 | 12/10/2017 |
| | | US 2019-0097986 A1 | 28/03/2019 |
| | | US 9215700 B2 | 15/12/2015 |
| | | US 9736129 B2 | 15/08/2017 |
| | | WO 2014-015478 A1 | 30/01/2014 |
| US 2018-0083688 A1 | 22/03/2018 | CN 109691155 A | 26/04/2019 |
| | | EP 3494756 A1 | 12/06/2019 |
| | | EP 3494756 A4 | 31/07/2019 |
| | | KR 10-2019-0029741 A | 20/03/2019 |
| | | US 10432291 B2 | 01/10/2019 |
| | | WO 2018-030798 A1 | 15/02/2018 |
| KR 10-2018-0035809 A | 06/04/2018 | AU 2016-298481 A1 | 18/01/2018 |
| | | BR 112018001598 A2 | 18/09/2018 |
| | | CN 108353340 A | 31/07/2018 |
| | | EP 3329721 A1 | 06/06/2018 |
| | | JP 2018-522496 A | 09/08/2018 |
| | | US 10349329 B2 | 09/07/2019 |

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.

**PCT/KR2019/012173**

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| | | US 2017-0034756 A1 | 02/02/2017 |
| | | WO 2017-019197 A1 | 02/02/2017 |