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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 December 2022 (29.12.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/266848 A1

(51) International Patent Classification:
H04W 74/08 (2009.01)

(21) International Application Number:
PCT/CN2021/101579

(22) International Filing Date:
22 June 2021 (22.06.2021)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicants *(for CN only)*: **NOKIA SHANGHAI BELL CO., LTD.** [CN/CN]; No.388, Ningqiao Road, Pudong Jinqiao, Shanghai 201206 (CN). **NOKIA SOLUTIONS AND NETWORKS OY** [FI/FI]; Karakaari 7, 02610 Espoo (FI).

(71) Applicant *(for all designated States except CN)*: **NOKIA TECHNOLOGIES OY** [FI/FI]; Karakaari 7, 02610 Espoo (FI).

(72) Inventors: **TURTINEN, Samuli Heikki**; Salongintie 15, 91100 Ii (FI). **KOSKINEN, Jussi-Pekka**; Kipinäkuja 10, 90420 Oulu (FI). **WU, Chunli**; Room 1208, No. 119 Zaolinqianjie Xicheng District, Beijing 100054 (CN).

(74) Agent: **KING & WOOD MALLESONS**; 20th Floor, East Tower, World Financial Centre, No. 1 Dongsanhuan Zhonglu, Chaoyang District, Beijing 100020 (CN).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, 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: DATA HANDLING DURING SDT

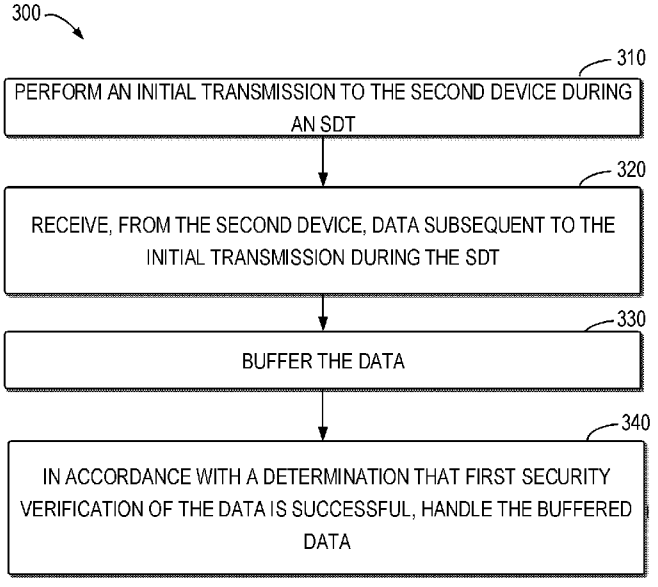

Fig. 3

(57) Abstract: Embodiments of the present disclosure relate to handling data during SDT. A first device in an inactive state performs an initial transmission to a second device during an SDT. The first device receives, from the second device, data subsequent to the initial transmission during the SDT. The first device buffers the data. The first device handles the buffered data in accordance with a determination that security verification is successful.

WO 2022/266848 A1

[Continued on next page]

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))*

DATA HANDLING DURING SDT

FIELD

[0001] Embodiments of the present disclosure generally relate to the field of telecommunication and in particular, to devices, methods, apparatuses and computer readable storage media for handling data during small data transmission (SDT).

BACKGROUND

[0002] New radio (NR) supports SDT in an inactive state to avoid the signaling overhead and delay associated with transition from the inactive state to a connected state to perform data transfer.

[0003] Multiple downlink (DL) packets may be transmitted from a network device to a terminal device as part of the same SDT procedure without transitioning to the connected state. Such multiple DL transmissions may be scheduled before DL radio resource control (RRC) message is transmitted which in turn may be used for security verification. This might be a possible security threat because a hostile network device can schedule multiple DL transmissions and the terminal device will be stuck.

SUMMARY

[0004] In general, example embodiments of the present disclosure provide a solution for handling data during SDT.

[0005] In a first aspect, there is provided a first device. The first device comprises at least one processor; and at least one memory including computer program codes; the at least one memory and the computer program codes are configured to, with the at least one processor, cause the first device in an inactive state to: perform an initial transmission to a second device during a small data transmission procedure; receive, from the second device, data subsequent to the initial transmission during the small data transmission procedure; buffer the data; and in accordance with a determination that security verification is successful, handle the buffered data.

[0006] In a second aspect, there is provided a method implemented at a first device. The method comprises: performing, at the first device, an initial transmission to a second device during a small data transmission procedure; receiving, from the second device, data

subsequent to the initial transmission during the small data transmission procedure; buffering the data; and in accordance with a determination that security verification is successful, handling the buffered data.

[0007] In a third aspect, there is provided an apparatus comprising: means for performing an initial transmission to a second device during a small data transmission procedure; means for receiving, from the second device, data subsequent to the initial transmission during the small data transmission procedure; means for buffering the data; and in accordance with a determination that security verification is successful, means for handling the buffered data.

[0008] In a fourth aspect, there is provided a non-transitory computer readable medium comprising a computer program for causing an apparatus to perform at least the method according to the above second aspect.

[0009] In a fifth aspect, there is provided a first device. The first device comprises at least one processor; and at least one memory including computer program codes; the at least one memory and the computer program codes are configured to, with the at least one processor, cause the first device in an inactive state to: receive, from a second device, configuration information indicating that security verification is enabled for at least one radio bearer for small data transmission; receive, from the second device, the small data transmission associated with the at least one radio bearer; and perform the security verification.

[0010] In a sixth aspect, there is provided a method implemented at a first device. The method comprises: receiving, at a first device and from a second device, configuration information indicating that security verification is enabled for at least one radio bearer for small data transmission; and receiving, from the second device, the small data transmission associated with the at least one radio bearer; and performing the security verification.

[0011] In a seventh aspect, there is provided an apparatus comprising: means for receiving, at a first device and from a second device, configuration information indicating that security verification is enabled for at least one radio bearer for small data transmission; and means for receiving, from the second device, the small data transmission associated with the at least one radio bearer; and means for performing the security verification.

[0012] In an eighth aspect, there is provided a non-transitory computer readable medium comprising a computer program for causing an apparatus to perform at least the method

according to the above sixth aspect.

[0013] In a ninth aspect, there is provided a second device. The second device comprises at least one processor; and at least one memory including computer program codes; the at least one memory and the computer program codes are configured to, with the at least one processor, cause the second device to: transmit, to a first device in an inactive state, configuration information indicating that security verification is enabled for at least one radio bearer for small data transmission; and transmit, to the first device, the small data transmission associated with the at least one radio bearer.

[0014] In a tenth aspect, there is provided a method implemented at a second device. The method comprises: transmitting, from the second device to a first device in an inactive state, configuration information indicating that security verification is enabled for at least one radio bearer for small data transmission; and transmitting, to the first device, the small data transmission associated with the at least one radio bearer.

[0015] In an eleventh aspect, there is provided an apparatus comprising: means for transmitting, from the second device to a first device in an inactive state, configuration information indicating that security verification is enabled for at least one radio bearer for small data transmission; and means for transmitting, to the first device, the small data transmission associated with the at least one radio bearer.

[0016] In a twelfth aspect, there is provided a non-transitory computer readable medium comprising a computer program for causing an apparatus to perform at least the method according to the above tenth aspect.

[0017] It is to be understood that the summary section is not intended to identify key or essential features of embodiments of the present disclosure, nor is it intended to be used to limit the scope of the present disclosure. Other features of the present disclosure will become easily comprehensible through the following description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] Some example embodiments will now be described with reference to the accompanying drawings, where:

[0019] Fig. 1 illustrates an example communication network in which embodiments of the present disclosure may be implemented;

[0020] Fig. 2 illustrates a signaling chart illustrating a process for handling data during SDT according to some example embodiments of the present disclosure;

[0021] Fig. 3 illustrates a flowchart of a method implemented at a first device according to some example embodiments of the present disclosure;

[0022] Fig. 4 illustrates a flowchart of a method implemented at a first device according to some example embodiments of the present disclosure;

[0023] Fig. 5 illustrates a flowchart of a method implemented at a first device according to some example embodiments of the present disclosure;

[0024] Fig. 6 illustrates a simplified block diagram of an apparatus that is suitable for implementing embodiments of the present disclosure; and

[0025] Fig. 7 illustrates a block diagram of an example computer readable medium in accordance with some example embodiments of the present disclosure.

[0026] Throughout the drawings, the same or similar reference numerals represent the same or similar element.

DETAILED DESCRIPTION

[0027] Principle of the present disclosure will now be described with reference to some example embodiments. It is to be understood that these embodiments are described only for the purpose of illustration and help those skilled in the art to understand and implement the present disclosure, without suggesting any limitation as to the scope of the disclosure. The disclosure described herein can be implemented in various manners other than the ones described below.

[0028] In the following description and claims, unless defined otherwise, all technical and scientific terms used herein have the same meaning as commonly understood by one of ordinary skills in the art to which this disclosure belongs.

[0029] References in the present disclosure to "one embodiment," "an embodiment," "an example embodiment," and the like indicate that the embodiment described may include a particular feature, structure, or characteristic, but it is not necessary that every embodiment includes the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an example embodiment, it is

submitted that it is within the knowledge of one skilled in the art to affect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.

[0030] It shall be understood that although the terms "first" and "second" etc. may be used herein to describe various elements, these elements should not be limited by these terms. These terms are only used to distinguish one element from another. For example, a first element could be termed a second element, and similarly, a second element could be termed a first element, without departing from the scope of example embodiments. As used herein, the term "and/or" includes any and all combinations of one or more of the listed terms.

[0031] The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of example embodiments. As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises", "comprising", "has", "having", "includes" and/or "including", when used herein, specify the presence of stated features, elements, and/or components etc., but do not preclude the presence or addition of one or more other features, elements, components and/ or combinations thereof.

[0032] As used in this application, the term "circuitry" may refer to one or more or all of the following:

(a) hardware-only circuit implementations (such as implementations in only analog and/or digital circuitry) and

(b) combinations of hardware circuits and software, such as (as applicable):

(i) a combination of analog and/or digital hardware circuit(s) with software/firmware and

(ii) any portions of hardware processor(s) with software (including digital signal processor(s)), software, and memory(ies) that work together to cause an apparatus, such as a mobile phone or server, to perform various functions) and

(c) hardware circuit(s) and or processor(s), such as a microprocessor(s) or a portion of a microprocessor(s), that requires software (e.g., firmware) for operation, but the software may not be present when it is not needed for operation.

[0033] This definition of circuitry applies to all uses of this term in this application, including in any claims. As a further example, as used in this application, the term circuitry also covers an implementation of merely a hardware circuit or processor (or multiple processors) or portion of a hardware circuit or processor and its (or their) accompanying software and/or firmware. The term circuitry also covers, for example and if applicable to the particular claim element, a baseband integrated circuit or processor integrated circuit for a mobile device or a similar integrated circuit in server, a cellular network device, or other computing or network device.

[0034] As used herein, the term "communication network" refers to a network following any suitable communication standards, such as fifth generation (5G) systems, Long Term Evolution (LTE), LTE-Advanced (LTE-A), Wideband Code Division Multiple Access (WCDMA), High-Speed Packet Access (HSPA), Narrow Band Internet of Things (NB-IoT) and so on. Furthermore, the communications between a terminal device and a network device in the communication network may be performed according to any suitable generation communication protocols, including, but not limited to, the first generation (1G), the second generation (2G), 2.5G, 2.75G, the third generation (3G), the fourth generation (4G), 4.5G, the fifth generation (5G) new radio (NR) communication protocols, and/or any other protocols either currently known or to be developed in the future. Embodiments of the present disclosure may be applied in various communication systems. Given the rapid development in communications, there will of course also be future type communication technologies and systems with which the present disclosure may be embodied. It should not be seen as limiting the scope of the present disclosure to only the aforementioned system.

[0035] As used herein, the term "network device" refers to a node in a communication network via which a terminal device accesses the network and receives services therefrom. The network device may refer to a base station (BS) or an access point (AP), for example, a node B (NodeB or NB), an evolved NodeB (eNodeB or eNB), a NR Next Generation NodeB (gNB), Integraged Access and Backhaul node, a Remote Radio Unit (RRU), a radio header (RH), a remote radio head (RRH), a relay, a low power node such as a femto, a pico, and so forth, depending on the applied terminology and technology. An RAN split architecture comprises a gNB-CU (Centralized unit, hosting RRC, SDAP and PDCP) controlling a plurality of gNB-DUs (Distributed unit, hosting RLC, MAC and PHY).

[0036] The term "terminal device" refers to any end device that may be capable of

wireless communication. By way of example rather than limitation, a terminal device may also be referred to as a communication device, user equipment (UE), a Subscriber Station (SS), a Portable Subscriber Station, a Mobile Station (MS), or an Access Terminal (AT). The terminal device may include, but not limited to, a mobile phone, a cellular phone, a smart phone, voice over IP (VoIP) phones, wireless local loop phones, a tablet, a wearable terminal device, a personal digital assistant (PDA), portable computers, desktop computer, image capture terminal devices such as digital cameras, gaming terminal devices, music storage and playback appliances, vehicle-mounted wireless terminal devices, wireless endpoints, mobile stations, laptop-embedded equipment (LEE), laptop-mounted equipment (LME), USB dongles, smart devices, wireless customer-premises equipment (CPE), an Internet of Things (IoT) device, a watch or other wearable, a head-mounted display (HMD), a vehicle, a drone, a medical device and applications (e.g., remote surgery), an industrial device and applications (e.g., a robot and/or other wireless devices operating in an industrial and/or an automated processing chain contexts), a consumer electronics device, a device operating on commercial and/or industrial wireless networks, and the like. In the following description, the terms "terminal device", "communication device", "terminal", "user equipment" and "UE" may be used interchangeably.

[0037] Although functionalities described herein can be performed, in various example embodiments, in a fixed and/or a wireless network node may, in other example embodiments, functionalities may be implemented in a user equipment apparatus (such as a cell phone or tablet computer or laptop computer or desktop computer or mobile IOT device or fixed IOT device). This user equipment apparatus can, for example, be furnished with corresponding capabilities as described in connection with the fixed and/or the wireless network node(s), as appropriate. The user equipment apparatus may be the user equipment and/or or a control device, such as a chipset or processor, configured to control the user equipment when installed therein. Examples of such functionalities include the bootstrapping server function and/or the home subscriber server, which may be implemented in the user equipment apparatus by providing the user equipment apparatus with software configured to cause the user equipment apparatus to perform from the point of view of these functions/nodes.

[0038] Fig. 1 shows an example communication network 100 in which embodiments of the present disclosure can be implemented. The network 100 includes a first device 110 and a second device 120 that can communicate with each other. In this example, the first

device 110 is illustrated as a terminal device, and the second device 120 is illustrated as a network device serving the terminal device. Thus, the serving area of the second device 120 is called as a cell 102. It is to be understood that the number of network devices and terminal devices is only for the purpose of illustration without suggesting any limitations. The system 100 may include any suitable number of network devices and terminal devices adapted for implementing embodiments of the present disclosure. Although not shown, it would be appreciated that one or more terminal devices may be located in the cell 102 and served by the second device 120.

[0039] Communications in the communication system 100 may be implemented according to any proper communication protocol(s), comprising, but not limited to, cellular communication protocols of the first generation (1G), the second generation (2G), the third generation (3G), the fourth generation (4G) and the fifth generation (5G) or NR and on the like, wireless local network communication protocols such as Institute for Electrical and Electronics Engineers (IEEE) 802.11 and the like, and/or any other protocols currently known or to be developed in the future. Moreover, the communication may utilize any proper wireless communication technology, comprising but not limited to: Code Division Multiple Access (CDMA), Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA), Frequency Division Duplex (FDD), Time Division Duplex (TDD), Multiple-Input Multiple-Output (MIMO), Orthogonal Frequency Division Multiple (OFDM), Discrete Fourier Transform spread OFDM (DFT-s-OFDM) and/or any other technologies currently known or to be developed in the future.

[0040] In some embodiments, the first device 110 may be in an inactive state and configured with SDT. In the inactive state, the first device 110 may perform SDT to the second device 120. Examples of SDT traffic may relate to smartphone applications or non-smartphone applications. The smartphone applications may relate to at least one of the following: traffic from Instant Messaging (IM) services (such as whatsapp, QQ, wechat and so on), heart-beat or keep-alive traffic from IM or email clients and other applications, or push notifications from various applications. The non-smartphone applications may relate to at least one of the following: traffic from wearables (such as periodic positioning information), sensors (Industrial Wireless Sensor Networks transmitting temperature, pressure readings periodically or in an event triggered manner and so on), or smart meters and smart meter networks sending periodic meter readings.

[0041] In some embodiments, in the case where Timing Advance for the first device 110

is valid, the first device 110 may perform the SDT on resources pre-configured by the second device 120. In other words, the first device 110 may perform the SDT by reusing the configured grant (CG) type 1 resources in the inactive state. Hereinafter, the CG type 1 resources are also referred to as CG resources. The second device 120 may pre-configure such CG resources for the first device 110 by using a dedicated signaling or a broadcast signaling. Examples of the CG resources may include, but are not limited to resources on a physical uplink shared channel (PUSCH).

[0042] In other embodiments, the first device 110 may perform the SDT by performing a random access (RA) procedure. In some embodiments, the RA procedure may be an RA procedure comprising two steps (also referred to as 2-step RACH). In such embodiments, the first device 110 may transmit small data for the SDT in a message A (MSGA) of the 2-step RACH. In other embodiments, the RA procedure may be an RA procedure comprising four steps (also referred to as 4-step RACH). In such embodiments, the first device 110 may transmit small data for the SDT in a message 3 (MSG3) of the 4-step RACH.

[0043] During an SDT procedure, transmission of the first (i.e., initial) data packet is referred to as an initial transmission. In some embodiments, the initial transmission may be performed during a random access procedure. For example, the data packet may be transmitted in MSGA or MSG3. In other embodiments, the data packet may be transmitted on a grant pre-configured by the second device 120.

[0044] When the first device 110 is in the inactive state, subsequent to the initial transmission, at least one transmission to the first device 110 may be performed by the second device 120 without transitioning to a connected state. Hereinafter, the transmission subsequent to the initial transmission is also referred to as subsequent transmission. It may be understood that the initial transmission and the subsequent transmission are included in the same SDT procedure. The subsequent transmission is beneficial because the size of the MSG3 may be limited, or to avoid another SDT procedure when new data arrives right after or soon after the initial transmission. It also allows the data for the subsequent transmission to be segmented and to be transmitted over multiple transport blocks (TBs) if the size of packet data convergence protocol (PDCP) service data unit (SDU) is too large to fit in one TB.

[0045] The subsequent transmission is scheduled before an RRC message is transmitted to

the first device 110. The RRC message may be used for security verification. This is possible security threat because a hostile network device can schedule DL subsequent transmissions to a terminal device and the terminal device will be stuck. In legacy, it is impossible to receive data on data radio bearer (DRBs) before DL RRC messages for RRC connection setup or RRC resume procedure are received.

[0046] In order to solve the above technical problems and potentially other technical problems in conventional solutions, embodiments of the present disclosure provide a solution for handling data during subsequent transmission. In some embodiments, upon receiving data subsequent to an initial transmission, a first device will not handle the data until security verification is successful. In this way, the data during subsequent transmission is handled in more secure manner.

[0047] Reference is now made to Fig. 2, which shows a signaling chart illustrating a process 200 for handling data during subsequent transmission according to some example embodiments of the present disclosure. For the purpose of discussion, the process 200 will be described with reference to Fig. 1. The process 200 may involve the first device 110 and the second device 120 as illustrated in Fig. 1. Although the process 200 has been described in the communication network 100 of Fig. 1, this process may be likewise applied to other communication scenarios. Although data handling by the first device 110 is discussed, a similar process can be applied to the second device.

[0048] In the process 200, the first device 110 is in an inactive state and configured with SDT. As shown, when data suitable for SDT becomes available for transmission, the first device 110 performs 210 an initial transmission to the second device 120 during an SDT.

[0049] In some embodiments, before performing the initial transmission to the second device 120, the first device 110 may transmit a request for the initial transmission to the second device 120. Alternatively, the first device 110 may transmit to the second device 120 the request for the initial transmission together with the data for the initial transmission. In some embodiments, the first device 110 may transmit the request for the initial transmission by transmitting an RRC resume request for SDT.

[0050] Following the initial transmission or subsequent to the initial transmission, the second device 120 may have data available for transmission to the first device 110. As such, the second device 120 transmits 220 to the first device 110 the data subsequent to the initial transmission during the SDT. In some embodiments, the data may be associated

with a first radio bearer (RB) configured for SDT. In other words, the second device 120 may transmit 220 the data on the first RB. Accordingly, the first device 110 may receive the data on the first RB. In some embodiments, security verification is disabled for the first RB. In other words, the first RB is not configured with security verification.

[0051] Examples of the first RB may include, but are not limited to data radio bearer (DRB) and signaling radio bearer (SRB). Examples of the SRB may include, but are not limited to SRB1, SRB2 and SRB3.

[0052] Upon receiving the data subsequent to the initial transmission, the first device 110 buffers 230 the data. In some embodiments, the data may be buffered at a first communication protocol layer. Examples of the first communication protocol layer may include, but are not limited to a physical (PHY) layer, a medium access control (MAC) layer, a radio link control (RLC) layer, a PDCP layer, or a service data adaptation protocol (SDAP) layer.

[0053] With continued reference to Fig. 2, the first device 110 determines 240 whether security verification is successful.

[0054] In some embodiments, the security verification may include, but are not limited to integrity protection verification of access stratum (AS) and ciphering verification of AS. RRC layer may handle the configuration of the AS security parameters which are part of the AS configuration. The examples of the AS security parameters may include, but are not limited to the integrity protection algorithm, the ciphering algorithm, if integrity protection and/or ciphering is enabled for a DRB and two parameters, namely the *keySetChangeIndicator* and the *nextHopChainingCount*. The first device 110 may use the AS security parameters to determine the AS security keys upon RRC connection resume.

[0055] The integrity protection algorithm is common for SRB1, SRB2, SRB3 (if configured) and DRBs configured with integrity protection, with the same keyToUse value. The ciphering algorithm is also common for SRB1, SRB2, SRB3 (if configured) and DRBs configured with the same keyToUse value.

[0056] In some embodiments, if the first device 110 successfully receives from the second device 120 a response to the request for the initial transmission, the first device 110 may determine that the security verification is successful. In some embodiments, the first device 110 may receive the response by receiving an RRC message. For example, the RRC message may comprise an RRC Release message indicating that the first device 110

shall maintain the inactive state.

[0057] In some embodiments, after receiving the data on the first RB, the first device 110 may receive further data on a second RB from the second device 120. The second RB is different from the first RB. For example, in case where the first RB is DRB1, the second RB may be any of DRB2, SRB1, SRB2 and SRB3. Security verification is enabled for the second RB. In other words, the second RB is configured with security verification. Examples of the second RB may include, but are not limited to DRB and SRB.

[0058] If the first device 110 determines that a security verification of the further data is successful, the first device 110 may determine that the second device 120 is a genuine device. As such, the first device 110 may handle the buffered data.

[0059] In some embodiments, the data may be buffered at the first communication protocol layer and the security verification may be performed at a second communication protocol layer of the first device 110. The second communication protocol layer is higher than the first communication protocol layer. In such embodiments, upon determining that the security verification is successful, the second communication protocol layer may provide the first communication protocol layer with an indication that the security verification is successful. For example, in case where the data may be buffered at one of PHY layer, MAC layer and RLC layer and the security verification is performed at PDCP layer, the PDCP layer may provide the one of PHY layer, MAC layer and RLC layer with the indication that the security verification is successful.

[0060] If the security verification is successful, the first device 110 handles 250 the buffered data. In some embodiments, the first device 110 may handle the buffered data by forwarding the buffered data from the first communication protocol layer to the second communication protocol layer higher than the first communication protocol layer. In other words, the data will not be forwarded to upper layers until the security verification is successful.

[0061] On the other hand, if the security verification fails, the first device 110 may discard the data. In such a case, the first device 110 may initiate a procedure for going into RRC_IDLE or remains in RRC_INACTIVE mode.

[0062] It will be understood that once the security verification is successful, security verification of other data received on the first RB will not be needed. In such a case, upon receiving other data on the first RB, the first device 110 may handle the other data

immediately. For example, the first device 110 may forward the other data from a lower layer to an upper layer immediately.

[0063] With the embodiments of the present disclosure, the data during subsequent transmission is handled in more secure manner. Possible corrupted DL data is not forwarded to upper layers of a terminal device. Thus, user can be protected from an attack.

[0064] Fig. 3 shows a flowchart of an example method 300 implemented at a first device in accordance with some example embodiments of the present disclosure. For the purpose of discussion, the method 300 will be described from the perspective of the first device 110 with reference to Fig. 1. It would be appreciated that the method 300 may also be implemented at the second device 120 in Fig. 1.

[0065] At block 310, the first device 110 in an inactive state performs an initial transmission to the second device 120 during an SDT. At block 320, the first device 110 receives, from the second device 120, data subsequent to the initial transmission during the SDT.

[0066] At block 330, the first device 110 buffers the data. At block 340, the first device 110 handles the buffered data in accordance with a determination that security verification is successful.

[0067] In some example embodiments, the data is associated with a first RB for which the security verification is disabled.

[0068] In some example embodiments, the first RB comprises one of the following: a DRB, or an SRB.

[0069] In some example embodiments, the at least one memory and the computer program code are configured to, with the at least one processor, further cause the first device 110 to determine that the security verification is successful by: transmitting a request for the initial transmission to the second device 120; and successfully receiving a response to the request from the second device 120.

[0070] In some example embodiments, the request comprises a radio resource control resume request for SDT, and the response comprises a radio resource control release message.

[0071] In some example embodiments, the at least one memory and the computer

program code are configured to, with the at least one processor, further cause the first device 110 to: receive, from the second device 120, further data associated with a RB for which security verification of the further data is enabled; and in accordance with a determination that the security verification is successful, determine that the security verification is successful.

[0072] In some example embodiments, the second RB comprises one of the following: a DRB, or an SRB.

[0073] In some example embodiments, the at least one memory and the computer program code are configured to, with the at least one processor, cause the first device 110 to handle the buffered data by: forwarding the buffered data from a first communication protocol layer of the first device 110 to a second communication protocol layer of the first device 110, the second communication protocol layer being higher than the first communication protocol layer.

[0074] In some example embodiments, the first communication protocol layer comprises one of the following: a physical layer, a medium access control layer, a radio link control layer, a packet data convergence protocol layer, or a service data adaptation protocol layer.

[0075] In some example embodiments, the first device 110 is a terminal device and the second device 120 is a network device.

[0076] In some embodiments, RBs that are allowed to use SDT are required to always be configured with security verification so that the first device 110 may perform security verification on RBs immediately. This will be described with reference to Figs. 4 and 5.

[0077] Fig. 4 shows a flowchart of an example method 400 implemented at a first device in accordance with some example embodiments of the present disclosure. For the purpose of discussion, the method 400 will be described from the perspective of the first device 110 with reference to Fig. 1. It would be appreciated that the method 400 may also be implemented at the second device 120 in Fig. 1.

[0078] At block 410, the first device 110 in an inactive state receives, from the second device 120, configuration information indicating that security verification is enabled for at least one RB for SDT.

[0079] At block 420, the first device 110 receives, from the second device 120, the SDT associated with the at least one RB.

[0080] At block 430, the first device 110 performs the security verification.

[0081] In some embodiments, the RB may be a DRB or an SRB.

[0082] In some embodiments, the first device 110 is a terminal device and the second device 120 is a network device.

[0083] Fig. 5 shows a flowchart of an example method 500 implemented at a second device in accordance with some example embodiments of the present disclosure. For the purpose of discussion, the method 500 will be described from the perspective of the second device 120 with reference to Fig. 1. It would be appreciated that the method 500 may also be implemented at the first device 110 in Fig. 1.

[0084] At block 510, the second device 120 transmits, to the first device 110 in an inactive state, configuration information indicating that security verification is enabled for at least one RB for SDT.

[0085] At block 520, the second device 120 transmits, to the first device 110 the SDT associated with the at least one RB.

[0086] In some embodiments, the RB may be a DRB or an SRB.

[0087] In some embodiments, the first device 110 is a terminal device and the second device 120 is a network device.

[0088] In some example embodiments, an apparatus capable of performing any of the method 300 (for example, the first device 110) may comprise means for performing the respective steps of the method 300. The means may be implemented in any suitable form. For example, the means may be implemented in a circuitry or software module.

[0001] In some example embodiments, the apparatus comprises: means for performing, at a first device, an initial transmission to a second device during an SDT; means for receiving, from the second device, data subsequent to the initial transmission during the SDT; means for buffering the data; and in accordance with a determination that security verification is successful, means for handling the buffered data.

[0002] In some example embodiments, the data is associated with a first RB for which the security verification is disabled.

[0003] In some example embodiments, the first RB comprises one of the following: a DRB, or an SRB.

[0004] In some example embodiments, the apparatus further comprises means for determining that the security verification is successful by: transmitting a request for the initial transmission to the second device; and successfully receiving a response to the request from the second device.

[0005] In some example embodiments, the request comprises a radio resource control resume request for SDT, and the response comprises a radio resource control release message.

[0006] In some example embodiments, the apparatus further comprises means for receiving, from the second device, further data associated with a RB for which security verification of the further data is enabled; and in accordance with a determination that the security verification is successful, means for determining that the security verification is successful.

[0007] In some example embodiments, the second RB comprises one of the following: a DRB, or an SRB.

[0008] In some example embodiments, means for handling the buffered data comprises: means for forwarding the buffered data from a first communication protocol layer of the first device to a second communication protocol layer of the first device, the second communication protocol layer being higher than the first communication protocol layer.

[0009] In some example embodiments, the first communication protocol layer comprises one of the following: a physical layer, a medium access control layer, a radio link control layer, a packet data convergence protocol layer, or a service data adaptation protocol layer.

[0010] In some example embodiments, the first device is a terminal device and the second device is a network device.

[0011] In some example embodiments, an apparatus capable of performing any of the method 400 (for example, the first device 110) may comprise means for performing the respective steps of the method 400. The means may be implemented in any suitable form. For example, the means may be implemented in a circuitry or software module.

[0012] In some example embodiments, the apparatus comprises: means for receiving, at a first device and from a second device, configuration information indicating that security verification is enabled for at least one radio bearer for small data transmission; and means for receiving, from the second device, the small data transmission associated with the at

least one radio bearer; and means for performing the security verification.

[0013] In some example embodiments, the first device is a terminal device and the second device is a network device.

[0014] In some example embodiments, an apparatus capable of performing any of the method 500 (for example, the second device 120) may comprise means for performing the respective steps of the method 500. The means may be implemented in any suitable form. For example, the means may be implemented in a circuitry or software module.

[0015] In some example embodiments, the apparatus comprises: means for transmitting, from the second device to a first device in an inactive state, configuration information indicating that security verification is enabled for at least one radio bearer for small data transmission; and means for transmitting, to the first device, the small data transmission associated with the at least one radio bearer.

[0016] In some example embodiments, the first device is a terminal device and the second device is a network device.

[0017] Fig. 6 is a simplified block diagram of a device 600 that is suitable for implementing embodiments of the present disclosure. The device 600 may be provided to implement the communication device, for example, the first device 110 or the second device 120 as shown in Fig. 1. As shown, the device 600 includes one or more processors 610, one or more memories 620 coupled to the processor 610, and one or more communication modules 640 coupled to the processor 610.

[0018] The communication module 640 is for bidirectional communications. The communication module 640 has at least one antenna to facilitate communication. The communication interface may represent any interface that is necessary for communication with other network elements.

[0019] The processor 610 may be of any type suitable to the local technical network and may include one or more of the following: general purpose computers, special purpose computers, microprocessors, digital signal processors (DSPs) and processors based on multicore processor architecture, as non-limiting examples. The device 600 may have multiple processors, such as an application specific integrated circuit chip that is slaved in time to a clock which synchronizes the main processor.

[0020] The memory 620 may include one or more non-volatile memories and one or more

volatile memories. Examples of the non-volatile memories include, but are not limited to, a Read Only Memory (ROM) 624, an electrically programmable read only memory (EPROM), a flash memory, a hard disk, a compact disc (CD), a digital video disk (DVD), and other magnetic storage and/or optical storage. Examples of the volatile memories include, but are not limited to, a random access memory (RAM) 622 and other volatile memories that will not last in the power-down duration.

[0021] A computer program 630 includes computer executable instructions that are executed by the associated processor 610. The program 630 may be stored in the ROM 624. The processor 610 may perform any suitable actions and processing by loading the program 630 into the RAM 622.

[0022] The embodiments of the present disclosure may be implemented by means of the program 630 so that the device 600 may perform any process of the disclosure as discussed with reference to Figs. 2 to 5. The embodiments of the present disclosure may also be implemented by hardware or by a combination of software and hardware.

[0023] In some example embodiments, the program 630 may be tangibly contained in a computer readable medium which may be included in the device 600 (such as in the memory 620) or other storage devices that are accessible by the device 600. The device 600 may load the program 630 from the computer readable medium to the RAM 622 for execution. The computer readable medium may include any types of tangible non-volatile storage, such as ROM, EPROM, a flash memory, a hard disk, CD, DVD, and the like. Fig. 7 shows an example of the computer readable medium 700 in form of CD or DVD. The computer readable medium has the program 630 stored thereon.

[0024] Generally, various embodiments of the present disclosure may be implemented in hardware or special purpose circuits, software, logic or any combination thereof. Some aspects may be implemented in hardware, while other aspects may be implemented in firmware or software which may be executed by a controller, microprocessor or other computing device. While various aspects of embodiments of the present disclosure are illustrated and described as block diagrams, flowcharts, or using some other pictorial representations, it is to be understood that the block, apparatus, system, technique or method described herein may be implemented in, as non-limiting examples, hardware, software, firmware, special purpose circuits or logic, general purpose hardware or controller or other computing devices, or some combination thereof.

[0025] The present disclosure also provides at least one computer program product tangibly stored on a non-transitory computer readable storage medium. The computer program product includes computer-executable instructions, such as those included in program modules, being executed in a device on a target real or virtual processor, to carry out the methods 300, 400 and 500 as described above with reference to Figs. 3-5. Generally, program modules include routines, programs, libraries, objects, classes, components, data structures, or the like that perform particular tasks or implement particular abstract data types. The functionality of the program modules may be combined or split between program modules as desired in various embodiments. Machine-executable instructions for program modules may be executed within a local or distributed device. In a distributed device, program modules may be located in both local and remote storage media.

[0026] Program code for carrying out methods of the present disclosure may be written in any combination of one or more programming languages. These program codes may be provided to a processor or controller of a general purpose computer, special purpose computer, or other programmable data processing apparatus, such that the program codes, when executed by the processor or controller, cause the functions/operations specified in the flowcharts and/or block diagrams to be implemented. The program code may execute entirely on a machine, partly on the machine, as a stand-alone software package, partly on the machine and partly on a remote machine or entirely on the remote machine or server.

[0027] In the context of the present disclosure, the computer program codes or related data may be carried by any suitable carrier to enable the device, apparatus or processor to perform various processes and operations as described above. Examples of the carrier include a signal, computer readable medium, and the like.

[0028] The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable medium may include but not limited to an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples of the computer readable storage medium would include an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable

combination of the foregoing.

[0029] Further, while operations are depicted in a particular order, this should not be understood as requiring that such operations be performed in the particular order shown or in sequential order, or that all illustrated operations be performed, to achieve desirable results. In certain circumstances, multitasking and parallel processing may be advantageous. Likewise, while several specific implementation details are contained in the above discussions, these should not be construed as limitations on the scope of the present disclosure, but rather as descriptions of features that may be specific to particular embodiments. Certain features that are described in the context of separate embodiments may also be implemented in combination in a single embodiment. Conversely, various features that are described in the context of a single embodiment may also be implemented in multiple embodiments separately or in any suitable sub-combination.

[0030] Although the present disclosure has been described in languages specific to structural features and/or methodological acts, it is to be understood that the present disclosure defined in the appended claims is not necessarily limited to the specific features or acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the claims.

WHAT IS CLAIMED IS:

1. A first device, comprising:

at least one processor; and

at least one memory including computer program code;

the at least one memory and the computer program code configured to, with the at least one processor, cause the first device in an inactive state to:

perform an initial transmission to a second device during a small data transmission procedure;

receive, from the second device, data subsequent to the initial transmission during the small data transmission procedure;

buffer the data; and

in accordance with a determination that security verification is successful, handle the buffered data.

2. The first device of claim 1, wherein the data is associated with a radio bearer for which the security verification is disabled.

3. The first device of claim 2, wherein the radio bearer comprises one of the following:

a data radio bearer, or

a signaling radio bearer.

4. The first device of claim 1, wherein the at least one memory and the computer program code are configured to, with the at least one processor, further cause the first device to determine that the security verification is successful by:

transmitting a request for the initial transmission to the second device; and

successfully receiving a response to the request from the second device.

5. The first device of claim 4, wherein the request comprises a radio resource control resume request for small data transmission, and the response comprises a radio resource control message.

6. The first device of claim 1, wherein the first device is caused to handle the

buffered data by:

receiving, from the second device, further data associated with a radio bearer for which the security verification is enabled; and

in accordance with a determination that the security verification of the further data is successful, handling the buffered data.

7. The first device of claim 6, wherein the radio bearer comprises one of the following:

a data radio bearer, or

a signaling radio bearer.

8. The first device of claim 1, wherein the at least one memory and the computer program code are configured to, with the at least one processor, cause the first device to handle the buffered data by:

forwarding the buffered data from a first communication protocol layer of the first device to a second communication protocol layer of the first device, the second communication protocol layer being higher than the first communication protocol layer.

9. The first device of claim 8, wherein the first communication protocol layer comprises one of the following:

a physical layer,

a medium access control layer,

a radio link control layer,

a packet data convergence protocol layer, or

a service data adaptation protocol layer.

10. The first device of claim 1, wherein the first device is caused to perform the initial transmission by:

performing the initial transmission during a random access procedure.

11. The first device of claim 1, wherein the first device is caused to perform the initial transmission by:

performing the initial transmission on a grant pre-configured by the second device.

12. The first device of any of claims 1 to 11, wherein the first device is a terminal device and the second device is a network device.

13. A first device, comprising:

at least one processor; and

at least one memory including computer program code;

the at least one memory and the computer program code configured to, with the at least one processor, cause the first device in an inactive state to:

receive, from a second device, configuration information indicating that security verification is enabled for at least one radio bearer for small data transmission;

receive, from the second device, the small data transmission associated with the at least one radio bearer; and

perform the security verification.

14. The first device of claim 13, wherein the first device is a terminal device and the second device is a network device.

15. A second device, comprising:

at least one processor; and

at least one memory including computer program code;

the at least one memory and the computer program code configured to, with the at least one processor, cause the second device to:

transmit, to a first device in an inactive state, configuration information indicating that security verification is enabled for at least one radio bearer for small data transmission; and

transmit, to the first device, the small data transmission associated with the at least one radio bearer.

16. The second device of claim 15, wherein the first device is a terminal device and the second device is a network device.

17. A method, comprising:

performing, at a first device, an initial transmission to a second device during a small data transmission procedure;

receiving, from the second device, data subsequent to the initial transmission during the small data transmission procedure;

buffering the data; and

in accordance with a determination that security verification is successful, handling the buffered data.

18. A method, comprising:

receiving, at a first device and from a second device, configuration information indicating that security verification is enabled for at least one radio bearer for small data transmission; and

receiving, from the second device, the small data transmission associated with the at least one radio bearer; and

performing the security verification.

19. A method, comprising:

transmitting, from a second device to a first device in an inactive state, configuration information indicating that security verification is enabled for at least one radio bearer for small data transmission; and

transmitting, to the first device, the small data transmission associated with the at least one radio bearer.

20. An apparatus, comprising:

means for performing, at a first device, an initial transmission to a second device during a small data transmission procedure;

means for receiving, from the second device, data subsequent to the initial transmission during the small data transmission procedure;

means for buffering the data; and

means for handling the buffered data in accordance with a determination that security verification is successful.

21. An apparatus, comprising:

means for receiving, at a first device and from a second device, configuration information indicating that security verification is enabled for at least one radio bearer for small data transmission; and

means for receiving, from the second device, the small data transmission associated with the at least one radio bearer; and

means for performing the security verification.

22. An apparatus, comprising:

means for transmitting, from a second device to a first device in an inactive state, configuration information indicating that security verification is enabled for at least one radio bearer for small data transmission; and

means for transmitting, to the first device, the small data transmission associated with the at least one radio bearer.

23. A computer readable medium comprising program instructions for causing an apparatus to perform at least the method of claim 17.

24. A computer readable medium comprising program instructions for causing an apparatus to perform at least the method of claim 18.

25. A computer readable medium comprising program instructions for causing an apparatus to perform at least the method of claim 19.

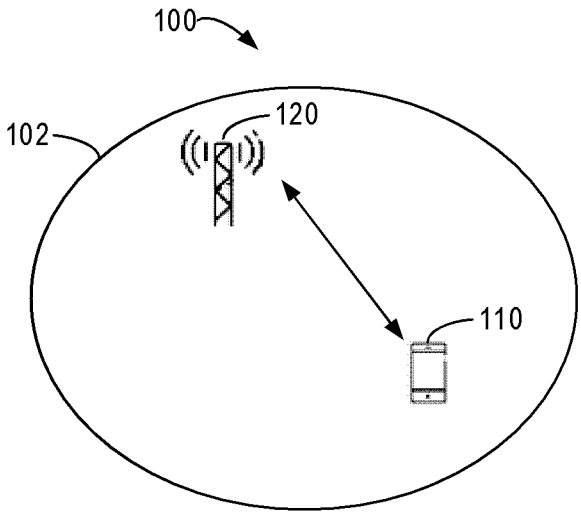

Fig. 1

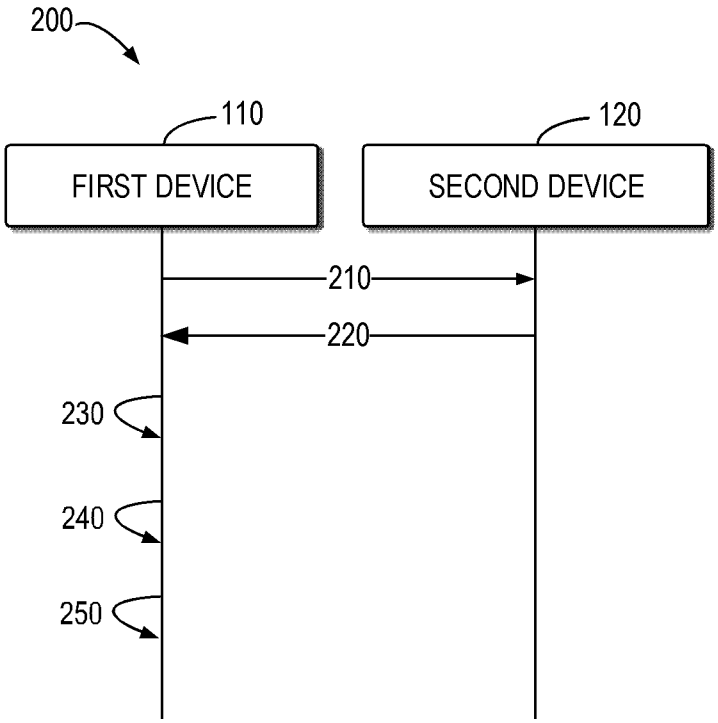

Fig. 2

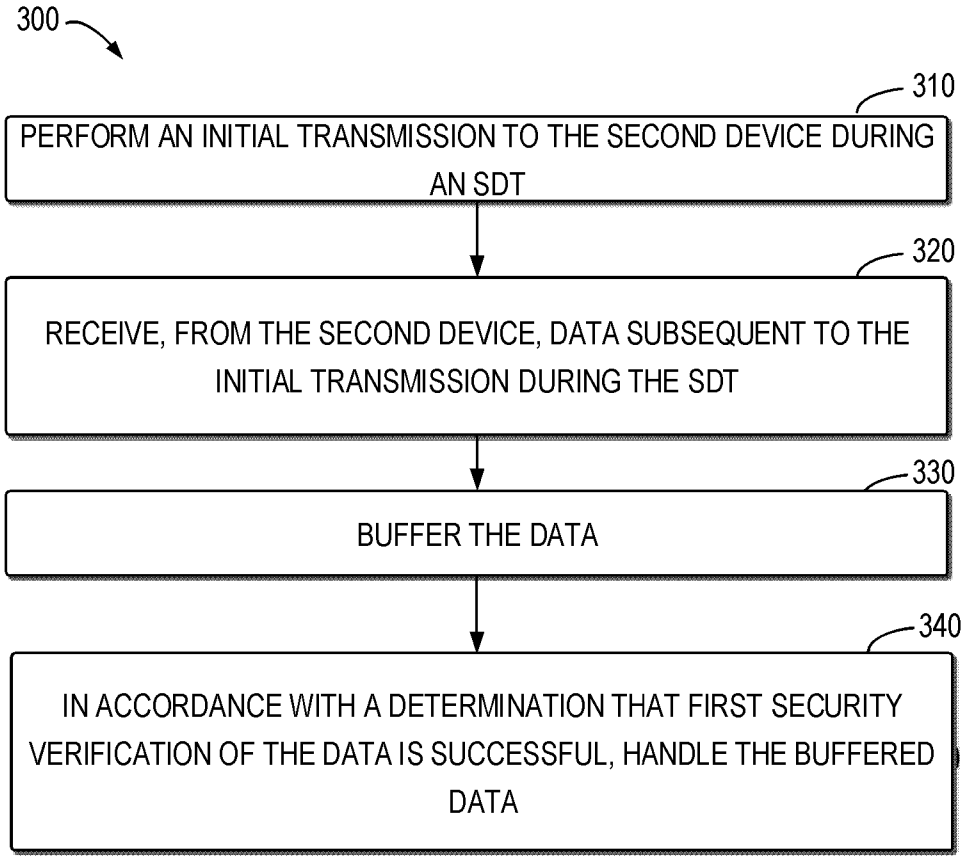
300
310
PERFORM AN INITIAL TRANSMISSION TO THE SECOND DEVICE DURING AN SDT
320
RECEIVE, FROM THE SECOND DEVICE, DATA SUBSEQUENT TO THE INITIAL TRANSMISSION DURING THE SDT
330
BUFFER THE DATA
340
IN ACCORDANCE WITH A DETERMINATION THAT FIRST SECURITY VERIFICATION OF THE DATA IS SUCCESSFUL, HANDLE THE BUFFERED DATA

Fig. 3

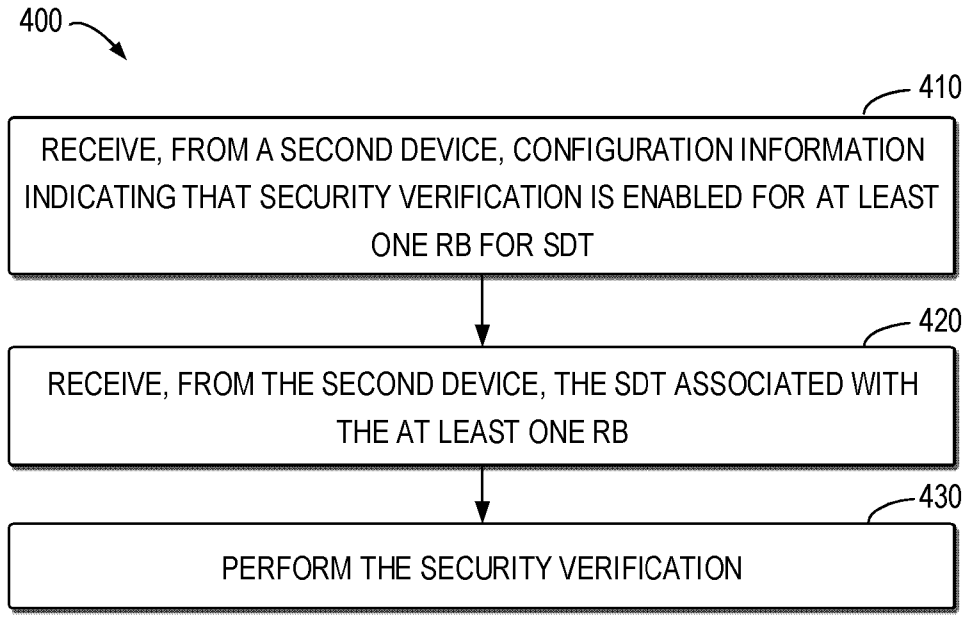
400
410
RECEIVE, FROM A SECOND DEVICE, CONFIGURATION INFORMATION INDICATING THAT SECURITY VERIFICATION IS ENABLED FOR AT LEAST ONE RB FOR SDT
420
RECEIVE, FROM THE SECOND DEVICE, THE SDT ASSOCIATED WITH THE AT LEAST ONE RB
430
PERFORM THE SECURITY VERIFICATION

Fig. 4

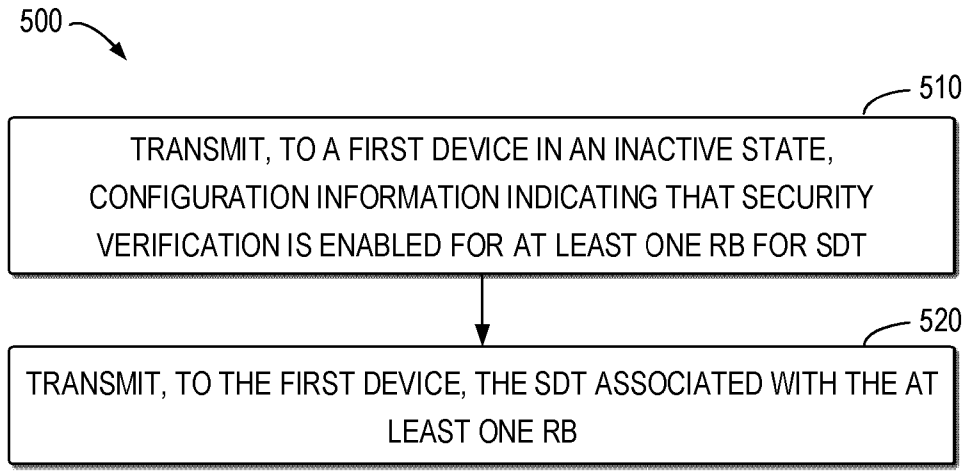
500
510
TRANSMIT, TO A FIRST DEVICE IN AN INACTIVE STATE, CONFIGURATION INFORMATION INDICATING THAT SECURITY VERIFICATION IS ENABLED FOR AT LEAST ONE RB FOR SDT
520
TRANSMIT, TO THE FIRST DEVICE, THE SDT ASSOCIATED WITH THE AT LEAST ONE RB

Fig. 5

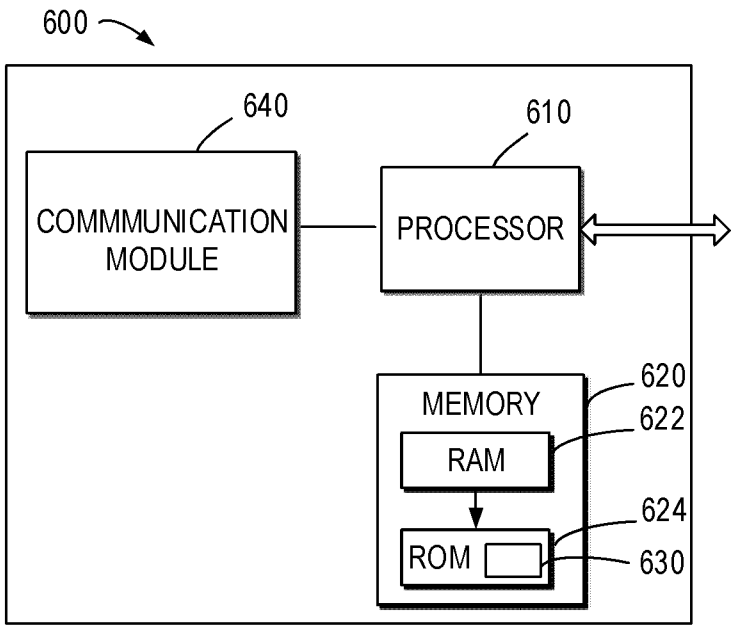
600
640
610
COMMMUNICATION MODULE
PROCESSOR
MEMORY
620
622
RAM
624
ROM
630

Fig. 6

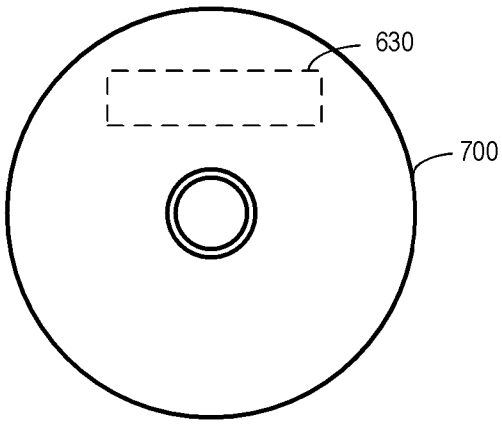
630
700

Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/101579

A. CLASSIFICATION OF SUBJECT MATTER

H04W 74/08(2009.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; H04L

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

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

CNPAT, WPI, EPODOC, CNKI, 3GPP: SDT, small data transmission, security, verification, inactive, state

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	VIVO. "Discussion on the Security for Small Data Transmission" *3GPP TSG-RAN WG2 Meeting #112-electronic, R2-2008958,* 13 November 2020 (2020-11-13), pages 1-3	1-25
A	INTEL CORPORATION. "Security aspects for SDT" *3GPP TSG-RAN WG2 Meeting #112-e, R2-2008992,* 13 November 2020 (2020-11-13), the whole document	1-25
A	CN 112913315 A (QUALCOMM INCORPORATED) 04 June 2021 (2021-06-04) the whole document	1-25
A	US 2018227962 A1 (MOTOROLA MOBILITY LLC) 09 August 2018 (2018-08-09) the whole document	1-25

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

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 February 2022	**25 February 2022**
Name and mailing address of the ISA/CN **National Intellectual Property Administration, PRC** **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing** **100088, China** Facsimile No. **(86-10)62019451**	Authorized officer **ZHANG,Pan** Telephone No. **86-(10)-53961577**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/101579

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 112913315 A	04 June 2021	EP 3874895 A1	08 September 2021
		WO 2020087280 A1	07 May 2020
		US 2021337602 A1	28 October 2021
		WO 2020088097 A1	07 May 2020
US 2018227962 A1	09 August 2018	WO 2018145037 A1	09 August 2018
		CN 110169194 A	23 August 2019
		US 2020084824 A1	12 March 2020
		US 2018227961 A1	09 August 2018
		EP 3578003 A1	11 December 2019