



(51) International Patent Classification:
H04W 72/20 (2023.01)

(21) International Application Number:
PCT/CN2024/072336

(22) International Filing Date:
15 January 2024 (15.01.2024)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **LENOVO (BEIJING) LIMITED** [CN/CN]; 6 Shangdi West Road, Haidian District, Beijing 100085 (CN).

(72) Inventors: **LEI, Haipeng**; Lenovo HQ East, Building No.1, No.10 Xibeiwang East Road, Haidian District, Beijing 100094 (CN). **YU, Xiaodong**; Lenovo HQ East, Building No.1, No.10 Xibeiwang East Road, Haidian District, Beijing 100094 (CN). **SUN, Zhennian**; Lenovo HQ East, Building No.1, No.10 Xibeiwang East Road, Haidian District, Beijing 100094 (CN). **GUO, Xin**; Lenovo HQ East, Building No.1, No.10 Xibeiwang East Road, Haidian District, Beijing 100094 (CN).

(74) Agent: **LEE AND LI - LEAVEN IPR AGENCY LTD.**; Unit 2202, Tower A, Beijing Pudi Hotel, No. 7, Jian Guo

Men South Avenue, Dongcheng District, Beijing 100005 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: METHODS AND APPARATUSES FOR DOWNLINK AND UPLINK TRANSMISSION FOR AMBIENT INTERNET OF THINGS (IOT) COMMUNICATION

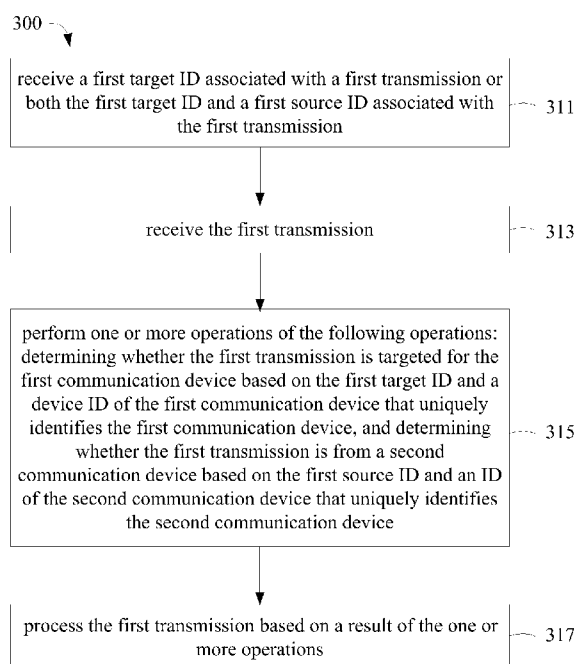


FIG. 3

(57) Abstract: Embodiments of the present disclosure relate to method and apparatus for downlink and uplink transmission for ambient IoT communication. A first communication device may: receive a first target ID associated with a first transmission or both the first target ID and a first source ID associated with the first transmission; receive the first transmission; perform one or more operations of the following operations: determining whether the first transmission is targeted for the first communication device based on the first target ID and a device ID of the first communication device, and determining whether the first transmission is from a second communication device based on the first source ID and an ID of the second communication device; and process the first transmission based on a result of the one or more operations.

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*
- *upon request of the applicant, before the expiration of the time limit referred to in Article 21(2)(a)*

METHODS AND APPARATUSES FOR DOWNLINK AND UPLINK TRANSMISSION FOR AMBIENT INTERNET OF THINGS (IOT) COMMUNICATION

TECHNICAL FIELD

[0001] Embodiments of the present disclosure generally relate to wireless communication technology, and more particularly to Internet of Things (IoT) technology.

BACKGROUND

[0002] A wireless communication system may include one or multiple network communication devices, such as base stations, which may support wireless communication for one or multiple user communication devices, which may be otherwise known as user equipment (UE), or other suitable terminology. The wireless communication system may support wireless communication with one or multiple user communication devices by utilizing resources of the wireless communication system (e.g., time resources (e.g., symbols, slots, subframes, frames, or the like)) or frequency resources (e.g., subcarriers, carriers, or the like). Additionally, the wireless communication system may support wireless communication across various radio access technologies including third generation (3G) radio access technology, fourth generation (4G) radio access technology, fifth generation (5G) (which is also known as new radio (NR)) radio access technology, among other suitable radio access technologies beyond 5G (e.g., sixth generation (6G)).

SUMMARY

[0003] An article “a” before an element is unrestricted and understood to refer to “at least one” of those elements or “one or more” of those elements. The terms “a,” “at least one,” “one or more,” and “at least one of one or more” may be interchangeable. As used herein, including in the claims, “or” as used in a list of items (e.g., a list of

items prefaced by a phrase such as “at least one of” or “one or more of” or “one or both of”) indicates an inclusive list such that, for example, a list of at least one of A, B, or C means A or B or C or AB or AC or BC or ABC (i.e., A and B and C). Also, as used herein, the phrase “based on” shall not be construed as a reference to a closed set of conditions. For example, an example step that is described as “based on condition A” may be based on both a condition A and a condition B without departing from the scope of the present disclosure. In other words, as used herein, the phrase “based on” shall be construed in the same manner as the phrase “based at least in part on.” Further, as used herein, including in the claims, a “set” may include one or more elements.

[0004] Some embodiments of the present disclosure provide a first communication device. The first communication device may include at least one transmitter; at least one receiver; and at least one processor coupled with the at least one transmitter and the at least one receiver and configured to cause the first communication device to: receive a first target ID associated with a first transmission or both the first target ID and a first source ID associated with the first transmission; receive the first transmission; perform one or more operations of the following operations: determining whether the first transmission is targeted for the first communication device based on the first target ID and a device ID of the first communication device that uniquely identifies the first communication device, and determining whether the first transmission is from a second communication device based on the first source ID and an ID of the second communication device that uniquely identifies the second communication device; and process the first transmission based on a result of the one or more operations.

[0005] In some embodiments, the first target ID is independently encoded within the first transmission. In some embodiments, the first target ID is jointly encoded with control information associated with the first transmission and is received in physical layer signaling. In some embodiments, the first target ID is jointly encoded with data carried by the first transmission and is received in high layer signaling. In some embodiments, the first target ID is used to scramble cyclic redundancy check (CRC) bits for control information associated with the first transmission. In some embodiments, the first target ID is included in control information associated with the first transmission.

[0006] In some embodiments, the first source ID is independently encoded within the first transmission. In some embodiments, the first source ID is jointly encoded with control information associated with the first transmission and is received in physical layer signaling. In some embodiments, the first source ID is jointly encoded with data carried by the first transmission and is received in high layer signaling. In some embodiments, the first source ID is included in control information associated with the first transmission. In some embodiments, the first source ID is used to scramble CRC bits for control information associated with the first transmission.

[0007] In some embodiments, the at least one processor is further configured to cause the first communication device to receive a temporary ID for the first communication device assigned by a network, a serving base station, or the second communication device.

[0008] In some embodiments, the at least one processor is further configured to cause the first communication device to: receive control information associated with the first transmission; and determine whether the first transmission is targeted for the first communication device based on a temporary ID of the first communication device and CRC bits for the control information associated with the first transmission.

[0009] In some embodiments, the at least one processor is further configured to cause the first communication device to receive control information associated with the first transmission, wherein CRC bits for the control information are scrambled by a temporary ID for a target device of the first transmission or by a sequence common to devices within a same cell or a same network as the target device.

[0010] In some embodiments, the at least one processor is further configured to cause the first communication device to: transmit, to the second communication device, a second source ID associated with a second transmission or both the second source ID and a second target ID associated with the second transmission, wherein the second source ID is set to the device ID of the first communication device and the second target ID is set to the ID of the second communication device; and transmit, to the second communication device, the second transmission.

[0011] In some embodiments, the second source ID is independently encoded within

the second transmission. In some embodiments, the second source ID is jointly encoded with control information associated with the second transmission and is transmitted in physical layer signaling. In some embodiments, the second source ID is jointly encoded with data carried by the second transmission and is transmitted in high layer signaling. In some embodiments, the second source ID is used to scramble CRC bits for control information associated with the second transmission. In some embodiments, the second source ID is included in control information with the second transmission.

[0012] In some embodiments, the second target ID is independently encoded within the second transmission. In some embodiments, the second target ID is jointly encoded with control information associated with the second transmission and is transmitted in physical layer signaling. In some embodiments, the second target ID is jointly encoded with data carried by the second transmission and is transmitted in high layer signaling. In some embodiments, the second target ID is included in control information associated with the second transmission. In some embodiments, the second target ID is used to scramble CRC bits for control information associated with the second transmission.

[0013] In some embodiments, the at least one processor is further configured to cause the first communication device to transmit control information associated with the second transmission, wherein CRC bits for the control information are scrambled by a temporary ID for the first communication device assigned by a network, a serving base station, or the second communication device, or scrambled by a sequence common to devices within a same cell or a same network as the first communication device.

[0014] In some embodiments, the first transmission further includes CRC bits for the independently encoded first target ID, CRC bits for the independently encoded first source ID, or both.

[0015] In some embodiments, the second transmission further includes CRC bits for the independently encoded second source ID, CRC bits for the independently encoded second target ID, or both.

[0016] In some embodiments, the at least one processor is further configured to cause

the first communication device to drop the first transmission in response to determining that the first transmission is not targeted for the first communication device or the first transmission is not from the second communication device.

[0017] In some embodiments, the first communication device is an ambient IoT device.

[0018] Some embodiments of the present disclosure provide a second communication device. The second communication device may include at least one transmitter; at least one receiver; and at least one processor coupled with the at least one transmitter and the at least one receiver, and configured to cause the second communication device to: transmit, to a first communication device, a first target ID associated with a first transmission or both the first target ID and a first source ID associated with the first transmission, wherein the first target ID is set to an ID of the first communication device that uniquely identifies the first communication device and the first source ID is set to an ID of the second communication device that uniquely identifies the second communication device; and transmit, to the first communication device, the first transmission.

[0019] In some embodiments, the first target ID is independently encoded within the first transmission. In some embodiments, the first target ID is jointly encoded with control information associated with the first transmission and is transmitted in physical layer signaling. In some embodiments, the first target ID is jointly encoded with data carried by the first transmission and is transmitted in high layer signaling. In some embodiments, the first target ID is used to scramble CRC bits for control information associated with the first transmission. In some embodiments, the first target ID is included in control information associated with the first transmission.

[0020] In some embodiments, the first source ID is independently encoded within the first transmission. In some embodiments, the first source ID is jointly encoded with control information associated with the first transmission and is transmitted in physical layer signaling. In some embodiments, the first source ID is jointly encoded with data carried by the first transmission and is transmitted in high layer signaling. In some embodiments, the first source ID is included in control information associated with the first transmission. In some embodiments, the first source ID is used to scramble CRC

bits for control information associated with the first transmission.

[0021] In some embodiments, the at least one processor is further configured to cause the second communication device to transmit, to the first communication device, a temporary ID for the first communication device.

[0022] In some embodiments, the at least one processor is further configured to cause the second communication device to transmit control information associated with the first transmission, wherein CRC bits for the control information are scrambled by the temporary ID for the first communication device or by a sequence common to devices within a same cell or a same network as the first communication device.

[0023] In some embodiments, the at least one processor is further configured to cause the second communication device to: receive a second source ID associated with a second transmission or both the second source ID and a second target ID associated with the second transmission; receive the second transmission; perform one or more operations of the following operations: determining whether the second transmission is from the first communication device based on the second source ID and the ID of the first communication device, and determining whether the second transmission is targeted for the second communication device based on the second target ID and the ID of the second communication device; and process the second transmission based on a result of the one or more operations.

[0024] In some embodiments, the second source ID is independently encoded within the second transmission. In some embodiments, the second source ID is jointly encoded with control information associated with the second transmission and is received in physical layer signaling. In some embodiments, the second source ID is jointly encoded with data carried by the second transmission and is received in high layer signaling. In some embodiments, the second source ID is used to scramble CRC bits for control information associated with the second transmission. In some embodiments, the second source ID is included in control information with the second transmission.

[0025] In some embodiments, the second target ID is independently encoded within the second transmission. In some embodiments, the second target ID is jointly

encoded with control information associated with the second transmission and is received in physical layer signaling. In some embodiments, the second target ID is jointly encoded with data carried by the second transmission and is received in high layer signaling. In some embodiments, the second target ID is included in control information associated with the second transmission. In some embodiments, the second target ID is used to scramble CRC bits for control information associated with the second transmission.

[0026] In some embodiments, the at least one processor is further configured to cause the second communication device to: receive control information associated with the second transmission; and determine whether the second transmission is from the first communication device based on a temporary ID for the first communication device and CRC bits for the control information associated with the second transmission.

[0027] In some embodiments, the at least one processor is further configured to cause the second communication device to receive control information associated with the second transmission, wherein CRC bits for the control information are scrambled by a temporary ID for a device transmitting the second transmission or by a sequence common to devices within a same cell or a same network as the device transmitting the second transmission.

[0028] In some embodiments, the first transmission further includes CRC bits for the independently encoded first target ID, CRC bits for the independently encoded first source ID, or both.

[0029] In some embodiments, the second transmission further includes CRC bits for the independently encoded second source ID, CRC bits for the independently encoded second target ID, or both.

[0030] In some embodiments, the at least one processor is further configured to cause the second communication device to drop the second transmission in response to determining that the second transmission is not from the first communication device or the second transmission is not targeted for the second communication device.

[0031] In some embodiments, the second communication device is a base station, a

UE, a relay node, an integrated access and backhaul (IAB) node, a wireless access backhaul (WAB) network, a repeater, or a UE-type reader.

[0032] Some embodiments of the present disclosure provide a processor. The processor may include at least one controller coupled with at least one memory and configured to cause the processor to: receive a first target ID associated with a first transmission or both the first target ID and a first source ID associated with the first transmission; receive the first transmission; perform one or more operations of the following operations: determining whether the first transmission is targeted for the first communication device based on the first target ID and a device ID of the first communication device that uniquely identifies the first communication device, and determining whether the first transmission is from a second communication device based on the first source ID and an ID of the second communication device that uniquely identifies the second communication device; and process the first transmission based on a result of the one or more operations.

[0033] Some embodiments of the present disclosure provide a processor. The processor may include at least one controller coupled with at least one memory and configured to cause the processor to: transmit, to a first communication device, a first target ID associated with a first transmission or both the first target ID and a first source ID associated with the first transmission, wherein the first target ID is set to an ID of the first communication device that uniquely identifies the first communication device and the first source ID is set to an ID of a second communication device that uniquely identifies the second communication device; and transmit, to the first communication device, the first transmission.

[0034] Some embodiments of the present disclosure provide a method for wireless communication. The method may include: receiving a first target ID associated with a first transmission or both the first target ID and a first source ID associated with the first transmission; receiving the first transmission; performing one or more operations of the following operations: determining whether the first transmission is targeted for a first communication device based on the first target ID and a device ID of the first communication device that uniquely identifies the first communication device, and determining whether the first transmission is from a second communication device

based on the first source ID and an ID of the second communication device that uniquely identifies the second communication device; and processing the first transmission based on a result of the one or more operations.

[0035] Some embodiments of the present disclosure provide a method for wireless communication. The method may include: transmitting, to a first communication device, a first target ID associated with a first transmission or both the first target ID and a first source ID associated with the first transmission, wherein the first target ID is set to an ID of the first communication device that uniquely identifies the first communication device and the first source ID is set to an ID of a second communication device that uniquely identifies the second communication device; and transmitting, to the first communication device, the first transmission.

[0036] Some embodiments of the present disclosure provide an apparatus. According to some embodiments of the present disclosure, the apparatus may include: at least one non-transitory computer-readable medium having stored thereon computer-executable instructions; at least one receiving circuitry; at least one transmitting circuitry; and at least one processor coupled to the at least one non-transitory computer-readable medium, the at least one receiving circuitry and the at least one transmitting circuitry, wherein the at least one non-transitory computer-readable medium and the computer executable instructions may be configured to, with the at least one processor, cause the apparatus to perform a method according to some embodiments of the present disclosure.

BRIEF DESCRIPTION OF THE DRAWINGS

[0037] In order to describe the manner in which the advantages and features of the disclosure can be obtained, a description of the disclosure is rendered by reference to specific embodiments thereof, which are illustrated in the appended drawings. These drawings depict only exemplary embodiments of the disclosure and are not therefore to be considered limiting of its scope.

[0038] FIG. 1 illustrates a schematic diagram of a wireless communication system in accordance with some embodiments of the present disclosure;

[0039] FIGs. 2A-2E illustrate exemplary topologies for IoT networks and devices in accordance with some embodiments of the present disclosure;

[0040] FIGs. 3 and 4 illustrate flowcharts of IoT communication methods in accordance with some embodiments of the present disclosure;

[0041] FIG. 5 illustrates a block diagram of exemplary apparatus in accordance with some embodiments of the present disclosure;

[0042] FIG. 6 illustrates an example of a UE in accordance with some embodiments of the present disclosure;

[0043] FIG. 7 illustrates an example of a processor in accordance with some embodiments of the present disclosure; and

[0044] FIG. 8 illustrates an example of a network equipment (NE) in accordance with some embodiments of the present disclosure.

DETAILED DESCRIPTION

[0045] The detailed description of the appended drawings is intended as a description of the preferred embodiments of the present disclosure and is not intended to represent the only form in which the present disclosure may be practiced. It should be understood that the same or equivalent functions may be accomplished by different embodiments that are intended to be encompassed within the spirit and scope of the present disclosure.

[0046] Reference will now be made in detail to some embodiments of the present disclosure, examples of which are illustrated in the accompanying drawings. To facilitate understanding, embodiments are provided under a specific network architecture(s) and new service scenarios, such as the 3rd generation partnership project (3GPP) 5G NR or 6G, 3GPP LTE, and so on. It is contemplated that along with the developments of network architectures and new service scenarios, all embodiments in the present disclosure are also applicable to similar technical problems; and moreover, the terminologies recited in the present disclosure may change, which should not affect

the principles of the present disclosure.

[0047] In recent years, IoT has attracted much attention in the wireless communication world. It is expected that further reductions of size, complexity, and power consumption of IoT devices can enable the deployment of tens or even hundreds of billions of IoT devices for various applications and provide added value across the entire value chain. However, existing technologies cannot meet all the requirements of target use cases.

[0048] As used herein, the term "ambient IoT device" or "A-IoT device" can refer to a device without batteries or with limited energy storage capabilities. For an A-IoT device, energy can be provided by harvesting radio waves, light, motion, heat, or any other suitable source. A-IoT device can also be called a zero-power terminal, a near-zero power terminal, a passive IoT device, an ambient backscatter communication (AmBC) device, tag, etc. Compared with low-power and wide-coverage services, such as narrow band (NB) IoT, enhanced machine type communication (eMTC), A-IoT is to be designed with ultra-low complexity and ultra-low power consumption, and is orders of magnitude lower than the existing 3GPP technologies. Hence, it is suitable for more application scenarios.

[0049] The present disclosure provides various methods and apparatuses for ambient IoT communication. For example, embodiments of the present disclosure provide methods for transmitting DL data or UL scheduling as well as UL data for (ambient) IoT applications. The proposed methods and apparatuses can address use cases and scenarios that cannot otherwise be fulfilled based on existing 3GPP technologies

[0050] FIG. 1 illustrates a schematic diagram of wireless communication system 100 in accordance with some embodiments of the present disclosure.

[0051] The wireless communication system 100 may include one or more NEs 102 (e.g., one or more BSs), one or more UEs 104, and a core network (CN) 106. The wireless communication system 100 may support various radio access technologies. In some implementations, the wireless communication system 100 may be a 4G network, such as an LTE network or an LTE-Advanced (LTE-A) network. In some other implementations, the wireless communication system 100 may be a NR network,

such as a 5G network, a 5G-Advanced (5G-A) network, or a 5G ultra-wideband (5G-UWB) network. In other implementations, the wireless communication system 100 may be a combination of a 4G network and a 5G network, or other suitable radio access technology including Institute of Electrical and Electronics Engineers (IEEE) 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), and IEEE 802.20. The wireless communication system 100 may support radio access technologies beyond 5G, for example, 6G. Additionally, the wireless communication system 100 may support technologies, such as time division multiple access (TDMA), frequency division multiple access (FDMA), or code division multiple access (CDMA), etc.

[0052] The one or more NEs 102 may be dispersed throughout a geographic region to form the wireless communication system 100. One or more of the NEs 102 described herein may be or include or may be referred to as a network node, a base station, a network element, a network function, a network entity, a radio access network (RAN), a NodeB, an eNodeB (eNB), a next-generation NodeB (gNB), or other suitable terminology. An NE 102 and a UE 104 may communicate via a communication link, which may be a wireless or wired connection. For example, an NE 102 and a UE 104 may perform wireless communication (e.g., receive signaling, transmit signaling) over a Uu interface.

[0053] An NE 102 may provide a geographic coverage area for which the NE 102 may support services for one or more UEs 104 within the geographic coverage area. For example, an NE 102 and a UE 104 may support wireless communication of signals related to services (e.g., voice, video, packet data, messaging, broadcast, etc.) according to one or multiple radio access technologies. In some implementations, an NE 102 may be moveable, for example, a satellite associated with a non-terrestrial network (NTN). In some implementations, different geographic coverage areas 112 associated with the same or different radio access technologies may overlap, but the different geographic coverage areas may be associated with a different NE 102.

[0054] The one or more UEs 104 may be dispersed throughout a geographic region of the wireless communication system 100. A UE 104 may include or may be referred to as a remote unit, a mobile device, a wireless device, a remote device, a subscriber device, a transmitter device, a receiver device, or some other suitable terminology. In

some implementations, the UE 104 may be referred to as a unit, a station, a terminal, or a client, among other examples. Additionally, or alternatively, the UE 104 may be referred to as an Internet-of-Things (IoT) device, an Internet-of-Everything (IoE) device, or machine-type communication (MTC) device, among other examples.

[0055] A UE 104 may be able to support wireless communication directly with other UEs 104 over a communication link. For example, a UE 104 may support wireless communication directly with another UE 104 over a device-to-device (D2D) communication link. In some implementations, such as vehicle-to-vehicle (V2V) deployments, vehicle-to-everything (V2X) deployments, or cellular-V2X deployments, the communication link 114 may be referred to as a sidelink. For example, a UE 104 may support wireless communication directly with another UE 104 over a PC5 interface.

[0056] An NE 102 may support communication with the CN 106, or with another NE 102, or both. For example, an NE 102 may interface with another NE 102 or the CN 106 through one or more backhaul links (e.g., S1, N2, N3 or another network interface). In some implementations, the NE 102 may communicate with each other directly. In some other implementations, the NE 102 may communicate with each other or indirectly (e.g., via the CN 106). In some implementations, one or more NEs 102 may include subcomponents, such as an access network entity, which may be an example of an access node controller (ANC). An ANC may communicate with the one or more UEs 104 through one or more other access network transmission entities, which may be referred to as radio heads, smart radio heads, or transmission-reception points (TRPs).

[0057] The CN 106 may support user authentication, access authorization, tracking, connectivity, and other access, routing, or mobility functions. The CN 106 may be an evolved packet core (EPC), or a 5G core (5GC), which may include a control plane entity that manages access and mobility (e.g., a mobility management entity (MME), an access and mobility management (AMF)) functions and a user plane entity that routes packets or interconnects to external networks (e.g., a serving gateway (S-GW), a Packet Data Network (PDN) gateway (P-GW), or a user plane function (UPF)). In some implementations, the control plane entity may manage non-access stratum (NAS) functions, such as mobility, authentication, and bearer management (e.g., data bearers,

signal bearers, etc.) for the one or more UEs 104 served by the one or more NEs 102 associated with the CN 106.

[0058] The CN 106 may communicate with a packet data network over one or more backhaul links (e.g., via an S1, N2, N3, or another network interface). The packet data network may include an application server. In some implementations, one or more UEs 104 may communicate with the application server. A UE 104 may establish a session (e.g., a protocol data unit (PDU) session, or the like) with the CN 106 via an NE 102. The CN 106 may route traffic (e.g., control information, data, and the like) between the UE 104 and the application server using the established session (e.g., the established PDU session). The PDU session may be an example of a logical connection between the UE 104 and the CN 106 (e.g., one or more network functions of the CN 106).

[0059] In the wireless communication system 100, the NEs 102 and the UEs 104 may use resources of the wireless communication system 100 (e.g., time resources (e.g., symbols, slots, subframes, frames, or the like) or frequency resources (e.g., subcarriers, carriers)) to perform various operations (e.g., wireless communication). In some implementations, the NEs 102 and the UEs 104 may support different resource structures. For example, the NEs 102 and the UEs 104 may support different frame structures. In some implementations, such as in 4G, the NEs 102 and the UEs 104 may support a single frame structure. In some other implementations, such as in 5G and among other suitable radio access technologies, the NEs 102 and the UEs 104 may support various frame structures (i.e., multiple frame structures). The NEs 102 and the UEs 104 may support various frame structures based on one or more numerologies.

[0060] In some embodiments, the NEs 102 may include one or more relay nodes, integrated access and backhaul (IAB) nodes or wireless access backhaul (WAB) nodes which can provide wireless access services for UEs 104. A relay node (or an IAB node or a WAB node) can directly connect to a BS or hop through one or more relay nodes (or one or more IAB or WAB nodes) before reaching the BS.

[0061] One or more numerologies may be supported in the wireless communication system 100, and a numerology may include a subcarrier spacing and a cyclic prefix. A first numerology (e.g., $\mu=0$) may be associated with a first subcarrier spacing (e.g.,

15 kHz) and a normal cyclic prefix. In some implementations, the first numerology (e.g., $\mu=0$) associated with the first subcarrier spacing (e.g., 15 kHz) may utilize one slot per subframe. A second numerology (e.g., $\mu=1$) may be associated with a second subcarrier spacing (e.g., 30 kHz) and a normal cyclic prefix. A third numerology (e.g., $\mu=2$) may be associated with a third subcarrier spacing (e.g., 60 kHz) and a normal cyclic prefix or an extended cyclic prefix. A fourth numerology (e.g., $\mu=3$) may be associated with a fourth subcarrier spacing (e.g., 120 kHz) and a normal cyclic prefix. A fifth numerology (e.g., $\mu=4$) may be associated with a fifth subcarrier spacing (e.g., 240 kHz) and a normal cyclic prefix. A sixth numerology (e.g., $\mu=5$) may be associated with a sixth subcarrier spacing (e.g., 480 kHz) and a normal cyclic prefix. A seventh numerology (e.g., $\mu=6$) may be associated with a seventh subcarrier spacing (e.g., 960 kHz) and a normal cyclic prefix. For ambient IoT communication, additional numerologies (e.g., $\mu=-1$ or $\mu=-2$) may be introduced corresponding to 7.5 kHz or 3.75 kHz respectively.

[0062] A time interval of a resource (e.g., a communication resource) may be organized according to frames (also referred to as radio frames). Each frame may have a duration, for example, a 10 millisecond (ms) duration. In some implementations, each frame may include multiple subframes. For example, each frame may include 10 subframes, and each subframe may have a duration, for example, a 1 ms duration. In some implementations, each frame may have the same duration. In some implementations, each subframe of a frame may have the same duration.

[0063] Additionally or alternatively, a time interval of a resource (e.g., a communication resource) may be organized according to slots. For example, a subframe may include a number (e.g., quantity) of slots. The number of slots in each subframe may also depend on the one or more numerologies supported in the wireless communication system 100. For instance, the first, second, third, fourth, and fifth numerologies (i.e., $\mu=0$, $\mu=1$, $\mu=2$, $\mu=3$, $\mu=4$) associated with respective subcarrier spacings of 15 kHz, 30 kHz, 60 kHz, 120 kHz, and 240 kHz may utilize a single slot per subframe, two slots per subframe, four slots per subframe, eight slots per subframe, and 16 slots per subframe, respectively. Each slot may include a number (e.g., quantity) of symbols (e.g., orthogonal frequency-division multiplexing (OFDM) symbols). In some implementations, the number (e.g., quantity) of slots for a

subframe may depend on a numerology. For a normal cyclic prefix, a slot may include 14 symbols. For an extended cyclic prefix (e.g., applicable for 60 kHz subcarrier spacing), a slot may include 12 symbols. The relationship between the number of symbols per slot, the number of slots per subframe, and the number of slots per frame for a normal cyclic prefix and an extended cyclic prefix may depend on a numerology. It should be understood that reference to a first numerology (e.g., $\mu=0$) associated with a first subcarrier spacing (e.g., 15 kHz) may be used interchangeably between subframes and slots.

[0064] In the wireless communication system 100, an electromagnetic (EM) spectrum may be split, based on frequency or wavelength, into various classes, frequency bands, frequency channels, etc. By way of example, the wireless communication system 100 may support one or multiple operating frequency bands, such as frequency range designations FR1 (410 MHz – 7.125 GHz), FR2 (24.25 GHz – 52.6 GHz), FR3 (7.125 GHz – 24.25 GHz), FR4 (52.6 GHz – 114.25 GHz), FR4a or FR4-1 (52.6 GHz – 71 GHz), and FR5 (114.25 GHz – 300 GHz). In some implementations, the NEs 102 and the UEs 104 may perform wireless communication over one or more of the operating frequency bands. In some implementations, FR1 may be used by the NEs 102 and the UEs 104, among other equipment or devices for cellular communication traffic (e.g., control information, data). In some implementations, FR2 may be used by the NEs 102 and the UEs 104, among other equipment or devices for short-range, high data rate capabilities.

[0065] FR1 may be associated with one or multiple numerologies (e.g., at least three numerologies). For example, FR1 may be associated with a first numerology (e.g., $\mu=0$), which includes 15 kHz subcarrier spacing; a second numerology (e.g., $\mu=1$), which includes 30 kHz subcarrier spacing; and a third numerology (e.g., $\mu=2$), which includes 60 kHz subcarrier spacing. FR2 may be associated with one or multiple numerologies (e.g., at least 2 numerologies). For example, FR2 may be associated with a third numerology (e.g., $\mu=2$), which includes 60 kHz subcarrier spacing; and a fourth numerology (e.g., $\mu=3$), which includes 120 kHz subcarrier spacing.

[0066] A UE 104 may include computing devices, such as desktop computers, laptop computers, personal digital assistants (PDAs), tablet computers, smart televisions (e.g.,

televisions connected to the Internet), set-top boxes, game consoles, security systems (including security cameras), vehicle on-board computers, network devices (e.g., routers, switches, and modems), or the like. According to some embodiments of the present disclosure, a UE 104 may include a portable wireless communication device, a smart phone, a cellular telephone, a flip phone, a device having a subscriber identity module, a personal computer, a selective call receiver, or any other device that is capable of sending and receiving communication signals on a wireless network. In some embodiments of the present disclosure, a UE 104 includes wearable devices, such as smart watches, fitness bands, optical head-mounted displays, or the like. Moreover, a UE 104 may be referred to as a subscriber unit, a mobile, a mobile station, a user, a terminal, a mobile terminal, a wireless terminal, a fixed terminal, a subscriber station, a user terminal, or a device, or described using other terminology used in the art. A UE 104 may communicate with an NE 102 (e.g., a BS) via UL (UL) communication signals. An NE 102 may communicate with a UE 104 via DL (DL) communication signals.

[0067] In some embodiments of the present disclosure, an NE 102 and a UE 104 may communicate over licensed spectrums, whereas in some other embodiments, an NE 102 and a UE 104 may communicate over unlicensed spectrums. The present disclosure is not intended to be limited to the implementation of any particular wireless communication system architecture or protocol. Persons skilled in the art should understand that as technology develops and advances, the terminologies described in the present disclosure may change, but should not affect or limit the principles and spirit of the present disclosure.

[0068] In recent years, IoT has attracted much attention in the wireless communication world. More "things" are expected to be interconnected to improve productivity efficiency and increasing comforts of life. It is expected that further reductions of size, complexity, and power consumption of IoT devices can enable the deployment of tens or even hundreds of billions of IoT devices for various applications and provide added value across the entire value chain. However, it is impossible to power all IoT devices by batteries that need to be replaced or recharged manually, which leads to high maintenance costs, serious environmental issues, and even safety hazards in some use cases (for example, wireless sensors in the electric power and

petroleum industries).

[0069] Most existing wireless communication devices are powered by batteries that need to be replaced or recharged manually. The automation and digitalization of various industries will open up numerous new markets requiring new IoT technologies supporting battery-less devices with no energy storage capability or devices with energy storage that do not need to be replaced or recharged manually. The form factors of such devices must be reasonably small to bring about the validity of target use cases. In some embodiments of the present disclosure, as will be described later, it is proposed that a capacitor may be used to support limited energy storage capability, and that the energy of such IoT devices is provided by the harvesting of radio waves, light, motion, heat, and/or any other power source(s) that may be deemed suitable.

[0070] Considering the limited size and complexity required by practical applications for battery-less devices with no energy storage capability or devices with limited energy storage that do not need to be replaced or recharged manually, the output power of an energy harvester may be typically from 1 μ W to a few hundreds μ W. Existing cellular devices may not work well with energy harvesting due to their peak power consumption of higher than 10 mW.

[0071] An example type of application is asset identification, which presently has to resort mainly to barcodes and RFID in most industries. The main advantage of these two technologies is their ultra-low complexity and small form factor of such tags. However, the limited reading range of a few meters usually requires handheld scanning which leads to labor intensive and time-consuming operations, or requires RFID portals/gates which leads to costly deployments. Moreover, the lack of an interference management scheme results in severe interference between RFID readers and capacity problems, especially in case of dense deployment. It is hard to support a large-scale network with seamless coverage of RFID.

[0072] Since existing technologies cannot meet all the requirements of target use cases, the present disclosure provides a new IoT technology to open up new markets within, for example, 3GPP systems, whose number of connections and/or device density can be orders of magnitude higher than existing IoT technologies. The new IoT technology can provide complexity and power consumption orders of magnitude lower

than the existing 3GPP low power wide area (LPWA) technologies (e.g., Narrow-Band IoT (NB-IoT) and enhanced machine type communication (eMTC)), and can address use cases and scenarios that cannot otherwise be fulfilled based on existing 3GPP LPWA IoT technologies.

[0073] FIGs. 2A-2E illustrate exemplary topologies for IoT networks and devices in accordance with some embodiments of the present disclosure. In these exemplary topologies, the ambient IoT device may be provided with a carrier wave from another node(s) either inside or outside the topology. The links in each topology may be bidirectional or unidirectional.

[0074] Although elements in each topology such as the BS, UE, assisting node, or intermediate node are described in the singular, the plural is also contemplated. The mixture of indoor and outdoor placements of such nodes is regarded as a network implementation choice. Consideration would need to be taken of potential impact on device or node complexity. In the connectivity topologies, this does not imply the existence of multi-hop assisting or intermediate nodes.

[0075] In FIG. 2A, an ambient IoT device can directly and bidirectionally communicate with a BS. The communication between the BS and the ambient IoT device includes ambient IoT data and/or signaling. This topology includes the possibility that the BS transmitting to the ambient IoT device is different than the BS receiving from the ambient IoT device.

[0076] In FIG. 2B, an ambient IoT device can communicate bidirectionally with an intermediate node between the IoT device and a BS. The intermediate node can be a relay, an IAB node, a WAB node, a UE, a repeater, a UE-type reader, etc. which is capable of ambient IoT. The intermediate node may transfer ambient IoT data and/or signaling between the BS and the ambient IoT device.

[0077] In FIG. 2C, an ambient IoT device can transmit data/signaling to a BS and can receive data/signaling from an assisting node (i.e., for DL assistance). The assisting node may receive the data/signaling from the BS. In this topology, the assisting node can be a relay, an IAB node, a WAB node, a UE, a repeater, a UE-type reader, etc. which is capable of ambient IoT.

[0078] In FIG. 2D, an ambient IoT device can receive data/signaling from a BS and can transmit data/signaling to the assisting node (i.e., for UL assistance). The assisting node may transmit the data/signaling to the BS. In this topology, the assisting node can be a relay, an IAB node, a WAB node, a UE, a repeater, a UE-type reader, etc. which is capable of ambient IoT.

[0079] In FIG. 2E, an ambient IoT device can communicate bidirectionally with a UE. The communication between the UE and the ambient IoT device includes ambient IoT data and/or signaling.

[0080] For the sake of convenience, in the context of the present disclosure, "DL transmission" can refer to the transmission from a BS, an intermediate node (e.g., an IAB node, a WAB node, a relay node, a UE, or a repeater), an assisting node (e.g., an IAB node, a WAB node, a relay node, a UE, or a repeater), or a UE-type reader (which is hereinafter referred to as a "sync source" for convenience) to an IoT device (e.g., a tag); and "UL transmission" can refer to the transmission from an IoT device (e.g., a tag) to a sync source (e.g., a BS, an intermediate node, an assisting node, or a UE-type reader).

[0081] Embodiments of the present disclosure provide various method for ambient IoT communication. For example, embodiments of the present disclosure provide methods for DL transmission (e.g., DL data, DL command or UL scheduling) and UL transmission (e.g., UL data) for (ambient) IoT applications. The proposed solutions can support ultra-low complexity and ultra-low power consumption for IoT (e.g., ambient IoT), simply the behavior of IoT devices, and can solve the aforementioned issues. More details on the embodiments of the present disclosure will be illustrated in the following text in combination with the appended drawings. For convenience, some embodiments of the present disclosure may be described with respect to ambient IoT or ambient IoT devices (e.g., an ambient IoT tag), and it should be appreciated by persons skilled in the art that these embodiments can also be applied to other IoT devices.

[0082] In some embodiments of the present disclosure, an IoT device (e.g., an ambient IoT tag) can be identified by a device ID (e.g., a tag ID) assigned by, for example, the manufacturer, factory, vendor, or network operator. In some examples, the IoT device

ID may be a unique ID within the cellular network of a given operator. The IoT device ID may be stored in the memory of the device and not changeable during future use. When the network intends to page an IoT device, or trigger an IoT device to feed back its data, location or other message (which can be stored in a memory), the network can indicate the IoT device ID in, for example, the paging or triggering signaling to uniquely identify this IoT device. In some examples, the IoT device ID may include 16 bits, 24 bits or 32 bits or other number of bits. In some examples, the IoT device ID can be shortened to, for example, 8, 10, 12, or 16 bits for overhead reduction where, for example, tag ID collision happens infrequently. As will be described later, such IoT device ID may be employed for IoT communication.

[0083] In some embodiments of the present disclosure, an energy harvester of an IoT device firstly collects energy from the environment (e.g., RF, solar, kinetics, and so on) by, for example, converting the forms of energy into electric energy. This may take for a period of time until the harvested energy is sufficient to wake up the processing module of the IoT device. Then, the IoT device may detect a DL synchronization signal within a time window with a predefined length to complete a DL synchronization procedure. The IoT device may then receive system information such as master information block (MIB) and system information block (SIB). The synchronization source which the IoT device is connecting with may be a BS, an intermediate node (e.g., an IAB node, a WAB node, a relay node, a UE, a repeater), an assisting node (e.g., an IAB node, a WAB node, a relay node, a UE, a repeater), or a UE-type reader (i.e., a sync source).

[0084] In some embodiments of the present disclosure, the sync source may have an ID that can be used to identify the sync source. For example, in the case that the sync source is a BS, the ID of the sync source can be a cell ID of the BS; in the case that the sync source is an intermediate node, an assisting node, or a UE-type reader, the ID the sync source can be assigned by the network where the intermediate node, the assisting node, or the UE-type reader is located, or by a BS (e.g., a serving BS) where the intermediate node, the assisting node, or the UE-type reader is located.

[0085] In some embodiments, the ID of a sync source may be broadcast when, for example, the sync source transmits a synchronization signal. The ID of a sync source

may be known to all the IoT devices (e.g., ambient IoT devices) in communication with the sync source. In some embodiments, when an IoT device is triggered for location reporting, the device can report the ID of the sync source as its finer location to the network. In some embodiments, this sync source ID can be shortened to, for example, 2, 3, 4, 8, or 10 bits for overhead reduction where, for example, ID collision happens infrequently. As will be described later, the sync source ID may be employed for IoT communication.

[0086] In some embodiments, in response to (e.g., after) receiving the system information from a sync source, an IoT device can receive a DL transmission (e.g., DL data, DL command or UL scheduling) from the sync source or transmit a UL transmission (e.g., UL data) to the sync source.

[0087] In some embodiments of the present disclosure, the ID of the IoT device and/or the ID of the sync source may be indicated for either the DL transmission or the UL transmission. For example, a transmitter (e.g., an IoT device or a sync source) may transmit a target ID and a source ID associated with a transmission (e.g., UL or DL transmission), wherein the target ID can be set to the ID of a desired receiver (e.g., a sync source or an IoT device) and the source ID can be set to the ID of the transmitter (e.g., an IoT device or a sync source). A receiver (e.g., a sync source or an IoT device) which receives this transmission can determine whether the transmission is targeted for it based on the target ID associated with the transmission and its own ID. The receiver can determine whether the transmission is from a desired transmitter based on the source ID associated with the transmission and the ID of the desired transmitter. Then, the receiver can act accordingly based on the determination. As will be described later, various methods may be employed for indicating or transmitting the IoT device ID and/or the sync source ID.

[0088] In some embodiments, the ID of an IoT device or the ID of a sync source may be explicitly indicated, for example, encoded within a corresponding transmission or encoded with control information or data associated with the corresponding transmission.

[0089] For a DL transmission, the ID of the target (e.g., a target IoT device) of the DL transmission is indicated so that any IoT device can easily identify whether this DL

transmission aims at itself. For a given IoT device, it may monitor the DL transmission and determine whether the DL transmission is targeted for it based on the target ID associated with the DL transmission and its own device ID (which may be stored in the memory of the IoT device). For example, the IoT device may detect the target ID associated with the DL transmission and compare the detected target ID with its own device ID. If the detected target ID matches (e.g., is equal to) its own device ID, the IoT device may process the DL transmission. For example, the IoT device may decode the data or control information carried by the DL transmission. Otherwise, if the detected target ID does not match its own device ID, the IoT device may drop the DL transmission and not process it so as to avoid unnecessary effort on decoding of DL data, DL control or UL scheduling signaling which is not targeted for the current IoT device and save power consumption.

[0090] For a DL transmission, the ID of the source (e.g., a sync source) of the DL transmission is indicated so that any IoT device can easily identify whether the DL transmission is sent from a desired sync source. For a given IoT device, it may monitor the DL transmission and determine whether the DL transmission is sent from the desired sync source based on the source ID associated with the DL transmission and the ID of the desired sync source (which may be stored in the memory of the IoT device). For example, the IoT device may detect the source ID associated with the DL transmission and compare the detected source ID with its desired sync source ID. If the detected source ID matches (e.g., is equal to) the desired sync source ID, the IoT device may process the DL transmission. For example, the IoT device may decode the data or control information carried by the DL transmission. Otherwise, if the detected source ID does not match the desired sync source ID, the IoT device may drop the DL transmission and not process it so as to avoid unnecessary effort on decoding of DL data, DL control or UL scheduling signaling which is not transmitted from desired sync source and save power consumption.

[0091] In some embodiments, an IoT device may process the DL transmission when it determines that the DL transmission is targeted for it and is sent from a desired sync source. Otherwise, the IoT device may drop the DL transmission.

[0092] Various methods may be employed for indicating or transmitting the target ID

(e.g., an IoT device ID) and the source ID (e.g., a sync source ID) associated with a DL transmission.

[0093] For example, in some embodiments, the target ID (e.g., an IoT device ID) associated with the DL transmission may be independently encoded within the DL transmission. For example, the ID is self-decodable and not jointly encoded with other data or control information (e.g., physical layer control information). In this way, any IoT device can easily and quickly decode the ID and further determine whether the DL transmission aims at the device itself.

[0094] In some embodiments, CRC bits may be generated for the target ID (e.g., an IoT device ID) associated with the DL transmission, to avoid a false alarm issue and/or a lost alarm issue. For example, 16-bit CRC or 24-bit CRC may be generated. In some examples, the ID and the CRC bits can be transmitted simultaneously, for example, both included in the DL transmission. In some other examples, the DL transmission may not include the CRC bits for the target ID. In some embodiments, to improve transmission reliability of the target ID, the target ID, the corresponding CRC bits or both can be repeatedly transmitted. For example, the DL transmission may include one or more repetitions of the target ID, the corresponding CRC bits or both.

[0095] In some embodiments, the source ID (e.g., a sync source ID) associated with the DL transmission may be independently encoded within the DL transmission. For example, the ID is self-decodable and not jointly encoded with other data or control information (e.g., physical layer control information). In this way, any IoT device can easily and quickly decode the ID and further determine whether the DL transmission is from a desired sync source.

[0096] In some embodiments, CRC bits may be generated for the source ID (e.g., a sync source ID) associated with the DL transmission, to avoid a false alarm issue and/or a lost alarm issue. For example, 16-bit CRC or 24-bit CRC may be generated. In some examples, the ID and the CRC bits can be transmitted simultaneously, for example, both included in the DL transmission. In some other examples, the DL transmission may not include the CRC bits for the source ID. In some embodiments, to improve transmission reliability of the source ID, the source ID, the corresponding CRC bits or both can be repeatedly transmitted. For example, the DL transmission may include

one or more repetitions of the source ID, the corresponding CRC bits or both.

[0097] For example, in some embodiments, the target ID (e.g., an IoT device ID) associated with the DL transmission may be independently encoded within the DL transmission. For example, the ID is self-decodable and not jointly encoded with other data or control information (e.g., physical layer control information). In this way, any IoT device can easily and quickly decode the ID and further determine whether the DL transmission aims at the device itself.

[0098] In some embodiments, CRC bits may be generated for the target ID (e.g., an IoT device ID) associated with the DL transmission, to avoid a false alarm issue and/or a lost alarm issue. For example, 16-bit CRC or 24-bit CRC may be generated. In some examples, the ID and the CRC bits can be transmitted simultaneously, for example, both included in the DL transmission. In some other examples, the DL transmission may not include the CRC bits for the target ID. In some embodiments, to improve transmission reliability of the target ID, the target ID, the corresponding CRC bits or both can be repeatedly transmitted. For example, the DL transmission may include one or more repetitions of the target ID, the corresponding CRC bits or both.

[0099] In some embodiments, the source ID (e.g., a sync source ID) associated with the DL transmission may be jointly encoded with control information associated with the DL transmission and may be transmitted in physical layer signaling (e.g., a physical downlink control channel (PDCCH)). In some embodiments, the source ID (e.g., a sync source ID) associated with the DL transmission may be encoded with data carried by the DL transmission and may be transmitted in high layer signaling (e.g., a media access control (MAC) control element (CE) or radio resource control (RRC) signaling).

[00100] For example, in some embodiments, the target ID (e.g., an IoT device ID) associated with the DL transmission may be jointly encoded with control information associated with the DL transmission and may be transmitted in physical layer signaling (e.g., a PDCCH). In some embodiments, the target ID (e.g., an IoT device ID) associated with the DL transmission may be encoded with data carried by the DL transmission and may be transmitted in high layer signaling (e.g., an MAC CE or RRC signaling).

[00101] In some embodiments, the source ID (e.g., a sync source ID) associated with the DL transmission may be independently encoded within the DL transmission. For example, the ID is self-decodable and not jointly encoded with other data or control information (e.g., physical layer control information). In this way, any IoT device can easily and quickly decode the ID and further determine whether the DL transmission is from a desired sync source.

[00102] In some embodiments, CRC bits may be generated for the source ID (e.g., a sync source ID) associated with the DL transmission, to avoid a false alarm issue and/or a lost alarm issue. For example, 16-bit CRC or 24-bit CRC may be generated. In some examples, the ID and the CRC bits can be transmitted simultaneously, for example, both included in the DL transmission. In some other examples, the DL transmission may not include the CRC bits for the source ID. In some embodiments, to improve transmission reliability of the source ID, the source ID, the corresponding CRC bits or both can be repeatedly transmitted. For example, the DL transmission may include one or more repetitions of the source ID, the corresponding CRC bits or both.

[00103] In some embodiments, the target ID (e.g., an IoT device ID) associated with the DL transmission may be jointly encoded with control information associated with the DL transmission and may be transmitted in physical layer signaling (e.g., a PDCCH). The source ID (e.g., a sync source ID) associated with the DL transmission may be jointly encoded with control information associated with the DL transmission and may be transmitted in physical layer signaling (e.g., a PDCCH).

[00104] In some embodiments, the target ID (e.g., an IoT device ID) associated with the DL transmission may be encoded with data carried by the DL transmission and may be transmitted in high layer signaling (e.g., an MAC CE or RRC signaling). The source ID (e.g., a sync source ID) associated with the DL transmission may be encoded with data carried by the DL transmission and may be transmitted in high layer signaling (e.g., an MAC CE or RRC signaling).

[00105] For a UL transmission, the ID of the source (e.g., an IoT device) of the UL transmission is indicated so that any sync source (e.g., a BS, an intermediate node, an assisting node, or a UE-type reader) can easily identify whether this UL transmission is from a desired IoT device. This is especially true considering there may be a

significant number of IoT devices (e.g., tags) within one cell and non-orthogonal multiple access (NOMA) adopted for UL transmission. For NOMA, an IoT device-specific (e.g., tag-specific) signature is mandatory for a receiver to differentiate each IoT device (e.g., tag). In that sense, an IoT device ID that can uniquely identify the device is appropriate as the specific signature.

[00106] For a given sync source, it may monitor the UL transmission and determine whether the UL transmission is from a desired IoT device based on the source ID associated with the UL transmission and the ID of the desired IoT device (which may be stored in the memory of the sync source). For example, the sync source may detect the source ID associated with the UL transmission and compare the detected source ID with the desired IoT device ID. If the detected source ID matches (e.g., is equal to) the desired IoT device ID, the sync source may process the UL transmission. For example, the sync source may decode the data or control information carried by the UL transmission. Otherwise, if the detected source ID does not match the desired IoT device ID, the sync source may drop the UL transmission and not process it so as to avoid unnecessary effort on decoding of UL data or UL control information which is not from the desired IoT device and save power consumption.

[00107] For a UL transmission, the ID of the target (e.g., a sync source) of the UL transmission is indicated so that any sync source (e.g., a BS, an intermediate node, an assisting node, or a UE-type reader) can easily identify whether the UL transmission aims at itself. For a given sync source, it may monitor the UL transmission and determine whether the UL transmission is targeted for the current sync source based on the target ID associated with the UL transmission and its own ID (which may be stored in the memory of the sync source). For example, the sync source may detect the target ID associated with the UL transmission and compare the detected target ID with its own ID. If the detected target ID matches (e.g., is equal to) its own ID, the sync source may process the UL transmission. For example, the sync source may decode the data or control information carried by the UL transmission. Otherwise, if the detected target ID does not match its own ID, the sync source may drop the UL transmission and not process it so as to avoid unnecessary effort on decoding of UL data or UL control information which is not targeted for the current sync source and save power consumption.

[00108] In some embodiments, a sync source may process the UL transmission when it determines that the UL transmission is targeted for it and is sent from a desired IoT device. Otherwise, the IoT device may drop the DL transmission.

[00109] Various methods may be employed for indicating or transmitting the source ID (e.g., an IoT device ID) and the target ID (e.g., a sync source ID) associated with a UL transmission.

[00110] For example, in some embodiments, the source ID (e.g., an IoT device ID) associated with the UL transmission may be independently encoded within the UL transmission. For example, the ID is self-decodable and not jointly encoded with other data or control information (e.g., physical layer control information).

[00111] In some embodiments, CRC bits may be generated for the source ID (e.g., an IoT device ID) associated with the UL transmission, to avoid a false alarm issue and/or a lost alarm issue. For example, 16-bit CRC or 24-bit CRC may be generated. In some examples, the ID and the CRC bits can be transmitted simultaneously, for example, both included in the UL transmission. In some other examples, the UL transmission may not include the CRC bits for the source ID. In some embodiments, to improve transmission reliability of the source ID, the source ID, the corresponding CRC bits or both can be repeatedly transmitted. For example, the UL transmission may include one or more repetitions of the source ID, the corresponding CRC bits or both.

[00112] In some embodiments, the target ID (e.g., a sync source ID) associated with the UL transmission may be independently encoded within the UL transmission. For example, the ID is self-decodable and not jointly encoded with other data or control information (e.g., physical layer control information).

[00113] In some embodiments, CRC bits may be generated for the target ID (e.g., a sync source ID) associated with the UL transmission, to avoid a false alarm issue and/or a lost alarm issue. For example, 16-bit CRC or 24-bit CRC may be generated. In some examples, the ID and the CRC bits can be transmitted simultaneously, for example, both included in the UL transmission. In some other examples, the UL transmission may not include the CRC bits for the target ID. In some embodiments, to improve transmission reliability of the target ID, the target ID, the corresponding CRC bits or

both can be repeatedly transmitted. For example, the UL transmission may include one or more repetitions of the target ID, the corresponding CRC bits or both.

[00114] For example, in some embodiments, the source ID (e.g., an IoT device ID) associated with the UL transmission may be independently encoded within the UL transmission. For example, the ID is self-decodable and not jointly encoded with other data or control information (e.g., physical layer control information).

[00115] In some embodiments, CRC bits may be generated for the source ID (e.g., an IoT device ID) associated with the UL transmission, to avoid a false alarm issue and/or a lost alarm issue. For example, 16-bit CRC or 24-bit CRC may be generated. In some examples, the ID and the CRC bits can be transmitted simultaneously, for example, both included in the UL transmission. In some other examples, the UL transmission may not include the CRC bits for the source ID. In some embodiments, to improve transmission reliability of the source ID, the source ID, the corresponding CRC bits or both can be repeatedly transmitted. For example, the UL transmission may include one or more repetitions of the source ID, the corresponding CRC bits or both.

[00116] In some embodiments, the target ID (e.g., a sync source ID) associated with the UL transmission may be jointly encoded with control information associated with the UL transmission and may be transmitted in physical layer signaling (e.g., a physical uplink control channel (PUCCH)). In some embodiments, the target ID (e.g., a sync source ID) associated with the UL transmission may be encoded with data carried by the UL transmission and may be transmitted in high layer signaling (e.g., an MAC CE or RRC signaling).

[00117] For example, in some embodiments, the source ID (e.g., an IoT device ID) associated with the UL transmission may be jointly encoded with control information associated with the UL transmission and may be transmitted in physical layer signaling (e.g., a PUCCH). In some embodiments, the source ID (e.g., an IoT device ID) associated with the UL transmission may be encoded with data carried by the UL transmission and may be transmitted in high layer signaling (e.g., an MAC CE or RRC signaling).

[00118] In some embodiments, the target ID (e.g., a sync source ID) associated with

the UL transmission may be independently encoded within the UL transmission. For example, the ID is self-decodable and not jointly encoded with other data or control information (e.g., physical layer control information).

[00119] In some embodiments, CRC bits may be generated for the target ID (e.g., a sync source ID) associated with the UL transmission, to avoid a false alarm issue and/or a lost alarm issue. For example, 16-bit CRC or 24-bit CRC may be generated. In some examples, the ID and the CRC bits can be transmitted simultaneously, for example, both included in the UL transmission. In some other examples, the UL transmission may not include the CRC bits for the target ID. In some embodiments, to improve transmission reliability of the target ID, the target ID, the corresponding CRC bits or both can be repeatedly transmitted. For example, the UL transmission may include one or more repetitions of the target ID, the corresponding CRC bits or both.

[00120] In some embodiments, the source ID (e.g., an IoT device ID) associated with the UL transmission may be jointly encoded with control information associated with the UL transmission and may be transmitted in physical layer signaling (e.g., a PUCCH). The target ID (e.g., a sync source ID) associated with the UL transmission may be jointly encoded with control information associated with the UL transmission and may be transmitted in physical layer signaling (e.g., a PUCCH).

[00121] In some embodiments, the source ID (e.g., an IoT device ID) associated with the UL transmission may be encoded with data carried by the UL transmission and may be transmitted in high layer signaling (e.g., an MAC CE or RRC signaling). The target ID (e.g., a sync source ID) associated with the UL transmission may be encoded with data carried by the UL transmission and may be transmitted in high layer signaling (e.g., an MAC CE or RRC signaling).

[00122] In some embodiments, the ID of an IoT device or the ID of a sync source may be indicated in association with control information associated with the corresponding transmission. The control information may include information for decoding the corresponding transmission. CRC bits may be generated for the control information.

[00123] Various methods may be employed for indicating or transmitting the target ID (e.g., an IoT device ID) and the source ID (e.g., a sync source ID) associated with a DL

transmission.

[00124] For example, in some embodiments, the source ID (e.g., the ID of a sync source) associated with a DL transmission may be included in the control information (e.g., physical layer control information) associated with the DL transmission. In this way, any IoT device can easily identify whether the DL transmission is from a desired sync source.

[00125] The sync source which transmits the DL transmission (i.e., the source associated with the DL transmission) may generate CRC bits for the control information associated with the DL transmission and further scramble the CRC bits by the target ID (e.g., the ID of an IoT device in communication with the sync source) associated with the DL transmission. In some embodiments, to match the length of the CRC bits, the target ID (e.g., an IoT device ID) associated with the DL transmission may be repeated or shortened for the scrambling.

[00126] From the perspective of a given IoT device, it may monitor the DL transmission and determine whether the DL transmission is targeted for it based on the target ID associated with the DL transmission and its own device ID (which may be stored in the memory of the IoT device). For example, the IoT device may detect the CRC bits of the received control information associated with the DL transmission, generate CRC bits based on its own device ID, and compare the detected CRC bits with the generated CRC bits. If the detected CRC bits match (e.g., are the same as) the generated CRC bits, the IoT device may further determine whether the DL transmission is from a desired sync source based on the source ID associated with the DL transmission (which is included in the control information associated with the DL transmission) and the ID of the desired sync source (which may be stored in the memory of the IoT device). For example, if the source ID in the control information matches (e.g., is equal to) the desired sync source ID, the IoT device may process the DL transmission (e.g., process the received data and/or the control information carried by the DL transmission). Otherwise, if the DL transmission is not targeted for the current IoT device or if the DL transmission is not from a desired sync source, the current IoT device may drop the DL transmission and not process it so as to avoid unnecessary effort on processing of DL data, DL control or UL scheduling signaling and save power

consumption.

[00127] In some embodiments, an IoT device may process a DL transmission when it determines that the DL transmission is targeted for it (e.g., based on the CRC bits). Otherwise, the IoT device may drop the DL transmission.

[00128] For example, in some embodiments, the target ID (e.g., the ID of an IoT device) associated with a DL transmission may be included in the control information (e.g., physical layer control information) associated with the DL transmission. In this way, any IoT device can easily identify whether the DL transmission is targeted for itself.

[00129] The sync source which transmits the DL transmission may generate CRC bits for the control information associated with the DL transmission and further scramble the CRC bits by the source ID (e.g., the ID of the sync source) associated with the DL transmission. In some embodiments, to match the length of the CRC bits, the source ID (e.g., the ID of the sync source) associated with the DL transmission may be repeated or shortened for the scrambling.

[00130] From the perspective of a given IoT device, it may monitor the DL transmission and determine whether the DL transmission is from a desired sync source based on the source ID associated with the DL transmission and the ID of the desired sync source (which may be stored in the memory of the IoT device). For example, the IoT device may detect the CRC bits of the received control information associated with the DL transmission, generate CRC bits based on the desired sync source ID, and compare the detected CRC bits with the generated CRC bits. If the detected CRC bits match (e.g., are the same as) the generated CRC bits, the IoT device may further determine whether the DL transmission is targeted for itself based on the target ID associated with the DL transmission (which is included in the control information associated with the DL transmission) and its own device ID (which may be stored in the memory of the IoT device). For example, if the target ID in the control information matches (e.g., is equal to) the ID of the IoT device, the IoT device may process the DL transmission (e.g., process the received data and/or the control information carried by the DL transmission). Otherwise, if the DL transmission is not from a desired sync source or if the DL transmission is not targeted for the current IoT device, the current IoT device may drop the DL transmission and not process it so as to avoid unnecessary

effort on processing of DL data, DL control or UL scheduling signaling and save power consumption.

[00131] In some embodiments, an IoT device may process the DL transmission when it determines that the DL transmission is from a desired sync source (e.g., based on the CRC bits). Otherwise, the IoT device may drop the DL transmission.

[00132] For example, in some embodiments, a sync source which transmits a DL transmission may generate CRC bits for control information (e.g., physical layer control information) associated with the DL transmission and further scramble the CRC bits by both the target ID (e.g., the ID of an IoT device) and the source ID (e.g., the ID of the sync source) associated with the DL transmission. In some embodiments, to match the length of the CRC bits, the target ID (e.g., the IoT device ID), the source ID (e.g., the ID of the sync source) or both may be repeated or shortened for the scrambling.

[00133] From the perspective of a given IoT device, it may monitor the DL transmission and determine whether the DL transmission is target for itself or from a desired sync source based on the target ID and the source ID associated with the DL transmission, its own ID and the ID of the desired sync source (the latter two may be stored in the memory of the IoT device). For example, the IoT device may detect the CRC bits of the received control information associated with the DL transmission, generate CRC bits based on the ID of the IoT device and the desired sync source ID, and compare the detected CRC bits with the generated CRC bits. If the detected CRC bits match (e.g., are the same as) the generated CRC bits, the IoT device may process the DL transmission (e.g., process the received data and/or the control information carried by the DL transmission). Otherwise, if the detected CRC bits do not match the generated CRC bits, the current IoT device may drop the DL transmission and not process it so as to avoid unnecessary effort on processing of DL data, DL control or UL scheduling signaling and save power consumption.

[00134] For example, in some embodiments, the target ID (e.g., the ID of an IoT device) and the source ID (e.g., the ID of a sync source) associated with a DL transmission may be included in the control information (e.g., physical layer control information) associated with the DL transmission. In this way, any IoT device can easily identify whether the DL transmission is targeted for itself or from a desired sync source.

[00135] The sync source which transmits the DL transmission may generate CRC bits for the control information associated with the DL transmission and further scramble the CRC bits by a sequence. In some examples, the sequence may be common to the IoT devices and sync sources within the same cell or the same network. In some examples, the sequence generator can be initialized based on at least the cell ID, or a parameter common to all the IoT devices within the same network.

[00136] From the perspective of a given IoT device, it may monitor the DL transmission and determine whether the DL transmission is targeted for itself or from a desired sync source based on the target ID and the source ID associated with the DL transmission (which are included in the control information associated with the DL transmission), its own device ID and the ID of the desired sync source (the latter two IDs may be stored in the memory of the IoT device). For example, the IoT device may determine whether the DL transmission is targeted for itself based on the target ID associated with the DL transmission and its own device ID. For example, if the target ID in the control information matches (e.g., is equal to) the ID of the IoT device, the IoT device may process the DL transmission (e.g., process the received data and/or the control information carried by the DL transmission). For example, the IoT device may determine whether the DL transmission is from the desired sync source based on the source ID associated with the DL transmission and the ID of the desired sync source. For example, if the source ID in the control information matches (e.g., is equal to) the desired sync source ID, the IoT device may process the DL transmission (e.g., process the received data and/or the control information carried by the DL transmission). Otherwise, if the DL transmission is not from a desired sync source or if the DL transmission is not targeted for the current IoT device, the current IoT device may drop the DL transmission and not process it so as to avoid unnecessary effort on processing of DL data, DL control or UL scheduling signaling and save power consumption.

[00137] In some embodiments, an IoT device may process the DL transmission when it determines that the DL transmission is from the desired sync source and is targeted for the IoT device. Otherwise, the IoT device may drop the UL transmission.

[00138] Various methods may be employed for indicating or transmitting the target ID (e.g., a sync source ID) and the source ID (e.g., an IoT device ID) associated with a UL

transmission.

[00139] For example, in some embodiments, the target ID (e.g., the ID of a sync source) associated with a UL transmission may be included in the control information (e.g., physical layer control information) associated with the UL transmission. In this way, any sync source (e.g., a BS, an intermediate node, an assisting node, or a UE-type reader) can easily identify whether the UL transmission is sent to itself.

[00140] The IoT device which transmits the UL transmission may generate CRC bits for the control information associated with the UL transmission and further scramble the CRC bits by the source ID (e.g., the ID of the IoT device) associated with the UL transmission. In some embodiments, to match the length of the CRC bits, the source ID (e.g., the IoT device ID) associated with the UL transmission may be repeated or shortened for the scrambling.

[00141] From the perspective of a given sync source, it may monitor the UL transmission and determine whether the UL transmission is from a desired IoT device based on the source ID associated with the UL transmission and the ID of the desired IoT device (which may be stored in the memory of the sync source). For example, the sync source may detect the CRC bits of the received control information associated with the UL transmission, generate CRC bits based on the ID of the desired IoT device, and compare the detected CRC bits with the generated CRC bits. If the detected CRC bits match (e.g., are the same as) the generated CRC bits, the sync source may further determine whether the UL transmission is targeted for itself based on the target ID associated with the UL transmission (which is included in the control information associated with the UL transmission) and its own ID (which may be stored in the memory of the sync source). For example, if the target ID in the control information matches (e.g., is equal to) the ID of the sync source, the sync source may process the UL transmission (e.g., process the received data and/or the control information carried by the UL transmission). Otherwise, if the UL transmission is not from a desired IoT device or if the UL transmission is not targeted for the current sync source, the current sync source may drop the UL transmission and not process it so as to avoid unnecessary effort on processing of UL data and save power consumption.

[00142] In some embodiments, a sync source may process the UL transmission when

it determines that the UL transmission is from a desired IoT device (e.g., based on the CRC bits). Otherwise, the sync source may drop the UL transmission.

[00143] For example, in some embodiments, the source ID (e.g., the ID of an IoT device) associated with a UL transmission may be included in the control information (e.g., physical layer control information) associated with the UL transmission. In this way, any sync source can easily identify whether the UL transmission is from a desired IoT device.

[00144] The IoT device which transmits the UL transmission may generate CRC bits for the control information associated with the UL transmission and further scramble the CRC bits by the target ID (e.g., the ID of a sync source in communication with the IoT device) associated with the UL transmission. In some embodiments, to match the length of the CRC bits, the target ID (e.g., the sync source ID) associated with the UL transmission may be repeated or shortened for the scrambling.

[00145] From the perspective of a given sync source, it may monitor the UL transmission and determine whether the UL transmission is targeted for itself based on the target ID associated with the UL transmission and its own ID (which may be stored in the memory of the sync source). For example, the sync source may detect the CRC bits of the received control information associated with the UL transmission, generate CRC bits based on its own ID, and compare the detected CRC bits with the generated CRC bits. If the detected CRC bits match (e.g., are the same as) the generated CRC bits, the sync source may further determine whether the UL transmission is from a desired IoT device based on the source ID associated with the UL transmission (which is included in the control information associated with the UL transmission) and the ID of the desired IoT device (which may be stored in the memory of the sync source). For example, if the source ID in the control information matches (e.g., is equal to) the ID of the desired IoT device, the sync source may process the UL transmission (e.g., process the received data and/or the control information carried by the UL transmission). Otherwise, if the UL transmission is not targeted for the current sync source or if the UL transmission is not from a desired IoT device, the current sync source may drop the UL transmission and not process it so as to avoid unnecessary effort on processing of UL data and save power consumption.

[00146] In some embodiments, a sync source may process the UL transmission when it determines that the UL transmission is targeted for itself (e.g., based on the CRC bits). Otherwise, the sync source may drop the UL transmission.

[00147] For example, in some embodiments, an IoT device which transmits a UL transmission may generate CRC bits for control information (e.g., physical layer control information) associated with the UL transmission and further scramble the CRC bits by both the source ID (e.g., the ID of the IoT device) and the target ID (e.g., the ID of a sync source in communication with the IoT device) associated with the UL transmission. In some embodiments, to match the length of the CRC bits, the source ID (e.g., the IoT device ID), the target ID (e.g., the sync source ID) or both may be repeated or shortened for the scrambling.

[00148] From the perspective of a given sync source, it may monitor the UL transmission and determine whether the UL transmission is target for itself or from a desired IoT device based on the target ID and the source ID associated with the UL transmission, its own ID and the ID of the desired IoT device (the latter two may be stored in the memory of the sync source). For example, the sync source may detect the CRC bits of the received control information associated with the UL transmission, generate CRC bits based on its own ID and the desired IoT device ID, and compare the detected CRC bits with the generated CRC bits. If the detected CRC bits match (e.g., are the same as) the generated CRC bits, the IoT device may process the UL transmission (e.g., process the received data and/or the control information carried by the UL transmission). Otherwise, if the detected CRC bits do not match the generated CRC bits, the current IoT device may drop the UL transmission and not process it so as to avoid unnecessary effort on processing of UL data and save power consumption.

[00149] For example, in some embodiments, the source ID (e.g., the ID of an IoT device) and the target ID (e.g., the ID of a sync source in communication with the IoT device) associated with a UL transmission may be included in the control information (e.g., physical layer control information) associated with the UL transmission. In this way, any sync source can easily identify whether the UL transmission is from a desired IoT device or is targeted for itself.

[00150] The IoT device which transmits the UL transmission may generate CRC bits

for the control information associated with the UL transmission and further scramble the CRC bits by a sequence. In some examples, the sequence may be common to the IoT devices and sync sources within the same cell or the same network. In some examples, the sequence generator can be initialized based on at least the cell ID, or a parameter common to all the IoT devices within the same network.

[00151] From the perspective of a given sync source, it may monitor the UL transmission and determine whether the UL transmission is targeted for itself or from a desired IoT device based on the target ID and the source ID associated with the UL transmission (which are included in the control information associated with the UL transmission), its own device ID and the ID of the desired IoT device (the latter two IDs may be stored in the memory of the IoT device). For example, the sync source may determine whether the UL transmission is targeted for itself based on the target ID associated with the UL transmission and its own ID. For example, if the target ID in the control information matches (e.g., is equal to) the ID of the sync source, the sync source may process the UL transmission (e.g., process the received data and/or the control information carried by the UL transmission). For example, the sync source may determine whether the UL transmission is from the desired IoT device based on the source ID associated with the UL transmission and the ID of the desired IoT device. For example, if the source ID in the control information matches (e.g., is equal to) the desired IoT device, the sync source may process the UL transmission (e.g., process the received data and/or the control information carried by the UL transmission). Otherwise, if the UL transmission is not from a desired IoT device or if the UL transmission is not targeted for the current sync source, the current sync source may drop the UL transmission and not process it so as to avoid unnecessary effort on processing of UL data and save power consumption.

[00152] In some embodiments, a sync source may process the UL transmission when it determines that the UL transmission is from the desired IoT device and is targeted for the sync source. Otherwise, the sync source may drop the UL transmission.

[00153] In some embodiments of the present disclosure, the same downlink synchronization signals may be transmitted by the sync source (e.g., a BS, an intermediate node, an assisting node, or a UE-type reader) so that the downlink

synchronization signals are transparent to any IoT device within the same cell. From the perspective of a given IoT device, it cannot differentiate the type of the synchronization source (e.g., whether the source is a BS or a UE) while communicates with the source.

[00154] In some embodiments, in response to (e.g., after) receiving the system information from a sync source, an IoT device may trigger an initial access procedure. In response to (e.g., after) the completion of the initial access procedure, the IoT device may be assigned a temporary ID (e.g., cell-radio network temporary identifier (C-RNTI)) by the sync source, the network, a serving BS. The IoT device may receive the temporary ID via the sync source.

[00155] In some embodiments of the present disclosure, the ID of the IoT device may be indicated for either the DL transmission or the UL transmission. For example, an IoT device may transmit a source ID associated with a UL transmission, wherein the source ID can be set to the ID of the IoT device (i.e., the transmitter). A sync source which receives this UL transmission can determine whether the transmission is from a desired IoT device based on the source ID associated with the UL transmission and the ID of the desired IoT device. Then, the sync source can act accordingly based on the determination. For example, a sync source may transmit a target ID associated with a DL transmission, wherein the target ID can be set to the ID of a desired IoT device. An IoT device which receives this transmission can determine whether the transmission is targeted for it based on the target ID associated with the transmission and its own ID. Then, the IoT device can act accordingly based on the determination.

[00156] As will be described later, various methods may be employed for indicating or transmitting the ID of the IoT device.

[00157] In some embodiments, the ID of an IoT device may be explicitly indicated, for example, encoded within a corresponding transmission or encoded with control information or data associated with the corresponding transmission.

[00158] For a DL transmission, the ID of the target (e.g., a target IoT device) of the DL transmission is indicated so that any IoT device can easily identify whether this DL transmission aims at itself. For a given IoT device, it may monitor the DL

transmission and determine whether the DL transmission is targeted for it based on the target ID associated with the DL transmission and its own device ID (which may be stored in the memory of the IoT device). For example, the IoT device may detect the target ID associated with the DL transmission and compare the detected target ID with its own device ID. If the detected target ID matches (e.g., is equal to) its own device ID, the IoT device may process the DL transmission. For example, the IoT device may decode the data or control information carried by the DL transmission. Otherwise, if the detected target ID does not match its own device ID, the IoT device may drop the DL transmission and not process it so as to avoid unnecessary effort on decoding of DL data, DL control or UL scheduling signaling which is not targeted for the current IoT device and save power consumption.

[00159] Various methods may be employed for indicating or transmitting the target ID (e.g., an IoT device ID) associated with a DL transmission.

[00160] For example, in some embodiments, the target ID (e.g., an IoT device ID) associated with the DL transmission may be independently encoded within the DL transmission. For example, the ID is self-decodable and not jointly encoded with other data or control information (e.g., physical layer control information). In this way, any IoT device can easily and quickly decode the ID and further determine whether the DL transmission aims at the device itself.

[00161] In some embodiments, CRC bits may be generated for the target ID (e.g., an IoT device ID) associated with the DL transmission, to avoid a false alarm issue and/or a lost alarm issue. For example, 16-bit CRC or 24-bit CRC may be generated. In some examples, the ID and the CRC bits can be transmitted simultaneously, for example, both included in the DL transmission. In some other examples, the DL transmission may not include the CRC bits for the target ID. In some embodiments, to improve transmission reliability of the target ID, the target ID, the corresponding CRC bits or both can be repeatedly transmitted. For example, the DL transmission may include one or more repetitions of the target ID, the corresponding CRC bits or both.

[00162] For example, in some embodiments, the target ID (e.g., an IoT device ID) associated with the DL transmission may be jointly encoded with control information (e.g., physical layer control information) associated with the DL transmission and may

be transmitted in physical layer signaling (e.g., a PDCCH). In some embodiments, the target ID (e.g., an IoT device ID) associated with the DL transmission may be encoded with data carried by the DL transmission and may be transmitted in high layer signaling (e.g., an MAC CE or RRC signaling).

[00163] In some embodiments, CRC bits may be generated for the control information associated with the DL transmission and further scrambled by the temporary ID (e.g., the C-RNTI) assigned for the target (e.g., an IoT device) of the DL transmission. To match the length of CRC bits, the temporary ID may be repeated or shortened for the scrambling.

[00164] For example, in some embodiments, the target ID (e.g., an IoT device ID) associated with the DL transmission may be jointly encoded with control information (e.g., physical layer control information) associated with the DL transmission and may be transmitted in physical layer signaling (e.g., a PDCCH). In some embodiments, the target ID (e.g., an IoT device ID) associated with the DL transmission may be encoded with data carried by the DL transmission and may be transmitted in high layer signaling (e.g., an MAC CE or RRC signaling).

[00165] In some embodiments, CRC bits may be generated for the control information associated with the DL transmission and further scrambled by a sequence. In some examples, the sequence may be common to the IoT devices and sync sources within the same cell or the same network. In some examples, the sequence generator can be initialized based on at least the cell ID, or a parameter common to all the IoT devices within the same network.

[00166] For a UL transmission, the ID of the source (e.g., an IoT device) of the UL transmission is indicated so that any sync source (e.g., a BS, an intermediate node, an assisting node, or a UE-type reader) can easily identify whether this UL transmission is from a desired IoT device. This is especially true considering there may be a significant number of IoT devices (e.g., tags) within one cell and NOMA adopted for UL transmission. For NOMA, an IoT device-specific (e.g., tag-specific) signature is mandatory for a receiver to differentiate each IoT device (e.g., tag). In that sense, an IoT device ID that can uniquely identify the device is appropriate as the specific signature.

[00167] For a given sync source, it may monitor the UL transmission and determine whether the UL transmission is from a desired IoT device based on the source ID associated with the UL transmission and the ID of the desired IoT device (which may be stored in the memory of the sync source). For example, the sync source may detect the source ID associated with the UL transmission and compare the detected source ID with the desired IoT device ID. If the detected source ID matches (e.g., is equal to) the desired IoT device ID, the sync source may process the UL transmission. For example, the sync source may decode the data or control information carried by the UL transmission. Otherwise, if the detected source ID does not match the desired IoT device ID, the sync source may drop the UL transmission and not process it so as to avoid unnecessary effort on decoding of UL data or UL control information which is not from the desired IoT device and save power consumption.

[00168] Various methods may be employed for indicating or transmitting the source ID (e.g., an IoT device ID) associated with a UL transmission.

[00169] For example, in some embodiments, the source ID (e.g., an IoT device ID) associated with the UL transmission may be independently encoded within the UL transmission. For example, the ID is self-decodable and not jointly encoded with other data or control information (e.g., physical layer control information).

[00170] In some embodiments, CRC bits may be generated for the source ID (e.g., an IoT device ID) associated with the UL transmission, to avoid a false alarm issue and/or a lost alarm issue. For example, 16-bit CRC or 24-bit CRC may be generated. In some examples, the ID and the CRC bits can be transmitted simultaneously, for example, both included in the UL transmission. In some other examples, the UL transmission may not include the CRC bits for the source ID. In some embodiments, to improve transmission reliability of the source ID, the source ID, the corresponding CRC bits or both can be repeatedly transmitted. For example, the UL transmission may include one or more repetitions of the source ID, the corresponding CRC bits or both.

[00171] For example, in some embodiments, the source ID (e.g., an IoT device ID) associated with the UL transmission may be jointly encoded with control information (e.g., physical layer control information) associated with the UL transmission and may be transmitted in physical layer signaling (e.g., a PUCCH). In some embodiments,

the source ID (e.g., an IoT device ID) associated with the UL transmission may be encoded with data carried by the UL transmission and may be transmitted in high layer signaling (e.g., an MAC CE or RRC signaling).

[00172] In some embodiments, CRC bits may be generated for the control information associated with the UL transmission and further scrambled by the temporary ID (e.g., the C-RNTI) assigned for the source (e.g., an IoT device) of the UL transmission. To match the length of CRC bits, the temporary ID may be repeated or shortened for the scrambling.

[00173] For example, in some embodiments, the source ID (e.g., an IoT device ID) associated with the UL transmission may be jointly encoded with control information (e.g., physical layer control information) associated with the UL transmission and may be transmitted in physical layer signaling (e.g., a PUCCH). In some embodiments, the source ID (e.g., an IoT device ID) associated with the UL transmission may be encoded with data carried by the UL transmission and may be transmitted in high layer signaling (e.g., an MAC CE or RRC signaling).

[00174] In some embodiments, CRC bits may be generated for the control information associated with the UL transmission and further scrambled by a sequence. In some examples, the sequence may be common to the IoT devices and sync sources within the same cell or the same network. In some examples, the sequence generator can be initialized based on at least the cell ID, or a parameter common to all the IoT devices within the same network.

[00175] In some embodiments, the ID of an IoT device may be indicated in association with control information associated with the corresponding transmission. The control information may include information for decoding the corresponding transmission. CRC bits may be generated for the control information. In some embodiments, the ID of an IoT device may be encoded with data associated with the corresponding transmission and transmitted via high layer signaling.

[00176] Various methods may be employed for indicating or transmitting the target ID (e.g., an IoT device ID) associated with a DL transmission.

[00177] For example, in some embodiments, a sync source (e.g., a BS, an intermediate node, an assisting node, or a UE-type reader) which transmits the DL transmission (i.e., the source associated with the DL transmission) may generate CRC bits for the control information (e.g., physical layer control information) associated with the DL transmission and further scramble the CRC bits by the target ID (e.g., the ID of an IoT device in communication with the sync source) associated with the DL transmission. In some embodiments, to match the length of the CRC bits, the target ID (e.g., an IoT device ID) associated with the DL transmission may be repeated or shortened for the scrambling.

[00178] From the perspective of a given IoT device, it may monitor the DL transmission and determine whether the DL transmission is targeted for it based on the target ID associated with the DL transmission and its own device ID (which may be stored in the memory of the IoT device). For example, the IoT device may detect the CRC bits of the received control information associated with the DL transmission, generate CRC bits based on its own device ID, and compare the detected CRC bits with the generated CRC bits. If the detected CRC bits match (e.g., are the same as) the generated CRC bits, the IoT device may process the DL transmission (e.g., process the received data and/or the control information carried by the DL transmission). Otherwise, if the DL transmission is not targeted for the current IoT device the current IoT device may drop the DL transmission and not process it so as to avoid unnecessary effort on processing of DL data, DL control or UL scheduling signaling and save power consumption.

[00179] For example, in some embodiments, the target ID (e.g., the ID of an IoT device) associated with a DL transmission may be jointly encoded with control information (e.g., physical layer control information) associated with the DL transmission and may be transmitted in physical layer signaling (e.g., a PDCCH). In some embodiments, the target ID (e.g., the ID of an IoT device) associated with the DL transmission may be encoded with data carried by the DL transmission and may be transmitted in high layer signaling (e.g., an MAC CE or RRC signaling).

[00180] In some embodiments, CRC bits may be generated for the control information associated with the DL transmission and further scrambled by the temporary ID (e.g.,

the C-RNTI) assigned for the target (e.g., an IoT device) of the DL transmission. To match the length of CRC bits, the temporary ID may be repeated or shortened for the scrambling.

[00181] From the perspective of a given IoT device, it may monitor the DL transmission and determine whether the DL transmission is targeted for it based on the CRC bits for the control information associated with the DL transmission and its own temporary ID (e.g., the C-RNTI, which may be stored in the memory of the IoT device). For example, the IoT device may detect the CRC bits of the received control information associated with the DL transmission, generate CRC bits based on its own temporary ID, and compare the detected CRC bits with the generated CRC bits. If the detected CRC bits match (e.g., are the same as) the generated CRC bits, the IoT device may process the DL transmission (e.g., process the received data and/or the control information carried by the DL transmission). Otherwise, if the DL transmission is not targeted for the current IoT device, the current IoT device may drop the DL transmission and not process it so as to avoid unnecessary effort on processing of DL data, DL control or UL scheduling signaling and save power consumption.

[00182] For example, in some embodiments, the target ID (e.g., the ID of an IoT device) associated with a DL transmission may be jointly encoded with control information (e.g., physical layer control information) associated with the DL transmission and may be transmitted in physical layer signaling (e.g., a PDCCH). In some embodiments, the target ID (e.g., the ID of an IoT device) associated with the DL transmission may be encoded with data carried by the DL transmission and may be transmitted in high layer signaling (e.g., an MAC CE or RRC signaling).

[00183] In some embodiments, CRC bits may be generated for the control information associated with the DL transmission and further scrambled by a sequence. In some examples, the sequence may be common to the IoT devices and sync sources within the same cell or the same network. In some examples, the sequence generator can be initialized based on at least the cell ID, or a parameter common to all the IoT devices within the same network.

[00184] From the perspective of a given IoT device, it may monitor the DL transmission and determine whether the DL transmission is target for itself based on

the target ID associated with the DL transmission and its own device ID. For example, the IoT device may detect the physical layer signaling or high layer signaling associated with the DL transmission and compare the detected target ID (e.g., in the physical layer signaling or high layer signaling) with its own device ID (which may be stored in the memory of the IoT device). If the two IDs match (e.g., the same), the IoT device may process the DL transmission (e.g., process the received data and/or the control information carried by the DL transmission). Otherwise, if the two IDs do not match, the current IoT device may drop the DL transmission and not process it so as to avoid unnecessary effort on processing of DL data, DL control or UL scheduling signaling and save power consumption.

[00185] Various methods may be employed for indicating or transmitting the source ID (e.g., an IoT device ID) associated with a UL transmission.

[00186] For example, in some embodiments, an IoT device which transmits a UL transmission may generate CRC bits for the control information (e.g., physical layer control information) associated with the UL transmission and further scramble the CRC bits by the source ID (e.g., the ID of the IoT device) associated with the UL transmission. In some embodiments, to match the length of the CRC bits, the source ID (e.g., the IoT device ID) associated with the UL transmission may be repeated or shortened for the scrambling.

[00187] From the perspective of a given sync source, it may monitor the UL transmission and determine whether the UL transmission is from a desired IoT device based on the source ID associated with the UL transmission and the ID of the desired IoT device (which may be stored in the memory of the sync source). For example, the sync source may detect the CRC bits of the received control information associated with the UL transmission, generate CRC bits based on the ID of the desired IoT device, and compare the detected CRC bits with the generated CRC bits. If the detected CRC bits match (e.g., are the same as) the generated CRC bits, the sync source may process the UL transmission (e.g., process the received data and/or the control information carried by the UL transmission). Otherwise, if the UL transmission is not from a desired IoT device, the current sync source may drop the UL transmission and not process it so as to avoid unnecessary effort on processing of UL data and save power

consumption.

[00188] For example, in some embodiments, the source ID (e.g., the ID of an IoT device) associated with a UL transmission may be jointly encoded with control information (e.g., physical layer control information) associated with the UL transmission and may be transmitted in physical layer signaling (e.g., a PUCCH). In some embodiments, the source ID (e.g., the ID of an IoT device) associated with the UL transmission may be encoded with data carried by the UL transmission and may be transmitted in high layer signaling (e.g., an MAC CE or RRC signaling).

[00189] In some embodiments, CRC bits may be generated for the control information associated with the UL transmission and further scrambled by the temporary ID (e.g., the C-RNTI) assigned for the source (e.g., an IoT device) of the UL transmission. To match the length of CRC bits, the temporary ID may be repeated or shortened for the scrambling.

[00190] From the perspective of a given sync source, it may monitor the UL transmission and determine whether the UL transmission is from a desired IoT device based on the CRC bits for the control information associated with the UL transmission and the temporary ID of the desired IoT device (which may be stored in the memory of the sync source). For example, the sync source may detect the CRC bits of the received control information associated with the UL transmission, generate CRC bits based on the temporary ID of the desired IoT device, and compare the detected CRC bits with the generated CRC bits. If the detected CRC bits match (e.g., are the same as) the generated CRC bits, the sync source may process the UL transmission (e.g., process the received data and/or the control information carried by the UL transmission). Otherwise, if the UL transmission is not from the desired IoT device, the current sync source may drop the UL transmission and not process it so as to avoid unnecessary effort on processing of UL data or UL control and save power consumption.

[00191] For example, in some embodiments, the source ID (e.g., the ID of an IoT device) associated with a UL transmission may be jointly encoded with control information (e.g., physical layer control information) associated with the UL transmission and may be transmitted in physical layer signaling (e.g., a PUCCH). In some embodiments, the source ID (e.g., the ID of an IoT device) associated with the

UL transmission may be encoded with data carried by the UL transmission and may be transmitted in high layer signaling (e.g., an MAC CE or RRC signaling).

[00192] In some embodiments, CRC bits may be generated for the control information associated with the UL transmission and further scrambled by a sequence. In some examples, the sequence may be common to the IoT devices and sync sources within the same cell or the same network. In some examples, the sequence generator can be initialized based on at least the cell ID, or a parameter common to all the IoT devices within the same network.

[00193] From the perspective of a given sync source, it may monitor the UL transmission and determine whether the UL transmission is from a desired IoT device based on the source ID associated with the UL transmission and the ID of the desired IoT device. For example, the sync source may detect the physical layer signaling or high layer signaling associated with the UL transmission and compare the detected source ID (e.g., in the physical layer signaling or high layer signaling) with the desired IoT device ID (which may be stored in the memory of the sync source). If the two IDs match (e.g., the same), the sync source may process the UL transmission (e.g., process the received data and/or the control information carried by the UL transmission). Otherwise, if the two IDs do not match, the current sync source may drop the UL transmission and not process it so as to avoid unnecessary effort on processing of UL data or UL control and save power consumption.

[00194] FIG. 3 illustrates a flowchart of method 300 for wireless communication in accordance with some embodiments of the present disclosure. Details described in all of the foregoing embodiments of the present disclosure are applicable for the embodiments shown in FIG. 3. In some examples, method 300 may be performed by an IoT device (e.g., an ambient IoT device such as a tag). In some embodiments, the IoT device may execute a set of instructions to control the functional elements of the IoT device to perform the described functions or operations. In some examples, a processor or controller of an IoT device may cause the IoT device to perform method 300.

[00195] At 311, a first communication device may receive a first target ID associated with a first transmission or both the first target ID and a first source ID associated with

the first transmission. At 313, the first communication device may receive the first transmission. At 315, the first communication device may perform one or more operations of the following operations: determining whether the first transmission is targeted for the first communication device based on the first target ID and a device ID of the first communication device that uniquely identifies the first communication device, and determining whether the first transmission is from a second communication device based on the first source ID and an ID of the second communication device that uniquely identifies the second communication device. At 317, the first communication device may process the first transmission based on a result of the one or more operations.

[00196] In some embodiments, the first target ID is independently encoded within the first transmission. In some embodiments, the first target ID is jointly encoded with control information associated with the first transmission and is received in physical layer signaling. In some embodiments, the first target ID is jointly encoded with data carried by the first transmission and is received in high layer signaling. In some embodiments, the first target ID is used to scramble cyclic redundancy check (CRC) bits for control information associated with the first transmission. In some embodiments, the first target ID is included in control information associated with the first transmission.

[00197] In some embodiments, the first source ID is independently encoded within the first transmission. In some embodiments, the first source ID is jointly encoded with control information associated with the first transmission and is received in physical layer signaling. In some embodiments, the first source ID is jointly encoded with data carried by the first transmission and is received in high layer signaling. In some embodiments, the first source ID is included in control information associated with the first transmission. In some embodiments, the first source ID is used to scramble CRC bits for control information associated with the first transmission.

[00198] In some embodiments, the first communication device may receive a temporary ID for the first communication device assigned by a network, a serving base station, or the second communication device.

[00199] In some embodiments, the first communication device may: receive control

information associated with the first transmission; and determine whether the first transmission is targeted for the first communication device based on a temporary ID of the first communication device and CRC bits for the control information associated with the first transmission.

[00200] In some embodiments, the first communication device may receive control information associated with the first transmission, wherein CRC bits for the control information are scrambled by a temporary ID for a target device of the first transmission or by a sequence common to devices within a same cell or a same network as the target device.

[00201] In some embodiments, the first communication device may: transmit, to the second communication device, a second source ID associated with a second transmission or both the second source ID and a second target ID associated with the second transmission, wherein the second source ID is set to the device ID of the first communication device and the second target ID is set to the ID of the second communication device; and transmit, to the second communication device, the second transmission.

[00202] In some embodiments, the second source ID is independently encoded within the second transmission. In some embodiments, the second source ID is jointly encoded with control information associated with the second transmission and is transmitted in physical layer signaling. In some embodiments, the second source ID is jointly encoded with data carried by the second transmission and is transmitted in high layer signaling. In some embodiments, the second source ID is used to scramble CRC bits for control information associated with the second transmission. In some embodiments, the second source ID is included in control information with the second transmission.

[00203] In some embodiments, the second target ID is independently encoded within the second transmission. In some embodiments, the second target ID is jointly encoded with control information associated with the second transmission and is transmitted in physical layer signaling. In some embodiments, the second target ID is jointly encoded with data carried by the second transmission and is transmitted in high layer signaling. In some embodiments, the second target ID is included in control

information associated with the second transmission. In some embodiments, the second target ID is used to scramble CRC bits for control information associated with the second transmission.

[00204] In some embodiments, the first communication device may transmit control information associated with the second transmission, wherein CRC bits for the control information are scrambled by a temporary ID for the first communication device assigned by a network, a serving base station, or the second communication device, or scrambled by a sequence common to devices within a same cell or a same network as the first communication device.

[00205] In some embodiments, the first transmission further includes CRC bits for the independently encoded first target ID, CRC bits for the independently encoded first source ID, or both.

[00206] In some embodiments, the second transmission further includes CRC bits for the independently encoded second source ID, CRC bits for the independently encoded second target ID, or both.

[00207] In some embodiments, the first communication device may drop the first transmission in response to determining that the first transmission is not targeted for the first communication device or the first transmission is not from the second communication device.

[00208] In some embodiments, the first communication device is an ambient IoT device.

[00209] It should be appreciated by persons skilled in the art that the sequence of the operations in exemplary method 300 may be changed and some of the operations in exemplary method 300 may be eliminated or modified, without departing from the spirit and scope of the disclosure.

[00210] FIG. 4 illustrates a flowchart of method 400 for wireless communication in accordance with some embodiments of the present disclosure. Details described in all of the foregoing embodiments of the present disclosure are applicable for the

embodiments shown in FIG. 4. In some examples, method 400 may be performed by a sync source, for example, an NE (e.g., NE 102 in FIG. 1), a BS, a relay node, an IAB node, a WAB network, a UE (e.g., UE 104 in FIG. 1), a repeater, or a UE-type reader. In some embodiments, the sync source may execute a set of instructions to control the functional elements of the sync source to perform the described functions or operations. In some examples, a processor or controller of the sync source may cause the sync source to perform method 400.

[00211] At 411, a second communication device may transmit, to a first communication device, a first target ID associated with a first transmission or both the first target ID and a first source ID associated with the first transmission, wherein the first target ID is set to an ID of the first communication device that uniquely identifies the first communication device and the first source ID is set to an ID of the second communication device that uniquely identifies the second communication device. At 413, the second communication device may transmit, to the first communication device, the first transmission.

[00212] In some embodiments, the first target ID is independently encoded within the first transmission. In some embodiments, the first target ID is jointly encoded with control information associated with the first transmission and is transmitted in physical layer signaling. In some embodiments, the first target ID is jointly encoded with data carried by the first transmission and is transmitted in high layer signaling. In some embodiments, the first target ID is used to scramble CRC bits for control information associated with the first transmission. In some embodiments, the first target ID is included in control information associated with the first transmission.

[00213] In some embodiments, the first source ID is independently encoded within the first transmission. In some embodiments, the first source ID is jointly encoded with control information associated with the first transmission and is transmitted in physical layer signaling. In some embodiments, the first source ID is jointly encoded with data carried by the first transmission and is transmitted in high layer signaling. In some embodiments, the first source ID is included in control information associated with the first transmission. In some embodiments, the first source ID is used to scramble CRC bits for control information associated with the first transmission.

[00214] In some embodiments, the second communication device may transmit, to the first communication device, a temporary ID for the first communication device.

[00215] In some embodiments, the second communication device may transmit control information associated with the first transmission, wherein CRC bits for the control information are scrambled by the temporary ID for the first communication device or by a sequence common to devices within a same cell or a same network as the first communication device.

[00216] In some embodiments, the second communication device may: receive a second source ID associated with a second transmission or both the second source ID and a second target ID associated with the second transmission; receive the second transmission; perform one or more operations of the following operations: determining whether the second transmission is from the first communication device based on the second source ID and the ID of the first communication device, and determining whether the second transmission is targeted for the second communication device based on the second target ID and the ID of the second communication device; and process the second transmission based on a result of the one or more operations.

[00217] In some embodiments, the second source ID is independently encoded within the second transmission. In some embodiments, the second source ID is jointly encoded with control information associated with the second transmission and is received in physical layer signaling. In some embodiments, the second source ID is jointly encoded with data carried by the second transmission and is received in high layer signaling. In some embodiments, the second source ID is used to scramble CRC bits for control information associated with the second transmission. In some embodiments, the second source ID is included in control information with the second transmission.

[00218] In some embodiments, the second target ID is independently encoded within the second transmission. In some embodiments, the second target ID is jointly encoded with control information associated with the second transmission and is received in physical layer signaling. In some embodiments, the second target ID is jointly encoded with data carried by the second transmission and is received in high layer signaling. In some embodiments, the second target ID is included in control

information associated with the second transmission. In some embodiments, the second target ID is used to scramble CRC bits for control information associated with the second transmission.

[00219] In some embodiments, the second communication device may: receive control information associated with the second transmission; and determine whether the second transmission is from the first communication device based on a temporary ID for the first communication device and CRC bits for the control information associated with the second transmission.

[00220] In some embodiments, the second communication device may receive control information associated with the second transmission, wherein CRC bits for the control information are scrambled by a temporary ID for a device transmitting the second transmission or by a sequence common to devices within a same cell or a same network as the device transmitting the second transmission.

[00221] In some embodiments, the first transmission further includes CRC bits for the independently encoded first target ID, CRC bits for the independently encoded first source ID, or both.

[00222] In some embodiments, the second transmission further includes CRC bits for the independently encoded second source ID, CRC bits for the independently encoded second target ID, or both.

[00223] In some embodiments, the second communication device may drop the second transmission in response to determining that the second transmission is not from the first communication device or the second transmission is not targeted for the second communication device.

[00224] In some embodiments, the second communication device is an NE, a base station, a UE, a relay node, an IAB node, a WAB network, a repeater, or a UE-type reader.

[00225] It should be appreciated by persons skilled in the art that the sequence of the operations in exemplary method 400 may be changed and some of the operations in

exemplary method 400 may be eliminated or modified, without departing from the spirit and scope of the disclosure.

[00226] FIG. 5 illustrates a block diagram of exemplary apparatus 500 according to some embodiments of the present disclosure. As shown in FIG. 5, the apparatus 500 may include at least one processor 506 and at least one transceiver 502 coupled to the processor 506. The apparatus 500 may be an IoT device (e.g., an ambient IoT tag) or a sync source (e.g., an NE, a BS, an IAB node, a WAB node, a relay node, a UE, a repeater or a UE-type reader).

[00227] Although in this figure, elements such as the at least one transceiver 502 and processor 506 are described in the singular, the plural is contemplated unless a limitation to the singular is explicitly stated. In some embodiments of the present disclosure, the transceiver 502 may be divided into two devices, such as a receiving circuitry and a transmitting circuitry. In some embodiments of the present disclosure, the apparatus 500 may further include an input device, a memory, and/or other components.

[00228] In some embodiments of the present disclosure, the apparatus 500 may be an IoT device. The transceiver 502 and the processor 506 may interact with each other so as to perform the operations with respect to the IoT device or the first communication device described in the foregoing embodiments such as FIGs. 3 and 4. In some embodiments of the present disclosure, the apparatus 500 may be a sync source. The transceiver 502 and the processor 506 may interact with each other so as to perform the operations with respect to the sync source or the second communication device described in the foregoing embodiments such as FIGs. 3 and 4.

[00229] In some embodiments of the present disclosure, the apparatus 500 may further include at least one non-transitory computer-readable medium.

[00230] For example, in some embodiments of the present disclosure, the non-transitory computer-readable medium may have stored thereon computer-executable instructions to cause the processor 506 to implement the method with respect to the IoT device or the first communication device as described above. For example, the computer-executable instructions, when executed, cause the processor 506 interacting

with transceiver 502 to perform the operations with respect to the first communication device described in FIGs. 3 and 4.

[00231] In some embodiments of the present disclosure, the non-transitory computer-readable medium may have stored thereon computer-executable instructions to cause the processor 506 to implement the method with respect to the sync source or the second communication device as described above. For example, the computer-executable instructions, when executed, cause the processor 506 interacting with transceiver 502 to perform the operations with respect to the second communication device described in FIGs. 3 and 4.

[00232] FIG. 6 illustrates an example of a UE 600 in accordance with aspects of the present disclosure. The UE 600 may include a processor 602, a memory 604, a controller 606, and a transceiver 608. The processor 602, the memory 604, the controller 606, or the transceiver 608, or various combinations thereof or various components thereof may be examples of means for performing various aspects of the present disclosure as described herein. These components may be coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces.

[00233] The processor 602, the memory 604, the controller 606, or the transceiver 608, or various combinations or components thereof may be implemented in hardware (e.g., circuitry). The hardware may include a processor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), or other programmable logic device, or any combination thereof configured as or otherwise supporting a means for performing the functions described in the present disclosure.

[00234] The processor 602 may include an intelligent hardware device (e.g., a general-purpose processor, a DSP, a CPU, an ASIC, an FPGA, or any combination thereof). In some implementations, the processor 602 may be configured to operate the memory 604. In some other implementations, the memory 604 may be integrated into the processor 602. The processor 602 may be configured to execute computer-readable instructions stored in the memory 604 to cause the UE 600 to perform various functions of the present disclosure.

[00235] The memory 604 may include volatile or non-volatile memory. The memory 604 may store computer-readable, computer-executable code including instructions when executed by the processor 602 cause the UE 600 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as the memory 604 or another type of memory. Computer-readable media includes both non-transitory computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A non-transitory storage medium may be any available medium that may be accessed by a general-purpose or special-purpose computer.

[00236] In some implementations, the processor 602 and the memory 604 coupled with the processor 602 may be configured to cause the UE 600 to perform one or more of the functions described herein (e.g., executing, by the processor 602, instructions stored in the memory 604). For example, the processor 602 may support wireless communication at the UE 600 in accordance with examples as disclosed herein. For example, the UE 600 may be configured to support means for performing the operations as described with respect to FIG. 4.

[00237] For example, the UE 600 may be configured to support: a means for transmitting transmit, to a first communication device, a first target ID associated with a first transmission or both the first target ID and a first source ID associated with the first transmission, wherein the first target ID is set to an ID of the first communication device that uniquely identifies the first communication device and the first source ID is set to an ID of the UE 600 that uniquely identifies the UE 600; and a means for transmitting, to the first communication device, the first transmission.

[00238] The controller 606 may manage input and output signals for the UE 600. The controller 606 may also manage peripherals not integrated into the UE 600. In some implementations, the controller 606 may utilize an operating system such as iOS®, ANDROID®, WINDOWS®, or other operating systems. In some implementations, the controller 606 may be implemented as part of the processor 602.

[00239] In some implementations, the UE 600 may include at least one transceiver 608. In some other implementations, the UE 600 may have more than one transceiver 608. The transceiver 608 may represent a wireless transceiver. The transceiver 608 may

include one or more receiver chains 610, one or more transmitter chains 612, or a combination thereof.

[00240] A receiver chain 610 may be configured to receive signals (e.g., control information, data, or packets) over a wireless medium. For example, the receiver chain 610 may include one or more antennas for receive the signal over the air or wireless medium. The receiver chain 610 may include at least one amplifier (e.g., a low-noise amplifier (LNA)) configured to amplify the received signal. The receiver chain 610 may include at least one demodulator configured to demodulate the receive signal and obtain the transmitted data by reversing the modulation technique applied during transmission of the signal. The receiver chain 610 may include at least one decoder for decoding the processing the demodulated signal to receive the transmitted data.

[00241] A transmitter chain 612 may be configured to generate and transmit signals (e.g., control information, data, or packets). The transmitter chain 612 may include at least one modulator for modulating data onto a carrier signal, preparing the signal for transmission over a wireless medium. The at least one modulator may be configured to support one or more techniques such as amplitude modulation (AM), frequency modulation (FM), or digital modulation schemes like phase-shift keying (PSK) or quadrature amplitude modulation (QAM). The transmitter chain 612 may also include at least one power amplifier configured to amplify the modulated signal to an appropriate power level suitable for transmission over the wireless medium. The transmitter chain 612 may also include one or more antennas for transmitting the amplified signal into the air or wireless medium.

[00242] It should be appreciated by persons skilled in the art that the components in exemplary UE 600 may be changed, for example, some of the components in exemplary UE 600 may be omitted or modified or a new component(s) may be added to exemplary UE 600, without departing from the spirit and scope of the disclosure. For example, in some embodiments, the UE 600 may not include the controller 606.

[00243] FIG. 7 illustrates an example of a processor 700 in accordance with aspects of the present disclosure. The processor 700 may be an example of a processor configured to perform various operations in accordance with examples as described

herein. The processor 700 may include a controller 702 configured to perform various operations in accordance with examples as described herein. The processor 700 may optionally include at least one memory 704, which may be, for example, an L1/L2/L3 cache. Additionally, or alternatively, the processor 700 may optionally include one or more arithmetic-logic units (ALUs) 706. One or more of these components may be in electronic communication or otherwise coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces (e.g., buses).

[00244] The processor 700 may be a processor chipset and include a protocol stack (e.g., a software stack) executed by the processor chipset to perform various operations (e.g., receiving, obtaining, retrieving, transmitting, outputting, forwarding, storing, determining, identifying, accessing, writing, reading) in accordance with examples as described herein. The processor chipset may include one or more cores, one or more caches (e.g., memory local to or included in the processor chipset (e.g., the processor 700) or other memory (e.g., random access memory (RAM), read-only memory (ROM), dynamic RAM (DRAM), synchronous dynamic RAM (SDRAM), static RAM (SRAM), ferroelectric RAM (FeRAM), magnetic RAM (MRAM), resistive RAM (RRAM), flash memory, phase change memory (PCM), and others).

[00245] The controller 702 may be configured to manage and coordinate various operations (e.g., signaling, receiving, obtaining, retrieving, transmitting, outputting, forwarding, storing, determining, identifying, accessing, writing, reading) of the processor 700 to cause the processor 700 to support various operations in accordance with examples as described herein. For example, the controller 702 may operate as a control unit of the processor 700, generating control signals that manage the operation of various components of the processor 700. These control signals include enabling or disabling functional units, selecting data paths, initiating memory access, and coordinating timing of operations.

[00246] The controller 702 may be configured to fetch (e.g., obtain, retrieve, receive) instructions from the memory 704 and determine a subsequent instruction(s) to be executed to cause the processor 700 to support various operations in accordance with examples as described herein. The controller 702 may be configured to track memory address of instructions associated with the memory 704. The controller 702 may be

configured to decode instructions to determine the operation to be performed and the operands involved. For example, the controller 702 may be configured to interpret the instruction and determine control signals to be output to other components of the processor 700 to cause the processor 700 to support various operations in accordance with examples as described herein. Additionally, or alternatively, the controller 702 may be configured to manage flow of data within the processor 700. The controller 702 may be configured to control transfer of data between registers, ALUs, and other functional units of the processor 700.

[00247] The memory 704 may include one or more caches (e.g., memory local to or included in the processor 700 or other memory, such RAM, ROM, DRAM, SDRAM, SRAM, MRAM, flash memory, etc. In some implementations, the memory 704 may reside within or on a processor chipset (e.g., local to the processor 700). In some other implementations, the memory 704 may reside external to the processor chipset (e.g., remote to the processor 700).

[00248] The memory 704 may store computer-readable, computer-executable code including instructions that, when executed by the processor 700, cause the processor 700 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as system memory or another type of memory. The controller 702 and/or the processor 700 may be configured to execute computer-readable instructions stored in the memory 704 to cause the processor 700 to perform various functions. For example, the processor 700 and/or the controller 702 may be coupled with or to the memory 704, the processor 700, the controller 702, and the memory 704 may be configured to perform various functions described herein. In some examples, the processor 700 may include multiple processors and the memory 704 may include multiple memories. One or more of the multiple processors may be coupled with one or more of the multiple memories, which may, individually or collectively, be configured to perform various functions herein.

[00249] The one or more ALUs 706 may be configured to support various operations in accordance with examples as described herein. In some implementations, the one or more ALUs 706 may reside within or on a processor chipset (e.g., the processor 700). In some other implementations, the one or more ALUs 706 may reside external to the

processor chipset (e.g., the processor 700). One or more ALUs 706 may perform one or more computations such as addition, subtraction, multiplication, and division on data. For example, one or more ALUs 706 may receive input operands and an operation code, which determines an operation to be executed. One or more ALUs 706 be configured with a variety of logical and arithmetic circuits, including adders, subtractors, shifters, and logic gates, to process and manipulate the data according to the operation. Additionally, or alternatively, the one or more ALUs 706 may support logical operations such as AND, OR, exclusive-OR (XOR), not-OR (NOR), and not-AND (NAND), enabling the one or more ALUs 706 to handle conditional operations, comparisons, and bitwise operations.

[00250] The processor 700 may support wireless communication in accordance with examples as disclosed herein.

[00251] For example, the processor 700 may be configured to support means for performing the operations as described with respect to FIG. 3. For example, the processor 700 may be configured to or operable to support: a means for receiving a first target ID associated with a first transmission or both the first target ID and a first source ID associated with the first transmission; a means for receiving the first transmission; a means for performing one or more operations of the following operations: determining whether the first transmission is targeted for a first communication device based on the first target ID and a device ID of the first communication device that uniquely identifies the first communication device, and determining whether the first transmission is from a second communication device based on the first source ID and an ID of the second communication device that uniquely identifies the second communication device; and a means for processing the first transmission based on a result of the one or more operations.

[00252] For example, the processor 700 may be configured to support means for performing the operations as described with respect to FIG. 4. For example, the processor 700 may be configured to or operable to support: a means for transmitting transmit, to a first communication device, a first target ID associated with a first transmission or both the first target ID and a first source ID associated with the first transmission, wherein the first target ID is set to an ID of the first communication device

that uniquely identifies the first communication device and the first source ID is set to an ID of a second communication device that uniquely identifies the second communication device; and a means for transmitting, to the first communication device, the first transmission.

[00253] It should be appreciated by persons skilled in the art that the components in exemplary processor 700 may be changed, for example, some of the components in exemplary processor 700 may be omitted or modified or a new component(s) may be added to exemplary processor 700, without departing from the spirit and scope of the disclosure. For example, in some embodiments, the processor 700 may not include the ALUs 706.

[00254] FIG. 8 illustrates an example of an NE 800 in accordance with aspects of the present disclosure. The NE 800 may include a processor 802, a memory 804, a controller 806, and a transceiver 808. The processor 802, the memory 804, the controller 806, or the transceiver 808, or various combinations thereof or various components thereof may be examples of means for performing various aspects of the present disclosure as described herein. These components may be coupled (e.g., operatively, communicatively, functionally, electronically, electrically) via one or more interfaces.

[00255] The processor 802, the memory 804, the controller 806, or the transceiver 808, or various combinations or components thereof may be implemented in hardware (e.g., circuitry). The hardware may include a processor, a DSP, an ASIC, or other programmable logic device, or any combination thereof configured as or otherwise supporting a means for performing the functions described in the present disclosure.

[00256] The processor 802 may include an intelligent hardware device (e.g., a general-purpose processor, a DSP, a CPU, an ASIC, an FPGA, or any combination thereof). In some implementations, the processor 802 may be configured to operate the memory 804. In some other implementations, the memory 804 may be integrated into the processor 802. The processor 802 may be configured to execute computer-readable instructions stored in the memory 804 to cause the NE 800 to perform various functions of the present disclosure.

[00257] The memory 804 may include volatile or non-volatile memory. The memory 804 may store computer-readable, computer-executable code including instructions when executed by the processor 802 cause the NE 800 to perform various functions described herein. The code may be stored in a non-transitory computer-readable medium such as the memory 804 or another type of memory. Computer-readable media includes both non-transitory computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A non-transitory storage medium may be any available medium that may be accessed by a general-purpose or special-purpose computer.

[00258] In some implementations, the processor 802 and the memory 804 coupled with the processor 802 may be configured to cause the NE 800 to perform one or more of the functions described herein (e.g., executing, by the processor 802, instructions stored in the memory 804). For example, the processor 802 may support wireless communication at the NE 800 in accordance with examples as disclosed herein. For example, the NE 800 may be configured to support means for performing the operations as described with respect to FIG. 4.

[00259] For example, the NE 800 may be configured to support: a means for transmitting transmit, to a first communication device, a first target ID associated with a first transmission or both the first target ID and a first source ID associated with the first transmission, wherein the first target ID is set to an ID of the first communication device that uniquely identifies the first communication device and the first source ID is set to an ID of the NE 800 that uniquely identifies the NE 800; and a means for transmitting, to the first communication device, the first transmission.

[00260] The controller 806 may manage input and output signals for the NE 800. The controller 806 may also manage peripherals not integrated into the NE 800. In some implementations, the controller 806 may utilize an operating system such as iOS®, ANDROID®, WINDOWS®, or other operating systems. In some implementations, the controller 806 may be implemented as part of the processor 802.

[00261] In some implementations, the NE 800 may include at least one transceiver 808. In some other implementations, the NE 800 may have more than one transceiver 808. The transceiver 808 may represent a wireless transceiver. The transceiver 808 may

include one or more receiver chains 810, one or more transmitter chains 812, or a combination thereof.

[00262] A receiver chain 810 may be configured to receive signals (e.g., control information, data, or packets) over a wireless medium. For example, the receiver chain 810 may include one or more antennas for receive the signal over the air or wireless medium. The receiver chain 810 may include at least one amplifier (e.g., an LNA) configured to amplify the received signal. The receiver chain 810 may include at least one demodulator configured to demodulate the receive signal and obtain the transmitted data by reversing the modulation technique applied during transmission of the signal. The receiver chain 810 may include at least one decoder for decoding the processing the demodulated signal to receive the transmitted data.

[00263] A transmitter chain 812 may be configured to generate and transmit signals (e.g., control information, data, or packets). The transmitter chain 812 may include at least one modulator for modulating data onto a carrier signal, preparing the signal for transmission over a wireless medium. The at least one modulator may be configured to support one or more techniques such as AM, FM, or digital modulation schemes like PSK or QAM. The transmitter chain 812 may also include at least one power amplifier configured to amplify the modulated signal to an appropriate power level suitable for transmission over the wireless medium. The transmitter chain 812 may also include one or more antennas for transmitting the amplified signal into the air or wireless medium.

[00264] It should be appreciated by persons skilled in the art that the components in exemplary NE 800 may be changed, for example, some of the components in exemplary NE 800 may be omitted or modified or a new component(s) may be added to exemplary NE 800, without departing from the spirit and scope of the disclosure. For example, in some embodiments, the NE 800 may not include the controller 806.

[00265] Those having ordinary skill in the art would understand that the operations or steps of the methods described in connection with the aspects disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, a hard disk, a

removable disk, a CD-ROM, or any other form of storage medium known in the art. Additionally, in some aspects, the operations or steps of the methods may reside as one or any combination or set of codes and/or instructions on a non-transitory computer-readable medium, which may be incorporated into a computer program product.

[00266] While this disclosure has been described with specific embodiments thereof, it is evident that many alternatives, modifications, and variations may be apparent to those skilled in the art. The disclosure is not limited to the examples and designs described herein but is to be accorded with the broadest scope consistent with the principles and novel features disclosed herein. For example, various components of the embodiments may be interchanged, added, or substituted in other embodiments. Also, all of the elements of each figure are not necessary for the operation of the disclosed embodiments. For example, one of ordinary skill in the art of the disclosed embodiments would be enabled to make and use the teachings of the disclosure by simply employing the elements of the independent claims. Accordingly, embodiments of the disclosure as set forth herein are intended to be illustrative, not limiting. Various changes may be made without departing from the spirit and scope of the disclosure.

[00267] In this document, the terms "includes," "including," or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or apparatus that includes a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. An element preceded by "a," "an," or the like does not, without more constraints, preclude the existence of additional identical elements in the process, method, article, or apparatus that includes the element. Also, the term "another" is defined as at least a second or more. The term "having" or the like, as used herein, is defined as "including." Expressions such as "A and/or B" or "at least one of A and B" may include any and all combinations of words enumerated along with the expression. For instance, the expression "A and/or B" or "at least one of A and B" may include A, B, or both A and B. The wording "the first," "the second" or the like is only used to clearly illustrate the embodiments of the present disclosure, but is not used to limit the substance of the present disclosure.

WHAT IS CLAIMED:

1. A first communication device, comprising:
 - at least one transmitter;
 - at least one receiver; and
 - at least one processor coupled with the at least one transmitter and the at least one receiver, and configured to cause the first communication device to:
 - receive a first target ID associated with a first transmission or both the first target ID and a first source ID associated with the first transmission;
 - receive the first transmission;
 - perform one or more operations of the following operations:
 - determining whether the first transmission is targeted for the first communication device based on the first target ID and a device ID of the first communication device that uniquely identifies the first communication device, and
 - determining whether the first transmission is from a second communication device based on the first source ID and an ID of the second communication device that uniquely identifies the second communication device; and
 - process the first transmission based on a result of the one or more operations.
2. The first communication device of claim 1, wherein the first target ID is independently encoded within the first transmission,
 - wherein the first target ID is jointly encoded with control information associated with the first transmission and is received in physical layer signaling,
 - wherein the first target ID is jointly encoded with data carried by the first transmission and is received in high layer signaling,
 - wherein the first target ID is used to scramble cyclic redundancy check (CRC) bits for control information associated with the first transmission, or
 - wherein the first target ID is included in control information associated with the first transmission; and

wherein the first source ID is independently encoded within the first transmission,

wherein the first source ID is jointly encoded with control information associated with the first transmission and is received in physical layer signaling,

wherein the first source ID is jointly encoded with data carried by the first transmission and is received in high layer signaling,

wherein the first source ID is included in control information associated with the first transmission, or

wherein the first source ID is used to scramble CRC bits for control information associated with the first transmission.

3. The first communication device of claim 1, wherein the at least one processor is further configured to cause the first communication device to receive a temporary ID for the first communication device assigned by a network, a serving base station, or the second communication device.

4. The first communication device of claim 1 or 3, wherein the at least one processor is further configured to cause the first communication device to:

receive control information associated with the first transmission; and

determine whether the first transmission is targeted for the first communication device based on a temporary ID of the first communication device and cyclic redundancy check (CRC) bits for the control information associated with the first transmission.

5. The first communication device of claim 1 or 3, wherein the at least one processor is further configured to cause the first communication device to receive control information associated with the first transmission, wherein cyclic redundancy check (CRC) bits for the control information are scrambled by a temporary ID for a target device of the first transmission or by a sequence common to devices within a same cell or a same network as the target device.

6. The first communication device of claim 1, wherein the at least one processor is further configured to cause the first communication device to:

transmit, to the second communication device, a second source ID associated with a second transmission or both the second source ID and a second target ID associated with the second transmission, wherein the second source ID is set to the device ID of the first communication device and the second target ID is set to the ID of the second communication device; and

transmit, to the second communication device, the second transmission.

7. The first communication device of claim 6, wherein the second source ID is independently encoded within the second transmission,

wherein the second source ID is jointly encoded with control information associated with the second transmission and is transmitted in physical layer signaling,

wherein the second source ID is jointly encoded with data carried by the second transmission and is transmitted in high layer signaling,

wherein the second source ID is used to scramble cyclic redundancy check (CRC) bits for control information associated with the second transmission, or

wherein the second source ID is included in control information with the second transmission; and

wherein the second target ID is independently encoded within the second transmission,

wherein the second target ID is jointly encoded with control information associated with the second transmission and is transmitted in physical layer signaling,

wherein the second target ID is jointly encoded with data carried by the second transmission and is transmitted in high layer signaling,

wherein the second target ID is included in control information associated with the second transmission, or

wherein the second target ID is used to scramble CRC bits for control information associated with the second transmission.

8. The first communication device of claim 6, wherein the at least one processor is further configured to cause the first communication device to transmit control information associated with the second transmission, wherein cyclic redundancy check (CRC) bits for the control information are scrambled by a temporary ID for the first communication device assigned by a network, a serving base station, or the second communication device, or scrambled by a sequence common to devices within a same cell or a same network as the first communication device.

9. The first communication device of claim 2, wherein the first transmission further comprises CRC bits for the independently encoded first target ID, CRC bits for the independently encoded first source ID, or both.

10. The first communication device of claim 7, wherein the second transmission further comprises CRC bits for the independently encoded second source ID, CRC bits for the independently encoded second target ID, or both.

11. A second communication device, comprising:

at least one transmitter;

at least one receiver; and

at least one processor coupled with the at least one transmitter and the at least one receiver, and configured to cause the second communication device to:

transmit, to a first communication device, a first target ID associated with a first transmission or both the first target ID and a first source ID associated with the first transmission, wherein the first target ID is set to an ID of the first communication device that uniquely identifies the first communication device and the first source ID is set to an ID of the second communication device that uniquely identifies the second communication device; and

transmit, to the first communication device, the first transmission.

12. The second communication device of claim 11, wherein the first target ID is independently encoded within the first transmission;

wherein the first target ID is jointly encoded with control information associated with the first transmission and is transmitted in physical layer signaling,

wherein the first target ID is jointly encoded with data carried by the first transmission and is transmitted in high layer signaling,

wherein the first target ID is used to scramble cyclic redundancy check (CRC) bits for control information associated with the first transmission, or

wherein the first target ID is included in control information associated with the first transmission; and

wherein the first source ID is independently encoded within the first transmission,

wherein the first source ID is jointly encoded with control information associated with the first transmission and is transmitted in physical layer signaling,

wherein the first source ID is jointly encoded with data carried by the first transmission and is transmitted in high layer signaling,

wherein the first source ID is included in control information associated with the first transmission, or

wherein the first source ID is used to scramble CRC bits for control information associated with the first transmission.

13. The second communication device of claim 11, wherein the at least one processor is further configured to cause the second communication device to transmit, to the first communication device, a temporary ID for the first communication device.

14. The second communication device of claim 13, wherein the at least one processor is further configured to cause the second communication device to transmit control information associated with the first transmission, wherein cyclic redundancy check (CRC) bits for the control information are scrambled by the temporary ID for the first communication device or by a sequence common to devices within a same cell or a same network as the first communication device.

15. The second communication device of claim 11, wherein the at least one processor is further configured to cause the second communication device to:

receive a second source ID associated with a second transmission or both the second source ID and a second target ID associated with the second transmission;

receive the second transmission;

perform one or more operations of the following operations:

determining whether the second transmission is from the first communication device based on the second source ID and the ID of the first communication device, and

determining whether the second transmission is targeted for the second communication device based on the second target ID and the ID of the second communication device; and

process the second transmission based on a result of the one or more operations.

16. The second communication device of claim 15, wherein the second source ID is independently encoded within the second transmission,

wherein the second source ID is jointly encoded with control information associated with the second transmission and is received in physical layer signaling,

wherein the second source ID is jointly encoded with data carried by the second transmission and is received in high layer signaling,

wherein the second source ID is used to scramble cyclic redundancy check (CRC) bits for control information associated with the second transmission, or

wherein the second source ID is included in control information with the second transmission; and

wherein the second target ID is independently encoded within the second transmission,

wherein the second target ID is jointly encoded with control information associated with the second transmission and is received in physical layer signaling,

wherein the second target ID is jointly encoded with data carried by the second transmission and is received in high layer signaling,

wherein the second target ID is included in control information associated with the second transmission, or

wherein the second target ID is used to scramble CRC bits for control information associated with the second transmission.

17. The second communication device of claim 15, wherein the at least one processor is further configured to cause the second communication device to:

receive control information associated with the second transmission; and

determine whether the second transmission is from the first communication device based on a temporary ID for the first communication device and cyclic redundancy check (CRC) bits for the control information associated with the second transmission.

18. The second communication device of claim 15, wherein the at least one processor is further configured to cause the second communication device to receive control information associated with the second transmission, wherein cyclic redundancy check (CRC) bits for the control information are scrambled by a temporary ID for a device transmitting the second transmission or by a sequence common to devices within a same cell or a same network as the device transmitting the second transmission.

19. A processor, comprising:

at least one controller coupled with at least one memory and configured to cause the processor to:

transmit, to a first communication device, a first target ID associated with a first transmission or both the first target ID and a first source ID associated with the first transmission, wherein the first target ID is set to an ID of the first communication device that uniquely identifies the first communication device and the first source ID is set to an ID of a second communication device that uniquely identifies the second communication device; and

transmit, to the first communication device, the first transmission.

20. A method for wireless communication, comprising:

receiving a first target ID associated with a first transmission or both the first target ID and a first source ID associated with the first transmission;

receiving the first transmission;

performing one or more operations of the following operations:

determining whether the first transmission is targeted for a first communication device based on the first target ID and a device ID of the first communication device that uniquely identifies the first communication device, and

determining whether the first transmission is from a second communication device based on the first source ID and an ID of the second communication device that uniquely identifies the second communication device; and

processing the first transmission based on a result of the one or more operations.

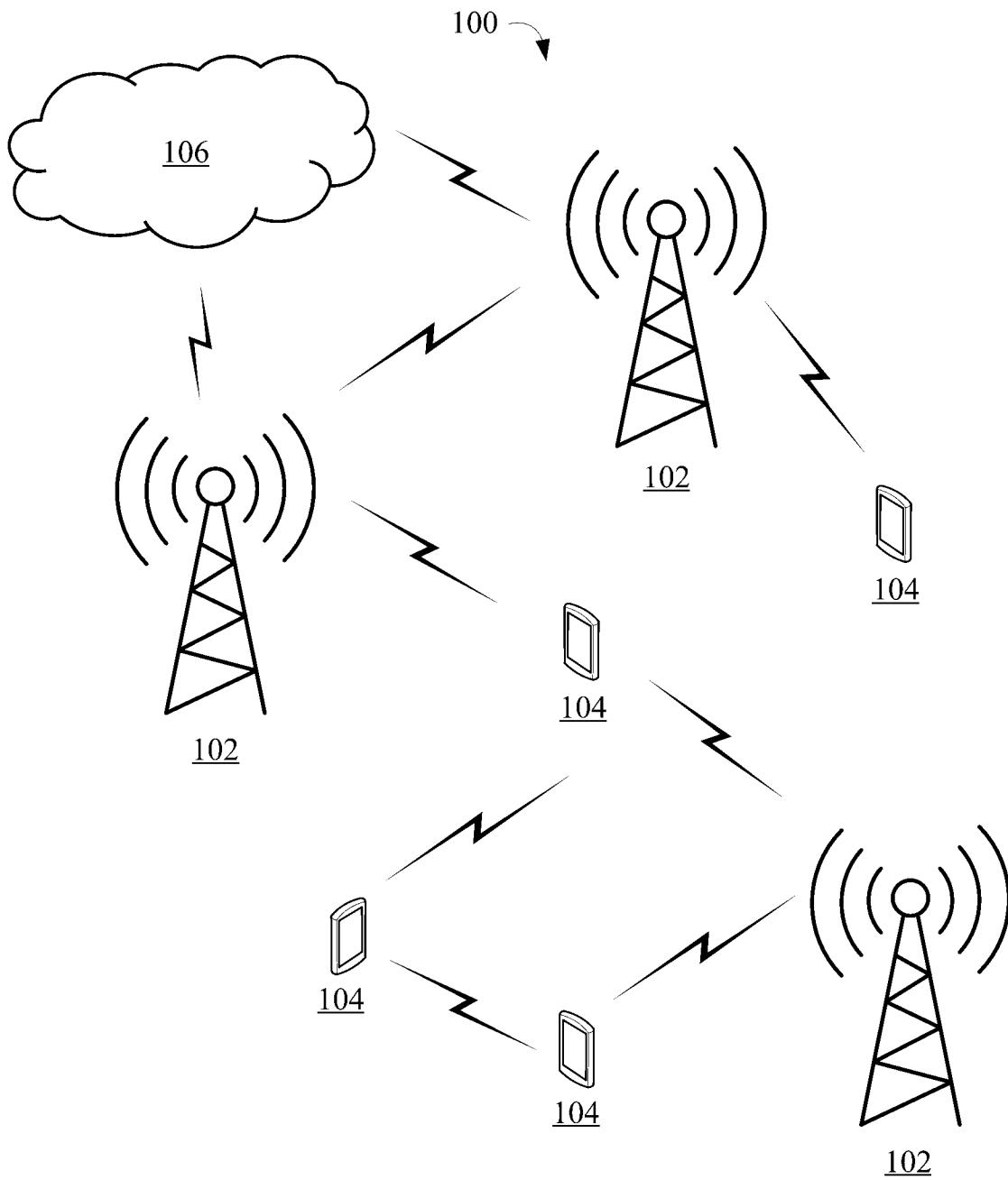


FIG. 1

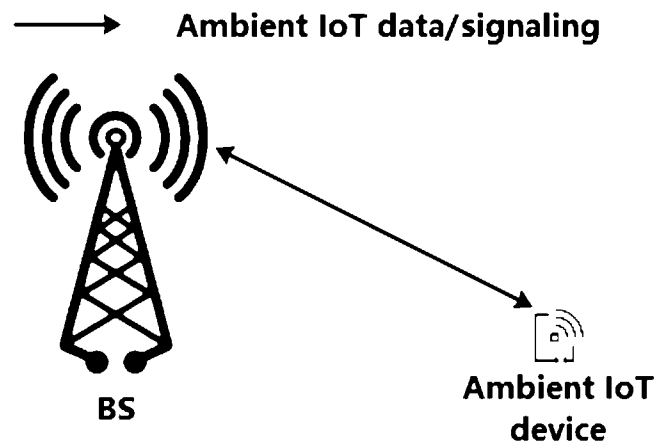


FIG. 2A

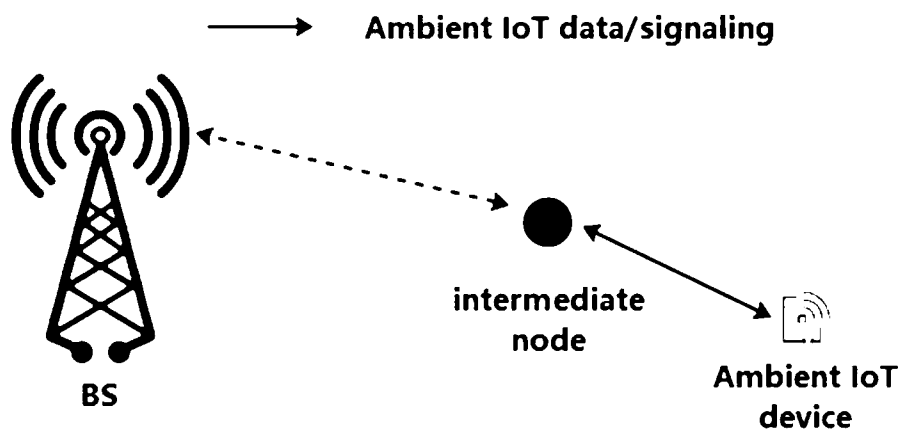


FIG. 2B

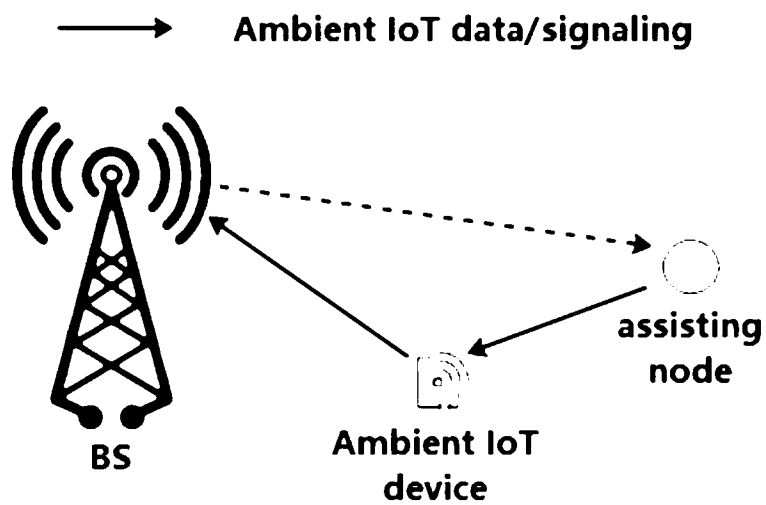


FIG. 2C

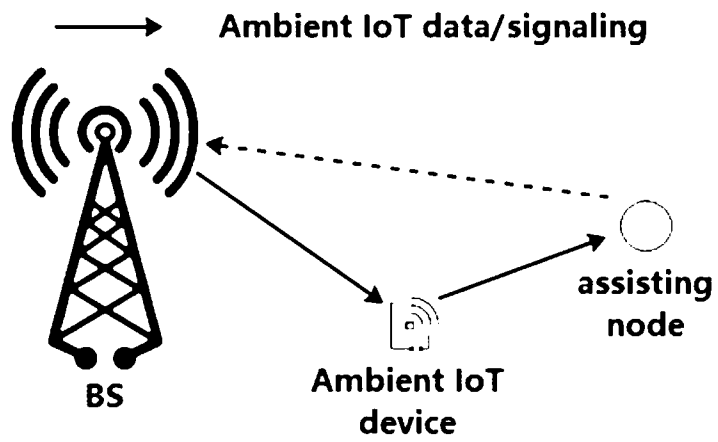


FIG. 2D

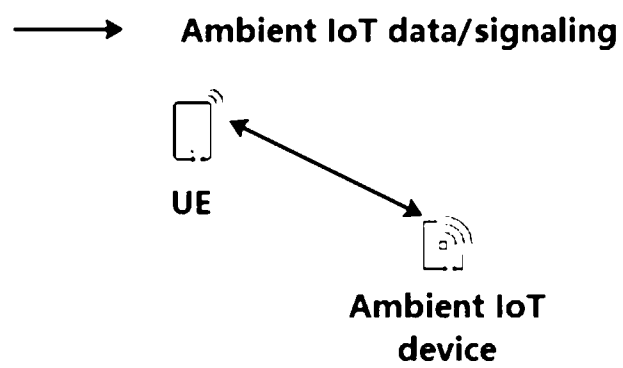


FIG. 2E

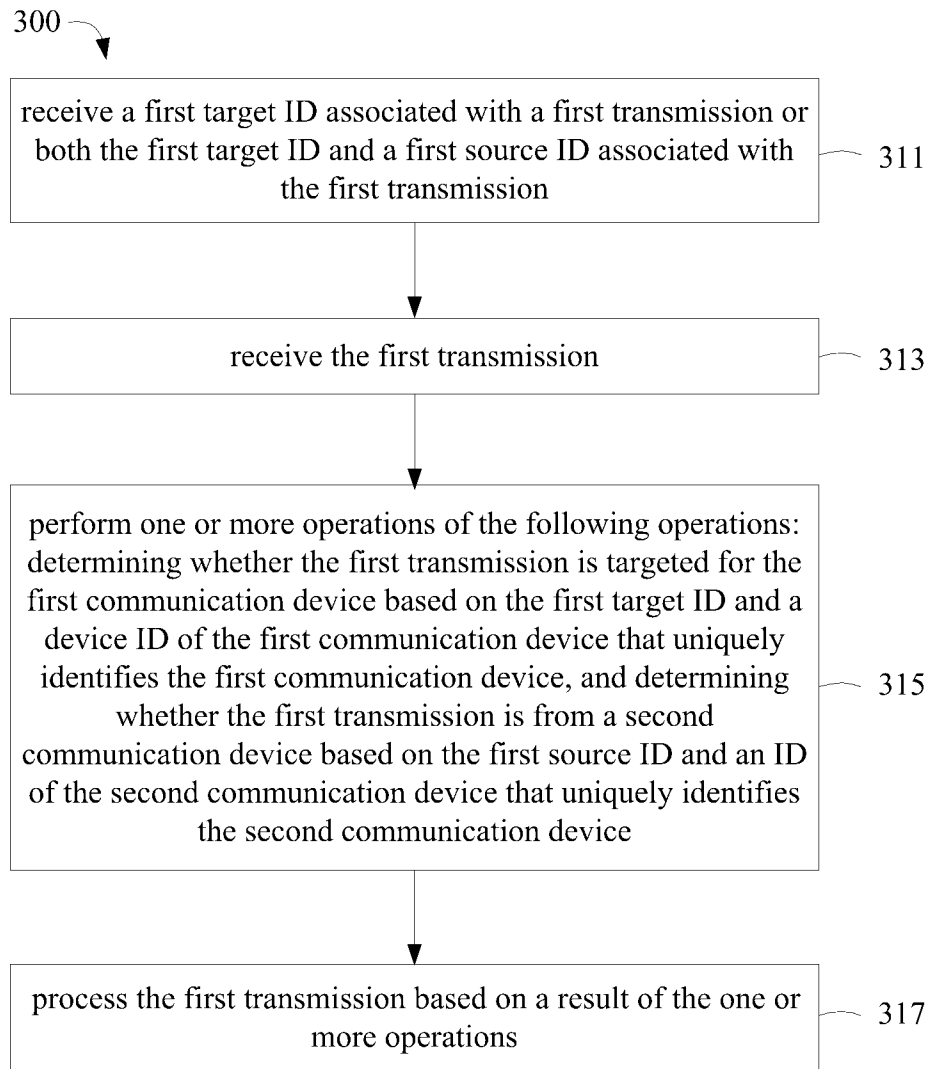


FIG. 3

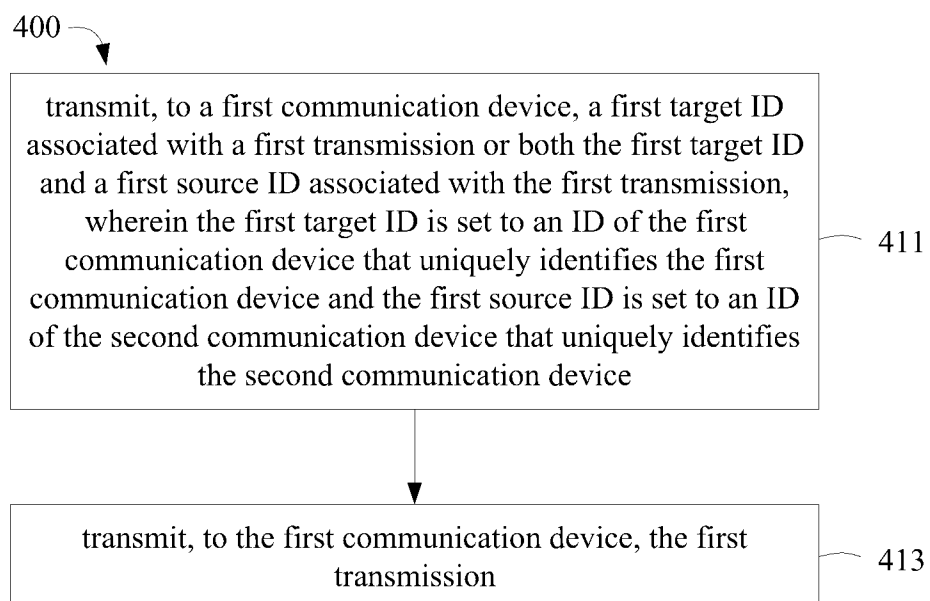


FIG. 4

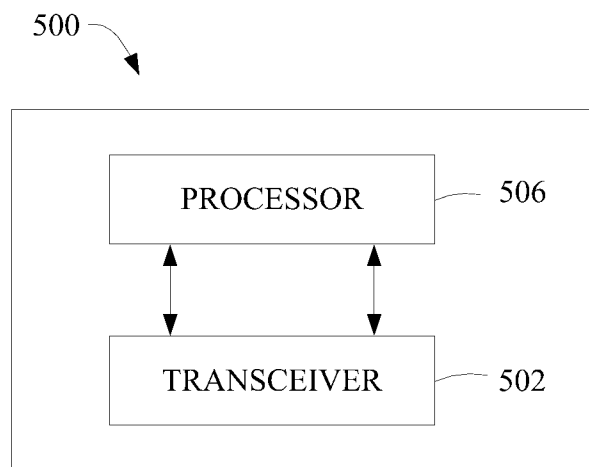


FIG. 5

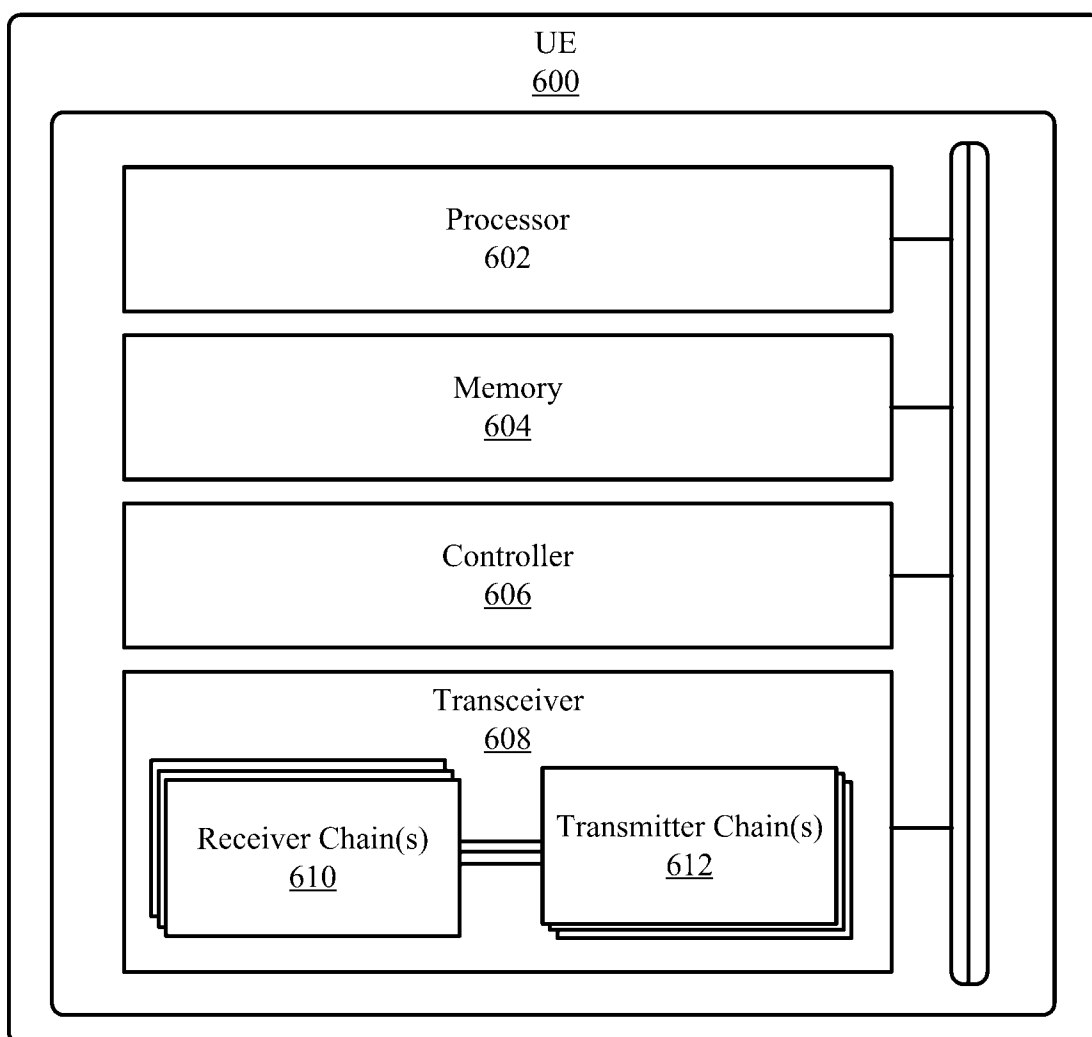


FIG. 6

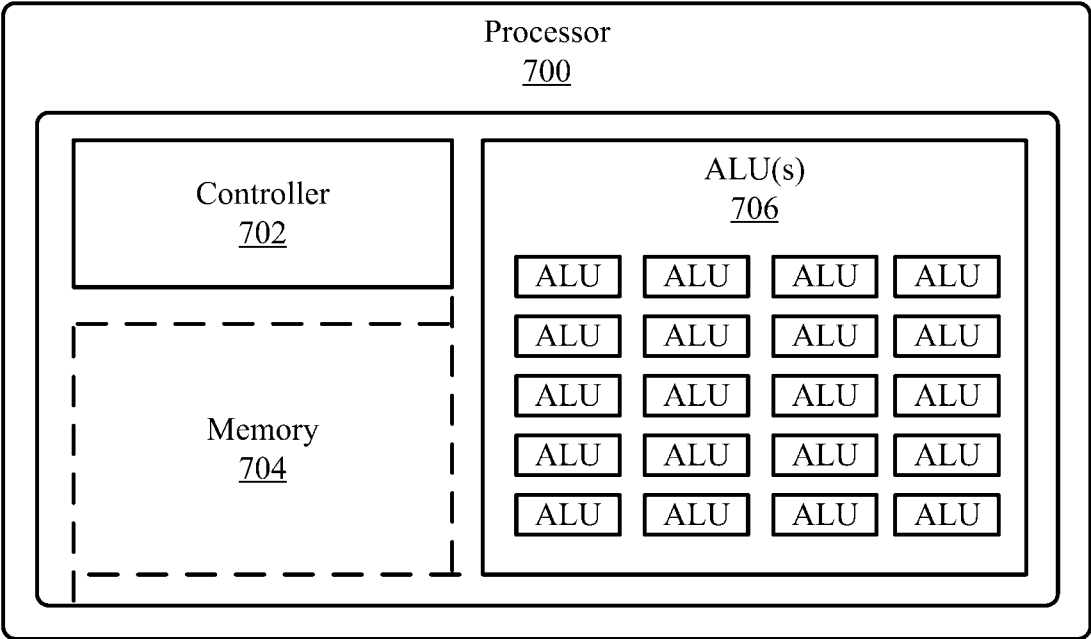


FIG. 7

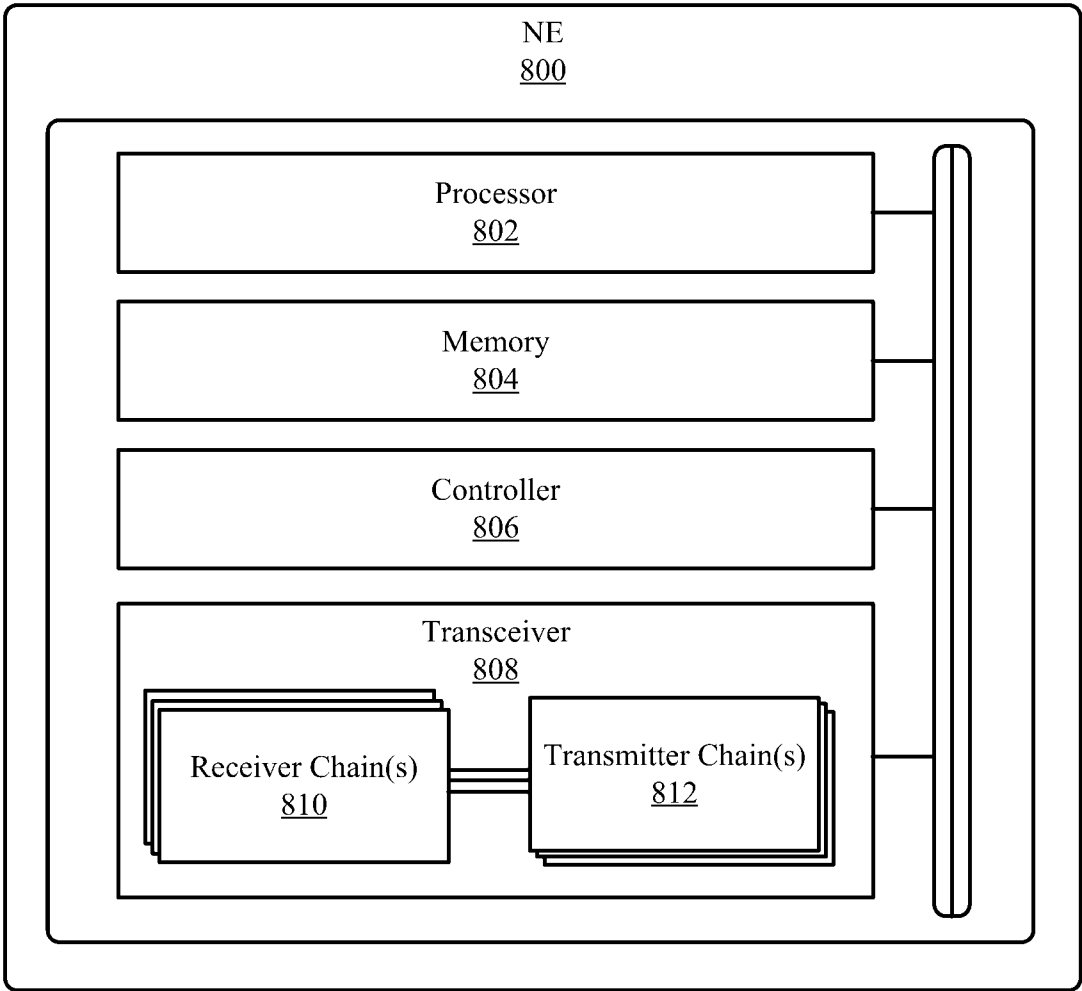


FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2024/072336

A. CLASSIFICATION OF SUBJECT MATTER H04W 72/20(2023.01)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) IPC: H04W, H04L, H04B 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) CNTXT, VCN, ENTXT, DWPI, CNKI, 3GPP: ambient w IoT, A-IoT, AMBC, tag, target w ID, source w ID, unique+, identif +, CRC, encod+		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103095594 A (BEIJING ITSYNCH TECHNOLOGIES CO., LTD.) 08 May 2013 (2013-05-08) description, paragraphs [0053]-[0069]	1-20
A	CN 111866797 A (HUAWEI TECHNOLOGIES CO., LTD.) 30 October 2020 (2020-10-30) the whole document	1-20
A	CN 117099326 A (BEIJING XIAOMI MOBILE SOFTWARE CO., LTD.) 21 November 2023 (2023-11-21) the whole document	1-20
A	US 2023141393 A1 (QUALCOMM INCORPORATED) 11 May 2023 (2023-05-11) the whole document	1-20
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents: “A” document defining the general state of the art which is not considered to be of particular relevance “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 27 September 2024		Date of mailing of the international search report 09 October 2024
Name and mailing address of the ISA/CN CHINA NATIONAL INTELLECTUAL PROPERTY ADMINISTRATION 6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088, China		Authorized officer LV,Miao Telephone No. (+86) 010-53961742

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2024/072336

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	103095594	A	08 May 2013	None	
CN	111866797	A	30 October 2020	None	
CN	117099326	A	21 November 2023	None	
US	2023141393	A1	11 May 2023	None	