

(51) International Patent Classification:  
*H04L 29/08* (2006.01)    *H04W 4/00* (2009.01)(21) International Application Number:  
PCT/US2015/044340(22) International Filing Date:  
7 August 2015 (07.08.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
62/035,580    11 August 2014 (11.08.2014)    US  
14/820,370    6 August 2015 (06.08.2015)    US(71) Applicant: QUALCOMM INCORPORATED [US/US];  
ATTN: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121-1714 (US).

(72) Inventor: GUPTA, Binita; 16208 Lone Bluff Way, San Diego, California 92127 (US).

(74) Agent: OLDS, Mark E.; Muncy, Geissler, Olds &amp; Lowe, P.C., 4000 Legato Road, Suite 310, Fairfax, Virginia 22033 (US).

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

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

## Published:

— with international search report (Art. 21(3))

(54) Title: METHOD AND APPARATUS FOR AUTOMATICALLY GENERATING AN EVENTS DICTIONARY IN AN INTERNET OF THINGS (IOT) NETWORK

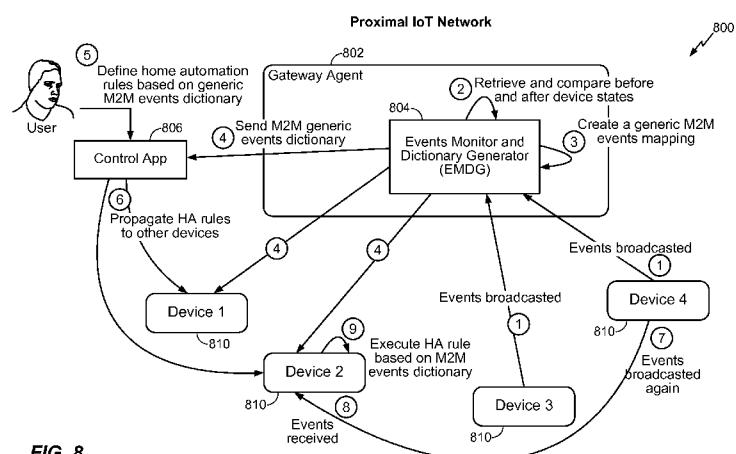


FIG. 8

(57) Abstract: Methods and systems are disclosed for automatically generating an events dictionary in an Internet of Things (IoT) network. In an aspect, a device receives a notification of an event from an IoT device, determines a state of the IoT device before and after the event, compares the states of the IoT device, determines a type of state change of the event, determines whether the type of the state change of the first event is present in the events dictionary, creates a generic entry based on the type of the state change of the first event not being present in the events dictionary, and stores, in the events dictionary, a mapping of an event description of the event to the generic entry.

## **METHOD AND APPARATUS FOR AUTOMATICALLY GENERATING AN EVENTS DICTIONARY IN AN INTERNET OF THINGS (IOT) NETWORK**

### **CROSS-REFERENCE TO RELATED APPLICATIONS**

[0001] The present Application for Patent claims the benefit of U.S. Provisional Application No. 62/035,580, entitled “AUTOMATICALLY GENERATING A MACHINE-TO-MACHINE (M2M) EVENTS DICTIONARY IN A DISTRIBUTED INTERNET OF THINGS (IOT) NETWORK,” filed August 11, 2014, assigned to the assignee hereof, and expressly incorporated herein by reference in its entirety.

### **TECHNICAL FIELD**

[0002] The disclosure is related to automatically generating a machine-to-machine (M2M) events dictionary in a distributed Internet of Things (IoT) network.

### **BACKGROUND**

[0003] The Internet is a global system of interconnected computers and computer networks that use a standard Internet protocol suite (e.g., the Transmission Control Protocol (TCP) and Internet Protocol (IP)) to communicate with each other. The Internet of Things (IoT) is based on the idea that everyday objects, not just computers and computer networks, can be readable, recognizable, locatable, addressable, and controllable via an IoT communications network (e.g., an ad-hoc system or the Internet).

[0004] A number of market trends are driving development of IoT devices. For example, increasing energy costs are driving governments’ strategic investments in smart grids and support for future consumption, such as for electric vehicles and public charging stations. Increasing health care costs and aging populations are driving development for remote/connected health care and fitness services. A technological revolution in the home is driving development for new “smart” services, including consolidation by service providers marketing ‘N’ play (e.g., data, voice, video, security, energy management, etc.) and expanding home networks. Buildings are getting smarter and more convenient as a means to reduce operational costs for enterprise facilities.

[0005] There are a number of key applications for the IoT. For example, in the area of

smart grids and energy management, utility companies can optimize delivery of energy to homes and businesses while customers can better manage energy usage. In the area of home and building automation, smart homes and buildings can have centralized control over virtually any device or system in the home or office, from appliances to plug-in electric vehicle (PEV) security systems. In the field of asset tracking, enterprises, hospitals, factories, and other large organizations can accurately track the locations of high-value equipment, patients, vehicles, and so on. In the area of health and wellness, doctors can remotely monitor patients' health while people can track the progress of fitness routines.

## SUMMARY

[0006] The following presents a simplified summary relating to one or more aspects and/or embodiments disclosed herein. As such, the following summary should not be considered an extensive overview relating to all contemplated aspects and/or embodiments, nor should the following summary be regarded to identify key or critical elements relating to all contemplated aspects and/or embodiments or to delineate the scope associated with any particular aspect and/or embodiment. Accordingly, the following summary has the sole purpose to present certain concepts relating to one or more aspects and/or embodiments relating to the mechanisms disclosed herein in a simplified form to precede the detailed description presented below.

[0007] The disclosure is related to automatically generating an events dictionary in an IoT network. A method for automatically generating an events dictionary in an IoT network includes receiving a notification of a first event from a first IoT device in the IoT network, determining a state of the first IoT device before and after the first event, comparing the states of the first IoT device, determining a type of state change of the first event based on the comparing, determining whether the type of state change of the first event is present in the events dictionary, creating a generic entry based on the type of state change of the first event not being present in the events dictionary, wherein the type of state change associated with the generic entry is common to IoT devices of a same type and/or class as the first IoT device, and storing, in the events dictionary, a mapping of an event description of the first event to the generic entry.

[0008] An apparatus for automatically generating an events dictionary in an IoT network includes a transceiver configured to receive a notification of a first event from a first IoT device in the IoT network and at least one processor configured to: determine a

state of the first IoT device before and the first event, compare the states of the first IoT device, determine a type of state change of the first event based on the comparison of the states of the first IoT device, determine whether the type of state change of the first event is present in the events dictionary, and create a generic entry based on the type of state change of the first event not being present in the events dictionary, wherein the type of state change associated with the generic entry is common to IoT devices of a same type and/or class as the first IoT device, and a memory configured to store, in the events dictionary, a mapping of an event description of the first event to the generic entry.

[0009] An apparatus for automatically generating an events dictionary in an IoT network includes means for receiving a notification of an event from an IoT device in the IoT network, means for determining a state of the IoT device before and after the event, means for comparing the states of the IoT device, means for determining a type of state change of the event based on a comparison of the states of the IoT device, means for determining whether the type of state change of the first event is present in the events dictionary, means for creating a generic entry based on the type of state change of the first event not being present in the events dictionary, wherein the type of state change associated with the generic entry is common to IoT devices of a same type and/or class as the IoT device, and means for storing, in the events dictionary, a mapping of an event description of the event to the generic entry.

[0010] A non-transitory computer-readable medium for automatically generating an events dictionary in an IoT network includes at least one instruction to receive a notification of an event from an IoT device in the IoT network, at least one instruction to determine a state of the IoT device before and after the event, at least one instruction to compare the states of the IoT device, at least one instruction to determine a type of state change of the event based on a comparison of the states of the IoT device, at least one instruction to determine whether the type of state change of the first event is present in the events dictionary, at least one instruction to create a generic entry based on the type of state change of the first event not being present in the events dictionary, wherein the type of state change associated with the generic entry is common to IoT devices of a same type and/or class as the IoT device, and at least one instruction to store, in the events dictionary, a mapping of an event description of the event to the generic entry.

[0011] Other objects and advantages associated with the aspects and embodiments disclosed herein will be apparent to those skilled in the art based on the accompanying

drawings and detailed description.

#### BRIEF DESCRIPTION OF THE DRAWINGS

[0012] A more complete appreciation of aspects of the disclosure and many of the attendant advantages thereof will be readily obtained as the same becomes better understood by reference to the following detailed description when considered in connection with the accompanying drawings which are presented solely for illustration and not limitation of the disclosure, and in which:

[0013] FIG. 1A illustrates a high-level system architecture of a wireless communications system in accordance with an aspect of the disclosure.

[0014] FIG. 1B illustrates a high-level system architecture of a wireless communications system in accordance with another aspect of the disclosure.

[0015] FIG. 1C illustrates a high-level system architecture of a wireless communications system in accordance with an aspect of the disclosure.

[0016] FIG. 1D illustrates a high-level system architecture of a wireless communications system in accordance with an aspect of the disclosure.

[0017] FIG. 1E illustrates a high-level system architecture of a wireless communications system in accordance with an aspect of the disclosure.

[0018] FIG. 2A illustrates an exemplary Internet of Things (IoT) device in accordance with aspects of the disclosure.

[0019] FIG. 2B illustrates an exemplary passive IoT device in accordance with aspects of the disclosure.

[0020] FIG. 3 illustrates a communication device that includes logic configured to perform functionality in accordance with an aspect of the disclosure.

[0021] FIG. 4 illustrates an exemplary server according to various aspects of the disclosure.

[0022] FIG. 5 illustrates a wireless communication network that may support discoverable peer-to-peer (P2P) services, in accordance with one aspect of the disclosure.

[0023] FIG. 6 illustrates an exemplary environment in which discoverable P2P services may be used to establish a proximity-based distributed bus over which various devices may communicate, in accordance with one aspect of the disclosure.

[0024] FIG. 7 illustrates an exemplary message sequence in which discoverable P2P services may be used to establish a proximity-based distributed bus over which various

devices may communicate, in accordance with one aspect of the disclosure.

[0025] FIG. 8 illustrates an exemplary proximal IoT network 800 according to at least one aspect of the disclosure.

[0026] FIG. 9 illustrates an exemplary flow for automatically generating an events dictionary for an inter-device communication protocol

[0027] FIG. 10 illustrates an exemplary block diagram that may correspond to a device that uses discoverable P2P services to communicate over a proximity-based distributed bus, in accordance with one aspect of the disclosure.

[0028] FIG. 11 is a simplified block diagram of several sample aspects of an apparatus configured to support communication as taught herein.

#### DETAILED DESCRIPTION

[0029] Methods and systems for automatically generating an events dictionary in an Internet of Things (IoT) network are disclosed. An aspect receives a notification of a first event from a first IoT device in the IoT network, determines a state of the first IoT device before and after the first event, compares the states of the first IoT device, determines a type of state change of the first event based on the comparing, determines whether the type of state change of the first event is present in the events dictionary, creates a generic entry based on the type of state change of the first event not being present in the events dictionary, wherein the type of state change associated with the generic entry is common to IoT devices of a same type and/or class as the first IoT device, and stores, in the events dictionary, a mapping of an event description of the first event to the generic entry.

[0030] The and other aspects are disclosed in the following description and related drawings to show specific examples relating to exemplary embodiments. Alternate embodiments will be apparent to those skilled in the pertinent art upon reading this disclosure, and may be constructed and practiced without departing from the scope or spirit of the disclosure. Additionally, well-known elements will not be described in detail or may be omitted so as to not obscure the relevant details of the aspects and embodiments disclosed herein.

[0031] The word “exemplary” is used herein to mean “serving as an example, instance, or illustration.” Any embodiment described herein as “exemplary” is not necessarily to be construed as preferred or advantageous over other embodiments. Likewise, the term “embodiments” does not require that all embodiments include the discussed feature,

advantage or mode of operation.

[0032] The terminology used herein describes particular embodiments only and should be construed to limit any embodiments disclosed herein. As used herein, the singular forms “a,” “an,” and “the” are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms “comprises,” “comprising,” “includes,” and/or “including,” when used herein, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

[0033] Further, many aspects are described in terms of sequences of actions to be performed by, for example, elements of a computing device. It will be recognized that various actions described herein can be performed by specific circuits (e.g., an application specific integrated circuit (ASIC)), by program instructions being executed by one or more processors, or by a combination of both. Additionally, these sequences of actions described herein can be considered to be embodied entirely within any form of computer-readable storage medium having stored therein a corresponding set of computer instructions that upon execution would cause an associated processor to perform the functionality described herein. Thus, the various aspects of the disclosure may be embodied in a number of different forms, all of which have been contemplated to be within the scope of the claimed subject matter. In addition, for each of the aspects described herein, the corresponding form of any such aspects may be described herein as, for example, “logic configured to” perform the described action.

[0034] As used herein, the term “Internet of Things device” (or “IoT device”) may refer to any object (e.g., an appliance, a sensor, etc.) that has an addressable interface (e.g., an Internet protocol (IP) address, a Bluetooth identifier (ID), a near-field communication (NFC) ID, etc.) and can transmit information to one or more other devices over a wired or wireless connection. An IoT device may have a passive communication interface, such as a quick response (QR) code, a radio-frequency identification (RFID) tag, an NFC tag, or the like, or an active communication interface, such as a modem, a transceiver, a transmitter-receiver, or the like. An IoT device can have a particular set of attributes (e.g., a device state or status, such as whether the IoT device is on or off, open or closed, idle or active, available for task execution or busy, and so on, a cooling or heating function, an environmental monitoring or recording function, a light-emitting function, a sound-emitting function, etc.) that can be embedded in and/or

controlled/monitored by a central processing unit (CPU), microprocessor, ASIC, or the like, and configured for connection to an IoT network such as a local ad-hoc network or the Internet. For example, IoT devices may include, but are not limited to, refrigerators, toasters, ovens, microwaves, freezers, dishwashers, dishes, hand tools, clothes washers, clothes dryers, furnaces, air conditioners, thermostats, televisions, light fixtures, vacuum cleaners, sprinklers, electricity meters, gas meters, etc., so long as the devices are equipped with an addressable communications interface for communicating with the IoT network. IoT devices may also include cell phones, desktop computers, laptop computers, tablet computers, personal digital assistants (PDAs), etc. Accordingly, the IoT network may be comprised of a combination of “legacy” Internet-accessible devices (e.g., laptop or desktop computers, cell phones, etc.) in addition to devices that do not typically have Internet-connectivity (e.g., dishwashers, etc.).

[0035] FIG. 1A illustrates a high-level system architecture of a wireless communications system 100A in accordance with an aspect of the disclosure. The wireless communications system 100A contains a plurality of IoT devices 110-118, which include a television 110, an outdoor air conditioning unit 112, a thermostat 114, a refrigerator 116, and a washer and dryer 118.

[0036] Referring to FIG. 1A, IoT devices 110-118 are configured to communicate with an access network (e.g., an access point 125) over a physical communications interface or layer, shown in FIG. 1A as air interface 108 and a direct wired connection 109. The air interface 108 can comply with a wireless Internet protocol (IP), such as IEEE 802.11. Although FIG. 1A illustrates IoT devices 110-118 communicating over the air interface 108 and IoT device 118 communicating over the direct wired connection 109, each IoT device may communicate over a wired or wireless connection, or both.

[0037] The Internet 175 includes a number of routing agents and processing agents (not shown in FIG. 1A for the sake of convenience). The Internet 175 is a global system of interconnected computers and computer networks that uses a standard Internet protocol suite (e.g., the Transmission Control Protocol (TCP) and IP) to communicate among disparate devices/networks. TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination.

[0038] In FIG. 1A, a computer 120, such as a desktop or personal computer (PC), is shown as connecting to the Internet 175 directly (e.g., over an Ethernet connection or Wi-Fi or 802.11-based network). The computer 120 may have a wired connection to the Internet 175, such as a direct connection to a modem or router, which, in an

example, can correspond to the access point 125 itself (e.g., for a Wi-Fi router with both wired and wireless connectivity). Alternatively, rather than being connected to the access point 125 and the Internet 175 over a wired connection, the computer 120 may be connected to the access point 125 over air interface 108 or another wireless interface, and access the Internet 175 over the air interface 108. Although illustrated as a desktop computer, computer 120 may be a laptop computer, a tablet computer, a PDA, a smart phone, or the like. The computer 120 may be an IoT device and/or contain functionality to manage an IoT network/group, such as the network/group of IoT devices 110-118.

[0039] The access point 125 may be connected to the Internet 175 via, for example, an optical communication system, such as FiOS, a cable modem, a digital subscriber line (DSL) modem, or the like. The access point 125 may communicate with IoT devices 110-120 and the Internet 175 using the standard Internet protocols (e.g., TCP/IP).

[0040] Referring to FIG. 1A, an IoT server 170 is shown as connected to the Internet 175. The IoT server 170 can be implemented as a plurality of structurally separate servers, or alternately may correspond to a single server. In an aspect, the IoT server 170 is optional (as indicated by the dotted line), and the group of IoT devices 110-120 may be a peer-to-peer (P2P) network. In such a case, the IoT devices 110-120 can communicate with each other directly over the air interface 108 and/or the direct wired connection 109. Alternatively, or additionally, some or all of IoT devices 110-120 may be configured with a communication interface independent of air interface 108 and direct wired connection 109. For example, if the air interface 108 corresponds to a Wi-Fi interface, one or more of the IoT devices 110-120 may have Bluetooth or NFC interfaces for communicating directly with each other or other Bluetooth or NFC-enabled devices.

[0041] In a peer-to-peer network, service discovery schemes can multicast the presence of nodes, their capabilities, and group membership. The peer-to-peer devices can establish associations and subsequent interactions based on this information.

[0042] In accordance with an aspect of the disclosure, FIG. 1B illustrates a high-level architecture of another wireless communications system 100B that contains a plurality of IoT devices. In general, the wireless communications system 100B shown in FIG. 1B may include various components that are the same and/or substantially similar to the wireless communications system 100A shown in FIG. 1A, which was described in greater detail above (e.g., various IoT devices 110-120, including the television 110, outdoor air conditioning unit 112, thermostat 114, refrigerator 116, and washer and

dryer 118, that are configured to communicate with the access point 125 over the air interface 108 and/or the direct wired connection 109, the computer 120 that directly connects to the Internet 175 and/or connects to the Internet 175 through access point 125, and the IoT server 170 accessible via the Internet 175, etc.). As such, for brevity and ease of description, various details relating to certain components in the wireless communications system 100B shown in FIG. 1B may be omitted herein to the extent that the same or similar details have already been provided above in relation to the wireless communications system 100A illustrated in FIG. 1A.

[0043] Referring to FIG. 1B, the wireless communications system 100B may include a supervisor device 130, which may alternatively be referred to as an IoT manager 130 or IoT manager device 130. As such, where the following description uses the term “supervisor device” 130, those skilled in the art will appreciate that any references to an IoT manager, group owner, or similar terminology may refer to the supervisor device 130 or another physical or logical component that provides the same or substantially similar functionality.

[0044] In one embodiment, the supervisor device 130 may generally observe, monitor, control, or otherwise manage the various other components in the wireless communications system 100B. For example, the supervisor device 130 can communicate with an access network (e.g., access point 125) over air interface 108 and/or a direct wired connection 109 to monitor or manage attributes, activities, or other states associated with the various IoT devices 110-120 in the wireless communications system 100B. The supervisor device 130 may have a wired or wireless connection to the Internet 175 and optionally to the IoT server 170 (shown as a dotted line). The supervisor device 130 may obtain information from the Internet 175 and/or the IoT server 170 that can be used to further monitor or manage attributes, activities, or other states associated with the various IoT devices 110-120. The supervisor device 130 may be a standalone device or one of IoT devices 110-120, such as computer 120. The supervisor device 130 may be a physical device or a software application running on a physical device. The supervisor device 130 may include a user interface that can output information relating to the monitored attributes, activities, or other states associated with the IoT devices 110-120 and receive input information to control or otherwise manage the attributes, activities, or other states associated therewith. Accordingly, the supervisor device 130 may generally include various components and support various wired and wireless communication interfaces to observe, monitor, control, or otherwise

manage the various components in the wireless communications system 100B.

[0045] The wireless communications system 100B shown in FIG. 1B may include one or more passive IoT devices 105 (in contrast to the active IoT devices 110-120) that can be coupled to or otherwise made part of the wireless communications system 100B. In general, the passive IoT devices 105 may include barcoded devices, Bluetooth devices, radio frequency (RF) devices, RFID tagged devices, infrared (IR) devices, NFC tagged devices, or any other suitable device that can provide its identifier and attributes to another device when queried over a short range interface. Active IoT devices may detect, store, communicate, act on, and/or the like, changes in attributes of passive IoT devices.

[0046] For example, passive IoT devices 105 may include a coffee cup and a container of orange juice that each have an RFID tag or barcode. A cabinet IoT device and the refrigerator IoT device 116 may each have an appropriate scanner or reader that can read the RFID tag or barcode to detect when the coffee cup and/or the container of orange juice passive IoT devices 105 have been added or removed. In response to the cabinet IoT device detecting the removal of the coffee cup passive IoT device 105 and the refrigerator IoT device 116 detecting the removal of the container of orange juice passive IoT device, the supervisor device 130 may receive one or more signals that relate to the activities detected at the cabinet IoT device and the refrigerator IoT device 116. The supervisor device 130 may then infer that a user is drinking orange juice from the coffee cup and/or likes to drink orange juice from a coffee cup.

[0047] Although the foregoing describes the passive IoT devices 105 as having some form of RFID tag or barcode communication interface, the passive IoT devices 105 may include one or more devices or other physical objects that do not have such communication capabilities. For example, certain IoT devices may have appropriate scanner or reader mechanisms that can detect shapes, sizes, colors, and/or other observable features associated with the passive IoT devices 105 to identify the passive IoT devices 105. In this manner, any suitable physical object may communicate its identity and attributes and become part of the wireless communications system 100B and be observed, monitored, controlled, or otherwise managed with the supervisor device 130. Further, passive IoT devices 105 may be coupled to or otherwise made part of the wireless communications system 100A in FIG. 1A and observed, monitored, controlled, or otherwise managed in a substantially similar manner.

[0048] In accordance with another aspect of the disclosure, FIG. 1C illustrates a high-

level architecture of another wireless communications system 100C that contains a plurality of IoT devices 110-118. In general, the wireless communications system 100C shown in FIG. 1C may include various components that are the same and/or substantially similar to the wireless communications systems 100A and 100B shown in FIGS. 1A and 1B, respectively, which were described in greater detail above. As such, for brevity and ease of description, various details relating to certain components in the wireless communications system 100C shown in FIG. 1C may be omitted herein to the extent that the same or similar details have already been provided above in relation to the wireless communications systems 100A and 100B illustrated in FIGS. 1A and 1B, respectively.

[0049] The wireless communications system 100C shown in FIG. 1C illustrates exemplary peer-to-peer communications between the IoT devices 110-118 and the supervisor device 130. As shown in FIG. 1C, the supervisor device 130 communicates with each of the IoT devices 110-118 over an IoT supervisor interface. Further, IoT devices 110 and 114, IoT devices 112, 114, and 116, and IoT devices 116 and 118, communicate directly with each other.

[0050] The IoT devices 110-118 make up an IoT device group 160. The IoT device group 160 is a group of locally connected IoT devices, such as the IoT devices connected to a user's home network. Although not shown, multiple IoT device groups may be connected to and/or communicate with each other via an IoT SuperAgent 140 connected to the Internet 175. At a high level, the supervisor device 130 manages intra-group communications, while the IoT SuperAgent 140 can manage inter-group communications. Although shown as separate devices, the supervisor device 130 and the IoT SuperAgent 140 may be, or reside on, the same device (e.g., a standalone device or an IoT device, such as computer 120 in FIG. 1A). Alternatively, the IoT SuperAgent 140 may correspond to or include the functionality of the access point 125. As yet another alternative, the IoT SuperAgent 140 may correspond to or include the functionality of an IoT server, such as IoT server 170. The IoT SuperAgent 140 may encapsulate gateway functionality 145.

[0051] Each IoT device 110-118 can treat the supervisor device 130 as a peer and transmit attribute/schema updates to the supervisor device 130. When an IoT device needs to communicate with another IoT device, it can request the pointer to that IoT device from the supervisor device 130 and then communicate with the target IoT device as a peer. The IoT devices 110-118 communicate with each other over a peer-to-peer

communication network using a common messaging protocol (CMP). As long as two IoT devices are CMP-enabled and connected over a common communication transport, they can communicate with each other. In the protocol stack, the CMP layer 154 is below the application layer 152 and above the transport layer 156 and the physical layer 158.

[0052] In accordance with another aspect of the disclosure, FIG. 1D illustrates a high-level architecture of another wireless communications system 100D that contains a plurality of IoT devices 110-120. In general, the wireless communications system 100D shown in FIG. 1D may include various components that are the same and/or substantially similar to the wireless communications systems 100A-C shown in FIGS. 1A-C, respectively, which were described in greater detail above. As such, for brevity and ease of description, various details relating to certain components in the wireless communications system 100D shown in FIG. 1D may be omitted herein to the extent that the same or similar details have already been provided above in relation to the wireless communications systems 100A-C illustrated in FIGS. 1A-C, respectively.

[0053] The Internet 175 is a “resource” that can be regulated using the concept of the IoT. However, the Internet 175 is just one example of a resource that is regulated, and any resource could be regulated using the concept of the IoT. Other resources that can be regulated include, but are not limited to, electricity, gas, storage, security, and the like. An IoT device may be connected to the resource and thereby regulate it, or the resource could be regulated over the Internet 175. FIG. 1D illustrates several resources 180, such as natural gas, gasoline, hot water, and electricity, wherein the resources 180 can be regulated in addition to and/or over the Internet 175.

[0054] IoT devices can communicate with each other to regulate their use of a resource 180. For example, IoT devices such as a toaster, a computer, and a hairdryer may communicate with each other over a Bluetooth communication interface to regulate their use of electricity (the resource 180). As another example, IoT devices such as a desktop computer, a telephone, and a tablet computer may communicate over a Wi-Fi communication interface to regulate their access to the Internet 175 (the resource 180). As yet another example, IoT devices such as a stove, a clothes dryer, and a water heater may communicate over a Wi-Fi communication interface to regulate their use of gas. Alternatively, or additionally, each IoT device may be connected to an IoT server, such as IoT server 170, which has logic to regulate their use of the resource 180 based on information received from the IoT devices.

[0055] In accordance with another aspect of the disclosure, FIG. 1E illustrates a high-level architecture of another wireless communications system 100E that contains a plurality of IoT devices. In general, the wireless communications system 100E shown in FIG. 1E may include various components that are the same and/or substantially similar to the wireless communications systems 100A-D shown in FIGS. 1A-D, respectively, which were described in greater detail above. As such, for brevity and ease of description, various details relating to certain components in the wireless communications system 100E shown in FIG. 1E may be omitted herein to the extent that the same or similar details have already been provided above in relation to the wireless communications systems 100A-D illustrated in FIGS. 1A-D, respectively.

[0056] The wireless communications system 100E includes two IoT device groups 160A and 160B. Multiple IoT device groups may be connected to and/or communicate with each other via an IoT SuperAgent connected to the Internet 175. At a high level, an IoT SuperAgent may manage inter-group communications among IoT device groups. For example, in FIG. 1E, the IoT device group 160A includes IoT devices 116A, 122A, and 124A and an IoT SuperAgent 140A, while IoT device group 160B includes IoT devices 116B, 122B, and 124B and an IoT SuperAgent 140B. As such, the IoT SuperAgents 140A and 140B may connect to the Internet 175 and communicate with each other over the Internet 175 and/or communicate with each other directly to facilitate communication between the IoT device groups 160A and 160B. Furthermore, although FIG. 1E illustrates two IoT device groups 160A and 160B communicating with each other via IoT SuperAgents 140A and 140B, those skilled in the art will appreciate that any number of IoT device groups may suitably communicate with each other using IoT SuperAgents.

[0057] FIG. 2A illustrates a high-level example of an IoT device 200A in accordance with aspects of the disclosure. IoT device 200A may correspond to any of IoT devices 110-120, and may additionally correspond to supervisor device 130 and/or gateway 145 when the functionality of the supervisor device 130 and the gateway 145 are embodied in an IoT device (e.g., computer 120). While external appearances and/or internal components can differ significantly among IoT devices, most IoT devices will have some sort of user interface, which may comprise a display and a means for user input. IoT devices without a user interface can be communicated with remotely over a wired or wireless network, such as air interface 108 in FIGS. 1A-B.

[0058] As shown in FIG. 2A, in an example configuration for the IoT device 200A, an

external casing of IoT device 200A may be configured with a display 226, a power button 222, and two control buttons 224A and 224B, among other components, as is known in the art. The display 226 may be a touchscreen display, in which case the control buttons 224A and 224B may not be necessary. While not shown explicitly as part of IoT device 200A, the IoT device 200A may include one or more external antennas and/or one or more integrated antennas that are built into the external casing, including but not limited to Wi-Fi antennas, cellular antennas, satellite position system (SPS) antennas (e.g., global positioning system (GPS) antennas), and so on.

[0059] While internal components of IoT devices, such as IoT device 200A, can be embodied with different hardware configurations, a basic high-level configuration for internal hardware components is shown as platform 202 in FIG. 2A. The platform 202 can receive and execute software applications, data and/or commands transmitted over a network interface, such as air interface 108 in FIGS. 1A-B and/or a wired interface. The platform 202 can also independently execute locally stored applications. The platform 202 can include one or more transceivers 206 configured for wired and/or wireless communication (e.g., a Wi-Fi transceiver, a Bluetooth transceiver, a cellular transceiver, a satellite transceiver, a GPS or SPS receiver, etc.) operably coupled to one or more processors 208, such as a microcontroller, microprocessor, application specific integrated circuit, digital signal processor (DSP), programmable logic circuit, or other data processing device, which will be generally referred to as processor 208. The processor 208 can execute application programming instructions within a memory 212 of the IoT device 200A. The memory 212 can include one or more of read-only memory (ROM), random-access memory (RAM), electrically erasable programmable ROM (EEPROM), flash cards, or any memory common to computer platforms. One or more input / output (I/O) interfaces 214 can be configured to allow the processor 208 to communicate with and control from various I/O devices such as the display 226, power button 222, control buttons 224A and 224B as illustrated, and any other devices, such as sensors, actuators, relays, valves, switches, and the like associated with the IoT device 200A.

[0060] Accordingly, an aspect of the disclosure can include an IoT device (e.g., IoT device 200A) including the ability to perform the functions described herein. As will be appreciated by those skilled in the art, the various logic elements can be embodied in discrete elements, software modules executed on a processor (e.g., processor 208) or any combination of software and hardware to achieve the functionality disclosed herein.

For example, transceiver 206, processor 208, memory 212, and I/O interface 214 may all be used cooperatively to load, store and execute the various functions disclosed herein and thus the logic to perform these functions may be distributed over various elements. Alternatively, the functionality could be incorporated into one discrete component. Therefore, the features of the IoT device 200A in FIG. 2A are to be considered merely illustrative and the disclosure is not limited to the illustrated features or arrangement.

[0061] For example, where the IoT device 200A corresponds to a supervisor device, such as supervisor device 130, configured to automatically generate an events dictionary in an IoT network, the IoT device 200A may also include an Events Monitor and Dictionary Generator (EMDG) module 210 configured to perform, or cause the performance of, the functionality described herein. The EMDG module 210 may be a hardware module, an software module executable by processor 208, or a combination of hardware and software. In an example embodiment, the transceiver 206 may receive a notification of an event from an IoT device in the IoT network, and processor 208 / EMDG module 210, in conjunction with transceiver 206, may determine a state of the IoT device before and after the event. Processor 208 / EMDG module 210 may also compare the states of the IoT device, determine a type of state change of the event based on the comparison, and determine whether the type of state change of the first event is present in the events dictionary. Processor 208 / EMDG module 210, in conjunction with memory 212, may create a generic entry based on the type of state change of the first event not being present in the events dictionary, wherein the type of state change associated with the generic entry is common to IoT devices of a same type and/or class as the IoT device, and memory 212 may store, in the events dictionary, a mapping of an event description of the event to the generic entry.

[0062] FIG. 2B illustrates a high-level example of a passive IoT device 200B in accordance with aspects of the disclosure. In general, the passive IoT device 200B shown in FIG. 2B may include various components that are the same and/or substantially similar to the IoT device 200A shown in FIG. 2A, which was described in greater detail above. As such, for brevity and ease of description, various details relating to certain components in the passive IoT device 200B shown in FIG. 2B may be omitted herein to the extent that the same or similar details have already been provided above in relation to the IoT device 200A illustrated in FIG. 2A.

[0063] The passive IoT device 200B shown in FIG. 2B may generally differ from the

IoT device 200A shown in FIG. 2A in that the passive IoT device 200B may not have a processor, internal memory, or certain other components. Instead, in one embodiment, the passive IoT device 200B may only include an I/O interface 214 or other suitable mechanism that allows the passive IoT device 200B to be observed, monitored, controlled, managed, or otherwise known within a controlled IoT network. For example, in one embodiment, the I/O interface 214 associated with the passive IoT device 200B may include a barcode, Bluetooth interface, radio frequency (RF) interface, RFID tag, IR interface, NFC interface, or any other suitable I/O interface that can provide an identifier and attributes associated with the passive IoT device 200B to another device when queried over a short range interface (e.g., an active IoT device, such as IoT device 200A, that can detect, store, communicate, act on, or otherwise process information relating to the attributes associated with the passive IoT device 200B).

[0064] Although the foregoing describes the passive IoT device 200B as having some form of RF, barcode, or other I/O interface 214, the passive IoT device 200B may comprise a device or other physical object that does not have such an I/O interface 214. For example, certain IoT devices may have appropriate scanner or reader mechanisms that can detect shapes, sizes, colors, and/or other observable features associated with the passive IoT device 200B to identify the passive IoT device 200B. In this manner, any suitable physical object may communicate its identity and attributes and be observed, monitored, controlled, or otherwise managed within a controlled IoT network.

[0065] FIG. 3 illustrates a communication device 300 that includes logic configured to perform functionality. The communication device 300 can correspond to any of the above-noted communication devices, including but not limited to IoT devices 110-120, IoT device 200A, any components coupled to the Internet 175 (e.g., the IoT server 170), and so on. Thus, communication device 300 can correspond to any electronic device that is configured to communicate with (or facilitate communication with) one or more other entities over the wireless communications systems 100A-D of FIGS. 1A-D.

[0066] Referring to FIG. 3, the communication device 300 includes logic configured to receive and/or transmit information 305. In an example, if the communication device 300 corresponds to a wireless communications device (e.g., IoT device 200A and/or passive IoT device 200B), the logic configured to receive and/or transmit information 305 can include a wireless communications interface (e.g., Bluetooth, Wi-Fi, Wi-Fi Direct, Long-Term Evolution (LTE) Direct, etc.) such as a wireless transceiver and

associated hardware (e.g., an RF antenna, a MODEM, a modulator and/or demodulator, etc.). In another example, the logic configured to receive and/or transmit information 305 can correspond to a wired communications interface (e.g., a serial connection, a USB or Firewire connection, an Ethernet connection through which the Internet 175 can be accessed, etc.). Thus, if the communication device 300 corresponds to some type of network-based server (e.g., the IoT server 170), the logic configured to receive and/or transmit information 305 can correspond to an Ethernet card, in an example, that connects the network-based server to other communication entities via an Ethernet protocol. In a further example, the logic configured to receive and/or transmit information 305 can include sensory or measurement hardware by which the communication device 300 can monitor its local environment (e.g., an accelerometer, a temperature sensor, a light sensor, an antenna for monitoring local RF signals, etc.). The logic configured to receive and/or transmit information 305 can also include software that, when executed, permits the associated hardware of the logic configured to receive and/or transmit information 305 to perform its reception and/or transmission function(s). However, the logic configured to receive and/or transmit information 305 does not correspond to software alone, and the logic configured to receive and/or transmit information 305 relies at least in part upon hardware to achieve its functionality.

[0067] Referring to FIG. 3, the communication device 300 further includes logic configured to process information 310. In an example, the logic configured to process information 310 can include at least a processor. Example implementations of the type of processing that can be performed by the logic configured to process information 310 includes but is not limited to performing determinations, establishing connections, making selections between different information options, performing evaluations related to data, interacting with sensors coupled to the communication device 300 to perform measurement operations, converting information from one format to another (e.g., between different protocols such as .wmv to .avi, etc.), and so on. The processor included in the logic configured to process information 310 can correspond to a general purpose processor, a DSP, an ASIC, a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state

machine. A processor may also be implemented as a combination of computing devices (e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration). The logic configured to process information 310 can also include software that, when executed, permits the associated hardware of the logic configured to process information 310 to perform its processing function(s). However, the logic configured to process information 310 does not correspond to software alone, and the logic configured to process information 310 relies at least in part upon hardware to achieve its functionality.

[0068] Referring to FIG. 3, the communication device 300 further includes logic configured to store information 315. In an example, the logic configured to store information 315 can include at least a non-transitory memory and associated hardware (e.g., a memory controller, etc.). For example, the non-transitory memory included in the logic configured to store information 315 can correspond to RAM, flash memory, ROM, erasable programmable ROM (EPROM), EEPROM, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. The logic configured to store information 315 can also include software that, when executed, permits the associated hardware of the logic configured to store information 315 to perform its storage function(s). However, the logic configured to store information 315 does not correspond to software alone, and the logic configured to store information 315 relies at least in part upon hardware to achieve its functionality.

[0069] Where the communication device 300 corresponds to a supervisor device, such as supervisor device 130, configured to automatically generate an events dictionary in an IoT network, the logic configured to receive and/or transmit information 305 may receive a notification of an event from an IoT device in the IoT network, and the logic configured to process information 310, in conjunction with the logic configured to receive and/or transmit information 305, may determine a state of the IoT device before and after the event. The logic configured to process information 310 may also compare the states of the IoT device, determine a type of state change of the event based on the comparison, and determine whether the type of state change of the first event is present in the events dictionary. The logic configured to process information 310, in conjunction with the logic configured to store information 315, may create a generic entry based on the type of state change of the first event not being present in the events dictionary, wherein the type of state change associated with the generic entry is

common to IoT devices of a same type and/or class as the IoT device, and the logic configured to store information 315 may store, in the events dictionary, a mapping of an event description of the event to the generic entry.

[0070] Referring to FIG. 3, the communication device 300 further optionally includes logic configured to present information 320. In an example, the logic configured to present information 320 can include at least an output device and associated hardware. For example, the output device can include a video output device (e.g., a display screen, a port that can carry video information such as USB, HDMI, etc.), an audio output device (e.g., speakers, a port that can carry audio information such as a microphone jack, USB, HDMI, etc.), a vibration device and/or any other device by which information can be formatted for output or actually outputted by a user or operator of the communication device 300. For example, if the communication device 300 corresponds to the IoT device 200A as shown in FIG. 2A and/or the passive IoT device 200B as shown in FIG. 2B, the logic configured to present information 320 can include the display 226. In a further example, the logic configured to present information 320 can be omitted for certain communication devices, such as network communication devices that do not have a local user (e.g., network switches or routers, remote servers, etc.). The logic configured to present information 320 can also include software that, when executed, permits the associated hardware of the logic configured to present information 320 to perform its presentation function(s). However, the logic configured to present information 320 does not correspond to software alone, and the logic configured to present information 320 relies at least in part upon hardware to achieve its functionality.

[0071] Referring to FIG. 3, the communication device 300 further optionally includes logic configured to receive local user input 325. In an example, the logic configured to receive local user input 325 can include at least a user input device and associated hardware. For example, the user input device can include buttons, a touchscreen display, a keyboard, a camera, an audio input device (e.g., a microphone or a port that can carry audio information such as a microphone jack, etc.), and/or any other device by which information can be received from a user or operator of the communication device 300. For example, if the communication device 300 corresponds to the IoT device 200A as shown in FIG. 2A and/or the passive IoT device 200B as shown in FIG. 2B, the logic configured to receive local user input 325 can include the power buttons 222, the control buttons 224A and 224B, and the display 226 (if a touchscreen), etc. In a further

example, the logic configured to receive local user input 325 can be omitted for certain communication devices, such as network communication devices that do not have a local user (e.g., network switches or routers, remote servers, etc.). The logic configured to receive local user input 325 can also include software that, when executed, permits the associated hardware of the logic configured to receive local user input 325 to perform its input reception function(s). However, the logic configured to receive local user input 325 does not correspond to software alone, and the logic configured to receive local user input 325 relies at least in part upon hardware to achieve its functionality.

[0072] Referring to FIG. 3, while the configured logics of 305 through 325 are shown as separate or distinct blocks in FIG. 3, it will be appreciated that the hardware and/or software by which the respective configured logic performs its functionality can overlap in part. For example, any software used to facilitate the functionality of the configured logics of 305 through 325 can be stored in the non-transitory memory associated with the logic configured to store information 315, such that the configured logics of 305 through 325 each performs their functionality (i.e., in this case, software execution) based in part upon the operation of software stored by the logic configured to store information 315. Likewise, hardware that is directly associated with one of the configured logics can be borrowed or used by other configured logics from time to time. For example, the processor of the logic configured to process information 310 can format data into an appropriate format before being transmitted by the logic configured to receive and/or transmit information 305, such that the logic configured to receive and/or transmit information 305 performs its functionality (i.e., in this case, transmission of data) based in part upon the operation of hardware (i.e., the processor) associated with the logic configured to process information 310.

[0073] Generally, unless explicitly stated otherwise, the phrase “logic configured to” as used throughout this disclosure is intended to invoke an aspect that is at least partially implemented with hardware, and is not intended to map to software-only implementations that are independent of hardware. Also, it will be appreciated that the configured logic or “logic configured to” in the various blocks are not limited to specific logic gates or elements, but generally refer to the ability to perform the functionality described herein (either via hardware or a combination of hardware and software). Thus, the configured logics or “logic configured to” as illustrated in the various blocks are not necessarily implemented as logic gates or logic elements despite sharing the

word “logic.” Other interactions or cooperation between the logic in the various blocks will become clear to one of ordinary skill in the art from a review of the aspects described below in more detail.

[0074] The various embodiments may be implemented on any of a variety of commercially available server devices, such as server 400 illustrated in FIG. 4. In an example, the server 400 may correspond to one example configuration of the supervisor device 130 or the IoT server 170 described above. In FIG. 4, the server 400 includes a processor 401 coupled to volatile memory 402 and a large capacity nonvolatile memory, such as a disk drive 403. The server 400 may also include a floppy disc drive, compact disc (CD) or DVD disc drive 406 coupled to the processor 401. The server 400 may also include network access ports 404 coupled to the processor 401 for establishing data connections with a network 407, such as a local area network coupled to other broadcast system computers and servers or to the Internet.

[0075] Where the server 400 is configured to automatically generate an events dictionary for an inter-device communication protocol in an IoT network, the server 400 may also include an EMDG module 410 configured to perform, or cause the performance of, the functionality described herein. The EMDG module 410 may be a hardware module, an executable software module, or a combination of hardware and software. In an example embodiment, the network access ports 404 may receive a notification of an event from an IoT device in the IoT network, and processor 401 / EMDG module 410, in conjunction with network access ports 404, may determine a state of the IoT device before and after the event. Processor 401 / EMDG module 410 may also compare the states of the IoT device, determine a type of state change of the event based on the comparison, and determine whether the type of state change of the first event is present in the events dictionary. Processor 401 / EMDG module 410, in conjunction with disk drive 403, may create a generic entry based on the type of state change of the first event not being present in the events dictionary, wherein the type of state change associated with the generic entry is common to IoT devices of a same type and/or class as the IoT device, and disk drive 403 may store, in the events dictionary, a mapping of an event description of the event to the generic entry.

[0076] In context with FIG. 3, it will be appreciated that the server 400 of FIG. 4 illustrates one example implementation of the communication device 300, whereby the logic configured to receive and/or transmit information 305 corresponds to the network access ports 404 used by the server 400 to communicate with the network 407, the logic

configured to process information 310 corresponds to the processor 401 and, where the EMDG module 410 is a hardware module, the EMDG module 410, and the logic configured to store information 315 corresponds to any combination of the volatile memory 402, the disk drive 403, the disc drive 406, and, where the EMDG module 410 is an executable software module, the EMDG module 410. The optional logic configured to present information 320 and the optional logic configured to receive local user input 325 are not shown explicitly in FIG. 4 and may or may not be included therein. Thus, FIG. 4 helps to demonstrate that the communication device 300 may be implemented as a server, in addition to an IoT device implementation as in FIG. 2A.

[0077] In general, user equipment (UE) such as telephones, tablet computers, laptop and desktop computers, certain vehicles, etc., can be configured to connect with each other either locally (e.g., Bluetooth, local Wi-Fi, etc.) or remotely (e.g., via cellular networks, through the Internet, etc.). Furthermore, certain UEs may also support proximity-based peer-to-peer (P2P) communication using certain wireless networking technologies (e.g., Wi-Fi, Bluetooth, Wi-Fi Direct, etc.) that enable devices to make a one-to-one connection or simultaneously connect to a group that includes several devices in order to directly communicate with one another. To that end, FIG. 5 illustrates an exemplary wireless communication network, or WAN, 500 that may support discoverable P2P services. For example, in one embodiment, the wireless communication network 500 may comprise an LTE network or another suitable WAN that includes various base stations 510 and other network entities. For simplicity, only three base stations 510a, 510b and 510c, one network controller 530, and one Dynamic Host Configuration Protocol (DHCP) server 540 are shown in FIG. 5. A base station 510 may be an entity that communicates with devices 520 and may also be referred to as a Node B, an evolved Node B (eNB), an access point, etc. Each base station 510 may provide communication coverage for a particular geographic area and may support communication for the devices 520 located within the coverage area. To improve network capacity, the overall coverage area of a base station 510 may be partitioned into multiple (e.g., three) smaller areas, wherein each smaller area may be served by a respective base station 510. In 3GPP, the term “cell” can refer to a coverage area of a base station 510 and/or a base station subsystem 510 serving this coverage area, depending on the context in which the term is used. In 3GPP2, the term “sector” or “cell-sector” can refer to a coverage area of a base station 510 and/or a base station 510 serving this coverage area. For clarity, the 3GPP concept of “cell” may be used in the

description herein.

[0078] A base station 510 may provide communication coverage for a macro cell, a pico cell, a femto cell, and/or other cell types. A macro cell may cover a relatively large geographic area (e.g., several kilometers in radius) and may allow unrestricted access by devices 520 with service subscription. A pico cell may cover a relatively small geographic area and may allow unrestricted access by devices 520 with service subscription. A femto cell may cover a relatively small geographic area (e.g., a home) and may allow restricted access by devices 520 having association with the femto cell (e.g., devices 520 in a Closed Subscriber Group (CSG)). In the example shown in FIG. 5, wireless communication network 500 includes macro base stations 510a, 510b and 510c for macro cells. wireless communication network 500 may also include pico base stations 510 for pico cells and/or home base stations 510 for femto cells (not shown in FIG. 5).

[0079] Network controller 530 may couple to a set of base stations 510 and may provide coordination and control for these base stations 510. Network controller 530 may be a single network entity or a collection of network entities that can communicate with the base stations via a backhaul. The base stations 510 may also communicate with one another, e.g., directly or indirectly via wireless or wireline backhaul. DHCP server 540 may support P2P communication, as described below. DHCP server 540 may be part of wireless communication network 500, external to wireless communication network 500, run via Internet Connection Sharing (ICS), or any suitable combination thereof. DHCP server 540 may be a separate entity (e.g., as shown in FIG. 5) or may be part of a base station 510, network controller 530, or some other entity. In any case, DHCP server 540 may be reachable by devices 520 desiring to communicate peer-to-peer.

[0080] Devices 520 may be dispersed throughout wireless communication network 500, and each device 520 may be stationary or mobile. A device 520 may also be referred to as a node, user equipment (UE), a station, a mobile station, a terminal, an access terminal, a subscriber unit, etc. A device 520 may be a cellular phone, a personal digital assistant (PDA), a wireless modem, a wireless communication device, a handheld device, a laptop computer, a cordless phone, a wireless local loop (WLL) station, a smart phone, a netbook, a smartbook, a tablet, etc. A device 520 may communicate with base stations 510 in the wireless communication network 500 and may further communicate peer-to-peer with other devices 520. For example, as shown in FIG. 5,

devices 520a and 520b may communicate peer-to-peer, devices 520c and 520d may communicate peer-to-peer, devices 520e and 520f may communicate peer-to-peer, and devices 520g, 520h, and 520i may communicate peer-to-peer, while remaining devices 520 may communicate with base stations 510. As further shown in FIG. 5, devices 520a, 520d, 520f, and 520h may also communicate with base stations 510, e.g., when not engaged in P2P communication or possibly concurrent with P2P communication.

[0081] In the description herein, WAN communication may refer to communication between a device 520 and a base station 510 in wireless communication network 500, e.g., for a call with a remote entity such as another device 520. A WAN device is a device 520 that is interested or engaged in WAN communication. P2P communication refers to direct communication between two or more devices 520, without going through any base station 510. A P2P device is a device 520 that is interested or engaged in P2P communication, e.g., a device 520 that has traffic data for another device 520 within proximity of the P2P device. Two devices may be considered to be within proximity of one another, for example, if each device 520 can detect the other device 520. In general, a device 520 may communicate with another device 520 either directly for P2P communication or via at least one base station 510 for WAN communication.

[0082] In one embodiment, direct communication between devices 520 may be organized into P2P groups. More particularly, a P2P group generally refers to a group of two or more devices 520 interested or engaged in P2P communication and a P2P link refers to a communication link for a P2P group. Furthermore, in one embodiment, a P2P group may include one device 520 designated a P2P group owner (or a P2P server) and one or more devices 520 designated P2P clients that are served by the P2P group owner. The P2P group owner may perform certain management functions such as exchanging signaling with a WAN, coordinating data transmission between the P2P group owner and P2P clients, etc. For example, as shown in FIG. 5, a first P2P group includes devices 520a and 520b under the coverage of base station 510a, a second P2P group includes devices 520c and 520d under the coverage of base station 510b, a third P2P group includes devices 520e and 520f under the coverage of different base stations 510b and 510c, and a fourth P2P group includes devices 520g, 520h and 520i under the coverage of base station 510c. Devices 520a, 520d, 520f, and 520h may be P2P group owners for their respective P2P groups and devices 520b, 520c, 520e, 520g, and 520i may be P2P clients in their respective P2P groups. The other devices 520 in FIG. 5 may be engaged in WAN communication.

[0083] In one embodiment, P2P communication may occur only within a P2P group and may further occur only between the P2P group owner and the P2P clients associated therewith. For example, if two P2P clients within the same P2P group (e.g., devices 520g and 520i) desire to exchange information, one of the P2P clients may send the information to the P2P group owner (e.g., device 520h) and the P2P group owner may then relay transmissions to the other P2P client. In one embodiment, a particular device 520 may belong to multiple P2P groups and may behave as either a P2P group owner or a P2P client in each P2P group. Furthermore, in one embodiment, a particular P2P client may belong to only one P2P group or belong to multiple P2P group and communicate with devices 520 in any of the multiple P2P groups at any particular moment. In general, communication may be facilitated via transmissions on the downlink and uplink. For WAN communication, the downlink (or forward link) refers to the communication link from base stations 510 to devices 520, and the uplink (or reverse link) refers to the communication link from devices 520 to base stations 510. For P2P communication, the P2P downlink refers to the communication link from P2P group owners to P2P clients and the P2P uplink refers to the communication link from P2P clients to P2P group owners. In certain embodiments, rather than using WAN technologies to communicate P2P, two or more devices may form smaller P2P groups and communicate P2P on a wireless local area network (WLAN) using technologies such as Wi-Fi, Bluetooth, or Wi-Fi Direct. For example, P2P communication using Wi-Fi, Bluetooth, Wi-Fi Direct, or other WLAN technologies may enable P2P communication between two or more mobile phones, game consoles, laptop computers, or other suitable communication entities.

[0084] According to one aspect of the disclosure, FIG. 6 illustrates an exemplary environment 600 in which discoverable P2P services may be used to establish a proximity-based distributed bus 625 over which various devices 610, 630, 640 may communicate. For example, in one embodiment, communications between applications and the like, on a single platform may be facilitated using an interprocess communication protocol (IPC) framework over the distributed bus 625, which may comprise a software bus used to enable application-to-application communications in a networked computing environment where applications register with the distributed bus 625 to offer services to other applications and other applications query the distributed bus 625 for information about registered applications. Such a protocol may provide asynchronous notifications and remote procedure calls (RPCs) in which signal messages

(e.g., notifications) may be point-to-point or broadcast, method call messages (e.g., RPCs) may be synchronous or asynchronous, and the distributed bus 625 (e.g., a “daemon” bus process) may handle message routing between the various devices 610, 630, 640.

[0085] In one embodiment, the distributed bus 625 may be supported by a variety of transport protocols (e.g., Bluetooth, TCP/IP, Wi-Fi, CDMA, GPRS, UMTS, etc.). For example, according to one aspect, a first device 610 may include a distributed bus node 612 and one or more local endpoints 614, wherein the distributed bus node 612 may facilitate communications between local endpoints 614 associated with the first device 610 and local endpoints 634 and 644 associated with a second device 630 and a third device 640 through the distributed bus 625 (e.g., via distributed bus nodes 632 and 642 on the second device 630 and the third device 640). As will be described in further detail below with reference to FIG. 7, the distributed bus 625 may support symmetric multi-device network topologies and may provide a robust operation in the presence of device drops-outs. As such, the distributed bus 625, which may generally be independent from any underlying transport protocol (e.g., Bluetooth, TCP/IP, Wi-Fi, etc.) may allow various security options, from unsecured (e.g., open) to secured (e.g., authenticated and encrypted), wherein the security options can be used while facilitating spontaneous connections with among the first device 610, the second device 630, and the third device 640 without intervention when the various devices 610, 630, 640 come into range or proximity to each other.

[0086] According to one aspect of the disclosure, FIG. 7 illustrates an exemplary message sequence 700 in which discoverable P2P services may be used to establish a proximity-based distributed bus over which a first device (“Device A”) 710 and a second device (“Device B”) 730 may communicate. Generally, Device A 710 may request to communicate with Device B 730, wherein Device A 710 may include a local endpoint 714 (e.g., a local application, service, etc.), which may make a request to communicate, in addition to a bus node 712 that may assist in facilitating such communications. Further, Device B 730 may include a local endpoint 734 with which the local endpoint 714 may be attempting to communicate, in addition to a bus node 732 that may assist in facilitating communications between the local endpoint 714 on the Device A 710 and the local endpoint 734 on Device B 730.

[0087] In one embodiment, the bus nodes 712 and 732 may perform a suitable discovery mechanism at message sequence step 754. For example, mechanisms for

discovering connections supported by Bluetooth, TCP/IP, UNIX, or the like may be used. At message sequence step 756, the local endpoint 734 on Device B 730 may request to connect to an entity, service, endpoint etc, available through bus node 732. In one embodiment, the request may include a request-and-response process between local endpoint 734 and bus node 732. At message sequence step 758, a distributed message bus may be formed to connect bus node 732 to bus node 712 and thereby establish a P2P connection between Device A 710 and Device B 730. In one embodiment, communications to/form the distributed bus between the bus nodes 712 and 732 may be facilitated using a suitable proximity-based P2P protocol (e.g., the AllJoyn™ software framework designed to enable interoperability among connected products and software applications from different manufacturers to dynamically create proximal networks and facilitate proximal P2P communication). Alternatively, in one embodiment, a server (not shown) may facilitate the connection between the bus nodes 712 and 732. Furthermore, in one embodiment, a suitable authentication mechanism may be used prior to forming the connection between bus nodes 712 and 732 (e.g., SASL authentication in which a client may send an authentication command to initiate an authentication conversation). Still further, during message sequence step 758, bus nodes 712 and 732 may exchange information about other available endpoints (e.g., local endpoints 644 on Device C 640 in FIG. 6). In such embodiments, each local endpoint that a bus node maintains may be advertised to other bus nodes, wherein the advertisement may include unique endpoint names, transport types, connection parameters, or other suitable information.

[0088] In one embodiment, at message sequence step 760, bus node 712 and bus node 732 may use obtained information associated with the local endpoints 734 and 714, respectively, to create virtual endpoints that may represent the real obtained endpoints available through various bus nodes. In one embodiment, message routing on the bus node 712 may use real and virtual endpoints to deliver messages. Further, there may be one local virtual endpoint for every endpoint that exists on remote devices (e.g., Device A 710). Still further, such virtual endpoints may multiplex and/or de-multiplex messages sent over the distributed bus (e.g., a connection between bus node 712 and bus node 732). In one aspect, virtual endpoints may receive messages from the local bus node 712 or 732, just like real endpoints, and may forward messages over the distributed bus. As such, the virtual endpoints may forward messages to the local bus nodes 712 and 732 from the endpoint multiplexed distributed bus connection.

Furthermore, in one embodiment, virtual endpoints that correspond to virtual endpoints on a remote device may be reconnected at any time to accommodate desired topologies of specific transport types. In such an aspect, UNIX based virtual endpoints may be considered local and as such may not be considered candidates for reconnection. Further, TCP-based virtual endpoints may be optimized for one hop routing (e.g., each bus node 712 and 732 may be directly connected to each other). Still further, Bluetooth-based virtual endpoints may be optimized for a single pico-net (e.g., one master and n slaves) in which the Bluetooth-based master may be the same bus node as a local master node.

[0089] At message sequence step 762, the bus node 712 and the bus node 732 may exchange bus state information to merge bus instances and enable communication over the distributed bus. For example, in one embodiment, the bus state information may include a well-known to unique endpoint name mapping, matching rules, routing group, or other suitable information. In one embodiment, the state information may be communicated between the bus node 712 and the bus node 732 instances using an interface with local endpoints 714 and 734 communicating with using a distributed bus based local name. In another aspect, bus node 712 and bus node 732 may each may maintain a local bus controller responsible for providing feedback to the distributed bus, wherein the bus controller may translate global methods, arguments, signals, and other information into the standards associated with the distributed bus. At message sequence step 764, the bus node 712 and the bus node 732 may communicate (e.g., broadcast) signals to inform the respective local endpoints 714 and 734 about any changes introduced during bus node connections, such as described above. In one embodiment, new and/or removed global and/or translated names may be indicated with name owner changed signals. Furthermore, global names that may be lost locally (e.g., due to name collisions) may be indicated with name lost signals. Still further, global names that are transferred due to name collisions may be indicated with name owner changed signals and unique names that disappear if and/or when the bus node 712 and the bus node 732 become disconnected may be indicated with name owner changed signals.

[0090] As used above, well-known names may be used to uniquely describe local endpoints 714 and 734. In one embodiment, when communications occur between Device A 710 and Device B 730, different well-known name types may be used. For example, a device local name may exist only on the bus node 712 associated with Device A 710 to which the bus node 712 directly attaches. In another example, a global

name may exist on all known bus nodes 712 and 732, where only one owner of the name may exist on all bus segments. In other words, when the bus node 712 and bus node 732 are joined and any collisions occur, one of the owners may lose the global name. In still another example, a translated name may be used when a client is connected to other bus nodes associated with a virtual bus. In such an aspect, the translated name may include an appended end (e.g., a local endpoint 714 with well-known name “org.foo” connected to the distributed bus with Globally Unique Identifier “1234” may be seen as “G1234.org.foo”).

[0091] At message sequence step 766, the bus node 712 and the bus node 732 may communicate (e.g., broadcast) signals to inform other bus nodes of changes to endpoint bus topologies. Thereafter, traffic from local endpoint 714 may move through virtual endpoints to reach intended local endpoint 734 on Device B 730. Further, in operation, communications between local endpoint 714 and local endpoint 734 may use routing groups. In one aspect, routing groups may enable endpoints to receive signals, method calls, or other suitable information from a subset of endpoints. As such, a routing name may be determined by an application connected to a bus node 712 or 732. For example, a P2P application may use a unique, well-known routing group name built into the application. Further, bus nodes 712 and 732 may support registering and/or de-registering of local endpoints 714 and 734 with routing groups. In one embodiment, routing groups may have no persistence beyond a current bus instance. In another aspect, applications may register for their preferred routing groups each time they connect to the distributed bus. Still further, routing groups may be open (e.g., any endpoint can join) or closed (e.g., only the creator of the group can modify the group). Yet further, a bus node 712 or 732 may send signals to notify other remote bus nodes of additions, removals, or other changes to routing group endpoints. In such embodiments, the bus node 712 or 732 may send a routing group change signal to other group members whenever a member is added and/or removed from the group. Further, the bus node 712 or 732 may send a routing group change signal to endpoints that disconnect from the distributed bus without first removing themselves from the routing group.

[0092] In the near future, increasing development in IoT technologies will lead to numerous IoT devices surrounding a user at home, in vehicles, at work, and many other locations. As the IoT grows, it will become increasingly important to support a mechanism whereby different IoT devices can inter-operate and take actions by sending / receiving mutually understood machine-to-machine (M2M) events. Traditionally, this

requires the device manufacturer (or collectively a set of manufacturers for a given device class) to define an events dictionary and publish it via some globally accessible means, for example, a global database of M2M events dictionary. However, this requires a significant amount of collaboration among the different IoT parties involved, and requires a globally accessible infrastructure for M2M interactions, which is not a desirable a solution.

[0093] Accordingly, the disclosure provides a mechanism to automatically generate an M2M events dictionary in a distributed IoT network without prior collaboration among different IoT vendors. Such a dictionary can then be distributed to IoT devices to enable them to understand M2M events and take action(s) based on those events.

[0094] A given IoT network can include multiple IoT devices from different vendors that provide similar functionality. For example, a home IoT network may include window sensors from two different vendors. These IoT devices may implement the same P2P service interface, such as a window sensor interface, for inter-operability. However, the IoT devices may define similar events/state transitions using different textual descriptions that have same meaning to the end user. For example, the two window sensors may have “window closed” and “window shut” events, respectively, when their associated windows are closed.

[0095] If another IoT device is interested in taking actions based on broadcasted events, it needs to be able to interpret that two events with different descriptions are actually the same type of event. Continuing the window sensors example, there may be a rule that a HVAC system should turn “on” when it detects an event indicating that the window is closed. Accordingly, it is desirable to generate a common M2M events dictionary that can map multiple similar events to a single event. For example, the “window closed” and “window shut” events would map to a single generic event.

[0096] IoT devices in a given IoT network generally take actions only based on M2M events broadcasted by other IoT devices in that network. As such, these IoT devices only need the events dictionary for events from the other IoT devices in that network, instead of an events dictionary for the global universe of IoT devices. Thus, as long as a localized M2M events dictionary can be generated, the IoT devices in the given IoT network can take actions based on that dictionary.

[0097] Each IoT network can generate its own localized M2M events dictionary, which addresses the issue of generating an M2M events dictionary in a distributed fashion. This avoids requiring any centralized infrastructure for maintaining/sharing M2M

events dictionaries.

[0098] To automatically generate the M2M events dictionary, an Events Monitor and Dictionary Generator (EMDG) component, such as EMDG module 210 / 410, can be installed in a distributed IoT network that monitors all the broadcasted events from IoT devices in that IoT network. The EMDG component can be installed on the IoT network's gateway, such as supervisor 130, IoT SuperAgent 140, or gateway 145. In an aspect, events can be broadcasted so that they will be received by this component. In an alternative aspect, if events are shared using a publish / subscribe model, this component will subscribe to all IoT devices that broadcast events. The EMDG component can discover events broadcasters (e.g., IoT devices broadcasting events) based on discovery announcements from the IoT devices.

[0099] The EMDG component may also be aware of the device class/type for the various IoT devices on the network. For example, it would know that a window sensor X and a window sensor Y belong to the same device class/type. This information can also be learned from the discovery announcements from the IoT devices.

[00100] The EMDG component monitors the state of an IoT device before and after a broadcasted event. It can compare the before and after states and correlate the event with a state change, or changes in a system value. Referring again to the window sensors example, the EMDG component can compare the state of the first window sensor before and after the "window closed" event, and the state of the second window sensor before and after the "window shut" event. Based on the state change, the EMDG component can map these two events to a single generic M2M event in the M2M events dictionary entry for that class/type of IoT device.

[00101] Continuing with the window sensor example, after receiving the "window closed" event from the first window sensor, the EMDG component can compare the state of the first window sensor before the "window closed" event (e.g., "open") to the state of the first window sensor after the "window closed" event occurred (e.g., "closed"), and can map the event to the change in window state from "open" to "closed." The EMDG component can create a generic/common event entry for that device class/type and detected state change and assign it an enumeration and text description, such as the string "1: window is closed now."

[00102] The EMDG component can also keep a mapping of the generic event to the actual state change. For example, the string "1: window is closed now" would map to the state change of "open" to "closed." That is, the EMDG component creates a generic

entry describing the state change occurring around the detected event, and then maps that generic entry to the specific event received from the window sensor.

[00103] When a “window shut” event is received from the second window sensor, the EMDG component will map that event to the previously created generic/common event, i.e., “1: window is closed now,” for that device class/type based on the observed state change that matches the state change for the generic event. The EMDG component maintains a mapping of generic/common events to the actual broadcasted device events, that is, “1: window is closed now” maps to the “window closed” and “window shut” events. Thus, the EMDG component can create a generic/common M2M events dictionary for the window sensor device class, such as “1: window is closed now” and “2: window is open now.”

[00104] Referring to the EMDG component monitoring the state of IoT devices in greater detail, the EMDG component can periodically poll devices to obtain their current state information. After detecting an event, the EMDG component can poll the IoT device again to obtain the state of the IoT device after the event. Some IoT devices may also offer a service whereby they log their system state before and after events. Such a service can be activated by the EMDG component, so that the EMDG component can retrieve before and after device states upon receiving an event from a given IoT device.

[00105] The EMDG component learns about events and generates generic events dictionary entries as events are broadcasted by IoT devices on the IoT network. This self-learning process could take some time. To expedite this self-learning phase, each IoT device can be designed to have a special mode, such as an “Events Broadcasting Mode,” in which an IoT device will broadcast all the events it supports and simulate state changes for those events. This will expedite the self-learning / automatic generation aspect for M2M events. This mode can be triggered just after an IoT device is on-boarded onto the network as part of the onboarding process.

[00106] The M2M events dictionary can be used for home automation. Specifically, home automation rules can be defined based on the generic M2M events dictionary. This is most desirable from the user experience perspective, as the user does not need to tailor automation rules for different vendors. The EMDG component can send out the generated generic M2M events dictionary and, optionally, the actual IoT device events mapping, to the other nodes in the IoT network. For example, the EMDG component can send the M2M events dictionary to the control application that provides the UI for

defining home automation rules, as well as IoT devices interested in taking actions based on broadcasted events. These IoT devices can be programmed to take actions based on the generic M2M dictionary from home automation rules. When the actual broadcasted events are received, they are mapped to the generic M2M events for taking the desired action.

[00107] The described mechanism is self-learning. When a new IoT device is added to the IoT network, the EMDG component either maps broadcasted events from the new IoT device to an already defined generic M2M event dictionary entry or generates a new set of generic M2M event dictionary entries for that device class. As described above, mapping events from the new IoT device is done based on state changes observed before and after the event.

[00108] These and other aspects of the disclosure will now be described with reference to FIG. 8. FIG. 8 illustrates an exemplary proximal IoT network 800 according to at least one aspect of the disclosure. The IoT network 800 includes a gateway agent 802, an EMDG 804 (which may correspond to EMDG module 210 / 410), a control application 806, and four IoT devices 810. The gateway agent 802 may be installed on the supervisor device 130, the SuperAgent 140, or the gateway 145, for example. In FIG. 8, the circled reference numbers indicate the order of operations.

[00109] At operation 1, devices 3 and 4, identified by reference number 810, broadcast event notifications that are detected by the EMDG 804. As discussed above, devices 3 and 4 may broadcast the events, in which case the EMDG 804 intercepts the broadcasts, or the EMDG 804 may subscribe to the events published by each device 810 in the IoT network 800. At operation 2, the EMDG 804 retrieves and compares the states of devices 3 and 4 before and after the broadcasted events. As mentioned above, the EMDG fetches the device state information from the device before and after the event. At operation 3, the EMDG 804 creates a generic M2M event mapping based on the before and after device states.

[00110] At operation 4, the EMDG 804 sends the M2M generic events dictionary to the control application 806, which may be installed on the user's smartphone or supervisor device 130, for example. Also at operation 4, the EMDG 804 sends the M2M generic events dictionary to other devices 810 in the IoT network 800, such as devices 1 and 2, identified by reference number 810. Furthermore, the control application 806 and devices 810 can fetch the M2M generic events dictionary from the EMDG 804, for example, by fetching the M2M generic events dictionary upon start-up.

[00111] At operation 5, the user may define home automation (HA) rules based on the generic M2M events dictionary using the control application 806. Since the home automation rules are defined using the generic M2M events dictionary, the user only needs to be shown generic events and not different kinds of similar events from multiple vendors. This greatly simplifies the user experience for creating home automation rules.

[00112] At operation 6, the control application 806 propagates the home automation rules to other devices 810 in the IoT network 800, such as devices 1 and 2. Although FIG. 8 illustrates the home automation rules being propagated to only two devices, it will be appreciated that the rules may be propagated to any number of devices 810 in network 800, including all devices 810.

[00113] At operation 7, device 4 again broadcasts an event. At operation 8, the event is detected by device 2. At operation 9, device 2 determines that the received event maps to a generic event in the generated M2M events dictionary. The device 2 then executes one or more home automation rules defined for the associated generic event in the M2M events dictionary.

[00114] FIG. 9 illustrates an exemplary flow for automatically generating an events dictionary for an inter-device communication protocol, such as an M2M protocol, in an IoT network. The flow illustrated in FIG. 9 may be performed by the EMDG 804 in FIG. 8. At 910, the EMDG 804 receives a notification of an event broadcasted by an IoT device in the IoT network, such as one of IoT devices 810 in FIG. 8. The notification may be received either as a broadcast or as a subscription event, for example.

[00115] At 920, the EMDG 804 determines a state of the IoT device before the event and a state of the IoT device after the event. The EMDG 804 may periodically poll the IoT device, thereby retrieving the state of the IoT device before the event. Immediately after an event, the EMDG 804 may retrieve the state of the IoT device independently of the periodic polling. At 930, EMDG 804 compares the state of the IoT device before the event to the state of the IoT device after the event.

[00116] At 940, the EMDG 804 determines a type of state change of the event based on the comparing at 920. The determining at 940 may include polling the IoT device for the state of the IoT device before the event and polling the IoT device for the state of the IoT device after the event.

[00117] At 950, the EMDG 804 determines whether or not there is an entry in the events dictionary for a type of state change matching the type of state change of the event. If

the EMDG 804 determines that there is an entry in the events dictionary for the type of state change matching the type of state change of the event, the EMDG 804 does not need to do anything and the flow returns to the beginning.

[00118] If, however, the EMDG 804 determines that there is not an entry in the events dictionary for a type of state change matching the type of state change of the event, then at 960, the EMDG 804 creates a generic entry in the events dictionary for the type of state change of the event. The generic entry may include an enumeration and a text description of the type of state change associated with the generic entry. The type of state change associated with the generic entry is common to IoT devices of the same type and/or class as the IoT device. At 970, the EMDG 804 stores a mapping of an event description of the event with the generic entry.

[00119] In an aspect, the EMDG 804 may determine the type of the IoT device. In this case, determining whether or not there is a generic entry in the events dictionary (950) may include determining whether or not there is a generic entry in the events dictionary for a type of IoT device matching the type of the IoT device and a type of state change matching the type of state change of the event, and creating the generic entry in the events dictionary (960) may include creating the generic entry in the events dictionary based on there not being a generic entry in the events dictionary for a type of IoT device matching the type of the IoT device and a type of state change matching the type of state change of the event.

[00120] Although not illustrated in FIG. 9, the EMDG 804 may detect a second event from a second IoT device (similar to 910), determine a state of the second IoT device before the second event and a state of the second IoT device after the second event (similar to 920), compare the state of the second IoT device before the second event to the state of the second IoT device after the second event (similar to 930), detect a type of state change of the second event based on the comparing (similar to 940), map the second event to the generic entry based on the second event being a same type of state change as the state change of the event and a same type and/or class of as the IoT device, and store a mapping of an event description of the second event received from the second IoT device with the generic entry. The event description of the second event received from the second IoT device may be different from an event description of the event received from the IoT device. The generic entry may describe a generic state change common to the IoT device and the second IoT device and store event descriptions for events received from the IoT device and the second IoT device.

[00121] In an aspect, although not illustrated in FIG. 9, the EMDG 804 may transmit the events dictionary to other IoT devices in the IoT network. The EMDG 804 may also define home automation rules based on generic events defined in the events dictionary by a control application, and distribute the home automation rules to other IoT devices in the IoT network. A third IoT device in the IoT network may receive an event notification from the first or the second IoT device in the IoT network, map the received event to a generic entry in the events dictionary, and execute the home automation rules defined for the generic entry in the events dictionary.

[00122] According to one aspect of the disclosure, FIG. 10 illustrates an exemplary communications device 1000 that may correspond to one or more devices that may automatically generate an events dictionary for an inter-device communication protocol in an IoT network, as described herein (e.g., gateway agent 802 in FIG. 8, or another device embodying EMDG 804). In particular, as shown in FIG. 10, communications device 1000 may comprise a receiver 1002 that may receive a signal from, for instance, a receive antenna (not shown), perform typical actions on the received signal (e.g., filtering, amplifying, downconverting, etc.), and digitize the conditioned signal to obtain samples. The receiver 1002 can comprise a demodulator 1004 that can demodulate received symbols and provide them to a processor 1006 for channel estimation. The processor 1006 can be a processor dedicated to analyzing information received by the receiver 1002 and/or generating information for transmission by modulator 1018 and transmitter 1020, a processor that controls one or more components of communications device 1000, and/or a processor that both analyzes information received by receiver 1002, generates information for transmission by transmitter 1020, and controls one or more components of communications device 1000.

[00123] Communications device 1000 can additionally comprise a memory 1008 that is operatively coupled to processor 1006 and that can store data to be transmitted, received data, information related to available channels, data associated with analyzed signal and/or interference strength, information related to an assigned channel, power, rate, or the like, and any other suitable information for estimating a channel and communicating via the channel. Memory 1008 can additionally store protocols and/or algorithms associated with estimating and/or utilizing a channel (e.g., performance based, capacity based, etc.).

[00124] It will be appreciated that memory 1008 can be either volatile memory or nonvolatile memory, or can include both volatile and nonvolatile memory. By way of

illustration, and not limitation, nonvolatile memory can include read only memory (ROM), programmable ROM (PROM), electrically programmable ROM (EPROM), electrically erasable PROM (EEPROM), or flash memory. Volatile memory can include random access memory (RAM), which acts as external cache memory. By way of illustration and not limitation, RAM is available in many forms such as synchronous RAM (SRAM), dynamic RAM (DRAM), synchronous DRAM (SDRAM), double data rate SDRAM (DDR SDRAM), enhanced SDRAM (ESDRAM), Synchlink DRAM (SLDRAM), and direct Rambus RAM (DRRAM). Memory 1008 of the subject systems and methods may comprise, without being limited to, these and any other suitable types of memory.

[00125] In an embodiment, memory 1008 may store an EMDG module 1010. The EMDG module 1010 may be a software module executable by processor 1006. Alternatively, the EMDG module 1010 may be a hardware component of, or coupled to, processor 1006. As yet another alternative, the EMDG module 1010 may be a combination of hardware and software. The EMDG module 1010 may correspond to EMDG 804 in FIG. 8.

[00126] Communications device 1000 can further include distributed bus module 1030 to facilitate establishing connections with other devices, such as communications device 1000. Distributed bus module 1030 may further comprise bus node module 1032 to assist distributed bus module 1030 managing communications between multiple devices. In one aspect, a bus node module 1032 may further include object naming module 1034 to assist bus node module 1032 in communicating with endpoint applications associated with other devices. Still further, distributed bus module 1030 may include endpoint module 1036 to assist local endpoints in communicating with other local endpoints and/or endpoints accessible on other devices through an established distributed bus. In another aspect, distributed bus module 1030 may facilitate inter-device and/or intra-device communications over multiple available transports (e.g., Bluetooth, UNIX domain-sockets, TCP/IP, Wi-Fi, etc.).

[00127] Additionally, in one embodiment, communications device 1000 may include a user interface 1040, which may include one or more input mechanisms 1042 for generating inputs into communications device 1000, and one or more output mechanisms 1044 for generating information for consumption by the user of the communications device 1000. For example, input mechanism 1042 may include a mechanism such as a key or keyboard, a mouse, a touch-screen display, a microphone,

etc. Further, for example, output mechanism 1044 may include a display, an audio speaker, a haptic feedback mechanism, a Personal Area Network (PAN) transceiver etc. In the illustrated aspects, the output mechanism 1044 may include an audio speaker operable to render media content in an audio form, a display operable to render media content in an image or video format and/or timed metadata in a textual or visual form, or other suitable output mechanisms. However, in one embodiment, where the communications device 1000 is a headless device, the communications device 1000 may not include certain input mechanisms 1042 and/or output mechanisms 1044 because headless devices generally refer to computer systems or device that have been configured to operate without a monitor, keyboard, and/or mouse.

[00128] Where the communications device 1000 is configured to automatically generate an events dictionary for an inter-device communication protocol in an IoT network, as described here, the receiver 1002, processor 1006, memory 1008, EMDG module 1010, transmitter 1020, and distributed bus module 1030 may cooperatively perform the functionality described herein. For example, upon the receiver 1002 receiving a notification of an event broadcasted by an IoT device in the IoT network, the EMDG module 1010 may, when executed by the processor 1006, cause the processor 1006 to determine a state of the IoT device before the event and a state of the IoT device after the event, compare the state of the IoT device before the event to the state of the IoT device after the event, determine a type of state change of the event based on the comparing, determine whether or not there is an entry in the events dictionary for a type of state change matching the type of state change of the event, and create a generic entry in the events dictionary for the type of state change of the event if there is not an entry in the events dictionary for a type of state change matching the type of state change of the event. The memory 1008 may then store a mapping of an event description of the event with the generic entry. Alternatively, where the EMDG module 1010 is a hardware module, the EMDG module 1010 may perform the functionality described above as being performed by the processor 1006.

[00129] FIG. 11 illustrates an example apparatus 1100 represented as a series of interrelated functional modules. A module for receiving 1102 may correspond at least in some aspects to, for example, a communication device, such as receiver 1002 in FIG. 10, as discussed herein. A module for determining 1104 may correspond at least in some aspects to, for example, a processing system, such as processor 1006 and/or EMDG module 1010 in FIG. 10, as discussed herein. A module for comparing 1106

may correspond at least in some aspects to, for example, a processing system, such as processor 1006 and/or EMDG module 1010 in FIG. 10, as discussed herein. A module for determining 1108 may correspond at least in some aspects to, for example, a processing system, such as processor 1006 and/or EMDG module 1010 in FIG. 10, as discussed herein. A module for determining 1110 may correspond at least in some aspects to, for example, a processing system, such as processor 1006 and/or EMDG module 1010 in FIG. 10, as discussed herein. A module for creating 1112 may correspond at least in some aspects to, for example, a processing system, such as processor 1006 and/or EMDG module 1010 in FIG. 10, in conjunction with a storage system, such as memory 1008 in FIG. 10, as discussed herein. A module for storing 1114 may correspond at least in some aspects to, for example, a processing system, such as processor 1006 and/or EMDG module 1010 in FIG. 10, in conjunction with a storage system, such as memory 1008 in FIG. 10, as discussed herein.

[00130] The functionality of the modules of FIG. 11 may be implemented in various ways consistent with the teachings herein. In some designs, the functionality of these modules may be implemented as one or more electrical components. In some designs, the functionality of these blocks may be implemented as a processing system including one or more processor components. In some designs, the functionality of these modules may be implemented using, for example, at least a portion of one or more integrated circuits (e.g., an ASIC). As discussed herein, an integrated circuit may include a processor, software, other related components, or some combination thereof. Thus, the functionality of different modules may be implemented, for example, as different subsets of an integrated circuit, as different subsets of a set of software modules, or a combination thereof. Also, it will be appreciated that a given subset (e.g., of an integrated circuit and/or of a set of software modules) may provide at least a portion of the functionality for more than one module.

[00131] In addition, the components and functions represented by FIG. 11, as well as other components and functions described herein, may be implemented using any suitable means. Such means also may be implemented, at least in part, using corresponding structure as taught herein. For example, the components described above in conjunction with the “module for” components of FIG. 11 also may correspond to similarly designated “means for” functionality. Thus, in some aspects one or more of such means may be implemented using one or more of processor components, integrated circuits, or other suitable structure as taught herein.

[00132] Those skilled in the art will appreciate that information and signals may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

[00133] Further, those skilled in the art will appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the aspects disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted to depart from the scope of the present disclosure.

[00134] The various illustrative logical blocks, modules, and circuits described in connection with the aspects disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices (e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration).

[00135] The methods, sequences and/or algorithms 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, flash memory, ROM, EPROM, EEPROM, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary

storage medium is coupled to the processor such that the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor. The processor and the storage medium may reside in an ASIC. The ASIC may reside in an IoT device. In the alternative, the processor and the storage medium may reside as discrete components in a user terminal.

[00136] In one or more exemplary aspects, the functions described may be implemented in hardware, software, firmware, or any combination thereof. If implemented in software, the functions may be stored on or transmitted over as one or more instructions or code on a computer-readable medium. Computer-readable media includes both computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A storage media may be any available media that can be accessed by a computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium that can be used to carry or store desired program code in the form of instructions or data structures and that can be accessed by a computer. Also, any connection is properly termed a computer-readable medium. For example, if the software is transmitted from a website, server, or other remote source using a coaxial cable, fiber optic cable, twisted pair, DSL, or wireless technologies such as infrared, radio, and microwave, then the coaxial cable, fiber optic cable, twisted pair, DSL, or wireless technologies such as infrared, radio, and microwave are included in the definition of medium. Disk and disc, as used herein, includes CD, laser disc, optical disc, DVD, floppy disk and Blu-ray disc where disks usually reproduce data magnetically and/or optically with lasers. Combinations of the above should also be included within the scope of computer-readable media.

[00137] While the foregoing disclosure shows illustrative aspects of the disclosure, it should be noted that various changes and modifications could be made herein without departing from the scope of the disclosure as defined by the appended claims. The functions, steps and/or actions of the method claims in accordance with the aspects of the disclosure described herein need not be performed in any particular order. Furthermore, although elements of the disclosure may be described or claimed in the singular, the plural is contemplated unless limitation to the singular is explicitly stated.

## CLAIMS

What is claimed is:

1. A method of automatically generating an events dictionary in an Internet of Things (IoT) network, comprising:
  - receiving a notification of a first event from a first IoT device in the IoT network;
  - determining a state of the first IoT device before and after the first event;
  - comparing the states of the first IoT device;
  - determining a type of state change of the first event based on the comparing;
  - determining whether the type of the state change of the first event is present in the events dictionary;
  - creating a generic entry based on the type of the state change of the first event not being present in the events dictionary, wherein the type of the state change associated with the generic entry is common to IoT devices of a same type and/or class as the first IoT device; and
  - storing, in the events dictionary, a mapping of an event description of the first event to the generic entry.
2. The method of claim 1,
  - wherein determining the state of the first IoT device before the first event includes periodically polling the first IoT device to retrieve the state of the first IoT device before the first event, and
  - wherein determining the state of the first IoT device after the first event includes retrieving the state of the first IoT device after the first event.
3. The method of claim 1, further comprising:
  - determining a type of the first IoT device, wherein the creating comprises creating the generic entry in the events dictionary for a type of IoT device matching the type of the first IoT device and a type of state change matching the type of the state change of the first event.
4. The method of claim 1, wherein the generic entry comprises an enumeration and a text description of the type of the state change associated with the generic entry.

5. The method of claim 1, further comprising:
  - receiving a second notification of a second event by a second IoT device in the IoT network;
  - determining a state of the second IoT device before and after the second event;
  - comparing the states of the second IoT device;
  - determining a type of state change of the second event based on the comparing;
  - mapping the second event to the generic entry based on the second event being a same type of state change as the state change of the first event and a same type and/or class as the first IoT device; and
  - storing a mapping of an event description of the second event received from the second IoT device to the generic entry.
6. The method of claim 5, wherein the event description of the second event is different from the event description of the first event.
7. The method of claim 5, wherein the generic entry describes a generic state change that is common to the first IoT device and the second IoT device, and further wherein, the generic entry includes event descriptions for events received from the first IoT device and the second IoT device.
8. The method of claim 1, further comprising:
  - transmitting the events dictionary to other IoT devices in the IoT network.
9. The method of claim 8, further comprising:
  - defining home automation rules based on generic events defined in the events dictionary; and
  - distributing the home automation rules to the other IoT devices in the IoT network.
10. The method of claim 9, wherein a third IoT device in the IoT network receives an event notification from the first or the second IoT device in the IoT network, maps event information in the received event notification to the generic entry in the events

dictionary, and executes the home automation rules defined for the generic entry in the events dictionary.

11. An apparatus for automatically generating an events dictionary in an Internet of Things (IoT) network, comprising:

a transceiver configured to receive a notification of a first event from a first IoT device in the IoT network; and

at least one processor configured to:

determine a state of the first IoT device before and the first event;

compare the states of the first IoT device;

determine a type of state change of the first event based on the comparison of the states of the first IoT device;

determine whether the type of the state change of the first event is present in the events dictionary; and

create a generic entry based on the type of the state change of the first event not being present in the events dictionary, wherein the type of the state change associated with the generic entry is common to IoT devices of a same type and/or class as the first IoT device; and

a memory configured to store, in the events dictionary, a mapping of an event description of the first event to the generic entry.

12. The apparatus of claim 11,

wherein the at least one processor being configured to determine the state of the first IoT device before the first event includes the at least one processor being configured to periodically poll the first IoT device to retrieve the state of the first IoT device before the first event, and

wherein the at least one processor being configured to determine the state of the first IoT device after the first event includes the at least one processor being configured to retrieve the state of the first IoT device after the first event.

13. The apparatus of claim 11, wherein the at least one processor is further configured to determine a type of the first IoT device, wherein the at least one processor being configured to create comprises the at least one processor being configured to create the generic entry in the events dictionary for a type of IoT device

matching the type of the first IoT device and a type of state change matching the type of the state change of the first event.

14. The apparatus of claim 11, wherein the generic entry comprises an enumeration and a text description of the type of the state change associated with the generic entry.

15. The apparatus of claim 11,

wherein the transceiver is further configured to receive a second notification of a second event broadcasted by a second IoT device in the IoT network;

wherein the at least one processor is further configured to:

determine a state of the second IoT device before and after the second

event;

compare the states of the second IoT device;

determine a type of state change of the second event based on a comparison of the states of the second IoT device; and

map the second event to the generic entry based on the second event being a same type of state change as the state change of the first event and a same type and/or class as the first IoT device; and

wherein the memory is further configured to store a mapping of an event description of the second event received from the second IoT device to the generic entry.

16. The apparatus of claim 15, wherein the event description of the second event is different from the event description of the first event.

17. The apparatus of claim 15, wherein the generic entry describes a generic state change that is common to the first IoT device and the second IoT device, and further wherein, the generic entry includes event descriptions for events received from the first IoT device and the second IoT device.

18. The apparatus of claim 11, wherein the transceiver is further configured to transmit the events dictionary to other IoT devices in the IoT network.

19. The apparatus of claim 18,

wherein the at least one processor is further configured to define home automation rules based on generic events defined in the events dictionary; and  
wherein the transceiver is further configured to distribute the home automation rules to the other IoT devices in the IoT network.

20. The apparatus of claim 19, wherein a third IoT device in the IoT network receives an event notification from the first or the second IoT device in the IoT network, maps event information in the received event notification to the generic entry in the events dictionary, and executes the home automation rules defined for the generic entry in the events dictionary.

21. A non-transitory computer-readable medium for automatically generating an events dictionary in an Internet of Things (IoT) network, comprising:

at least one instruction to receive a notification of a first event from a first IoT device in the IoT network;

at least one instruction to determine a state of the first IoT device before and after the first event;

at least one instruction to compare the states of the first IoT device;

at least one instruction to determine a type of state change of the first event based on a comparison of the states of the first IoT device;

at least one instruction to determine whether the type of the state change of the first event is present in the events dictionary;

at least one instruction to create a generic entry based on the type of the state change of the first event not being present in the events dictionary, wherein the type of the state change associated with the generic entry is common to IoT devices of a same type and/or class as the first IoT device; and

at least one instruction to store, in the events dictionary, a mapping of an event description of the first event to the generic entry.

22. The non-transitory computer-readable medium of claim 21,  
wherein the at least one instruction to determine the state of the first IoT device before the first event includes at least one instruction to periodically poll the first IoT device to retrieve the state of the first IoT device before the first event, and

wherein the at least one instruction to determine the state of the first IoT device after the first event includes at least one instruction to retrieve the state of the first IoT device after the first event.

23. The non-transitory computer-readable medium of claim 21, further comprising:
  - at least one instruction to determine a type of the first IoT device, wherein the at least one instruction to create comprises at least one instruction to create the generic entry in the events dictionary for a type of IoT device matching the type of the first IoT device and a type of state change matching the type of the state change of the first event.
24. The non-transitory computer-readable medium of claim 21, wherein the generic entry comprises an enumeration and a text description of the type of the state change associated with the generic entry.
25. The non-transitory computer-readable medium of claim 21, further comprising:
  - at least one instruction to receive a second notification of a second event from a second IoT device in the IoT network;
  - at least one instruction to determine a state of the second IoT device before and after the second event;
  - at least one instruction to compare the states of the second IoT device;
  - at least one instruction to determine a type of state change of the second event based on a comparison of the states of the second IoT device;
  - at least one instruction to map the second event to the generic entry based on the second event being a same type of state change as the state change of the first event and a same type and/or class as the first IoT device; and
  - at least one instruction to store a mapping of an event description of the second event received from the second IoT device to the generic entry.
26. The non-transitory computer-readable medium of claim 25, wherein the event description of the second event is different from an event description of the first event.
27. The non-transitory computer-readable medium of claim 25, wherein the generic entry describes a generic state change common to the first IoT device and the second

IoT device and stores event descriptions for events received from the first IoT device and the second IoT device.

28. The non-transitory computer-readable medium of claim 21, further comprising:
  - at least one instruction to transmit the events dictionary to other IoT devices in the IoT network.
29. The non-transitory computer-readable medium of claim 28, further comprising:
  - at least one instruction to define home automation rules based on generic events defined in the events dictionary; and
  - at least one instruction to distribute the home automation rules to the other IoT devices in the IoT network.
30. An apparatus for automatically generating an events dictionary in an Internet of Things (IoT) network, comprising:
  - means for receiving a notification of a first event from a first IoT device in the IoT network;
  - means for determining a state of the first IoT device before and after the first event;
  - means for comparing the states of the first IoT device;
  - means for determining a type of state change of the first event based on a comparison of the states of the first IoT device;
  - means for determining whether the type of the state change of the first event is present in the events dictionary;
  - means for creating a generic entry based on the type of the state change of the first event not being present in the events dictionary, wherein the type of the state change associated with the generic entry is common to IoT devices of a same type and/or class as the first IoT device; and
  - means for storing, in the events dictionary, a mapping of an event description of the first event to the generic entry.

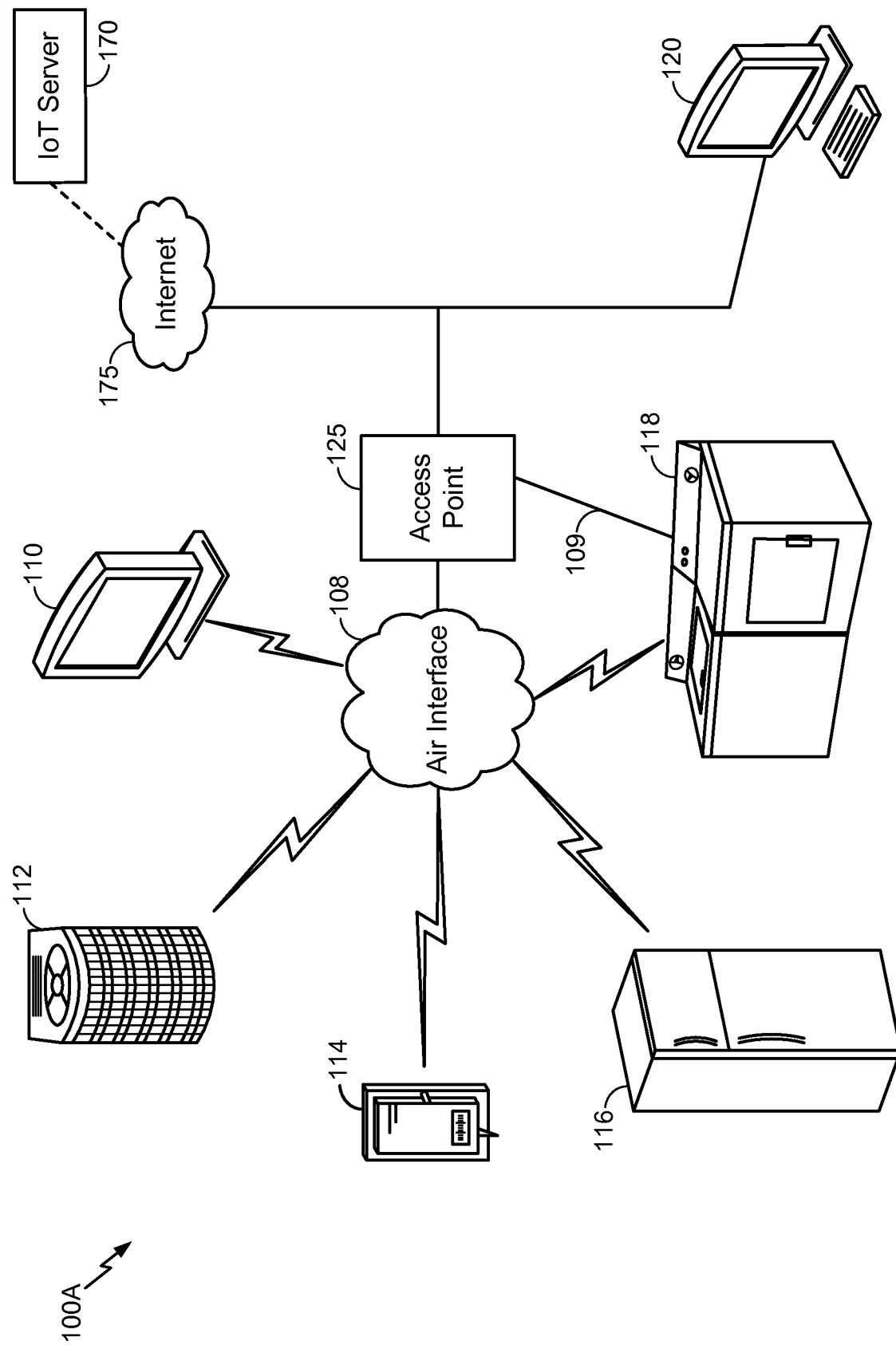


FIG. 1A

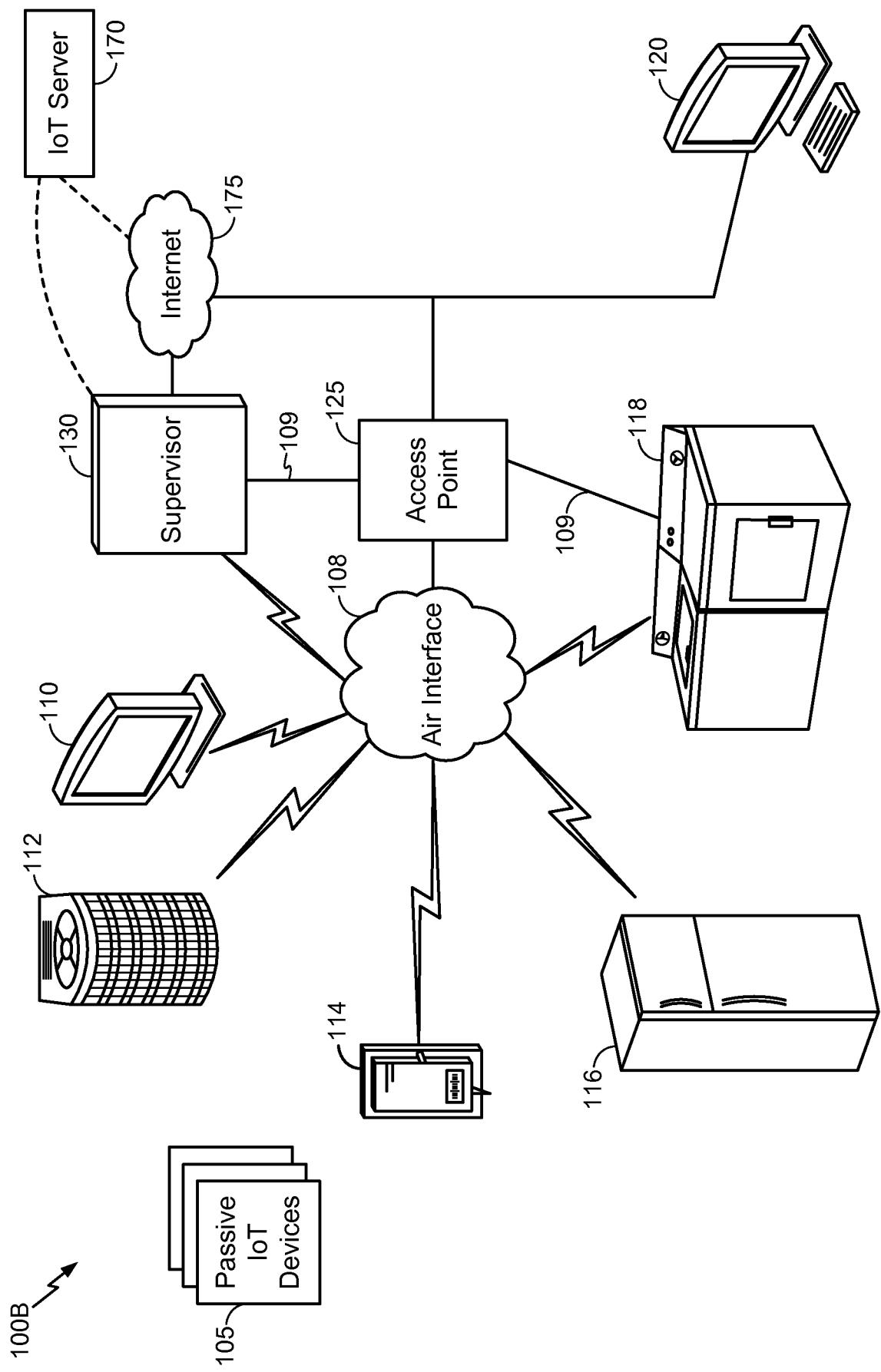
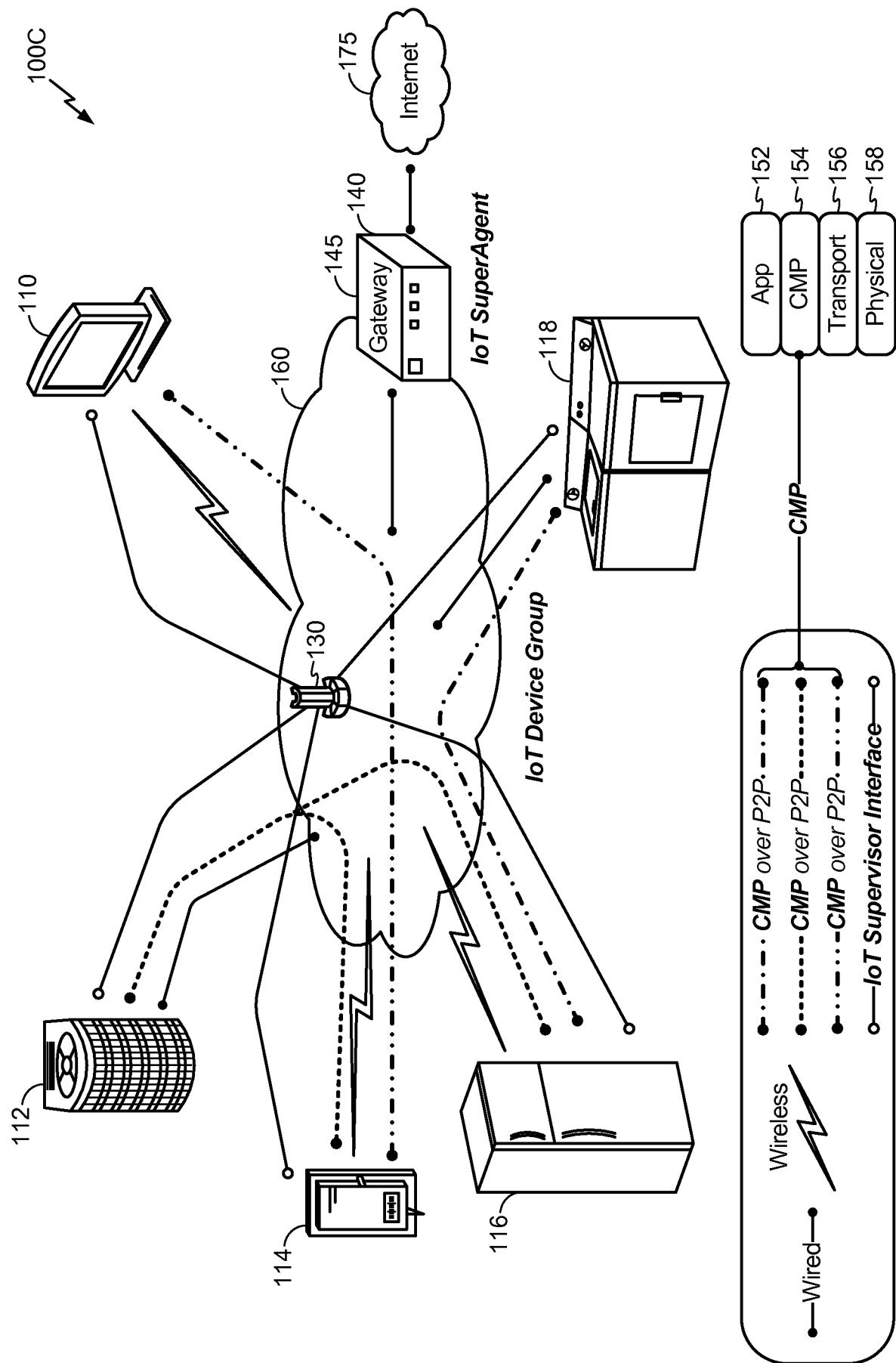


FIG. 1B



4/16

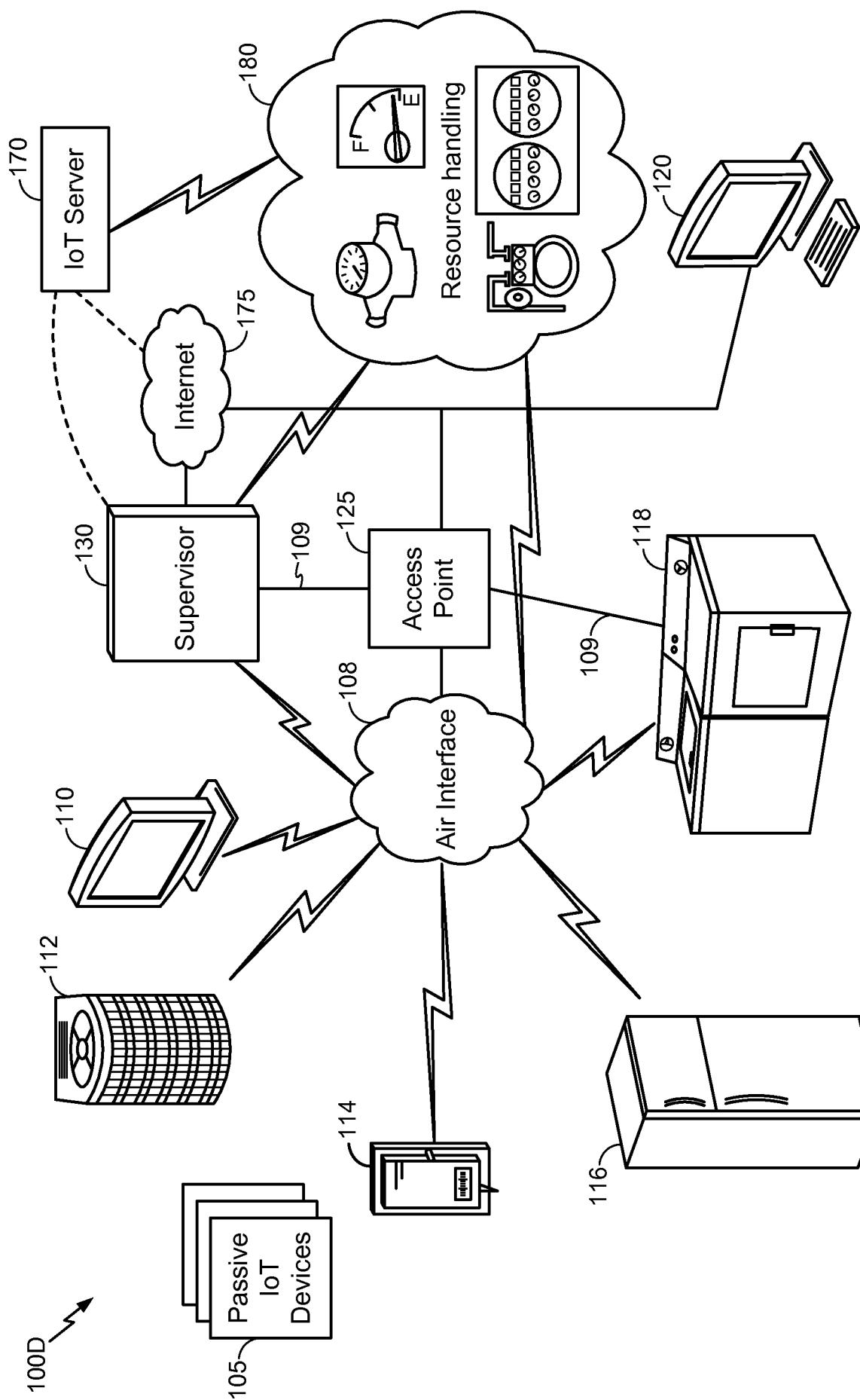


FIG. 1D

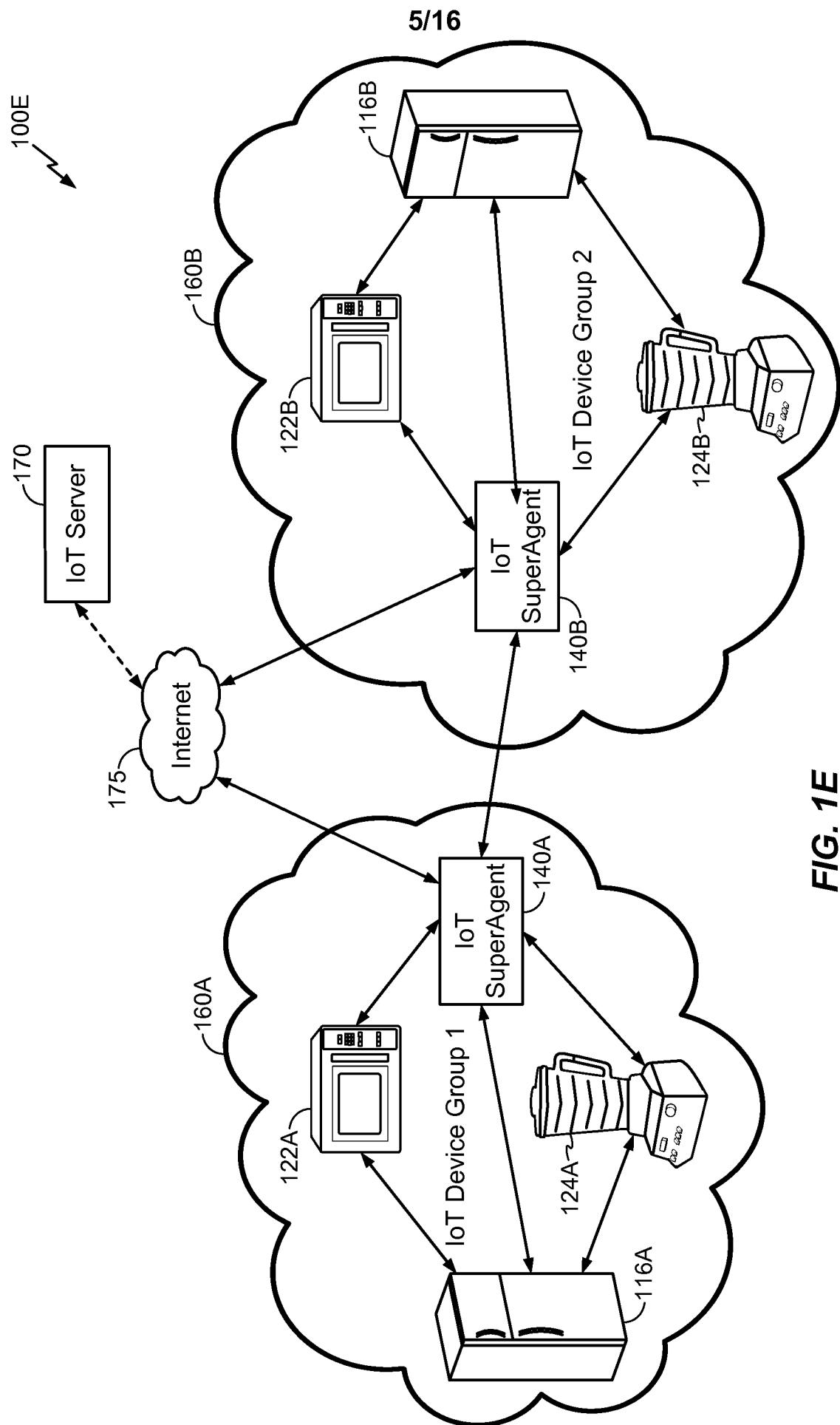


FIG. 1E

6/16

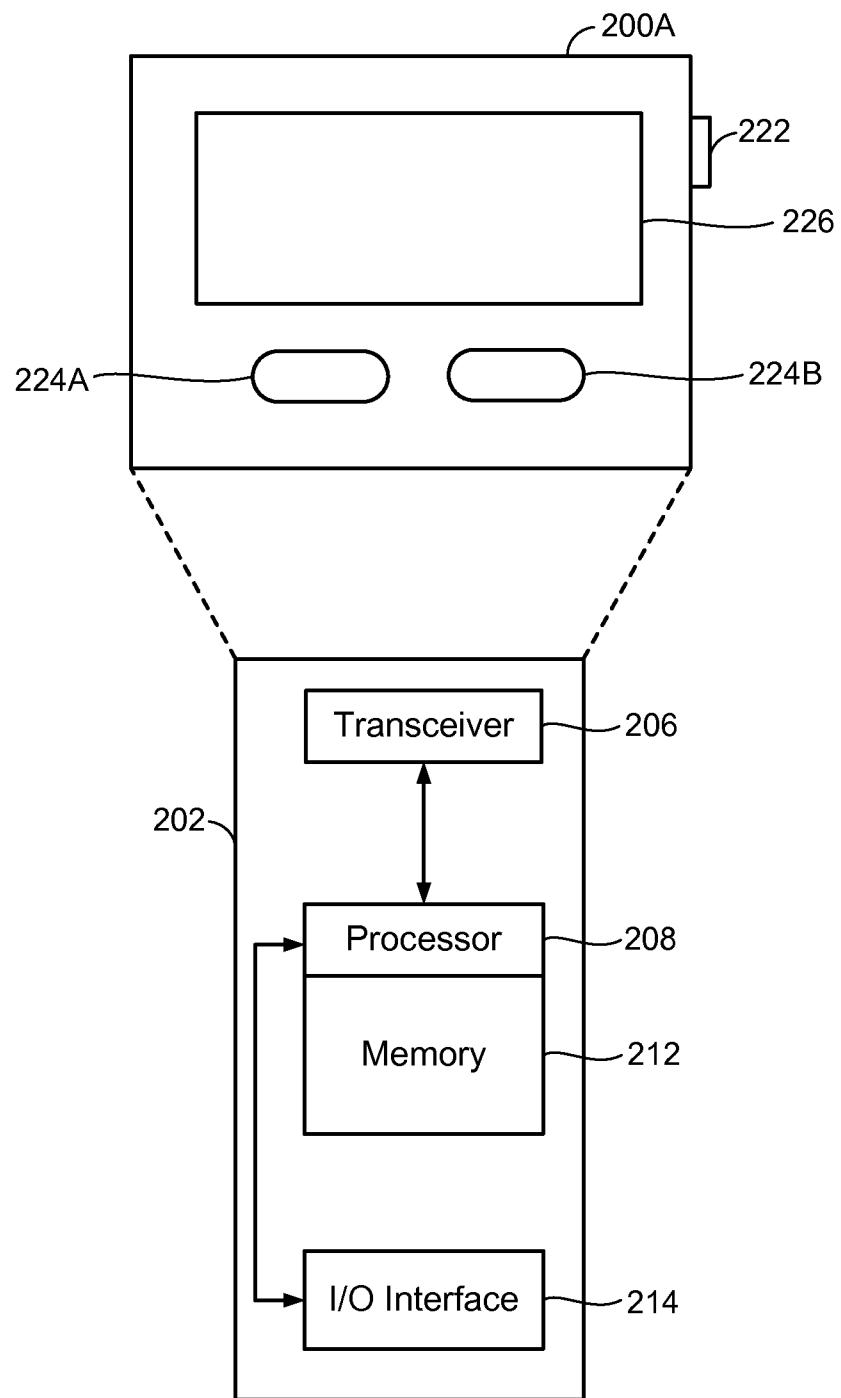
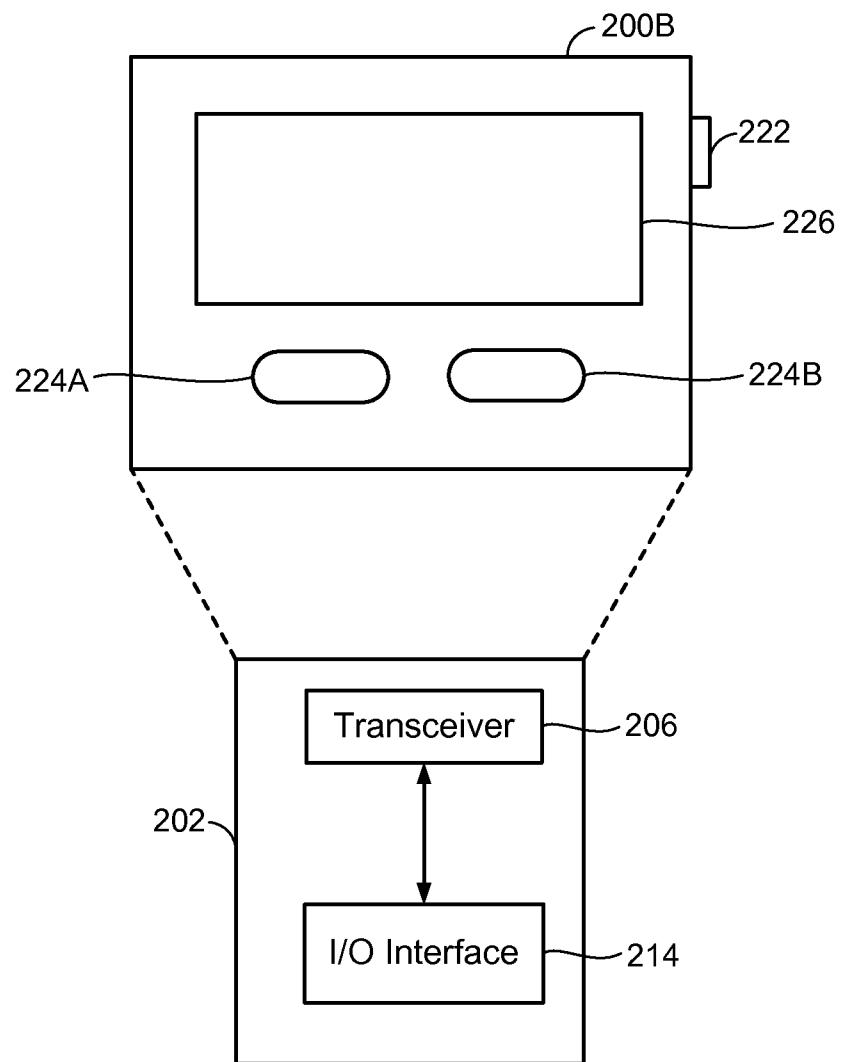
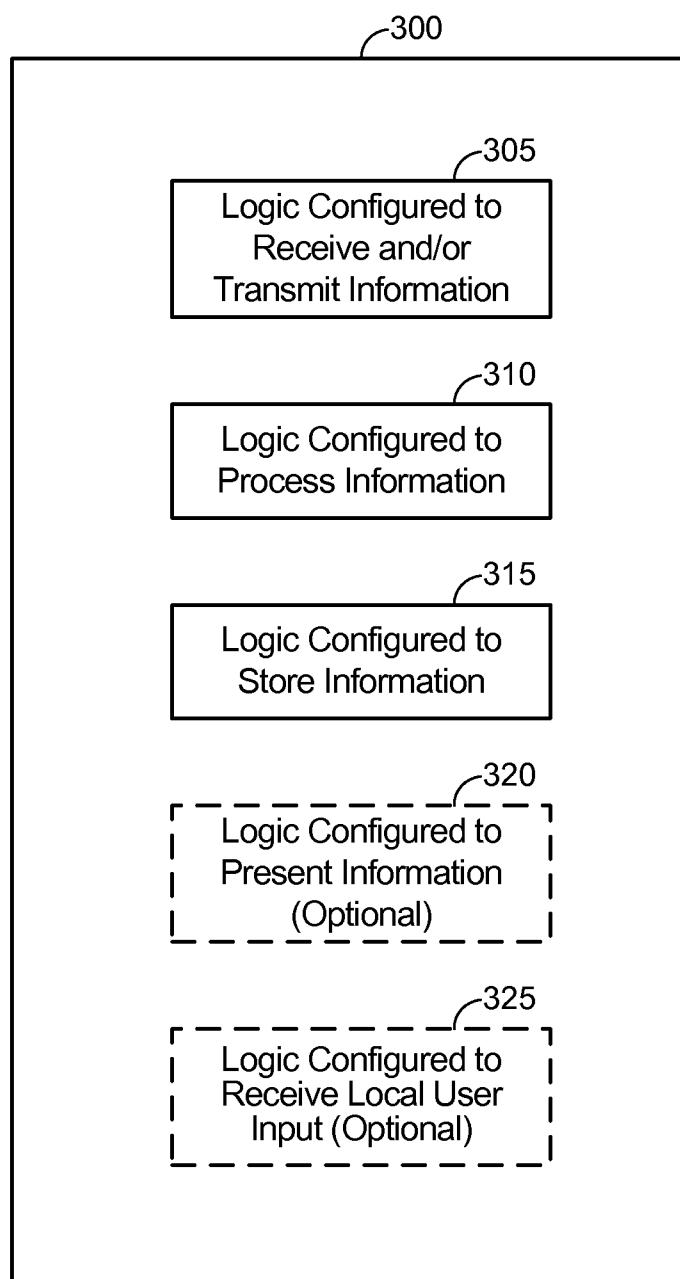


FIG. 2A

7/16

**FIG. 2B**

8/16

**FIG. 3**

9/16

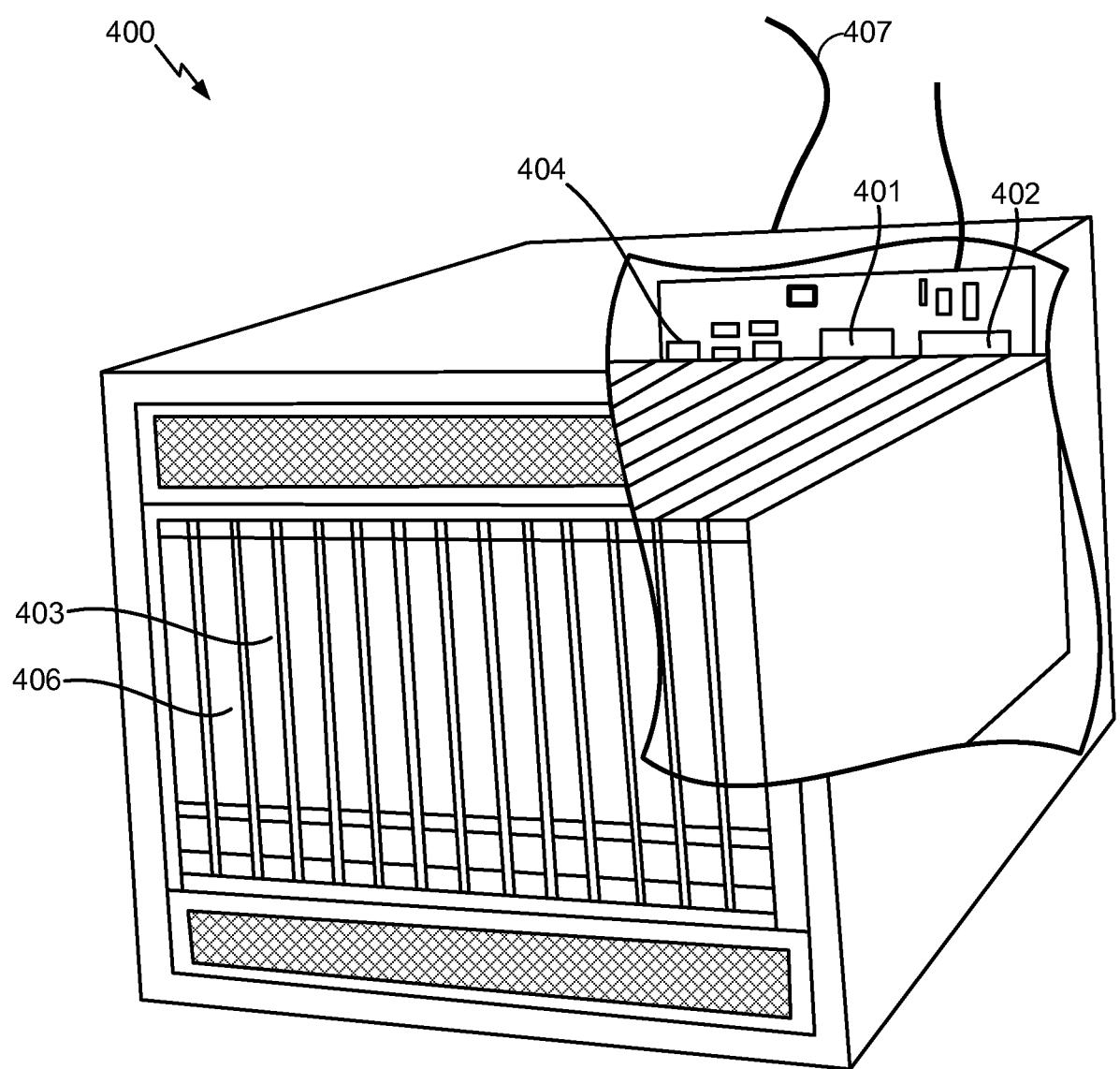


FIG. 4

10/16

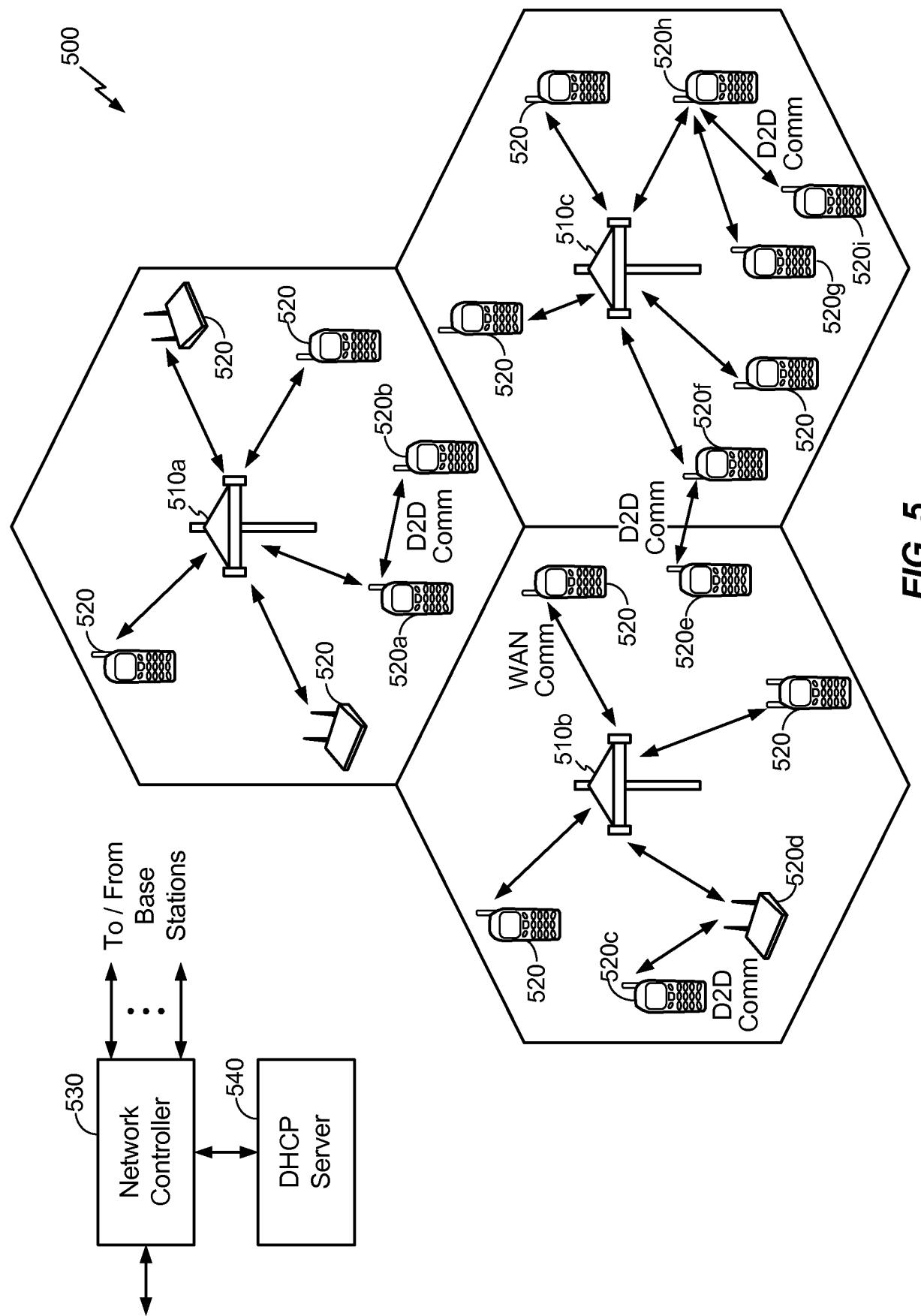
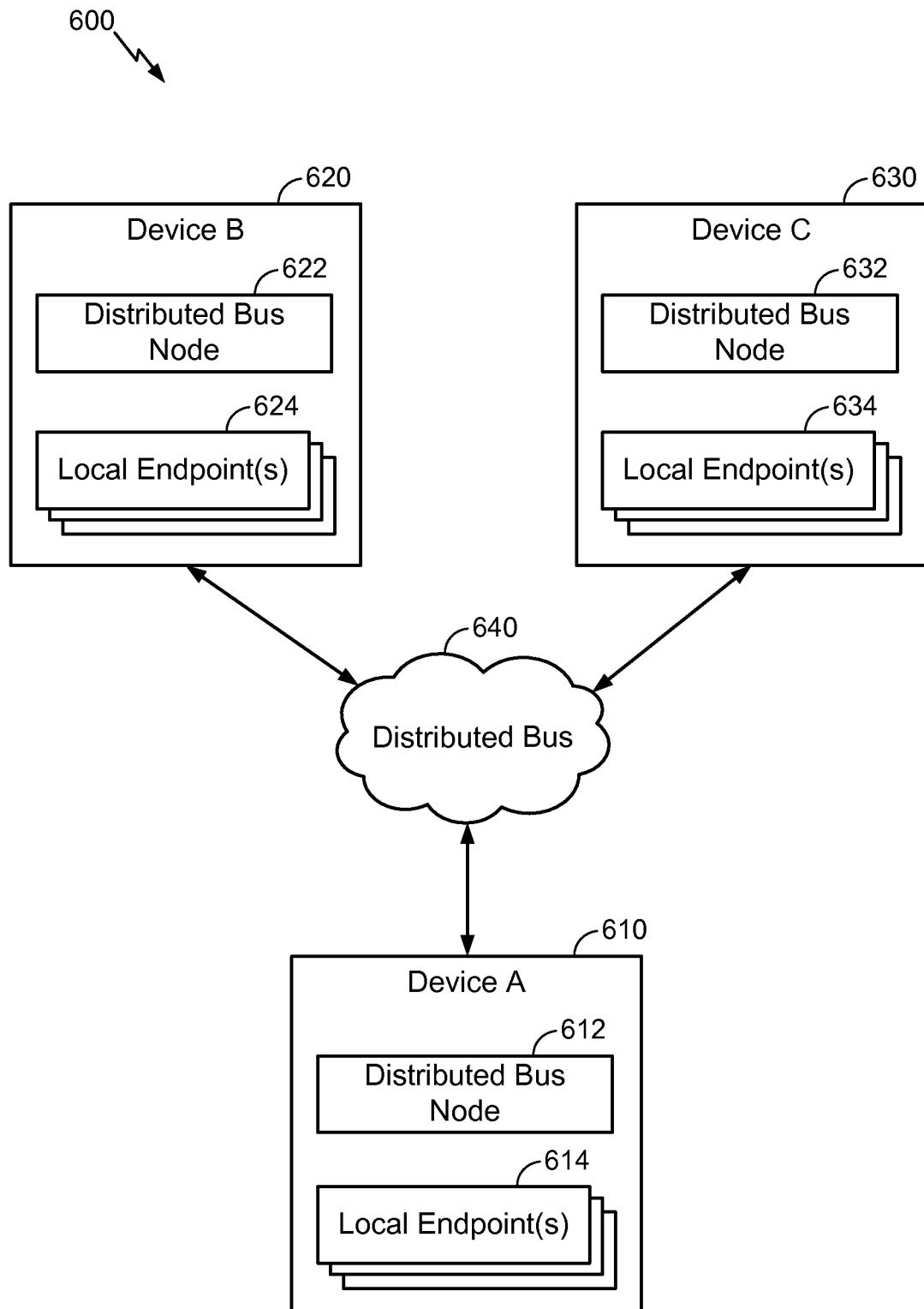
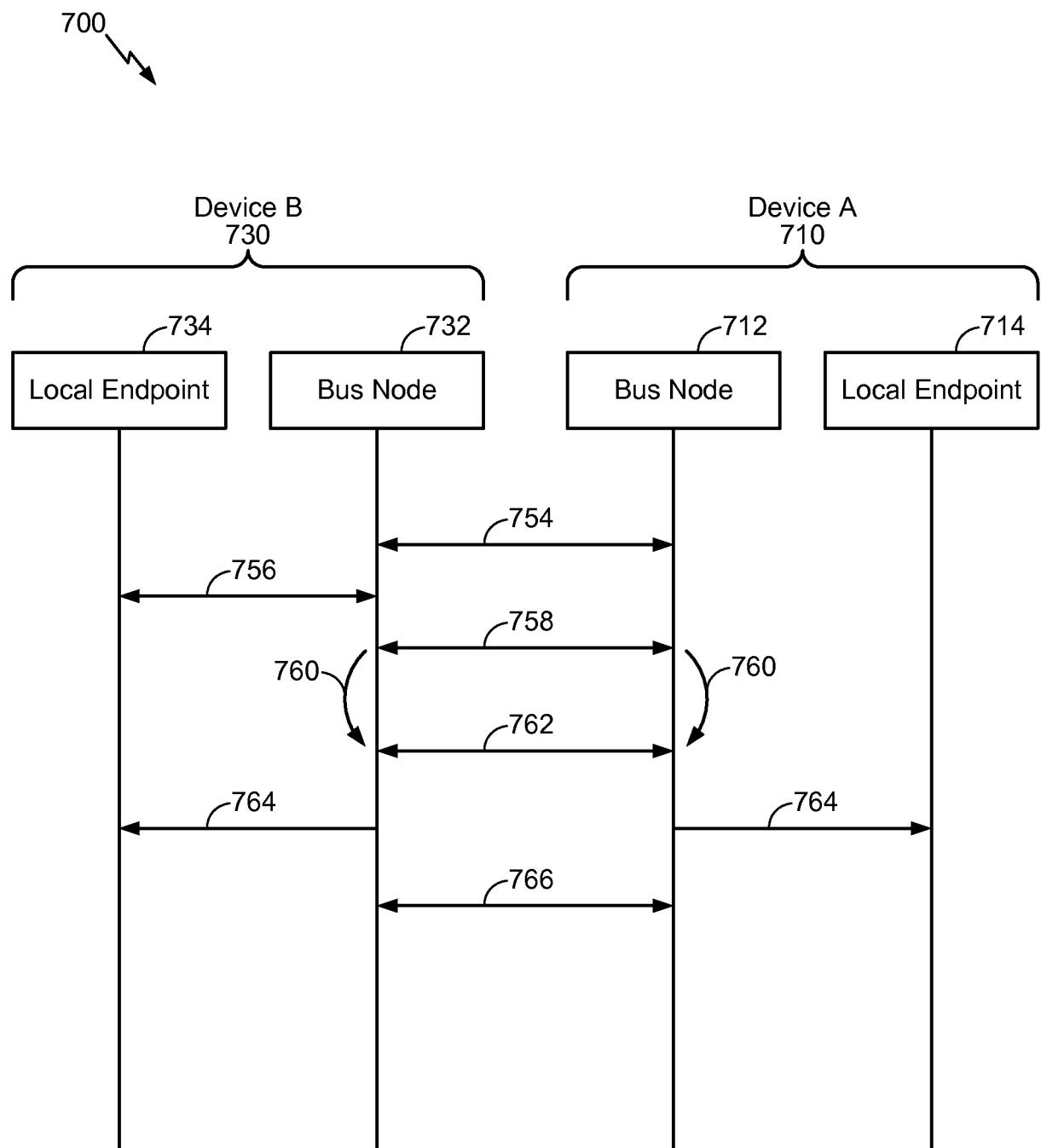


FIG. 5

11/16

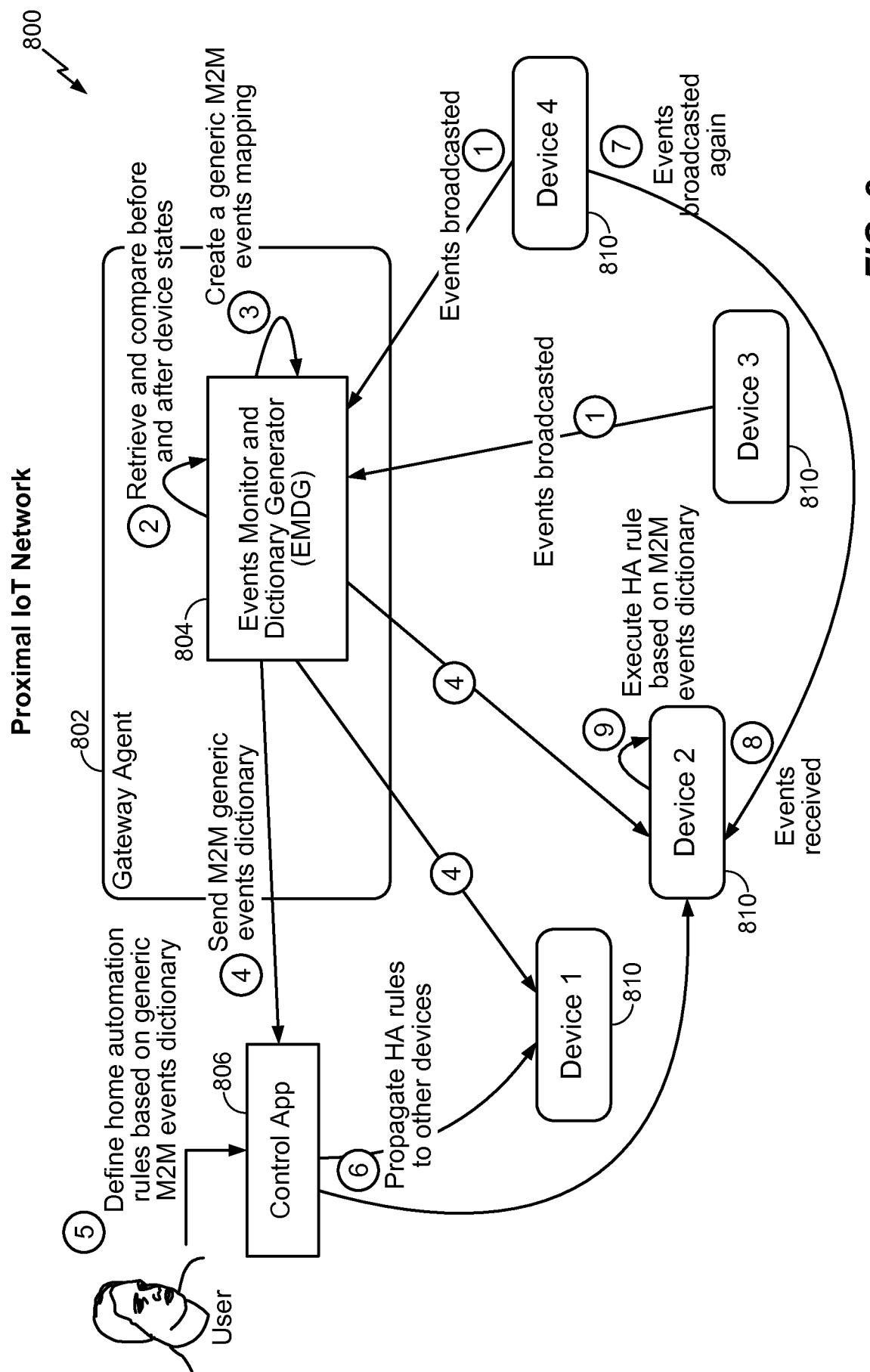
**FIG. 6**

12/16



**FIG. 7**

13/16



14/16

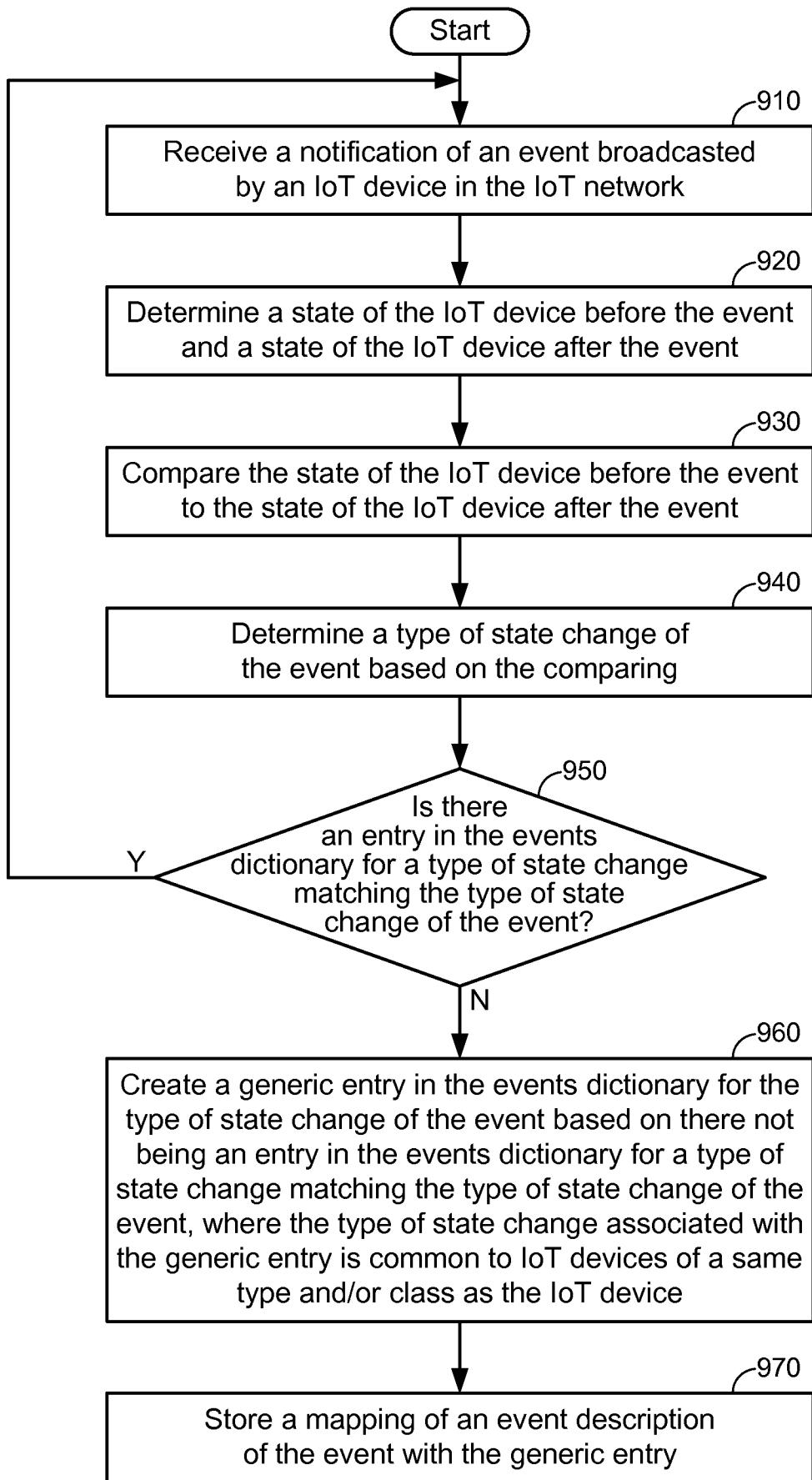


FIG. 9

15/16

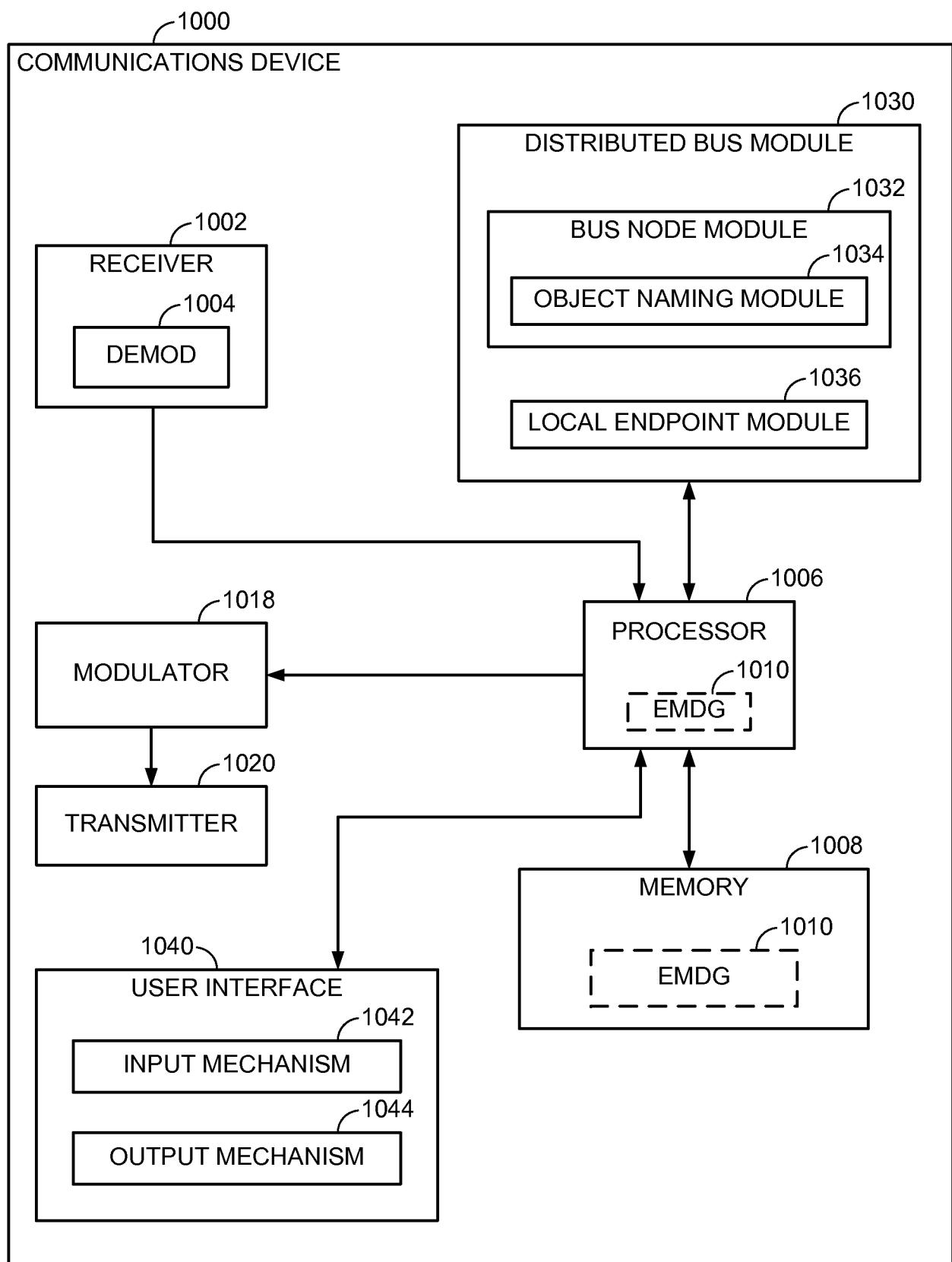


FIG. 10

16/16

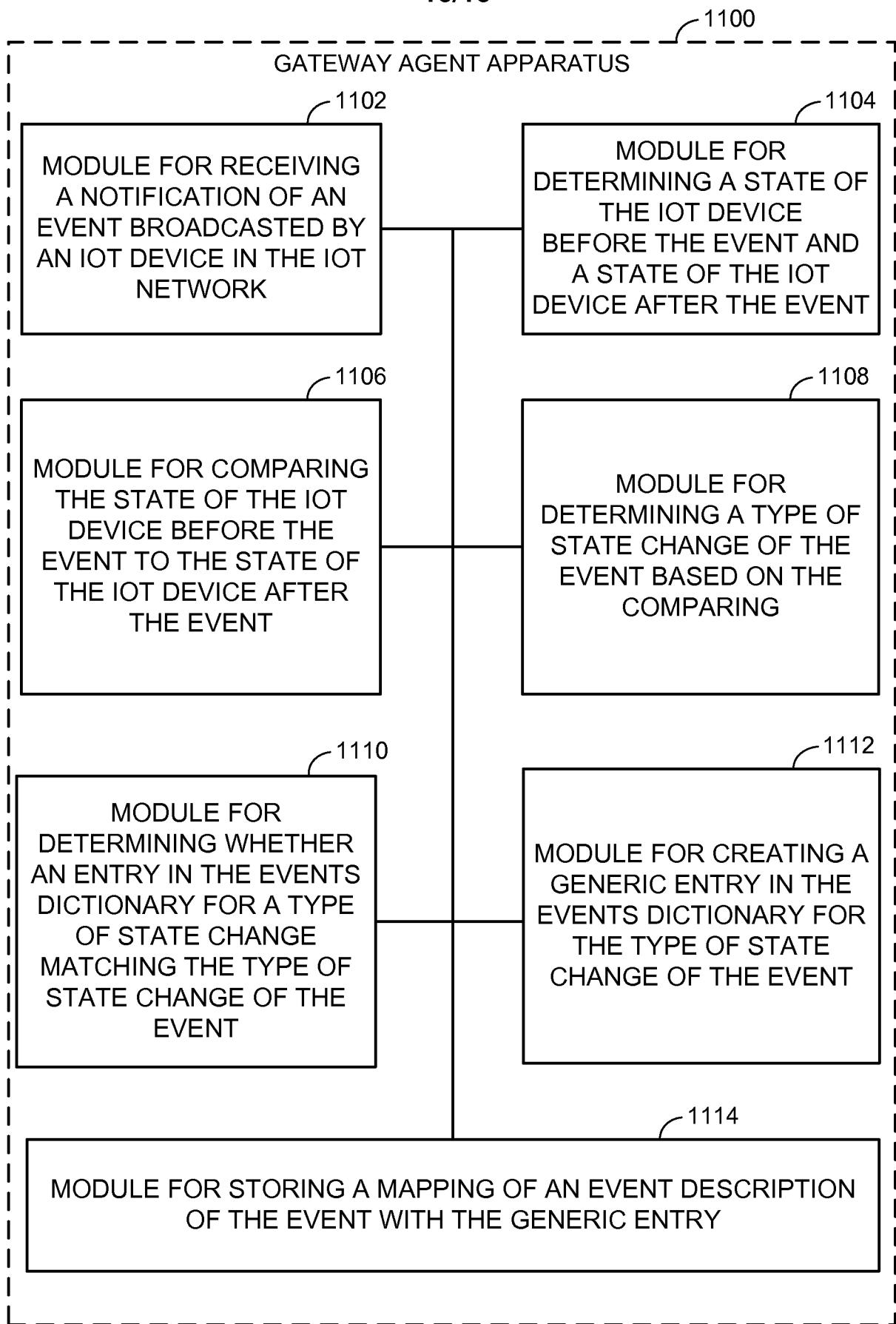


FIG. 11

# INTERNATIONAL SEARCH REPORT

International application No  
PCT/US2015/044340

**A. CLASSIFICATION OF SUBJECT MATTER**  
INV. H04L29/08 H04W4/00  
ADD.

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

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
H04L H04W

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

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

EPO-Internal, WPI Data, INSPEC

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>ZHENG HU ET AL: "Representation and self-configuration of physical entities in extended Smart Grid perimeter", INNOVATIVE SMART GRID TECHNOLOGIES (ISGT EUROPE), 2012 3RD IEEE PES INTERNATIONAL CONFERENCE AND EXHIBITION ON, IEEE, 14 October 2012 (2012-10-14), pages 1-7, XP032332863, DOI: 10.1109/ISGTEUROPE.2012.6465861 ISBN: 978-1-4673-2595-0 abstract page 1 - page 6; figures 1-7</p> <p>-----</p> <p style="text-align: center;">-/-</p>	1-30



Further documents are listed in the continuation of Box C.



See patent family annex.

\* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report

6 November 2015

18/11/2015

Name and mailing address of the ISA/  
European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040,  
Fax: (+31-70) 340-3016

Authorized officer

Florou, Rafaella

**INTERNATIONAL SEARCH REPORT**

International application No PCT/US2015/044340
---

**C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT**

Category <sup>*</sup>	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KONSTANTINOS KOTIS ET AL: "Semantic Interoperability on the Web of Things: The Semantic Smart Gateway Framework", COMPLEX, INTELLIGENT AND SOFTWARE INTENSIVE SYSTEMS (CISIS), 2012 SIXTH INTERNATIONAL CONFERENCE ON, IEEE, 4 July 2012 (2012-07-04), pages 630-635, XP032208337, DOI: 10.1109/CISIS.2012.200 ISBN: 978-1-4673-1233-2 abstract page 1 - page 6 -----	1-30