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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 June 2017 (22.06.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/106258 A1

(51) International Patent Classification:
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/US2016/066513

(22) International Filing Date:
14 December 2016 (14.12.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/967,627 14 December 2015 (14.12.2015) US
14/967,644 14 December 2015 (14.12.2015) US
14/967,680 14 December 2015 (14.12.2015) US

(71) Applicant: **AFERO, INC.** [US/US]; 4970 El Camino Real, Suite 210, Los Altos, California 94022 (US).

(72) Inventors: **BRITT, Joe**; 4970 El Camino Real, Suite 210, Los Altos, California 94022 (US). **ZIMMERMAN, Scott**; 4970 El Camino Real, Suite 210, Los Altos, California 94022 (US). **HOLLAND, Shannon**; 4970 El Camino Real, Suite 210, Los Altos, California 94022 (US). **ZAKARIA, Omar**; 4970 El Camino Real, Suite 210, Los Altos, California 94022 (US).

(74) Agent: **WEBSTER, Thomas C.**; Nicholson De Vos Webster & Elliot, LLP, 217 High Street, Palo Alto, California 94301 (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, DJ, 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, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, 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))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: SYSTEM AND METHOD FOR ESTABLISHING A SECONDARY COMMUNICATION CHANNEL TO CONTROL AN INTERNET OF THINGS (IOT) DEVICE

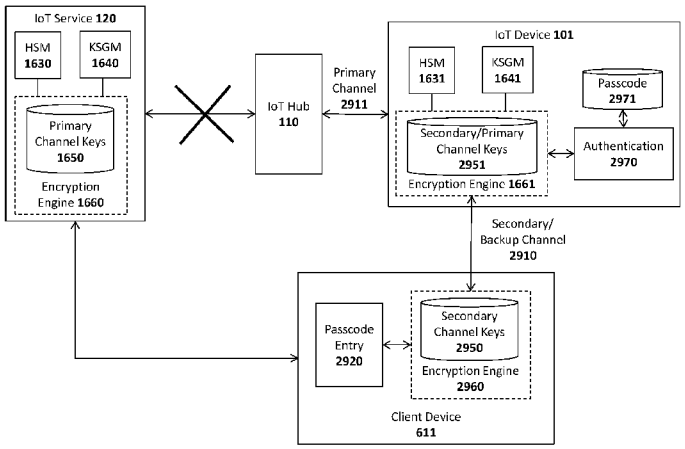

Fig. 29

(57) Abstract: A system and method are described for establishing a secondary communication channel between an IoT device and a client device. For example, one embodiment of a method comprises: establishing a primary secure communication channel between the IoT device and an IoT service using a primary set of keys; performing a secondary key exchange using the primary secure communication channel, the client device and the IoT device each being provided with a secondary set of keys following the secondary key exchange; detecting that the primary secure communication channel is inoperative; and responsively establishing a secondary secure wireless connection between the client device and the IoT device using the secondary set of keys, the client device being provided with access to data and functions made available by the IoT device over the secondary secure wireless connection.

WO 2017/106258 A1

SYSTEM AND METHOD FOR ESTABLISHING A SECONDARY COMMUNICATION CHANNEL TO CONTROL AN INTERNET OF THINGS (IOT) DEVICE

BACKGROUND

Field of the Invention

[0001] This invention relates generally to the field of computer systems. More particularly, the invention relates to a system and method for establishing a secondary communication channel to control and IoT device.

Description of the Related Art

[0002] The "Internet of Things" refers to the interconnection of uniquely-identifiable embedded devices within the Internet infrastructure. Ultimately, IoT is expected to result in new, wide-ranging types of applications in which virtually any type of physical thing may provide information about itself or its surroundings and/or may be controlled remotely via client devices over the Internet.

[0003] The assignee of the present application has developed a system in which IoT devices perform a secure key exchange to establish secure communication channels with an IoT service. Once a secure communication channel is established, the IoT service may securely control and receive data from the IoT device. In some cases, however, it may be desirable to allow a second channel to be established with the IoT device such as, for example, when the IoT service is inaccessible (e.g., when network connectivity is lost).

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] A better understanding of the present invention can be obtained from the following detailed description in conjunction with the following drawings, in which:

[0005] **FIGS. 1A-B** illustrates different embodiments of an IoT system architecture;

[0006] **FIG. 2** illustrates an IoT device in accordance with one embodiment of the invention;

[0007] **FIG. 3** illustrates an IoT hub in accordance with one embodiment of the invention;

[0008] **FIG. 4A-B** illustrate embodiments of the invention for controlling and collecting data from IoT devices, and generating notifications;

[0009] **FIG. 5** illustrates embodiments of the invention for collecting data from IoT devices and generating notifications from an IoT hub and/or IoT service;

[0010] **FIG. 6** illustrates one embodiment of a system in which an intermediary

mobile device collects data from a stationary IoT device and provides the data to an IoT hub;

[0011] **FIG. 7** illustrates intermediary connection logic implemented in one embodiment of the invention;

[0012] **FIG. 8** illustrates a method in accordance with one embodiment of the invention;

[0013] **FIG. 9A** illustrates an embodiment in which program code and data updates are provided to the IoT device;

[0014] **FIG. 9B** illustrates an embodiment of a method in which program code and data updates are provided to the IoT device;

[0015] **FIG. 10** illustrates a high level view of one embodiment of a security architecture;

[0016] **FIG. 11** illustrates one embodiment of an architecture in which a subscriber identity module (SIM) is used to store keys on IoT devices;

[0017] **FIG. 12A** illustrates one embodiment in which IoT devices are registered using barcodes or QR codes;

[0018] **FIG. 12B** illustrates one embodiment in which pairing is performed using barcodes or QR codes;

[0019] **FIG. 13** illustrates one embodiment of a method for programming a SIM using an IoT hub;

[0020] **FIG. 14** illustrates one embodiment of a method for registering an IoT device with an IoT hub and IoT service; and

[0021] **FIG. 15** illustrates one embodiment of a method for encrypting data to be transmitted to an IoT device;

[0022] **FIGS. 16A-B** illustrate different embodiments of the invention for encrypting data between an IoT service and an IoT device;

[0023] **FIG. 17** illustrates embodiments of the invention for performing a secure key exchange, generating a common secret, and using the secret to generate a key stream;

[0024] **FIG. 18** illustrates a packet structure in accordance with one embodiment of the invention;

[0025] **FIG. 19** illustrates techniques employed in one embodiment for writing and reading data to/from an IoT device without formally pairing with the IoT device;

[0026] **FIG. 20** illustrates an exemplary set of command packets employed in one embodiment of the invention;

[0027] **FIG. 21** illustrates an exemplary sequence of transactions using command

packets;

[0028] **FIG. 22** illustrates a method in accordance with one embodiment of the invention; and

[0029] **FIG. 23A-C** illustrates a method for secure pairing in accordance with one embodiment of the invention;

[0030] **FIG. 24** illustrates a system architecture in accordance with one embodiment of the invention;

[0031] **FIG. 25** illustrates a one piece security IoT device in accordance with one embodiment of the invention;

[0032] **FIG. 26** illustrates now the one piece security IoT device may be coupled to a door in accordance with one embodiment of the invention;

[0033] **FIG. 27A-B** illustrates another embodiment of the invention comprising a force-sensing resistor;

[0034] **FIG. 28** illustrates a method in accordance with one embodiment of the invention;

[0035] **FIG. 29** illustrates a system architecture which supports a secondary communication channel; and

[0036] **FIG. 30** illustrates a method for implementing a secondary communication channel.

[0037] **FIG. 31** illustrates one embodiment of the invention for adjusting an advertising interval to identify a data transmission condition;

[0038] **FIG. 32** illustrates a method in accordance with one embodiment of the invention;

[0039] **FIG. 33** illustrates a typical command and response pattern in accordance with one embodiment of the invention;

[0040] **FIG. 34** illustrates one embodiment of the invention for obscuring wireless communication patterns;

[0041] **Fig. 35** illustrates another embodiment for obfuscating communication between an IoT service and an IoT device 101;

[0042] **Fig. 36** illustrates a method in accordance with one embodiment of the invention;

[0043] **Fig. 37** illustrates another method in accordance with one embodiment.

[0044] **FIG. 38** illustrates one embodiment of the invention for adjusting an advertising interval to identify a data transmission condition; and

[0045] **FIG. 39** illustrates a method in accordance with one embodiment of the

invention.

DETAILED DESCRIPTION

[0046] In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the embodiments of the invention described below. It will be apparent, however, to one skilled in the art that the embodiments of the invention may be practiced without some of these specific details. In other instances, well-known structures and devices are shown in block diagram form to avoid obscuring the underlying principles of the embodiments of the invention.

[0047] One embodiment of the invention comprises an Internet of Things (IoT) platform which may be utilized by developers to design and build new IoT devices and applications. In particular, one embodiment includes a base hardware/software platform for IoT devices including a predefined networking protocol stack and an IoT hub through which the IoT devices are coupled to the Internet. In addition, one embodiment includes an IoT service through which the IoT hubs and connected IoT devices may be accessed and managed as described below. In addition, one embodiment of the IoT platform includes an IoT app or Web application (e.g., executed on a client device) to access and configured the IoT service, hub and connected devices. Existing online retailers and other Website operators may leverage the IoT platform described herein to readily provide unique IoT functionality to existing user bases.

[0048] **Figure 1A** illustrates an overview of an architectural platform on which embodiments of the invention may be implemented. In particular, the illustrated embodiment includes a plurality of IoT devices 101-105 communicatively coupled over local communication channels 130 to a central IoT hub 110 which is itself communicatively coupled to an IoT service 120 over the Internet 220. Each of the IoT devices 101-105 may initially be paired to the IoT hub 110 (e.g., using the pairing techniques described below) in order to enable each of the local communication channels 130. In one embodiment, the IoT service 120 includes an end user database 122 for maintaining user account information and data collected from each user's IoT devices. For example, if the IoT devices include sensors (e.g., temperature sensors, accelerometers, heat sensors, motion detectore, etc), the database 122 may be continually updated to store the data collected by the IoT devices 101-105. The data stored in the database 122 may then be made accessible to the end user via the IoT app or browser installed on the user's device 135 (or via a desktop or other client

computer system) and to web clients (e.g., such as websites 130 subscribing to the IoT service 120).

[0049] The IoT devices 101-105 may be equipped with various types of sensors to collect information about themselves and their surroundings and provide the collected information to the IoT service 120, user devices 135 and/or external Websites 130 via the IoT hub 110. Some of the IoT devices 101-105 may perform a specified function in response to control commands sent through the IoT hub 110. Various specific examples of information collected by the IoT devices 101-105 and control commands are provided below. In one embodiment described below, the IoT device 101 is a user input device designed to record user selections and send the user selections to the IoT service 120 and/or Website.

[0050] In one embodiment, the IoT hub 110 includes a cellular radio to establish a connection to the Internet 220 via a cellular service 115 such as a 4G (e.g., Mobile WiMAX, LTE) or 5G cellular data service. Alternatively, or in addition, the IoT hub 110 may include a WiFi radio to establish a WiFi connection through a WiFi access point or router 116 which couples the IoT hub 110 to the Internet (e.g., via an Internet Service Provider providing Internet service to the end user). Of course, it should be noted that the underlying principles of the invention are not limited to any particular type of communication channel or protocol.

[0051] In one embodiment, the IoT devices 101-105 are ultra low-power devices capable of operating for extended periods of time on battery power (e.g., years). To conserve power, the local communication channels 130 may be implemented using a low-power wireless communication technology such as Bluetooth Low Energy (LE). In this embodiment, each of the IoT devices 101-105 and the IoT hub 110 are equipped with Bluetooth LE radios and protocol stacks.

[0052] As mentioned, in one embodiment, the IoT platform includes an IoT app or Web application executed on user devices 135 to allow users to access and configure the connected IoT devices 101-105, IoT hub 110, and/or IoT service 120. In one embodiment, the app or web application may be designed by the operator of a Website 130 to provide IoT functionality to its user base. As illustrated, the Website may maintain a user database 131 containing account records related to each user.

[0053] **Figure 1B** illustrates additional connection options for a plurality of IoT hubs 110-111, 190 In this embodiment a single user may have multiple hubs 110-111 installed onsite at a single user premises 180 (e.g., the user's home or business). This may be done, for example, to extend the wireless range needed to connect all of the IoT

devices 101-105. As indicated, if a user has multiple hubs 110, 111 they may be connected via a local communication channel (e.g., Wifi, Ethernet, Power Line Networking, etc). In one embodiment, each of the hubs 110-111 may establish a direct connection to the IoT service 120 through a cellular 115 or WiFi 116 connection (not explicitly shown in **Figure 1B**). Alternatively, or in addition, one of the IoT hubs such as IoT hub 110 may act as a "master" hub which provides connectivity and/or local services to all of the other IoT hubs on the user premises 180, such as IoT hub 111 (as indicated by the dotted line connecting IoT hub 110 and IoT hub 111). For example, the master IoT hub 110 may be the only IoT hub to establish a direct connection to the IoT service 120. In one embodiment, only the "master" IoT hub 110 is equipped with a cellular communication interface to establish the connection to the IoT service 120. As such, all communication between the IoT service 120 and the other IoT hubs 111 will flow through the master IoT hub 110. In this role, the master IoT hub 110 may be provided with additional program code to perform filtering operations on the data exchanged between the other IoT hubs 111 and IoT service 120 (e.g., servicing some data requests locally when possible).

[0054] Regardless of how the IoT hubs 110-111 are connected, in one embodiment, the IoT service 120 will logically associate the hubs with the user and combine all of the attached IoT devices 101-105 under a single comprehensive user interface, accessible via a user device with the installed app 135 (and/or a browser-based interface).

[0055] In this embodiment, the master IoT hub 110 and one or more slave IoT hubs 111 may connect over a local network which may be a WiFi network 116, an Ethernet network, and/or a using power-line communications (PLC) networking (e.g., where all or portions of the network are run through the user's power lines). In addition, to the IoT hubs 110-111, each of the IoT devices 101-105 may be interconnected with the IoT hubs 110-111 using any type of local network channel such as WiFi, Ethernet, PLC, or Bluetooth LE, to name a few.

[0056] **Figure 1B** also shows an IoT hub 190 installed at a second user premises 181. A virtually unlimited number of such IoT hubs 190 may be installed and configured to collect data from IoT devices 191-192 at user premises around the world. In one embodiment, the two user premises 180-181 may be configured for the same user. For example, one user premises 180 may be the user's primary home and the other user premises 181 may be the user's vacation home. In such a case, the IoT service 120 will logically associate the IoT hubs 110-111, 190 with the user and combine all of the attached IoT devices 101-105, 191-192 under a single comprehensive user interface,

accessible via a user device with the installed app 135 (and/or a browser-based interface).

[0057] As illustrated in **Figure 2**, an exemplary embodiment of an IoT device 101 includes a memory 210 for storing program code and data 201-203 and a low power microcontroller 200 for executing the program code and processing the data. The memory 210 may be a volatile memory such as dynamic random access memory (DRAM) or may be a non-volatile memory such as Flash memory. In one embodiment, a non-volatile memory may be used for persistent storage and a volatile memory may be used for execution of the program code and data at runtime. Moreover, the memory 210 may be integrated within the low power microcontroller 200 or may be coupled to the low power microcontroller 200 via a bus or communication fabric. The underlying principles of the invention are not limited to any particular implementation of the memory 210.

[0058] As illustrated, the program code may include application program code 203 defining an application-specific set of functions to be performed by the IoT device 201 and library code 202 comprising a set of predefined building blocks which may be utilized by the application developer of the IoT device 101. In one embodiment, the library code 202 comprises a set of basic functions required to implement an IoT device such as a communication protocol stack 201 for enabling communication between each IoT device 101 and the IoT hub 110. As mentioned, in one embodiment, the communication protocol stack 201 comprises a Bluetooth LE protocol stack. In this embodiment, Bluetooth LE radio and antenna 207 may be integrated within the low power microcontroller 200. However, the underlying principles of the invention are not limited to any particular communication protocol.

[0059] The particular embodiment shown in **Figure 2** also includes a plurality of input devices or sensors 210 to receive user input and provide the user input to the low power microcontroller, which processes the user input in accordance with the application code 203 and library code 202. In one embodiment, each of the input devices include an LED 209 to provide feedback to the end user.

[0060] In addition, the illustrated embodiment includes a battery 208 for supplying power to the low power microcontroller. In one embodiment, a non-chargeable coin cell battery is used. However, in an alternate embodiment, an integrated rechargeable battery may be used (e.g., rechargeable by connecting the IoT device to an AC power supply (not shown)).

[0061] A speaker 205 is also provided for generating audio. In one embodiment, the low power microcontroller 299 includes audio decoding logic for decoding a compressed audio stream (e.g., such as an MPEG-4/Advanced Audio Coding (AAC) stream) to generate audio on the speaker 205. Alternatively, the low power microcontroller 200 and/or the application code/data 203 may include digitally sampled snippets of audio to provide verbal feedback to the end user as the user enters selections via the input devices 210.

[0062] In one embodiment, one or more other/alternate I/O devices or sensors 250 may be included on the IoT device 101 based on the particular application for which the IoT device 101 is designed. For example, an environmental sensor may be included to measure temperature, pressure, humidity, etc. A security sensor and/or door lock opener may be included if the IoT device is used as a security device. Of course, these examples are provided merely for the purposes of illustration. The underlying principles of the invention are not limited to any particular type of IoT device. In fact, given the highly programmable nature of the low power microcontroller 200 equipped with the library code 202, an application developer may readily develop new application code 203 and new I/O devices 250 to interface with the low power microcontroller for virtually any type of IoT application.

[0063] In one embodiment, the low power microcontroller 200 also includes a secure key store for storing encryption keys for encrypting communications and/or generating signatures. Alternatively, the keys may be secured in a subscriber identify module (SIM).

[0064] A wakeup receiver 207 is included in one embodiment to wake the IoT device from an ultra low power state in which it is consuming virtually no power. In one embodiment, the wakeup receiver 207 is configured to cause the IoT device 101 to exit this low power state in response to a wakeup signal received from a wakeup transmitter 307 configured on the IoT hub 110 as shown in **Figure 3**. In particular, in one embodiment, the transmitter 307 and receiver 207 together form an electrical resonant transformer circuit such as a Tesla coil. In operation, energy is transmitted via radio frequency signals from the transmitter 307 to the receiver 207 when the hub 110 needs to wake the IoT device 101 from a very low power state. Because of the energy transfer, the IoT device 101 may be configured to consume virtually no power when it is in its low power state because it does not need to continually "listen" for a signal from the hub (as is the case with network protocols which allow devices to be awakened via a network signal). Rather, the microcontroller 200 of the IoT device 101 may be

configured to wake up after being effectively powered down by using the energy electrically transmitted from the transmitter 307 to the receiver 207.

[0065] As illustrated in **Figure 3**, the IoT hub 110 also includes a memory 317 for storing program code and data 305 and hardware logic 301 such as a microcontroller for executing the program code and processing the data. A wide area network (WAN) interface 302 and antenna 310 couple the IoT hub 110 to the cellular service 115. Alternatively, as mentioned above, the IoT hub 110 may also include a local network interface (not shown) such as a WiFi interface (and WiFi antenna) or Ethernet interface for establishing a local area network communication channel. In one embodiment, the hardware logic 301 also includes a secure key store for storing encryption keys for encrypting communications and generating/verifying signatures. Alternatively, the keys may be secured in a subscriber identify module (SIM).

[0066] A local communication interface 303 and antenna 311 establishes local communication channels with each of the IoT devices 101-105. As mentioned above, in one embodiment, the local communication interface 303/antenna 311 implements the Bluetooth LE standard. However, the underlying principles of the invention are not limited to any particular protocols for establishing the local communication channels with the IoT devices 101-105. Although illustrated as separate units in **Figure 3**, the WAN interface 302 and/or local communication interface 303 may be embedded within the same chip as the hardware logic 301.

[0067] In one embodiment, the program code and data includes a communication protocol stack 308 which may include separate stacks for communicating over the local communication interface 303 and the WAN interface 302. In addition, device pairing program code and data 306 may be stored in the memory to allow the IoT hub to pair with new IoT devices. In one embodiment, each new IoT device 101-105 is assigned a unique code which is communicated to the IoT hub 110 during the pairing process. For example, the unique code may be embedded in a barcode on the IoT device and may be read by the barcode reader 106 or may be communicated over the local communication channel 130. In an alternate embodiment, the unique ID code is embedded magnetically on the IoT device and the IoT hub has a magnetic sensor such as an radio frequency ID (RFID) or near field communication (NFC) sensor to detect the code when the IoT device 101 is moved within a few inches of the IoT hub 110.

[0068] In one embodiment, once the unique ID has been communicated, the IoT hub 110 may verify the unique ID by querying a local database (not shown), performing a hash to verify that the code is acceptable, and/or communicating with the IoT service

120, user device 135 and/or Website 130 to validate the ID code. Once validated, in one embodiment, the IoT hub 110 pairs the IoT device 101 and stores the pairing data in memory 317 (which, as mentioned, may include non-volatile memory). Once pairing is complete, the IoT hub 110 may connect with the IoT device 101 to perform the various IoT functions described herein.

[0069] In one embodiment, the organization running the IoT service 120 may provide the IoT hub 110 and a basic hardware/software platform to allow developers to easily design new IoT services. In particular, in addition to the IoT hub 110, developers may be provided with a software development kit (SDK) to update the program code and data 305 executed within the hub 110. In addition, for IoT devices 101, the SDK may include an extensive set of library code 202 designed for the base IoT hardware (e.g., the low power microcontroller 200 and other components shown in Figure 2) to facilitate the design of various different types of applications 101. In one embodiment, the SDK includes a graphical design interface in which the developer needs only to specify input and outputs for the IoT device. All of the networking code, including the communication stack 201 that allows the IoT device 101 to connect to the hub 110 and the service 120, is already in place for the developer. In addition, in one embodiment, the SDK also includes a library code base to facilitate the design of apps for mobile devices (e.g., iPhone and Android devices).

[0070] In one embodiment, the IoT hub 110 manages a continuous bi-directional stream of data between the IoT devices 101-105 and the IoT service 120. In circumstances where updates to/from the IoT devices 101-105 are required in real time (e.g., where a user needs to view the current status of security devices or environmental readings), the IoT hub may maintain an open TCP socket to provide regular updates to the user device 135 and/or external Websites 130. The specific networking protocol used to provide updates may be tweaked based on the needs of the underlying application. For example, in some cases, where may not make sense to have a continuous bi-directional stream, a simple request/response protocol may be used to gather information when needed.

[0071] In one embodiment, both the IoT hub 110 and the IoT devices 101-105 are automatically upgradeable over the network. In particular, when a new update is available for the IoT hub 110 it may automatically download and install the update from the IoT service 120. It may first copy the updated code into a local memory, run and verify the update before swapping out the older program code. Similarly, when updates are available for each of the IoT devices 101-105, they may initially be downloaded by

the IoT hub 110 and pushed out to each of the IoT devices 101-105. Each IoT device 101-105 may then apply the update in a similar manner as described above for the IoT hub and report back the results of the update to the IoT hub 110. If the update is successful, then the IoT hub 110 may delete the update from its memory and record the latest version of code installed on each IoT device (e.g., so that it may continue to check for new updates for each IoT device).

[0072] In one embodiment, the IoT hub 110 is powered via A/C power. In particular, the IoT hub 110 may include a power unit 390 with a transformer for transforming A/C voltage supplied via an A/C power cord to a lower DC voltage.

[0073] **Figure 4A** illustrates one embodiment of the invention for performing universal remote control operations using the IoT system. In particular, in this embodiment, a set of IoT devices 101-103 are equipped with infrared (IR) and/or radio frequency (RF) blasters 401-403, respectively, for transmitting remote control codes to control various different types of electronics equipment including air conditioners/heaters 430, lighting systems 431, and audiovisual equipment 432 (to name just a few). In the embodiment shown in **Figure 4A**, the IoT devices 101-103 are also equipped with sensors 404-406, respectively, for detecting the operation of the devices which they control, as described below.

[0074] For example, sensor 404 in IoT device 101 may be a temperature and/or humidity sensor for sensing the current temperature/humidity and responsively controlling the air conditioner/heater 430 based on a current desired temperature. In this embodiment, the air conditioner/heater 430 is one which is designed to be controlled via a remote control device (typically a remote control which itself has a temperature sensor embedded therein). In one embodiment, the user provides the desired temperature to the IoT hub 110 via an app or browser installed on a user device 135. Control logic 412 executed on the IoT hub 110 receives the current temperature/humidity data from the sensor 404 and responsively transmits commands to the IoT device 101 to control the IR/RF blaster 401 in accordance with the desired temperature/humidity. For example, if the temperature is below the desired temperature, then the control logic 412 may transmit a command to the air conditioner/heater via the IR/RF blaster 401 to increase the temperature (e.g., either by turning off the air conditioner or turning on the heater). The command may include the necessary remote control code stored in a database 413 on the IoT hub 110. Alternatively, or in addition, the IoT service 421 may implement control logic 421 to

control the electronics equipment 430-432 based on specified user preferences and stored control codes 422.

[0075] IoT device 102 in the illustrated example is used to control lighting 431. In particular, sensor 405 in IoT device 102 may photosensor or photodetector configured to detect the current brightness of the light being produced by a light fixture 431 (or other lighting apparatus). The user may specify a desired lighting level (including an indication of ON or OFF) to the IoT hub 110 via the user device 135. In response, the control logic 412 will transmit commands to the IR/RF blaster 402 to control the current brightness level of the lights 431 (e.g., increasing the lighting if the current brightness is too low or decreasing the lighting if the current brightness is too high; or simply turning the lights ON or OFF).

[0076] IoT device 103 in the illustrated example is configured to control audiovisual equipment 432 (e.g., a television, A/V receiver, cable/satellite receiver, AppleTV™, etc). Sensor 406 in IoT device 103 may be an audio sensor (e.g., a microphone and associated logic) for detecting a current ambient volume level and/or a photosensor to detect whether a television is on or off based on the light generated by the television (e.g., by measuring the light within a specified spectrum). Alternatively, sensor 406 may include a temperature sensor connected to the audiovisual equipment to detect whether the audio equipment is on or off based on the detected temperature. Once again, in response to user input via the user device 135, the control logic 412 may transmit commands to the audiovisual equipment via the IR blaster 403 of the IoT device 103.

[0077] It should be noted that the foregoing are merely illustrative examples of one embodiment of the invention. The underlying principles of the invention are not limited to any particular type of sensors or equipment to be controlled by IoT devices.

[0078] In an embodiment in which the IoT devices 101-103 are coupled to the IoT hub 110 via a Bluetooth LE connection, the sensor data and commands are sent over the Bluetooth LE channel. However, the underlying principles of the invention are not limited to Bluetooth LE or any other communication standard.

[0079] In one embodiment, the control codes required to control each of the pieces of electronics equipment are stored in a database 413 on the IoT hub 110 and/or a database 422 on the IoT service 120. As illustrated in **Figure 4B**, the control codes may be provided to the IoT hub 110 from a master database of control codes 422 for different pieces of equipment maintained on the IoT service 120. The end user may specify the types of electronic (or other) equipment to be controlled via the app or browser executed on the user device 135 and, in response, a remote control code

learning module 491 on the IoT hub may retrieve the required IR/RF codes from the remote control code database 492 on the IoT service 120 (e.g., identifying each piece of electronic equipment with a unique ID).

[0080] In addition, in one embodiment, the IoT hub 110 is equipped with an IR/RF interface 490 to allow the remote control code learning module 491 to "learn" new remote control codes directly from the original remote control 495 provided with the electronic equipment. For example, if control codes for the original remote control provided with the air conditioner 430 is not included in the remote control database, the user may interact with the IoT hub 110 via the app/browser on the user device 135 to teach the IoT hub 110 the various control codes generated by the original remote control (e.g., increase temperature, decrease temperature, etc). Once the remote control codes are learned they may be stored in the control code database 413 on the IoT hub 110 and/or sent back to the IoT service 120 to be included in the central remote control code database 492 (and subsequently used by other users with the same air conditioner unit 430).

[0081] In one embodiment, each of the IoT devices 101-103 have an extremely small form factor and may be affixed on or near their respective electronics equipment 430-432 using double-sided tape, a small nail, a magnetic attachment, etc. For control of a piece of equipment such as the air conditioner 430, it would be desirable to place the IoT device 101 sufficiently far away so that the sensor 404 can accurately measure the ambient temperature in the home (e.g., placing the IoT device directly on the air conditioner would result in a temperature measurement which would be too low when the air conditioner was running or too high when the heater was running). In contrast, the IoT device 102 used for controlling lighting may be placed on or near the lighting fixture 431 for the sensor 405 to detect the current lighting level.

[0082] In addition to providing general control functions as described, one embodiment of the IoT hub 110 and/or IoT service 120 transmits notifications to the end user related to the current status of each piece of electronics equipment. The notifications, which may be text messages and/or app-specific notifications, may then be displayed on the display of the user's mobile device 135. For example, if the user's air conditioner has been on for an extended period of time but the temperature has not changed, the IoT hub 110 and/or IoT service 120 may send the user a notification that the air conditioner is not functioning properly. If the user is not home (which may be detected via motion sensors or based on the user's current detected location), and the sensors 406 indicate that audiovisual equipment 430 is on or sensors 405 indicate that

the lights are on, then a notification may be sent to the user, asking if the user would like to turn off the audiovisual equipment 432 and/or lights 431. The same type of notification may be sent for any equipment type.

[0083] Once the user receives a notification, he/she may remotely control the electronics equipment 430-432 via the app or browser on the user device 135. In one embodiment, the user device 135 is a touchscreen device and the app or browser displays an image of a remote control with user-selectable buttons for controlling the equipment 430-432. Upon receiving a notification, the user may open the graphical remote control and turn off or adjust the various different pieces of equipment. If connected via the IoT service 120, the user's selections may be forwarded from the IoT service 120 to the IoT hub 110 which will then control the equipment via the control logic 412. Alternatively, the user input may be sent directly to the IoT hub 110 from the user device 135.

[0084] In one embodiment, the user may program the control logic 412 on the IoT hub 110 to perform various automatic control functions with respect to the electronics equipment 430-432. In addition to maintaining a desired temperature, brightness level, and volume level as described above, the control logic 412 may automatically turn off the electronics equipment if certain conditions are detected. For example, if the control logic 412 detects that the user is not home and that the air conditioner is not functioning, it may automatically turn off the air conditioner. Similarly, if the user is not home, and the sensors 406 indicate that audiovisual equipment 430 is on or sensors 405 indicate that the lights are on, then the control logic 412 may automatically transmit commands via the IR/RF blasters 403 and 402, to turn off the audiovisual equipment and lights, respectively.

[0085] **Figure 5** illustrates additional embodiments of IoT devices 104-105 equipped with sensors 503-504 for monitoring electronic equipment 530-531. In particular, the IoT device 104 of this embodiment includes a temperature sensor 503 which may be placed on or near a stove 530 to detect when the stove has been left on. In one embodiment, the IoT device 104 transmits the current temperature measured by the temperature sensor 503 to the IoT hub 110 and/or the IoT service 120. If the stove is detected to be on for more than a threshold time period (e.g., based on the measured temperature), then control logic 512 may transmit a notification to the end user's device 135 informing the user that the stove 530 is on. In addition, in one embodiment, the IoT device 104 may include a control module 501 to turn off the stove, either in response to receiving an instruction from the user or automatically (if the control logic 512 is

programmed to do so by the user). In one embodiment, the control logic 501 comprises a switch to cut off electricity or gas to the stove 530. However, in other embodiments, the control logic 501 may be integrated within the stove itself.

[0086] **Figure 5** also illustrates an IoT device 105 with a motion sensor 504 for detecting the motion of certain types of electronics equipment such as a washer and/or dryer. Another sensor that may be used is an audio sensor (e.g., microphone and logic) for detecting an ambient volume level. As with the other embodiments described above, this embodiment may transmit notifications to the end user if certain specified conditions are met (e.g., if motion is detected for an extended period of time, indicating that the washer/dryer are not turning off). Although not shown in **Figure 5**, IoT device 105 may also be equipped with a control module to turn off the washer/dryer 531 (e.g., by switching off electric/gas), automatically, and/or in response to user input.

[0087] In one embodiment, a first IoT device with control logic and a switch may be configured to turn off all power in the user's home and a second IoT device with control logic and a switch may be configured to turn off all gas in the user's home. IoT devices with sensors may then be positioned on or near electronic or gas-powered equipment in the user's home. If the user is notified that a particular piece of equipment has been left on (e.g., the stove 530), the user may then send a command to turn off all electricity or gas in the home to prevent damage. Alternatively, the control logic 512 in the IoT hub 110 and/or the IoT service 120 may be configured to automatically turn off electricity or gas in such situations.

[0088] In one embodiment, the IoT hub 110 and IoT service 120 communicate at periodic intervals. If the IoT service 120 detects that the connection to the IoT hub 110 has been lost (e.g., by failing to receive a request or response from the IoT hub for a specified duration), it will communicate this information to the end user's device 135 (e.g., by sending a text message or app-specific notification).

APPARATUS AND METHOD FOR COMMUNICATING DATA THROUGH AN INTERMEDIARY DEVICE

[0089] As mentioned above, because the wireless technologies used to interconnect IoT devices such as Bluetooth LE are generally short range technologies, if the hub for an IoT implementation is outside the range of an IoT device, the IoT device will not be able to transmit data to the IoT hub (and vice versa).

[0090] To address this deficiency, one embodiment of the invention provides a mechanism for an IoT device which is outside of the wireless range of the IoT hub to

periodically connect with one or more mobile devices when the mobile devices are within range. Once connected, the IoT device can transmit any data which needs to be provided to the IoT hub to the mobile device which then forwards the data to the IoT hub.

[0091] As illustrated in **Figure 6** one embodiment includes an IoT hub 110, an IoT device 601 which is out of range of the IoT hub 110 and a mobile device 611. The out of range IoT device 601 may include any form of IoT device capable of collecting and communicating data. For example, the IoT device 601 may comprise a data collection device configured within a refrigerator to monitor the food items available in the refrigerator, the users who consume the food items, and the current temperature. Of course, the underlying principles of the invention are not limited to any particular type of IoT device. The techniques described herein may be implemented using any type of IoT device including those used to collect and transmit data for smart meters, stoves, washers, dryers, lighting systems, HVAC systems, and audiovisual equipment, to name just a few.

[0092] Moreover, the mobile device In operation, the IoT device 611 illustrated in **Figure 6** may be any form of mobile device capable of communicating and storing data. For example, in one embodiment, the mobile device 611 is a smartphone with an app installed thereon to facilitate the techniques described herein. In another embodiment, the mobile device 611 comprises a wearable device such as a communication token affixed to a neckless or bracelet, a smartwatch or a fitness device. The wearable token may be particularly useful for elderly users or other users who do not own a smartphone device.

[0093] In operation, the out of range IoT device 601 may periodically or continually check for connectivity with a mobile device 611. Upon establishing a connection (e.g., as the result of the user moving within the vicinity of the refrigerator) any collected data 605 on the IoT device 601 is automatically transmitted to a temporary data repository 615 on the mobile device 611. In one embodiment, the IoT device 601 and mobile device 611 establish a local wireless communication channel using a low power wireless standard such as BTLE. In such a case, the mobile device 611 may initially be paired with the IoT device 601 using known pairing techniques.

[0094] One the data has been transferred to the temporary data repository, the mobile device 611 will transmit the data once communication is established with the IoT hub 110 (e.g., when the user walks within the range of the IoT hub 110). The IoT hub may then store the data in a central data repository 413 and/or send the data over the

Internet to one or more services and/or other user devices. In one embodiment, the mobile device 611 may use a different type of communication channel to provide the data to the IoT hub 110 (potentially a higher power communication channel such as WiFi).

[0095] The out of range IoT device 601, the mobile device 611, and the IoT hub may all be configured with program code and/or logic to implement the techniques described herein. As illustrated in **Figure 7**, for example, the IoT device 601 may be configured with intermediary connection logic and/or application, the mobile device 611 may be configured with an intermediary connection logic/application, and the IoT hub 110 may be configured with an intermediary connection logic/application 721 to perform the operations described herein. The intermediary connection logic/application on each device may be implemented in hardware, software, or any combination thereof. In one embodiment, the intermediary connection logic/application 701 of the IoT device 601 searches and establishes a connection with the intermediary connection logic/application 711 on the mobile device (which may be implemented as a device app) to transfer the data to the temporary data repository 615. The intermediary connection logic/application 701 on the mobile device 611 then forwards the data to the intermediary connection logic/application on the IoT hub, which stores the data in the central data repository 413.

[0096] As illustrated in **Figure 7**, the intermediary connection logic/applications 701, 711, 721, on each device may be configured based on the application at hand. For example, for a refrigerator, the connection logic/application 701 may only need to transmit a few packets on a periodic basis. For other applications (e.g., temperature sensors), the connection logic/application 701 may need to transmit more frequent updates.

[0097] Rather than a mobile device 611, in one embodiment, the IoT device 601 may be configured to establish a wireless connection with one or more intermediary IoT devices, which are located within range of the IoT hub 110. In this embodiment, any IoT devices 601 out of range of the IoT hub may be linked to the hub by forming a "chain" using other IoT devices.

[0098] In addition, while only a single mobile device 611 is illustrated in **Figures 6-7** for simplicity, in one embodiment, multiple such mobile devices of different users may be configured to communicate with the IoT device 601. Moreover, the same techniques may be implemented for multiple other IoT devices, thereby forming an intermediary device data collection system across the entire home.

[0099] Moreover, in one embodiment, the techniques described herein may be used to collect various different types of pertinent data. For example, in one embodiment, each time the mobile device 611 connects with the IoT device 601, the identity of the user may be included with the collected data 605. In this manner, the IoT system may be used to track the behavior of different users within the home. For example, if used within a refrigerator, the collected data 605 may then include the identify of each user who passes by fridge, each user who opens the fridge, and the specific food items consumed by each user. Different types of data may be collected from other types of IoT devices. Using this data the system is able to determine, for example, which user washes clothes, which user watches TV on a given day, the times at which each user goes to sleep and wakes up, etc. All of this crowd-sourced data may then be compiled within the data repository 413 of the IoT hub and/or forwarded to an external service or user.

[00100] Another beneficial application of the techniques described herein is for monitoring elderly users who may need assistance. For this application, the mobile device 611 may be a very small token worn by the elderly user to collect the information in different rooms of the user's home. Each time the user opens the refrigerator, for example, this data will be included with the collected data 605 and transferred to the IoT hub 110 via the token. The IoT hub may then provide the data to one or more external users (e.g., the children or other individuals who care for the elderly user). If data has not been collected for a specified period of time (e.g., 12 hours), then this means that the elderly user has not been moving around the home and/or has not been opening the refrigerator. The IoT hub 110 or an external service connected to the IoT hub may then transmit an alert notification to these other individuals, informing them that they should check on the elderly user. In addition, the collected data 605 may include other pertinent information such as the food being consumed by the user and whether a trip to the grocery store is needed, whether and how frequently the elderly user is watching TV, the frequency with which the elderly user washes clothes, etc.

[00101] In another implementation, the if there is a problem with an electronic device such as a washer, refrigerator, HVAC system, etc, the collected data may include an indication of a part that needs to be replaced. In such a case, a notification may be sent to a technician with a request to fix the problem. The technician may then arrive at the home with the needed replacement part.

[00102] A method in accordance with one embodiment of the invention is illustrated in **Figure 8**. The method may be implemented within the context of the architectures described above, but is not limited to any particular architecture.

[00103] At 801, an IoT device which is out of range of the IoT hub periodically collects data (e.g., opening of the refrigerator door, food items used, etc). At 802 the IoT device periodically or continually checks for connectivity with a mobile device (e.g., using standard local wireless techniques for establishing a connection such as those specified by the BTLE standard). If the connection to the mobile device is established, determined at 802, then at 803, the collected data is transferred to the mobile device at 803. At 804, the mobile device transfers the data to the IoT hub, an external service and/or a user. As mentioned, the mobile device may transmit the data immediately if it is already connected (e.g., via a WiFi link).

[00104] In addition to collecting data from IoT devices, in one embodiment, the techniques described herein may be used to update or otherwise provide data to IoT devices. One example is shown in **Figure 9A**, which shows an IoT hub 110 with program code updates 901 that need to be installed on an IoT device 601 (or a group of such IoT devices). The program code updates may include system updates, patches, configuration data and any other data needed for the IoT device to operate as desired by the user. In one embodiment, the user may specify configuration options for the IoT device 601 via a mobile device or computer which are then stored on the IoT hub 110 and provided to the IoT device using the techniques described herein. Specifically, in one embodiment, the intermediary connection logic/application 721 on the IoT hub 110 communicates with the intermediary connection logic/application 711 on the mobile device 611 to store the program code updates within a temporary storage 615. When the mobile device 611 enters the range of the IoT device 601, the intermediary connection logic/application 711 on the mobile device 611 connects with the intermediary/connection logic/application 701 on the IoT device 601 to provide the program code updates to the device. In one embodiment, the IoT device 601 may then enter into an automated update process to install the new program code updates and/or data.

[00105] A method for updating an IoT device is shown in **Figure 9B**. The method may be implemented within the context of the system architectures described above, but is not limited to any particular system architectures.

[00106] At 900 new program code or data updates are made available on the IoT hub and/or an external service (e.g., coupled to the mobile device over the Internet). At 901,

the mobile device receives and stores the program code or data updates on behalf of the IoT device. The IoT device and/or mobile device periodically check to determine whether a connection has been established at 902. If a connection is established, determined at 903, then at 904 the updates are transferred to the IoT device and installed.

EMBODIMENTS FOR IMPROVED SECURITY

[00107] In one embodiment, the low power microcontroller 200 of each IoT device 101 and the low power logic/microcontroller 301 of the IoT hub 110 include a secure key store for storing encryption keys used by the embodiments described below (see, e.g., **Figures 10-15** and associated text). Alternatively, the keys may be secured in a subscriber identify module (SIM) as discussed below.

[00108] **Figure 10** illustrates a high level architecture which uses public key infrastructure (PKI) techniques and/or symmetric key exchange/encryption techniques to encrypt communications between the IoT Service 120, the IoT hub 110 and the IoT devices 101-102.

[00109] Embodiments which use public/private key pairs will first be described, followed by embodiments which use symmetric key exchange/encryption techniques. In particular, in an embodiment which uses PKI, a unique public/private key pair is associated with each IoT device 101-102, each IoT hub 110 and the IoT service 120. In one embodiment, when a new IoT hub 110 is set up, its public key is provided to the IoT service 120 and when a new IoT device 101 is set up, it's public key is provided to both the IoT hub 110 and the IoT service 120. Various techniques for securely exchanging the public keys between devices are described below. In one embodiment, all public keys are signed by a master key known to all of the receiving devices (i.e., a form of certificate) so that any receiving device can verify the validity of the public keys by validating the signatures. Thus, these certificates would be exchanged rather than merely exchanging the raw public keys.

[00110] As illustrated, in one embodiment, each IoT device 101, 102 includes a secure key storage 1001, 1003, respectively, for security storing each device's private key. Security logic 1002, 1304 then utilizes the securely stored private keys to perform the encryption/decryption operations described herein. Similarly, the IoT hub 110 includes a secure storage 1011 for storing the IoT hub private key and the public keys of the IoT devices 101-102 and the IoT service 120; as well as security logic 1012 for using the keys to perform encryption/decryption operations. Finally, the IoT service 120 may include a secure storage 1021 for security storing its own private key, the public

keys of various IoT devices and IoT hubs, and a security logic 1013 for using the keys to encrypt/decrypt communication with IoT hubs and devices. In one embodiment, when the IoT hub 110 receives a public key certificate from an IoT device it can verify it (e.g., by validating the signature using the master key as described above), and then extract the public key from within it and store that public key in it's secure key store 1011.

[00111] By way of example, in one embodiment, when the IoT service 120 needs to transmit a command or data to an IoT device 101 (e.g., a command to unlock a door, a request to read a sensor, data to be processed/displayed by the IoT device, etc) the security logic 1013 encrypts the data/command using the public key of the IoT device 101 to generate an encrypted IoT device packet. In one embodiment, it then encrypts the IoT device packet using the public key of the IoT hub 110 to generate an IoT hub packet and transmits the IoT hub packet to the IoT hub 110. In one embodiment, the service 120 signs the encrypted message with it's private key or the master key mentioned above so that the device 101 can verify it is receiving an unaltered message from a trusted source. The device 101 may then validate the signature using the public key corresponding to the private key and/or the master key. As mentioned above, symmetric key exchange/encryption techniques may be used instead of public/private key encryption. In these embodiments, rather than privately storing one key and providing a corresponding public key to other devices, the devices may each be provided with a copy of the same symmetric key to be used for encryption and to validate signatures. One example of a symmetric key algorithm is the Advanced Encryption Standard (AES), although the underlying principles of the invention are not limited to any type of specific symmetric keys.

[00112] Using a symmetric key implementation, each device 101 enters into a secure key exchange protocol to exchange a symmetric key with the IoT hub 110. A secure key provisioning protocol such as the Dynamic Symmetric Key Provisioning Protocol (DSKPP) may be used to exchange the keys over a secure communication channel (see, e.g., Request for Comments (RFC) 6063). However, the underlying principles of the invention are not limited to any particular key provisioning protocol.

[00113] Once the symmetric keys have been exchanged, they may be used by each device 101 and the IoT hub 110 to encrypt communications. Similarly, the IoT hub 110 and IoT service 120 may perform a secure symmetric key exchange and then use the exchanged symmetric keys to encrypt communications. In one embodiment a new symmetric key is exchanged periodically between the devices 101 and the hub 110 and

between the hub 110 and the IoT service 120. In one embodiment, a new symmetric key is exchanged with each new communication session between the devices 101, the hub 110, and the service 120 (e.g., a new key is generated and securely exchanged for each communication session). In one embodiment, if the security module 1012 in the IoT hub is trusted, the service 120 could negotiate a session key with the hub security module 1312 and then the security module 1012 would negotiate a session key with each device 120. Messages from the service 120 would then be decrypted and verified in the hub security module 1012 before being re-encrypted for transmission to the device 101.

[00114] In one embodiment, to prevent a compromise on the hub security module 1012 a one-time (permanent) installation key may be negotiated between the device 101 and service 120 at installation time. When sending a message to a device 101 the service 120 could first encrypt/MAC with this device installation key, then encrypt/MAC that with the hub's session key. The hub 110 would then verify and extract the encrypted device blob and send that to the device.

[00115] In one embodiment of the invention, a counter mechanism is implemented to prevent replay attacks. For example, each successive communication from the device 101 to the hub 110 (or vice versa) may be assigned a continually increasing counter value. Both the hub 110 and device 101 will track this value and verify that the value is correct in each successive communication between the devices. The same techniques may be implemented between the hub 110 and the service 120. Using a counter in this manner would make it more difficult to spoof the communication between each of the devices (because the counter value would be incorrect). However, even without this a shared installation key between the service and device would prevent network (hub) wide attacks to all devices.

[00116] In one embodiment, when using public/private key encryption, the IoT hub 110 uses its private key to decrypt the IoT hub packet and generate the encrypted IoT device packet, which it transmits to the associated IoT device 101. The IoT device 101 then uses its private key to decrypt the IoT device packet to generate the command/data originated from the IoT service 120. It may then process the data and/or execute the command. Using symmetric encryption, each device would encrypt and decrypt with the shared symmetric key. If either case, each transmitting device may also sign the message with it's private key so that the receiving device can verify it's authenticity.

[00117] A different set of keys may be used to encrypt communication from the IoT device 101 to the IoT hub 110 and to the IoT service 120. For example, using a public/private key arrangement, in one embodiment, the security logic 1002 on the IoT device 101 uses the public key of the IoT hub 110 to encrypt data packets sent to the IoT hub 110. The security logic 1012 on the IoT hub 110 may then decrypt the data packets using the IoT hub's private key. Similarly, the security logic 1002 on the IoT device 101 and/or the security logic 1012 on the IoT hub 110 may encrypt data packets sent to the IoT service 120 using the public key of the IoT service 120 (which may then be decrypted by the security logic 1013 on the IoT service 120 using the service's private key). Using symmetric keys, the device 101 and hub 110 may share a symmetric key while the hub and service 120 may share a different symmetric key.

[00118] While certain specific details are set forth above in the description above, it should be noted that the underlying principles of the invention may be implemented using various different encryption techniques. For example, while some embodiments discussed above use asymmetric public/private key pairs, an alternate embodiment may use symmetric keys securely exchanged between the various IoT devices 101-102, IoT hubs 110, and the IoT service 120. Moreover, in some embodiments, the data/command itself is not encrypted, but a key is used to generate a signature over the data/command (or other data structure). The recipient may then use its key to validate the signature.

[00119] As illustrated in **Figure 11**, in one embodiment, the secure key storage on each IoT device 101 is implemented using a programmable subscriber identity module (SIM) 1101. In this embodiment, the IoT device 101 may initially be provided to the end user with an un-programmed SIM card 1101 seated within a SIM interface 1100 on the IoT device 101. In order to program the SIM with a set of one or more encryption keys, the user takes the programmable SIM card 1101 out of the SIM interface 500 and inserts it into a SIM programming interface 1102 on the IoT hub 110. Programming logic 1125 on the IoT hub then securely programs the SIM card 1101 to register/pair the IoT device 101 with the IoT hub 110 and IoT service 120. In one embodiment, a public/private key pair may be randomly generated by the programming logic 1125 and the public key of the pair may then be stored in the IoT hub's secure storage device 411 while the private key may be stored within the programmable SIM 1101. In addition, the programming logic 525 may store the public keys of the IoT hub 110, the IoT service 120, and/or any other IoT devices 101 on the SIM card 1401 (to be used by the security logic 1302 on the IoT device 101 to encrypt outgoing data). Once the SIM 1101 is

programmed, the new IoT device 101 may be provisioned with the IoT Service 120 using the SIM as a secure identifier (e.g., using existing techniques for registering a device using a SIM). Following provisioning, both the IoT hub 110 and the IoT service 120 will securely store a copy of the IoT device's public key to be used when encrypting communication with the IoT device 101.

[00120] The techniques described above with respect to **Figure 11** provide enormous flexibility when providing new IoT devices to end users. Rather than requiring a user to directly register each SIM with a particular service provider upon sale/purchase (as is currently done), the SIM may be programmed directly by the end user via the IoT hub 110 and the results of the programming may be securely communicated to the IoT service 120. Consequently, new IoT devices 101 may be sold to end users from online or local retailers and later securely provisioned with the IoT service 120.

[00121] While the registration and encryption techniques are described above within the specific context of a SIM (Subscriber Identity Module), the underlying principles of the invention are not limited to a "SIM" device. Rather, the underlying principles of the invention may be implemented using any type of device having secure storage for storing a set of encryption keys. Moreover, while the embodiments above include a removable SIM device, in one embodiment, the SIM device is not removable but the IoT device itself may be inserted within the programming interface 1102 of the IoT hub 110.

[00122] In one embodiment, rather than requiring the user to program the SIM (or other device), the SIM is pre-programmed into the IoT device 101, prior to distribution to the end user. In this embodiment, when the user sets up the IoT device 101, various techniques described herein may be used to securely exchange encryption keys between the IoT hub 110/IoT service 120 and the new IoT device 101.

[00123] For example, as illustrated in **Figure 12A** each IoT device 101 or SIM 401 may be packaged with a barcode or QR code 1501 uniquely identifying the IoT device 101 and/or SIM 1001. In one embodiment, the barcode or QR code 1201 comprises an encoded representation of the public key for the IoT device 101 or SIM 1001. Alternatively, the barcode or QR code 1201 may be used by the IoT hub 110 and/or IoT service 120 to identify or generate the public key (e.g., used as a pointer to the public key which is already stored in secure storage). The barcode or QR code 601 may be printed on a separate card (as shown in **Figure 12A**) or may be printed directly on the IoT device itself. Regardless of where the barcode is printed, in one embodiment, the IoT hub 110 is equipped with a barcode reader 206 for reading the barcode and providing the resulting data to the security logic 1012 on the IoT hub 110 and/or the

security logic 1013 on the IoT service 120. The security logic 1012 on the IoT hub 110 may then store the public key for the IoT device within its secure key storage 1011 and the security logic 1013 on the IoT service 120 may store the public key within its secure storage 1021 (to be used for subsequent encrypted communication).

[00124] In one embodiment, the data contained in the barcode or QR code 1201 may also be captured via a user device 135 (e.g., such as an iPhone or Android device) with an installed IoT app or browser-based applet designed by the IoT service provider. Once captured, the barcode data may be securely communicated to the IoT service 120 over a secure connection (e.g., such as a secure sockets layer (SSL) connection). The barcode data may also be provided from the client device 135 to the IoT hub 110 over a secure local connection (e.g., over a local WiFi or Bluetooth LE connection).

[00125] The security logic 1002 on the IoT device 101 and the security logic 1012 on the IoT hub 110 may be implemented using hardware, software, firmware or any combination thereof. For example, in one embodiment, the security logic 1002, 1012 is implemented within the chips used for establishing the local communication channel 130 between the IoT device 101 and the IoT hub 110 (e.g., the Bluetooth LE chip if the local channel 130 is Bluetooth LE). Regardless of the specific location of the security logic 1002, 1012, in one embodiment, the security logic 1002, 1012 is designed to establish a secure execution environment for executing certain types of program code. This may be implemented, for example, by using TrustZone technology (available on some ARM processors) and/or Trusted Execution Technology (designed by Intel). Of course, the underlying principles of the invention are not limited to any particular type of secure execution technology.

[00126] In one embodiment, the barcode or QR code 1501 may be used to pair each IoT device 101 with the IoT hub 110. For example, rather than using the standard wireless pairing process currently used to pair Bluetooth LE devices, a pairing code embedded within the barcode or QR code 1501 may be provided to the IoT hub 110 to pair the IoT hub with the corresponding IoT device.

[00127] **Figure 12B** illustrates one embodiment in which the barcode reader 206 on the IoT hub 110 captures the barcode/QR code 1201 associated with the IoT device 101. As mentioned, the barcode/QR code 1201 may be printed directly on the IoT device 101 or may be printed on a separate card provided with the IoT device 101. In either case, the barcode reader 206 reads the pairing code from the barcode/QR code 1201 and provides the pairing code to the local communication module 1280. In one embodiment, the local communication module 1280 is a Bluetooth LE chip and

associated software, although the underlying principles of the invention are not limited to any particular protocol standard. Once the pairing code is received, it is stored in a secure storage containing pairing data 1285 and the IoT device 101 and IoT hub 110 are automatically paired. Each time the IoT hub is paired with a new IoT device in this manner, the pairing data for that pairing is stored within the secure storage 685. In one embodiment, once the local communication module 1280 of the IoT hub 110 receives the pairing code, it may use the code as a key to encrypt communications over the local wireless channel with the IoT device 101.

[00128] Similarly, on the IoT device 101 side, the local communication module 1590 stores pairing data within a local secure storage device 1595 indicating the pairing with the IoT hub. The pairing data 1295 may include the pre-programmed pairing code identified in the barcode/QR code 1201. The pairing data 1295 may also include pairing data received from the local communication module 1280 on the IoT hub 110 required for establishing a secure local communication channel (e.g., an additional key to encrypt communication with the IoT hub 110).

[00129] Thus, the barcode/QR code 1201 may be used to perform local pairing in a far more secure manner than current wireless pairing protocols because the pairing code is not transmitted over the air. In addition, in one embodiment, the same barcode/QR code 1201 used for pairing may be used to identify encryption keys to build a secure connection from the IoT device 101 to the IoT hub 110 and from the IoT hub 110 to the IoT service 120.

[00130] A method for programming a SIM card in accordance with one embodiment of the invention is illustrated in **Figure 13**. The method may be implemented within the system architecture described above, but is not limited to any particular system architecture.

[00131] At 1301, a user receives a new IoT device with a blank SIM card and, at 1602, the user inserts the blank SIM card into an IoT hub. At 1303, the user programs the blank SIM card with a set of one or more encryption keys. For example, as mentioned above, in one embodiment, the IoT hub may randomly generate a public/private key pair and store the private key on the SIM card and the public key in its local secure storage. In addition, at 1304, at least the public key is transmitted to the IoT service so that it may be used to identify the IoT device and establish encrypted communication with the IoT device. As mentioned above, in one embodiment, a programmable device other than a "SIM" card may be used to perform the same functions as the SIM card in the method shown in **Figure 13**.

[00132] A method for integrating a new IoT device into a network is illustrated in **Figure 14**. The method may be implemented within the system architecture described above, but is not limited to any particular system architecture.

[00133] At 1401, a user receives a new IoT device to which an encryption key has been pre-assigned. At 1402, the key is securely provided to the IoT hub. As mentioned above, in one embodiment, this involves reading a barcode associated with the IoT device to identify the public key of a public/private key pair assigned to the device. The barcode may be read directly by the IoT hub or captured via a mobile device via an app or bowser. In an alternate embodiment, a secure communication channel such as a Bluetooth LE channel, a near field communication (NFC) channel or a secure WiFi channel may be established between the IoT device and the IoT hub to exchange the key. Regardless of how the key is transmitted, once received, it is stored in the secure keystore of the IoT hub device. As mentioned above, various secure execution technologies may be used on the IoT hub to store and protect the key such as Secure Enclaves, Trusted Execution Technology (TXT), and/or Trustzone. In addition, at 803, the key is securely transmitted to the IoT service which stores the key in its own secure keystore. It may then use the key to encrypt communication with the IoT device. One again, the exchange may be implemented using a certificate/signed key. Within the hub 110 it is particularly important to prevent modification/addition/ removal of the stored keys.

[00134] A method for securely communicating commands/data to an IoT device using public/private keys is illustrated in **Figure 15**. The method may be implemented within the system architecture described above, but is not limited to any particular system architecture.

[00135] At 1501, the IoT service encrypts the data/commands using the IoT device public key to create an IoT device packet. It then encrypts the IoT device packet using IoT hub's public key to create the IoT hub packet (e.g., creating an IoT hub wrapper around the IoT device packet). At 1502, the IoT service transmits the IoT hub packet to the IoT hub. At 1503, the IoT hub decrypts the IoT hub packet using the IoT hub's private key to generate the IoT device packet. At 1504 it then transmits the IoT device packet to the IoT device which, at 1505, decrypts the IoT device packet using the IoT device private key to generate the data/commands. At 1506, the IoT device processes the data/commands.

[00136] In an embodiment which uses symmetric keys, a symmetric key exchange may be negotiated between each of the devices (e.g., each device and the hub and

between the hub and the service). Once the key exchange is complete, each transmitting device encrypts and/or signs each transmission using the symmetric key before transmitting data to the receiving device.

APPARATUS AND METHOD FOR ESTABLISHING SECURE COMMUNICATION CHANNELS IN AN INTERNET OF THINGS (IOT) SYSTEM

[00137] In one embodiment of the invention, encryption and decryption of data is performed between the IoT service 120 and each IoT device 101, regardless of the intermediate devices used to support the communication channel (e.g., such as the user's mobile device 611 and/or the IoT hub 110). One embodiment which communicates via an IoT hub 110 is illustrated in **Figure 16A** and another embodiment which does not require an IoT hub is illustrated in **Figure 16B**.

[00138] Turning first to **Figure 16A**, the IoT service 120 includes an encryption engine 1660 which manages a set of "service session keys" 1650 and each IoT device 101 includes an encryption engine 1661 which manages a set of "device session keys" 1651 for encrypting/decrypting communication between the IoT device 101 and IoT service 120. The encryption engines may rely on different hardware modules when performing the security/encryption techniques described herein including a hardware security module 1630-1631 for (among other things) generating a session public/private key pair and preventing access to the private session key of the pair and a key stream generation module 1640-1641 for generating a key stream using a derived secret. In one embodiment, the service session keys 1650 and the device session keys 1651 comprise related public/private key pairs. For example, in one embodiment, the device session keys 1651 on the IoT device 101 include a public key of the IoT service 120 and a private key of the IoT device 101. As discussed in detail below, in one embodiment, to establish a secure communication session, the public/private session key pairs, 1650 and 1651, are used by each encryption engine, 1660 and 1661, respectively, to generate the same secret which is then used by the SKGMs 1640-1641 to generate a key stream to encrypt and decrypt communication between the IoT service 120 and the IoT device 101. Additional details associated with generation and use of the secret in accordance with one embodiment of the invention are provided below.

[00139] In **Figure 16A**, once the secret has been generated using the keys 1650-1651, the client will always send messages to the IoT device 101 through the IoT service 120, as indicated by Clear transaction 1611. "Clear" as used herein is meant to indicate that the underlying message is not encrypted using the encryption techniques described herein. However, as illustrated, in one embodiment, a secure sockets layer

(SSL) channel or other secure channel (e.g., an Internet Protocol Security (IPSEC) channel) is established between the client device 611 and IoT service 120 to protect the communication. The encryption engine 1660 on the IoT service 120 then encrypts the message using the generated secret and transmits the encrypted message to the IoT hub 110 at 1602. Rather than using the secret to encrypt the message directly, in one embodiment, the secret and a counter value are used to generate a key stream, which is used to encrypt each message packet. Details of this embodiment are described below with respect to **Figure 17**.

[00140] As illustrated, an SSL connection or other secure channel may be established between the IoT service 120 and the IoT hub 110. The IoT hub 110 (which does not have the ability to decrypt the message in one embodiment) transmits the encrypted message to the IoT device at 1603 (e.g., over a Bluetooth Low Energy (BTLE) communication channel). The encryption engine 1661 on the IoT device 101 may then decrypt the message using the secret and process the message contents. In an embodiment which uses the secret to generate a key stream, the encryption engine 1661 may generate the key stream using the secret and a counter value and then use the key stream for decryption of the message packet.

[00141] The message itself may comprise any form of communication between the IoT service 120 and IoT device 101. For example, the message may comprise a command packet instructing the IoT device 101 to perform a particular function such as taking a measurement and reporting the result back to the client device 611 or may include configuration data to configure the operation of the IoT device 101.

[00142] If a response is required, the encryption engine 1661 on the IoT device 101 uses the secret or a derived key stream to encrypt the response and transmits the encrypted response to the IoT hub 110 at 1604, which forwards the response to the IoT service 120 at 1605. The encryption engine 1660 on the IoT service 120 then decrypts the response using the secret or a derived key stream and transmits the decrypted response to the client device 611 at 1606 (e.g., over the SSL or other secure communication channel).

[00143] **Figure 16B** illustrates an embodiment which does not require an IoT hub. Rather, in this embodiment, communication between the IoT device 101 and IoT service 120 occurs through the client device 611 (e.g., as in the embodiments described above with respect to **Figures 6-9B**). In this embodiment, to transmit a message to the IoT device 101 the client device 611 transmits an unencrypted version of the message to the IoT service 120 at 1611. The encryption engine 1660 encrypts the message using

the secret or the derived key stream and transmits the encrypted message back to the client device 611 at 1612. The client device 611 then forwards the encrypted message to the IoT device 101 at 1613, and the encryption engine 1661 decrypts the message using the secret or the derived key stream. The IoT device 101 may then process the message as described herein. If a response is required, the encryption engine 1661 encrypts the response using the secret and transmits the encrypted response to the client device 611 at 1614, which forwards the encrypted response to the IoT service 120 at 1615. The encryption engine 1660 then decrypts the response and transmits the decrypted response to the client device 611 at 1616.

[00144] **Figure 17** illustrates a key exchange and key stream generation which may initially be performed between the IoT service 120 and the IoT device 101. In one embodiment, this key exchange may be performed each time the IoT service 120 and IoT device 101 establish a new communication session. Alternatively, the key exchange may be performed and the exchanged session keys may be used for a specified period of time (e.g., a day, a week, etc). While no intermediate devices are shown in **Figure 17** for simplicity, communication may occur through the IoT hub 110 and/or the client device 611.

[00145] In one embodiment, the encryption engine 1660 of the IoT service 120 sends a command to the HSM 1630 (e.g., which may be such as a CloudHSM offered by Amazon®) to generate a session public/private key pair. The HSM 1630 may subsequently prevent access to the private session key of the pair. Similarly, the encryption engine on the IoT device 101 may transmit a command to the HSM 1631 (e.g., such as an Atecc508 HSM from Atmel Corporation®) which generates a session public/private key pair and prevents access to the session private key of the pair. Of course, the underlying principles of the invention are not limited to any specific type of encryption engine or manufacturer.

[00146] In one embodiment, the IoT service 120 transmits its session public key generated using the HSM 1630 to the IoT device 101 at 1701. The IoT device uses its HSM 1631 to generate its own session public/private key pair and, at 1702, transmits its public key of the pair to the IoT service 120. In one embodiment, the encryption engines 1660-1661 use an Elliptic curve Diffie–Hellman (ECDH) protocol, which is an anonymous key agreement that allows two parties with an elliptic curve public–private key pair, to establish a shared secret. In one embodiment, using these techniques, at 1703, the encryption engine 1660 of the IoT service 120 generates the secret using the IoT device session public key and its own session private key. Similarly, at 1704, the

encryption engine 1661 of the IoT device 101 independently generates the same secret using the IoT service 120 session public key and its own session private key. More specifically, in one embodiment, the encryption engine 1660 on the IoT service 120 generates the secret according to the formula *secret = IoT device session pub key * IoT service session private key*, where '*' means that the IoT device session public key is point-multiplied by the IoT service session private key. The encryption engine 1661 on the IoT device 101 generates the secret according to the formula *secret = IoT service session pub key * IoT device session private key*, where the IoT service session public key is point multiplied by the IoT device session private key. In the end, the IoT service 120 and IoT device 101 have both generated the same secret to be used to encrypt communication as described below. In one embodiment, the encryption engines 1660-1661 rely on a hardware module such as the KSGMs 1640-1641 respectively to perform the above operations for generating the secret.

[00147] Once the secret has been determined, it may be used by the encryption engines 1660 and 1661 to encrypt and decrypt data directly. Alternatively, in one embodiment, the encryption engines 1660-1661 send commands to the KSGMs 1640-1641 to generate a new key stream using the secret to encrypt/decrypt each data packet (i.e., a new key stream data structure is generated for each packet). In particular, one embodiment of the key stream generation module 1640-1641 implements a Galois/Counter Mode (GCM) in which a counter value is incremented for each data packet and is used in combination with the secret to generate the key stream. Thus, to transmit a data packet to the IoT service 120, the encryption engine 1661 of the IoT device 101 uses the secret and the current counter value to cause the KSGMs 1640-1641 to generate a new key stream and increment the counter value for generating the next key stream. The newly-generated key stream is then used to encrypt the data packet prior to transmission to the IoT service 120. In one embodiment, the key stream is XORed with the data to generate the encrypted data packet. In one embodiment, the IoT device 101 transmits the counter value with the encrypted data packet to the IoT service 120. The encryption engine 1660 on the IoT service then communicates with the KSGM 1640 which uses the received counter value and the secret to generate the key stream (which should be the same key stream because the same secret and counter value are used) and uses the generated key stream to decrypt the data packet.

[00148] In one embodiment, data packets transmitted from the IoT service 120 to the IoT device 101 are encrypted in the same manner. Specifically, a counter is

incremented for each data packet and used along with the secret to generate a new key stream. The key stream is then used to encrypt the data (e.g., performing an XOR of the data and the key stream) and the encrypted data packet is transmitted with the counter value to the IoT device 101. The encryption engine 1661 on the IoT device 101 then communicates with the KSGM 1641 which uses the counter value and the secret to generate the same key stream which is used to decrypt the data packet. Thus, in this embodiment, the encryption engines 1660-1661 use their own counter values to generate a key stream to encrypt data and use the counter values received with the encrypted data packets to generate a key stream to decrypt the data.

[00149] In one embodiment, each encryption engine 1660-1661 keeps track of the last counter value it received from the other and includes sequencing logic to detect whether a counter value is received out of sequence or if the same counter value is received more than once. If a counter value is received out of sequence, or if the same counter value is received more than once, this may indicate that a replay attack is being attempted. In response, the encryption engines 1660-1661 may disconnect from the communication channel and/or may generate a security alert.

[00150] **Figure 18** illustrates an exemplary encrypted data packet employed in one embodiment of the invention comprising a 4-byte counter value 1800, a variable-sized encrypted data field 1801, and a 6-byte tag 1802. In one embodiment, the tag 1802 comprises a checksum value to validate the decrypted data (once it has been decrypted).

[00151] As mentioned, in one embodiment, the session public/private key pairs 1650-1651 exchanged between the IoT service 120 and IoT device 101 may be generated periodically and/or in response to the initiation of each new communication session.

[00152] One embodiment of the invention implements additional techniques for authenticating sessions between the IoT service 120 and IoT device 101. In particular, in one embodiment, hierarchy of public/private key pairs is used including a master key pair, a set of factory key pairs, and a set of IoT service key pairs, and a set of IoT device key pairs. In one embodiment, the master key pair comprises a root of trust for all of the other key pairs and is maintained in a single, highly secure location (e.g., under the control of the organization implementing the IoT systems described herein). The master private key may be used to generate signatures over (and thereby authenticate) various other key pairs such as the factory key pairs. The signatures may then be verified using the master public key. In one embodiment, each factory which manufactures IoT devices is assigned its own factory key pair which may then be used to authenticate IoT

service keys and IoT device keys. For example, in one embodiment, a factory private key is used to generate a signature over IoT service public keys and IoT device public keys. These signature may then be verified using the corresponding factory public key. Note that these IoT service/device public keys are not the same as the "session" public/private keys described above with respect to **Figures 16A-B**. The session public/private keys described above are temporary (i.e., generated for a service/device session) while the IoT service/device key pairs are permanent (i.e., generated at the factory).

[00153] With the foregoing relationships between master keys, factory keys, service/device keys in mind, one embodiment of the invention performs the following operations to provide additional layers of authentication and security between the IoT service 120 and IoT device 101:

A. In one embodiment, the IoT service 120 initially generates a message containing the following:

1. The IoT service's unique ID:
   - The IoT service's serial number;
   - a Timestamp;
   - The ID of the factory key used to sign this unique ID;
   - a Class of the unique ID (i.e., a service);
   - IoT service's public key
   - The signature over the unique ID.
2. The Factory Certificate including:
   - A timestamp
   - The ID of the master key used to sign the certificate
   - The factory public key
   - The signature of the Factory Certificate
3. IoT service session public key (as described above with respect to **Figures 16A-B**)
4. IoT service session public key signature (e.g., signed with the IoT service's private key)

B. In one embodiment, the message is sent to the IoT device on the negotiation channel (described below). The IoT device parses the message and:

1. Verifies the signature of the factory certificate (only if present in the message payload)

2. Verifies the signature of the unique ID using the key identified by the unique ID
3. Verifies the IoT service session public key signature using the IoT service's public key from the unique ID
4. Saves the IoT service's public key as well as the IoT service's session public key
5. Generates the IoT device session key pair

C. The IoT device then generates a message containing the following:

1. IoT device's unique ID
    - IoT device serial number
    - Timestamp
    - ID of factory key used to sign this unique ID
    - Class of unique ID (i.e., IoT device)
    - IoT device's public key
    - Signature of unique ID
2. IoT device's session public key
3. Signature of (IoT device session public key + IoT service session public key) signed with IoT device's key

D. This message is sent back to the IoT service. The IoT service parses the message and:

1. Verifies the signature of the unique ID using the factory public key
2. Verifies the signature of the session public keys using the IoT device's public key
3. Saves the IoT device's session public key

E. The IoT service then generates a message containing a signature of (IoT device session public key + IoT service session public key) signed with the IoT service's key.

F. The IoT device parses the message and:

1. Verifies the signature of the session public keys using the IoT service's public key

2. Generates the key stream from the IoT device session private key and the IoT service's session public key
3. The IoT device then sends a “messaging available” message.

G. The IoT service then does the following:
1. Generates the key stream from the IoT service session private key and the IoT device's session public key
2. Creates a new message on the messaging channel which contains the following:
- Generates and stores a random 2 byte value
- Set attribute message with the boomerang attribute Id (discussed below) and the random value

H. The IoT device receives the message and:
1. Attempts to decrypt the message
2. Emits an Update with the same value on the indicated attribute Id

I. The IoT service recognizes the message payload contains a boomerang attribute update and:
1. Sets its paired state to true
2. Sends a pairing complete message on the negotiator channel

J. IoT device receives the message and sets his paired state to true

[00154] While the above techniques are described with respect to an “IoT service” and an “IoT device,” the underlying principles of the invention may be implemented to establish a secure communication channel between any two devices including user client devices, servers, and Internet services.

[00155] The above techniques are highly secure because the private keys are never shared over the air (in contrast to current Bluetooth pairing techniques in which a secret is transmitted from one party to the other). An attacker listening to the entire conversation will only have the public keys, which are insufficient to generate the shared secret. These techniques also prevent a man-in-the-middle attack by exchanging signed public keys. In addition, because GCM and separate counters are used on each device, any kind of "replay attack" (where a man in the middle captures the data and

sends it again) is prevented. Some embodiments also prevent replay attacks by using asymmetrical counters.

TECHNIQUES FOR EXCHANGING DATA AND COMMANDS WITHOUT FORMALLY PAIRING DEVICES

[00156] GATT is an acronym for the Generic Attribute Profile, and it defines the way that two Bluetooth Low Energy (BTLE) devices transfer data back and forth. It makes use of a generic data protocol called the Attribute Protocol (ATT), which is used to store Services, Characteristics and related data in a simple lookup table using 16-bit Characteristic IDs for each entry in the table. Note that while the "characteristics" are sometimes referred to as "attributes."

[00157] On Bluetooth devices, the most commonly used characteristic is the devices "name" (having characteristic ID 10752 (0x2A00)). For example, a Bluetooth device may identify other Bluetooth devices within its vicinity by reading the "Name" characteristic published by those other Bluetooth devices using GATT. Thus, Bluetooth device have the inherent ability to exchange data without formally pairing/bonding the devices (note that "paring" and "bonding" are sometimes used interchangeably; the remainder of this discussion will use the term "pairing").

[00158] One embodiment of the invention takes advantage of this capability to communicate with BTLE-enabled IoT devices without formally pairing with these devices. Pairing with each individual IoT device would extremely inefficient because of the amount of time required to pair with each device and because only one paired connection may be established at a time.

[00159] **Figure 19** illustrates one particular embodiment in which a Bluetooth (BT) device 1910 establishes a network socket abstraction with a BT communication module 1901 of an IoT device 101 without formally establishing a paired BT connection. The BT device 1910 may be included in an IoT hub 110 and/or a client device 611 such as shown in **Figure 16A**. As illustrated, the BT communication module 1901 maintains a data structure containing a list of characteristic IDs, names associated with those characteristic IDs and values for those characteristic IDs. The value for each characteristic may be stored within a 20-byte buffer identified by the characteristic ID in accordance with the current BT standard. However, the underlying principles of the invention are not limited to any particular buffer size.

[00160] In the example in **Figure 19**, the "Name" characteristic is a BT-defined characteristic which is assigned a specific value of "IoT Device 14." One embodiment of

the invention specifies a first set of additional characteristics to be used for negotiating a secure communication channel with the BT device 1910 and a second set of additional characteristics to be used for encrypted communication with the BT device 1910. In particular, a "negotiation write" characteristic, identified by characteristic ID <65532> in the illustrated example, may be used to transmit outgoing negotiation messages and the "negotiation read" characteristic, identified by characteristic ID <65533> may be used to receive incoming negotiation messages. The "negotiation messages" may include messages used by the BT device 1910 and the BT communication module 1901 to establish a secure communication channel as described herein. By way of example, in **Figure 17**, the IoT device 101 may receive the IoT service session public key 1701 via the "negotiation read" characteristic <65533>. The key 1701 may be transmitted from the IoT service 120 to a BTLE-enabled IoT hub 110 or client device 611 which may then use GATT to write the key 1701 to the negotiation read value buffer identified by characteristic ID <65533>. IoT device application logic 1902 may then read the key 1701 from the value buffer identified by characteristic ID <65533> and process it as described above (e.g., using it to generate a secret and using the secret to generate a key stream, etc).

[00161] If the key 1701 is greater than 20 bytes (the maximum buffer size in some current implementations), then it may be written in 20-byte portions. For example, the first 20 bytes may be written by the BT communication module 1903 to characteristic ID <65533> and read by the IoT device application logic 1902, which may then write an acknowledgement message to the negotiation write value buffer identified by characteristic ID <65532>. Using GATT, the BT communication module 1903 may read this acknowledgement from characteristic ID <65532> and responsively write the next 20 bytes of the key 1701 to the negotiation read value buffer identified by characteristic ID <65533>. In this manner, a network socket abstraction defined by characteristic IDs <65532> and <65533> is established for exchanging negotiation messages used to establish a secure communication channel.

[00162] In one embodiment, once the secure communication channel is established, a second network socket abstraction is established using characteristic ID <65534> (for transmitting encrypted data packets from IoT device 101) and characteristic ID <65533> (for receiving encrypted data packets by IoT device). That is, when BT communication module 1903 has an encrypted data packet to transmit (e.g., such as encrypted message 1603 in **Figure 16A**), it starts writing the encrypted data packet, 20 bytes at a time, using the message read value buffer identified by characteristic ID <65533>. The

IoT device application logic 1902 will then read the encrypted data packet, 20 bytes at a time, from the read value buffer, sending acknowledgement messages to the BT communication module 1903 as needed via the write value buffer identified by characteristic ID <65532>.

[00163] In one embodiment, the commands of GET, SET, and UPDATE described below are used to exchange data and commands between the two BT communication modules 1901 and 1903. For example, the BT communication module 1903 may send a packet identifying characteristic ID <65533> and containing the SET command to write into the value field/buffer identified by characteristic ID <65533> which may then be read by the IoT device application logic 1902. To retrieve data from the IoT device 101, the BT communication module 1903 may transmit a GET command directed to the value field/buffer identified by characteristic ID <65534>. In response to the GET command, the BT communication module 1901 may transmit an UPDATE packet to the BT communication module 1903 containing the data from the value field/buffer identified by characteristic ID <65534>. In addition, UPDATE packets may be transmitted automatically, in response to changes in a particular attribute on the IoT device 101. For example, if the IoT device is associated with a lighting system and the user turns on the lights, then an UPDATE packet may be sent to reflect the change to the on/off attribute associated with the lighting application.

[00164] **Figure 20** illustrates exemplary packet formats used for GET, SET, and UPDATE in accordance with one embodiment of the invention. In one embodiment, these packets are transmitted over the message write <65534> and message read <65533> channels following negotiation. In the GET packet 2001, a first 1-byte field includes a value (0X10) which identifies the packet as a GET packet. A second 1-byte field includes a request ID, which uniquely identifies the current GET command (i.e., identifies the current transaction with which the GET command is associated). For example, each instance of a GET command transmitted from a service or device may be assigned a different request ID. This may be done, for example, by incrementing a counter and using the counter value as the request ID. However, the underlying principles of the invention are not limited to any particular manner for setting the request ID.

[00165] A 2-byte attribute ID identifies the application-specific attribute to which the packet is directed. For example, if the GET command is being sent to IoT device 101 illustrated in **Figure 19**, the attribute ID may be used to identify the particular application-specific value being requested. Returning to the above example, the GET

command may be directed to an application-specific attribute ID such as power status of a lighting system, which comprises a value identifying whether the lights are powered on or off (e.g., 1 = on, 0 = off). If the IoT device 101 is a security apparatus associated with a door, then the value field may identify the current status of the door (e.g., 1 = opened, 0 = closed). In response to the GET command, a response may be transmitting containing the current value identified by the attribute ID.

[00166] The SET packet 2002 and UPDATE packet 2003 illustrated in **Figure 20** also include a first 1-byte field identifying the type of packet (i.e., SET and UPDATE), a second 1-byte field containing a request ID, and a 2-byte attribute ID field identifying an application-defined attribute. In addition, the SET packet includes a 2-byte length value identifying the length of data contained in an n-byte value data field. The value data field may include a command to be executed on the IoT device and/or configuration data to configure the operation of the IoT device in some manner (e.g., to set a desired parameter, to power down the IoT device, etc). For example, if the IoT device 101 controls the speed of a fan, the value field may reflect the current fan speed.

[00167] The UPDATE packet 2003 may be transmitted to provide an update of the results of the SET command. The UPDATE packet 2003 includes a 2-byte length value field to identify the length of the n-byte value data field which may include data related to the results of the SET command. In addition, a 1-byte update state field may identify the current state of the variable being updated. For example, if the SET command attempted to turn off a light controlled by the IoT device, the update state field may indicate whether the light was successfully turned off.

[00168] **Figure 21** illustrates an exemplary sequence of transactions between the IoT service 120 and an IoT device 101 involving the SET and UPDATE commands. Intermediary devices such as the IoT hub and the user's mobile device are not shown to avoid obscuring the underlying principles of the invention. At 2101, the SET command 2101 is transmitted form the IoT service to the IoT device 101 and received by the BT communication module 1901 which responsively updates the GATT value buffer identified by the characteristic ID at 2102. The SET command is read from the value buffer by the low power microcontroller (MCU) 200 at 2103 (or by program code being executed on the low power MCU such as IoT device application logic 1902 shown in **Figure 19**). At 2104, the MCU 200 or program code performs an operation in response to the SET command. For example, the SET command may include an attribute ID specifying a new configuration parameter such as a new temperature or may include a state value such as on/off (to cause the IoT device to enter into an "on" or a low power

state). Thus, at 2104, the new value is set in the IoT device and an UPDATE command is returned at 2105 and the actual value is updated in a GATT value field at 2106. In some cases, the actual value will be equal to the desired value. In other cases, the updated value may be different (i.e., because it may take time for the IoT device 101 to update certain types of values). Finally, at 2107, the UPDATE command is transmitted back to the IoT service 120 containing the actual value from the GATT value field.

[00169] **Figure 22** illustrates a method for implementing a secure communication channel between an IoT service and an IoT device in accordance with one embodiment of the invention. The method may be implemented within the context of the network architectures described above but is not limited to any specific architecture.

[00170] At 2201, the IoT service creates an encrypted channel to communicate with the IoT hub using elliptic curve digital signature algorithm (ECDSA) certificates. At 2202, the IoT service encrypts data/commands in IoT device packets using the a session secret to create an encrypted device packet. As mentioned above, the session secret may be independently generated by the IoT device and the IoT service. At 2203, the IoT service transmits the encrypted device packet to the IoT hub over the encrypted channel. At 2204, without decrypting, the IoT hub passes the encrypted devic packet to the IoT device. At 22-5, the IoT device uses the session secret to decrypt the encrypted device packet. As mentioned, in one embodiment this may be accomplished by using the secret and a counter value (provided with the encrypted device packet) to generate a key stream and then using the key stream to decrypt the packet. At 2206, the IoT device then extracts and processes the data and/or commands contained within the device packet.

[00171] Thus, using the above techniques, bi-directional, secure network socket abstractions may be established between two BT-enabled devices without formally pairing the BT devices using standard pairing techniques. While these techniques are described above with respect to an IoT device 101 communicating with an IoT service 120, the underlying principles of the invention may be implemented to negotiate and establish a secure communication channel between any two BT-enabled devices.

[00172] **Figures 23A-C** illustrate a detailed method for pairing devices in accordance with one embodiment of the invention. The method may be implemented within the context of the system architectures described above, but is not limited to any specific system architectures.

[00173] At 2301, the IoT Service creates a packet containing serial number and public key of the IoT Service. At 2302, the IoT Service signs the packet using the

factory private key. At 2303, the IoT Service sends the packet over an encrypted channel to the IoT hub and at 2304 the IoT hub forwards the packet to IoT device over an unencrypted channel. At 2305, the IoT device verifies the signature of packet and, at 2306, the IoT device generates a packet containing the serial number and public key of the IoT Device. At 2307, the IoT device signs the packet using the factory private key and at 2308, the IoT device sends the packet over the unencrypted channel to the IoT hub.

[00174] At 2309, the IoT hub forwards the packet to the IoT service over an encrypted channel and at 2310, the IoT Service verifies the signature of the packet. At 2311, the IoT Service generates a session key pair, and at 2312 the IoT Service generates a packet containing the session public key. The IoT Service then signs the packet with IoT Service private key at 2313 and, at 2314, the IoT Service sends the packet to the IoT hub over the encrypted channel.

[00175] Turning to **Figure 23B**, the IoT hub forwards the packet to the IoT device over the unencrypted channel at 2315 and, at 2316, the IoT device verifies the signature of packet. At 2317 the IoT device generates session key pair (e.g., using the techniques described above), and, at 2318, an IoT device packet is generated containing the IoT device session public key. At 2319, the IoT device signs the IoT device packet with IoT device private key. At 2320, the IoT device sends the packet to the IoT hub over the unencrypted channel and, at 2321, the IoT hub forwards the packet to the IoT service over an encrypted channel.

[00176] At 2322, the IoT service verifies the signature of the packet (e.g., using the IoT device public key) and, at 2323, the IoT service uses the IoT service private key and the IoT device public key to generate the session secret (as described in detail above). At 2324, the IoT device uses the IoT device private key and IoT service public key to generate the session secret (again, as described above) and, at 2325, the IoT device generates a random number and encrypts it using the session secret. At 2326, the IoT service sends the encrypted packet to IoT hub over the encrypted channel. At 2327, the IoT hub forwards the encrypted packet to the IoT device over the unencrypted channel. At 2328, the IoT device decrypts the packet using the session secret.

[00177] Turning to **Figure 23C**, the IoT device re-encrypts the packet using the session secret at 2329 and, at 2330, the IoT device sends the encrypted packet to the IoT hub over the unencrypted channel. At 2331, the IoT hub forwards the encrypted packet to the IoT service over the encrypted channel. The IoT service decrypts the packet using the session secret at 2332. At 2333 the IoT service verifies that the

random number matches the random number it sent. The IoT service then sends a packet indicating that pairing is complete at 2334 and all subsequent messages are encrypted using the session secret at 2335.

SYSTEM AND METHOD FOR A SINGLE-PIECE INTERNET OF THINGS (IOT) SECURITY SENSOR

[00178] One embodiment of the invention comprises a single-piece Internet of Things (IoT) security sensor which addresses the limitations of existing wireless door/window sensors (e.g., difficulty with positioning, bulkiness, false triggers, etc). **Figure 24** illustrates a system architecture with three such IoT devices 2401-2403 coupled to various doors and/or windows within a user's home or business. The interaction between the various system components may occur as described above. For example, the illustrated architecture includes an IoT hub 2405 which communicates with the IoT devices 2401-2403 over low power wireless communication channels such as Bluetooth Low Energy (BTLE) channels and which, in one embodiment, establishes a communication channel with the IoT cloud service 2420.

[00179] As illustrated, the IoT cloud service 2420 may include an IoT device database 2430 comprising database records for each of the IoT devices 2401-2403 and IoT hubs 2405 configured in the system (which may include a plurality of IoT hubs and devices not shown in **Figure 24**). IoT device management logic 2415 creates the database records for new IoT devices and updates the IoT device records in response to data transmitted by each of the IoT devices 2401-2403. The IoT device management logic 2415 may also implement the various security/encryption functions described above to add new devices to the system (e.g., using QR codes/barcodes) and use keys to encrypt communications and/or generate digital signatures when communicating with the IoT devices 2401-2403. In one embodiment, a user may access information related to each of the devices 2401-2403 and/or control the devices via an app installed on a user device 2410 which may be a smartphone device such as an Android® device or iPhone®. In addition, the user may access and control the IoT devices via a browser or application installed on a desktop or laptop computer. In one embodiment, control signals transmitted from the app or application on the user device 2410 are passed to the IoT cloud service 2420 over the Internet 2422, then forwarded from the IoT clour service 2420 to the IoT hub 2405 and from the IoT hub 2405 to one or more of the IoT devices 2401-2403. Of course, the underlying principles of the invention are not limited to any particular manner in which the user accesses/controls the various IoT devices 2401-2403.

[00180] As mentioned, in one embodiment, the IoT devices 2401-2403 comprise single-piece security devices configured on doors and/or windows. **Figure 25** illustrates an exemplary IoT device 2401 which includes a radio microcontroller 2510 for reporting security status to the IoT hub 2405 (e.g., using a low power wireless link such as BTLE as described above), an accelerometer 2502 for detecting motion, and a proximity sensor and logic 2505 for generating and sensing electromagnetic radiation reflected from a nearby object. In one embodiment, the electromagnetic radiation is infrared (IR) radiation (i.e., within the IR spectrum). However, various other forms of electromagnetic radiation may be employed while complying with the underlying principles of the invention.

[00181] In another embodiment, the proximity sensor 2505 comprises a magnetometer to detect the current door position. For example, the magnetometer may be configured to detect the orientation of the door relative to the direction of the Earth's magnetic field. The magnetometer may be calibrated by taking readings when the door is in a closed position and in an open position. The current magnetometer reading may then be compared to the calibrated readings to determine whether the door is currently open or closed.

[00182] In the example shown in **Figure 25**, the IoT device 2401 is affixed to the inner portion of a door 2520 facing the doorjamb 2521. In one embodiment, for example, it may be sufficiently small to fit between the door and the doorjamb (the vertical portion of the frame onto which a door is secured). It should be noted, however, that this particular positioning is not required for complying with the underlying principles of the invention. Moreover, the underlying principles of the invention may also be implemented on windows or on any other moveable objects within a user's home or office.

[00183] In operation, when the door 2520 is still, the radio *u*C 2510 is maintained in a very low power or OFF state to preserve battery life. In one embodiment, when the door is moved, the accelerometer 2502 generates an interrupt to wake the radio *u*C 2510 which then uses the proximity sensor/logic 2505 to "see" if the doorjamb 2521 is still in front of it. If it is not, then the proximity sensor may generate an alert signal which the radio *u*C transmits to the IoT hub 2405.

[00184] In one embodiment, the proximity sensor/logic 2505 comprises an IR transmitter for transmitting IR radiation and an IR detector for detecting the IR radiation which reflects off of the doorjamb 2521. In one embodiment, the proximity sensor/logic 2505 measures the intensity of the reflected IR radiation. The proximity sensor/logic

2505 may then compare the current IR readings with readings known to exist when the door is closed (e.g., which may be collected via calibration as discussed below). If the readings match (or are within a specified threshold), then the proximity sensor/logic 2505 determines that the door is in the closed position. If, however, the readings do not match (e.g., are outside of the threshold), then the proximity sensor/logic 2505 determines that the door is opened, and may generate an alarm condition via the radio *u*C 2510.

[00185] In one embodiment, the proximity sensor/logic 2505 includes calibration logic to calibrate the IR readings to the "closed" position of the door 2520. In one embodiment, after the IoT device 2401 is affixed to the door, the user executes a calibration process via the app on the user device 2410 which will ask the user to confirm when the door is in a closed position. Once the user provides the indication, a command may be sent to notify the proximity sensor 2505 which will record the readings. These readings may then be compared against current readings as described above to determine whether the door is currently opened or closed.

[00186] **Figure 26** illustrates one embodiment in which the IoT device 2401 is positioned at the lower portion of a door 2520 between the internal surface of the door 2520 and the doorjamb 2521. The IoT device 2401 of this embodiment may use a right angled form factor such that only the proximity sensor/logic 2505 is positioned between the door 2520 and doorjamb 2521 while the remaining components of the IoT device 2401 (e.g., the radio *u*C and accelerometer 2502) are positioned on the face of the door. This embodiment will allow the portion which sits between the door 2520 and doorjamb 2521 to be as thin as possible (e.g., potentially only a few millimeters) while the other components such as the wireless radio uC (which may tend to be bulkier) do not interfere with the movement of the door. Of course, the underlying principles of the invention may include an IoT device 2401 in which all of the components are sufficiently small to fit in a single package between the door 2520 and doorjamb 2521.

[00187] Moreover, it will be appreciated that the IoT device 2401 may be placed in other positions such as the edge of the door furthest away from the doorjamb 2521. In this embodiment, the proximity sensor/logic 2505 may take IR measurements between the edge of the door and the directly adjacent portion of the door frame. Similarly, the IoT device 2401 may also be placed on or near the edge of a window. In this embodiment, the proximity sensor/logic 2505 will take IR measurements which are bounced off of nearby structural objects such as the window frame or window sill. Once again, a calibration process may be implemented to take measurements in a closed

and/or opened position and subsequent readings may be compared with these measurements to determine whether the window is opened or closed.

[00188] A variety of different types of sensors may be employed within or coupled to the IoT device 2401 to sense the position of a door, window, or other apparatus within the user's home or business. Several exemplary embodiments are described below.

[00189] As illustrated in **Figures 27A-B**, another embodiment of the invention includes a force sensing resistor (FSR) 2702 coupled to the inner side of a door 2710. In this illustrated embodiment, the FSR 2702 is affixed to a rubber bumper component 2701 which is itself affixed directly to the door as shown. The FSR 2702 is communicatively attached to the IoT device 2703 via a set of FSR leads 2704 (e.g., a set of wires to communicate the current force applied to the FSR 2702). Like the embodiment shown in **Figure 27**, in this embodiment, the IoT device 2703 may have a right angled form factor such that only the FSR sensor is positioned between the door 2710 and doorjamb while the remaining components of the IoT device 2703 (e.g., the radio *u*C and accelerometer 2502) are positioned on the face of the door, as shown. The IoT device 2703 may include a radio module and a small battery for power (as in the embodiments described above).

[00190] In an alternate embodiment, the FSR 2702 may be affixed to the outer edge of the door 2710 rather than the inner edge of the door and may also be coupled to the door frame (e.g., the doorjam 2521). The underlying principles of the invention are not limited to any particular attachment location for the IoT device 2703 and FSR 2702. Moreover, the same basic principles may be applied to use the FSR 2702 on windows or other devices in the user's home or business.

[00191] In the example shown in **Figures 27A-B**, the force sensing resistor (FSR) 2702 is capable of detecting when inner side of door comes into close proximity of the door frame. Over a short distance, the FSR 2702 provides a continuous measurement of the force being applied by the door through the FSR to the door frame. As mentioned, one embodiment of the FSR 2702 is affixed to a small rubber bumper 2701 that transmits the force from the door, through the FSR, to the frame. Size and consistency of the bumper 2701 may be varied to adapt to a variety of door gaps. In response to a force applied to the FSR (e.g., as a result of the door being closed), the FSR 2702 generates electrical signals which are received and processed by the IoT device 2703 and/or transmitted through to the IoT hub 2405 and IoT service 2420. For example, a different resistance may be measured across the FSR 2702 for different levels of applied force (i.e., resulting in a different amount of current, assuming a

consistent voltage). When a specified threshold force has been reached, the IoT device 2703 (or the IoT hub 2405 or service 2420) may interpret this to mean that the door is in a "closed" position. When a lower threshold force is detected, the IoT device 2703, IoT hub 2405, or IoT service 2420 may interpret this to mean that the door is only partially opened (e.g., slightly ajar, thereby only partially depressing the FSR). When no force is detected, the IoT device 2703, IoT hub 2410 and/or service 2420 may conclude that the door is opened. Thus, using a sensor which provides for a continuous measurement of force over a small dynamic range such as the FSR 2702 allows for a more precise determination of the position of the door (in contrast to existing security sensors which are simply on or off). As in prior embodiments, the FSR 2702/IoT device 2703 may be implemented as a one-piece device which may be affixed entirely on the door or door frame (as opposed to current styles of magnetic door sensors that are two piece).

[00192] In one embodiment, the user may calibrate the FSR 2702/IoT device 2703 when initially installed. For example, through the app on the user device 2410, the user may be asked to provide an indication of when the door is fully closed, fully open, and ajar. Sensor readings may be taken in each position and recorded by the IoT device 2703, IoT hub 2410 and/or service 2420. These readings may then be compared against current readings to determine the current status of the door. For example, if the current reading is within a specified range of the recorded reading for the door being closed, then the IoT device 2703, IoT hub 2410 and/or service 2420 may determine that the door is currently closed. Similar comparisons may be made for the open and ajar states.

[00193] Various mounting techniques may be employed including adhesives, pressure fittings, elastics, or mounted brackets, depending on the form factor and design goals. In the embodiment shown in **Figures 27A-B**, for example, an adhesive may be applied to the backing of the rubber bumper to affix the FSR 2702 and IoT device 2703 to the door. One example of an FSR that may be used is the FSR 402 Round Force Sensing Resistor available from Digi-Key Electronics.

[00194] Another embodiment includes all of the features shown in **Figures 27A-B** but also includes a piezo electric vibration sensor added to the package. For example, in one embodiment, the piezo electric vibration sensor may be positioned beneath or integrated within the rubber bumper 2701. As with the FSR, electrical leads communicatively couple the piezo electric vibration sensor to the IoT device 2703. In one embodiment, the piezo electric vibration sensor is passive, generating a high voltage when force, flexure, or vibration is applied without requiring an external device

to provide power. Thus, the vibration sensor may be configured to wake up the radio microcontroller 2510 and other components within the IoT device 2703 in response to vibration or motion, thereby allowing these components to enter into a very low power state in the absence of vibration or motion. The vibration sensor, for example, may be triggered by knocks/impacts on the door, may work as a pressure/tactile sensor, or may be configured as a simple accelerometer (such as accelerometer 2502 in **Figure 25**).

[00195] In one embodiment, the FSR 2702 in **Figures 27A-B** is replaced by a strain gauge bonded to a flat spring. As the door closes and comes in contact with the spring, the strain gage resistance changes in response to the strain on the spring surface. The resistance change corresponds to the spring flexure which, in turn, correlates to the spring angle and therefore the door angle. The results of this embodiment are similar to the FSR embodiment described above with the exception that a much larger dynamic range for the door angle is available. However, strain gage circuits require amplification to increase dynamic range and, consequently, this design may tend to consume more power than the FSR embodiments.

[00196] In another embodiment, the FSR 2702 sensor element in **Figures 27A-B** is replaced by a combination piezo electric film and piezo resistive film. The piezo electric film of this embodiment works as described above with respect to the piezo electric vibration sensor, generating a high voltage when force, flexure, or vibration is applied without requiring an external device to provide power. However, the piezo resistive film utilizes the piezo-resistive effect and has a variable resistance based on force and flexure. In one embodiment, these two films may be used in a similar manner to the flat spring/strain gage combination described above. However, in another embodiment, the piezo electric/piezo resistive film combination may be mounted inside the latch/bolt slot of the door mechanism and communicatively coupled to the IoT device 2703 via a set of conductors. Depending on whether the latch was locked and deforming the sensor or unlatched and leaving the sensor free, the locked state of the door may be determined from the generated electrical signals. In one embodiment, mounting is performed on either the frame or the door. In this embodiment, the films are adhered/secured to the surface near the door latch and protrude into the latch path so that the latch motion comes in contact with the films. As in prior embodiment, this embodiment may be calibrated after installation so that the open and closed states of the door are correlated with the corresponding resistance in the piezo-resistive film.

[00197] Yet another embodiment retains the same or similar components as the embodiment in **Figures 27A-B** but is mounted inside the door. Either through retrofit or

during assembly a small cavity may be created on the inside (hinge mount) of the door or frame into which the sensor is placed with only the FSR bumper extending beyond the plane of the surface. By embedding the FSR sensor in this manner, the size and form factor become lesser concerns and larger capacity batteries may be used, extending the unit lifetime up to a decade. In addition, this embodiment has almost no visible profile and is far less invasive visually. Limiting the size of a unit would be dependent on battery style.

[00198] While described within the context of a standard door 2710, all of the above embodiments are also applicable to sliding doors and windows. The swinging door is the most complex of the current proposed implementations. When mounted to a sliding window or sliding door, these embodiments perform the same underlying function despite having a purely linear path.

[00199] A method in accordance with one embodiment of the invention is illustrated in **Figure 28**. The method may be implemented within the context of the system architectures described above but is not limited to any particular architectures.

[00200] The door/window is initially in a resting position at 2801. If movement is detected at 2802, then at 2803 the wireless *u*C awakened from its low power/sleep state. At 2804, the wireless *u*C queries the proximity sensor to take a proximity reading (which may also have been in a low power state prior to the query and/or may have been activated by the accelerometer). In response, the proximity sensor makes a reading at 2805 to determine whether the door/window is in an opened or closed position. If the door/window is opened, determined at 2806, then at 2807, it may generate an alarm condition which may be transmitted to the IoT hub, the IoT service, and/or the user device. Eventually, after the alarm condition has been investigated, the alarm condition may be disabled at 2809. In one embodiment, the alarm condition may be disabled in response to a signal transmitted from the IoT hub, the IoT service and/or the user's mobile device. If the door/window is not determined to be opened at 2806, then at 2808, the wireless uC may be placed back in a low power/sleep state and the process returns to 2801.

[00201] In one embodiment, the user may configure the system to generate alarms as described above when the user's home is in a "protected" state (e.g., when the user leaves the home during the day or at night when the user is asleep). During other times, when the home is not in a protected state, the various components on the IoT device 2401 may enter into a low power/sleep state. A signal from the IoT hub 2405 may then place the IoT device 2401 into an operational mode in response to manual

input from the user (e.g., via the app on the user device) and/or in accordance with a daily schedule (e.g., during user-specified times of the day or evening).

[00202] Various techniques may be used to affix the IoT device 2401 to doors and windows including, for example, an adhesive (e.g., double-sided tape) and miniature screws sized to fit through attachment holes in the IoT device's enclosure.

SYSTEM AND METHOD FOR ESTABLISHING A SECONDARY COMMUNICATION CHANNEL TO CONTROL AN INTERNET OF THINGS (IOT) DEVICE

[00203] In the embodiments of the invention described above, a secure channel is established between each IoT device and the IoT service through an IoT hub or a client device (see, e.g., **Figures 16A-17** and associated text). Once established, the IoT service may securely send commands to control and configure each IoT device. In the reverse direction, each IoT device may transmit data back to the IoT service, where it may be stored and/or accessed by the end user. By way of example, when a door or window is opened in the user's home, the IoT device configured to detect this condition may transmit an indication that the door/window is opened to the IoT service over the secure communication channel. Similarly, if an IoT device is configured as a wireless lock on the user's front door, the user may cause a command to be transmitted from the IoT service to the IoT device over the secure communication channel to unlock the front door.

[00204] The above configuration assumes that there is a viable connection between the IoT device and the IoT service. In some instances, however, the connection to the IoT service may be disabled. For example, the IoT service may be down or the Internet connection to the IoT service (e.g., via the cellular data network or a leased home Internet connection) may be inoperative.

[00205] As illustrated in **Figure 29**, to address this issue, one embodiment of the invention provides techniques to establish a secondary communication channel 2910 between the user's client device 611 and an IoT device 101 so that the user may control and collect data from the IoT device 101, even when the connection to the IoT service 120 is lost (as indicated by the X over the communication path between the IoT hub 110 and the IoT service 120). Thus, if the IoT device 101 is a wireless door lock, the user may unlock his/her front door using the secondary communication channel 2910 even though the primary communication channel 2911 to the IoT service 120 is inoperative.

[00206] In one embodiment, the secondary channel 2910 comprises a Bluetooth Low Energy (BTLE) communication channel. However, the underlying principles of the invention are not limited to any particular wireless communication protocol.

[00207] In one embodiment, a set of secondary channel keys 2950-2951 are stored and maintained on the client device 611 and the IoT device 101 to be used for establishing the secure secondary communication channel 2910 between the IoT device 101 and the client device 611. The secondary channel keys 2950-2951 may be exchanged between the client device 611 and the IoT device 101 using a secure key exchange protocol. For example, the same key exchange protocols described above (or a subset thereof) may be used to exchange keys between the client device 611 and the IoT device 101. Alternatively, the keys may be generated randomly and securely provided to the IoT device 101 and the client device 611 from the IoT service 120 (i.e., during a period of time when the connection to the IoT service is operative).

[00208] Once the keys have been exchanged, the encryption engine 2960 on the client device 611 may use its key(s) 2950 to encrypt communication with the IoT device 101 and the encryption engine 1661 on the IoT device 101 may use its key(s) 2951 to decrypt the communications received from the client device 611. Conversely, the encryption engine 1661 on the IoT device 101 may use its key(s) to encrypt communication and the encryption engine 2960 on the client device 611 may use its key(s) to decrypt the communication.

[00209] Because storing keys on a client device may be less secure than the embodiments described above, the functionality exposed by the IoT device 101 may be limited when the second communication channel 2910 is used. The functionality exposed/allowed when the second channel 2910 is used may also be product-dependent. For example, the user may be allowed to retrieve a subset of data from the IoT device 101 and/or may be provided with a subset of the commands to configure or control the IoT device 101. By way of example, the IoT device may deny user access to data which is deemed "secure" data and may deny access to "secure" commands (e.g., such as changing security codes on the IoT device).

[00210] Certain types of IoT devices 101 such as wireless door locks may have a single, simple function. In one embodiment, access to these functions is provided via the secondary channel 2910 using an additional layer of security. For example, in one embodiment, an authentication module 2970 on the IoT device is configured with a security passcode 2971 such as an N-digit number or alphanumeric password. This may be done, for example, during a period when the primary secure communication channel 1911 is established between the IoT service 120 and the IoT device 101. Upon connecting to the IoT service 120, the user may choose the passcode via a passcode entry app 2920 on the client device 611. The passcode may then be securely

transmitted from the IoT service 120 and securely stored within a secure storage on the IoT device 101.

[00211] Subsequently, when the user establishes the secondary communication channel 2910 from the client device 611 (e.g., using the secondary channel keys as described above), the IoT device 101 may prompt the user to enter the secure passcode. If the user correctly enters the secure passcode from the passcode entry app 2920, then the authentication module 2970 will authenticate the user and provide access to the data and functions to be performed by the IoT device 101 (or a specified subset thereof). In one embodiment, the authentication engine 2970 will disconnect the secondary communication channel 2910 after a specified number of failed passcode attempts. If the IoT device 101 is a wireless door lock, for example, then the passcode acts as an extra layer of security for entry into the user's home.

[00212] A method in accordance with one embodiment of the invention is illustrated in **Figure 30**. The method may be implemented within the context of the system architectures described above but is not limited to any particular system architecture.

[00213] At 3001, a secure connection is established between the IoT service and the IoT device (e.g., through an IoT device using the secure key exchange techniques described above). At 3002, a secondary key exchange is performed between the IoT device and the client device. As mentioned, this may be accomplished in a variety of ways including directly between the client device and IoT device or via the IoT service (e.g., which may generate a random set of keys and securely provide the keys to each of the IoT device and client device).

[00214] At 3003, the IoT device is programmed with a secure passcode. As mentioned, this may be done via an app on the user's client device which prompts the user to enter an N-digit numerical code or alphanumeric code. The passcode may be securely transmitted to the IoT device via a secure channel established between the IoT service and the IoT device.

[00215] If the primary secure connection fails, determined at 3004, then at 3005 a secondary secure connection between the client device and the IoT device may be established using a secondary communication protocol. In one embodiment, the secondary protocol encrypts communication between the IoT device and the client device using the secondary keys exchanged at 3002. As mentioned, the underlying wireless communication protocol may be implemented using BTLE or other local wireless protocol.

[00216] At 3006, the IoT device prompts the user to enter the secure password via the user's client device. If the user enters the correct passcode, determined at 3007, then the IoT device permits access to its data and functions at 3008 (or a subset thereof). If the user does not enter the correct passcode, then access to the IoT device is denied at 3009.

[00217] Embodiments of the invention may include various steps, which have been described above. The steps may be embodied in machine-executable instructions which may be used to cause a general-purpose or special-purpose processor to perform the steps. Alternatively, these steps may be performed by specific hardware components that contain hardwired logic for performing the steps, or by any combination of programmed computer components and custom hardware components.

[00218] As described herein, instructions may refer to specific configurations of hardware such as application specific integrated circuits (ASICs) configured to perform certain operations or having a predetermined functionality or software instructions stored in memory embodied in a non-transitory computer readable medium. Thus, the techniques shown in the figures can be implemented using code and data stored and executed on one or more electronic devices (e.g., an end station, a network element, etc.). Such electronic devices store and communicate (internally and/or with other electronic devices over a network) code and data using computer machine-readable media, such as non-transitory computer machine-readable storage media (e.g., magnetic disks; optical disks; random access memory; read only memory; flash memory devices; phase-change memory) and transitory computer machine-readable communication media (e.g., electrical, optical, acoustical or other form of propagated signals – such as carrier waves, infrared signals, digital signals, etc.). In addition, such electronic devices typically include a set of one or more processors coupled to one or more other components, such as one or more storage devices (non-transitory machine-readable storage media), user input/output devices (e.g., a keyboard, a touchscreen, and/or a display), and network connections. The coupling of the set of processors and other components is typically through one or more busses and bridges (also termed as bus controllers). The storage device and signals carrying the network traffic respectively represent one or more machine-readable storage media and machine-readable communication media. Thus, the storage device of a given electronic device typically stores code and/or data for execution on the set of one or more processors of that electronic device. Of course, one or more parts of an embodiment of the invention

may be implemented using different combinations of software, firmware, and/or hardware.

[00219] Throughout this detailed description, for the purposes of explanation, numerous specific details were set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the invention may be practiced without some of these specific details. In certain instances, well known structures and functions were not described in elaborate detail in order to avoid obscuring the subject matter of the present invention. Accordingly, the scope and spirit of the invention should be judged in terms of the claims which follow.

[00220] **Figure 31** illustrates one embodiment of an IoT device 101 in which the BTLE communication interface 3110 includes advertising interval selection logic 3111 which adjusts the advertising interval when data is ready to be transmitted. In addition, the BTLE communication interface 3120 on the IoT hub 110 includes advertising interval detection logic 3121 to detect the change in the advertising interval, provide an acknowledgement, and receive the data.

[00221] In particular, in the illustrated embodiment, an application 3101 on the IoT device 101 indicates that it has data to be sent. In response, the advertising interval selection logic 3111 modifies the advertising interval to notify the IoT hub 110 that data is to be transmitted (e.g., changing the interval to .75T or some other value). When the advertising interval detection logic 3121 detects the change, the BTLE communication interface 3120 connects to the BTLE communication interface 3110 of the IoT device 101, indicating that it is ready to receive the data. The BTLE communication interface 3110 of the IoT device 101 then transmits the data to the BTLE communication interface 3120 of the IoT hub. The IoT hub may then pass the data through to the IoT service 120 and/or to the user's client device (not shown). After the data has been transmitted, the advertising interval selection logic 3111 may then revert back to the normal advertising interval (e.g., AI=T).

[00222] In one embodiment of the invention, a secure communication channel is established between the IoT device 101 and the IoT service 120 using one or more of the security/encryption techniques described above (see, e.g., **Figures 16A-23C** and associated text). For example, in one embodiment, the IoT service 120 performs a key exchange with the IoT device 101 as described above to encrypt all communication between the IoT device 101 and the IoT service 120.

[00223] A method in accordance with one embodiment of the invention is illustrated in **Figure 32**. The method may be implemented within the context of the system architectures described above, but is not limited to any particular system architectures.

[00224] At 3200, the IoT device uses the standard advertising interval when generating advertising packets (e.g., separated by time T). The IoT device maintains the standard advertising interval at 3202 until it has data to send, determined at 3201. Then, at 3203, the IoT device switches the advertising interval to indicate that it has data to transmit. At 3204, the IoT hub or other network device establishes a connection with the IoT device, thereby allowing the IoT device to transmit its data. Finally, at 3205, the IoT device transmits its pending data to the IoT hub.

[00225] It should be noted that while the advertising interval techniques are described herein within the context of the BTLE protocol, the underlying principles of the invention are not limited to BTLE. In fact, the underlying principles of the invention may be implemented on any system which selects an advertising interval for establishing wireless communication between devices.

[00226] In addition, while a dedicated IoT hub 110 is illustrated in many embodiments above, a dedicated IoT hub hardware platform is not required for complying with the underlying principles of the invention. For example, the various IoT hubs described above may be implemented as software executed within various other networking devices such as iPhones® and Android® devices. In fact, the IoT hubs described herein may be implemented on any device capable of communicating with IoT devices (e.g., using BTLE or other local wireless protocol) and establishing a connection over the Internet (e.g., to an IoT service using a WiFi or cellular data connection).

APPARATUS AND METHOD FOR OBSCURING WIRELESS COMMUNICATION PATTERNS

[00227] Even though the data transmitted between the IoT service and IoT devices is encrypted using the techniques described above, the wireless transactions between the IoT service and IoT devices may be collected and analyzed to determine user behavior. For example, as illustrated in **Figure 33**, the IoT service 120 may transmit a command 3302 to an IoT device at a specified point in time, t_0, to perform a particular function such as unlocking a door if the IoT device is a wireless door lock. As illustrated, the command may pass through the WAN interface 3321 and local wireless communication interface 3320 of the IoT hub 110 (or via a mobile device or other device implementing the IoT hub functionality). The application-specific program code 3315 on the IoT device 101 may then execute the command at 3303 and provide a response to the local

wireless communication module 3310 at a second time, t_1. The wireless communication module then transmits the response 3304 at t_2. In general, the timing between the command 3302 being transmitted over the wireless link, the execution of the command 3303, and the response 3304 transmitted back to the IoT service will all occur in a predictable fashion. For example, upon receipt of the command 3302, the application 3315 may generally take the same amount of time to execute the command and return the response 3304. Consequently, someone listening to wireless communication may be able to decipher the communication pattern to understand that the user is unlocking (or locking) his/her door, or performing various other device-specific functions.

[00228] To address these concerns, one embodiment of the invention performs techniques to obscure or obfuscate the communication patterns between the IoT device 101 and the IoT service 120. **Figure 34** illustrates one such embodiment in which the service program code 3321 and/or the local wireless communication interface 3310 of the IoT device 101 includes messaging obfuscation logic 3411, 3410 to implement the various techniques described herein. In particular, in one embodiment, upon receipt of the command 3302 at t_0, the application 3315 performs its application-specific function and provides the response at t_1. However, in contrast to the embodiment shown in **Figure 33**, in **Figure 34**, the messaging obfuscation logic 3410 introduces a timing delay for sending the response 3404. Thus, instead of sending the response at t_2, it sends the response at $t_2 + N$, where N may be randomly selected value within a specified range of time. In addition to changing the timing, in one embodiment, the messaging obfuscation logic 3410 may perform other techniques to obfuscate the response such as modifying the size of the response 3404 by a specified or random amount (e.g., adding M additional bytes to the response packet). In this manner, the transactions between the IoT service and IoT devices becomes less predictable than in prior embodiments.

[00229] **Figure 35** illustrates another embodiment for obfuscating communication between the IoT service 120 and IoT device 101. In this embodiment, the messaging obfuscation logic 3411 on the IoT service 120 transmits an obfuscation packet 3501 either before or after the command packet 3302. In the particular example shown in **Figure 35** it is transmitted before (i.e., at time t_x). In one embodiment, the obfuscation packet 3501 comprises an encrypted message which causes the messaging obfuscation logic 3410 on the IoT device 101 to transmit a reply message 3502 at some particular time in the future (e.g., 100ms, 200ms, etc; identified by the value L in **Figure 35**). The particular amount of time to wait before transmitting the reply 3502 may be

specified in the obfuscation packet 3501. Alternatively, the amount of time to wait may be specified by the messaging obfuscation logic 3410 on the IoT device 101. For example, the amount of time may be selected randomly by the messaging obfuscation logic 3411 on the IoT service 120 or by the messaging obfuscation logic 3410 on the IoT device 101. Randomizing the time at which the reply is sent makes it difficult for a hacker to discriminate between real traffic 2602, 2604 and the obfuscation traffic 2801, 2802 (which is essentially NO-OP traffic). As illustrated, the messaging obfuscation logic 2710 on the IoT device 101 may still implement a random delay for transmitting the actual response 2604, to further obfuscate the traffic.

[00230] In addition, in one embodiment, the obfuscation packet 2801 may instruct the messaging obfuscation logic 2710 on the IoT device 101 to transmit one or more decoy advertisement packets 2804. IoT devices which use the secure BTLE techniques described above perform “advertising” where, at some programmable interval, they send an RF "chirp" indicating that they are available. Anyone can listen and hear this advertisement packet. As part of the advertisement, a bit is used to indicate that the IoT device has data for the IoT service 120 to read. Thus, when the IoT service 120 sends an obfuscation packet 2801, it can also request that the device send a decoy advertisement at some programmable time in the future. This additional feature makes it difficult for a hacker listening in to advertisements (which are in the clear) to discriminate between real ones and decoys.

[00231] In one embodiment, the various obfuscation techniques described above are programmable based on a set of obfuscation rules 2712 in the IoT device 101 and obfuscation rules 2713 in the IoT service 120. The rules 2712 may specify, for example, the specific timing to be used for obfuscation packets 2801, replies 2802, and decoy advertisements 2804. In one embodiment, the rules 2712, 2713 specify the behavior of the messaging obfuscation logic 2710, 2711 in accordance with current state variables 2720, 2721, respectively, of the system. The current state variables 2720, 2721 may include high level factors such as the type of IoT device 101 for which communication is being obfuscated, the current battery level of the IoT device 101, the time of day, the current weather, etc. For example, certain IoT devices 101 may not inherently generate predictable, periodic communication patterns. For such IoT devices, the obfuscation techniques described herein may be set to a minimum. Moreover, if the battery life of an IoT device 101 is low (e.g., below a threshold), then the fewer obfuscation packets 2801 and decoy advertisements 2804 may be generated

to preserve battery life. Of course, various different types of rules may be specified while still complying with the underlying principles of the invention.

[00232] A method in accordance with one embodiment of the invention is illustrated in **Figure 29**. The method may be implemented within the context of the system architectures described above but is not limited to any specific system architectures.

[00233] At 2900, an IoT device receives a command from the IoT service and, at 2901, executes the command. At 2902, messaging obfuscation logic adjusts the timing of the response. As mentioned, this may be accomplished by inserting a random or preselected timing delay. At 2903, the IoT device transmits the response in accordance with the adjusted timing.

[00234] Another method in accordance with one embodiment is illustrated in Figure 30. At 3000, the IoT service transmits a command to the IoT device (e.g., a command to unlock a door). At 3001, the IoT service transmits an obfuscation packet to the IoT device. As mentioned, the obfuscation packet may be transmitted before or after the command. At 3002, the IoT device executes the command (e.g., unlocks the door) and transmits the response. In one embodiment, a timing delay may be used for the response (e.g., as described with respect to **Figure 29**). At 3003, the IoT device transmits the obfuscation response to the obfuscation packet. In one embodiment, the obfuscation packet indicates the timing to be used for the response. In another embodiment, the IoT device determines the timing for the response (e.g., selecting a random amount of time within a specified range). The obfuscation response may be sent before or after the response to the command, depending on the timing selected. At 3004, the IoT device transmits a decoy advertisement in response to the obfuscation packet. The decoy advertisement may be transmitted alone or in addition to the transmission of the obfuscation response.

[00235] **Figure 24** illustrates one embodiment of an IoT device 101 in which the BTLE communication interface 2410 includes advertising interval selection logic 2411 which adjusts the advertising interval when data is ready to be transmitted. In addition, the BTLE communication interface 2420 on the IoT hub 110 includes advertising interval detection logic 2421 to detect the change in the advertising interval, provide an acknowledgement, and receive the data.

[00236] In particular, in the illustrated embodiment, an application 2401 on the IoT device 101 indicates that it has data to be sent. In response, the advertising interval selection logic 2411 modifies the advertising interval to notify the IoT hub 110 that data is to be transmitted (e.g., changing the interval to .75T or some other value). When the

advertising interval detection logic 2421 detects the change, the BTLE communication interface 2420 connects to the BTLE communication interface 2410 of the IoT device 101, indicating that it is ready to receive the data. The BTLE communication interface 2410 of the IoT device 101 then transmits the data to the BTLE communication interface 2420 of the IoT hub. The IoT hub may then pass the data through to the IoT service 120 and/or to the user's client device (not shown). After the data has been transmitted, the advertising interval selection logic 2411 may then revert back to the normal advertising interval (e.g., AI=T).

[00237] In one embodiment of the invention, a secure communication channel is established between the IoT device 101 and the IoT service 120 using one or more of the security/encryption techniques described above (see, e.g., **Figures 16A-23C** and associated text). For example, in one embodiment, the IoT service 120 performs a key exchange with the IoT device 101 as described above to encrypt all communication between the IoT device 101 and the IoT service 120.

[00238] A method in accordance with one embodiment of the invention is illustrated in **Figure 25**. The method may be implemented within the context of the system architectures described above, but is not limited to any particular system architectures.

[00239] At 2500, the IoT device uses the standard advertising interval when generating advertising packets (e.g., separated by time T). The IoT device maintains the standard advertising interval at 2502 until it has data to send, determined at 2501. Then, at 2503, the IoT device switches the advertising interval to indicate that it has data to transmit. At 2504, the IoT hub or other network device establishes a connection with the IoT device, thereby allowing the IoT device to transmit its data. Finally, at 2505, the IoT device transmits its pending data to the IoT hub.

CLAIMS

What is claimed is:

1. A method to establish a secondary communication channel between an Internet of Things (IoT) device and a client device comprising:

establishing a primary secure communication channel between the IoT device and an IoT service using a primary set of keys;

performing a secondary key exchange using the primary secure communication channel, the client device and the IoT device each being provided with a secondary set of keys following the secondary key exchange;

detecting that the primary secure communication channel is inoperative; and

responsively establishing a secondary secure wireless connection between the client device and the IoT device using the secondary set of keys, the client device being provided with access to data and/or functions made available by the IoT device over the secondary secure wireless connection.

2. The method as in claim 1 wherein the access to data and/or functions over the secondary secure wireless connection comprises more limited access to the data and/or functions than when connected over the primary secure communication channel.

3. The method as in claim 1 further comprising:

storing a passcode on the IoT device;

requesting a user to enter the passcode from the client device; and

providing access to the data and/or functions of the IoT device only if the user enters the correct passcode from the wireless device.

4. The method as in claim 3 further comprising:

initially receiving the passcode from an app on the client device prior to storing the passcode on the IoT device, the user choosing the passcode and the passcode being transmitted to the IoT device over the primary secure communication channel.

5. The method as in claim 4 further comprising:

executing the app on the client device to prompt the user to enter the passcode upon establishing the secondary secure wireless connection, the passcode being transmitted from the app to the IoT device prior to the IoT device providing access to the data and/or functions.

6. The method as in claim 5 wherein the IoT device comprises a wireless door lock and wherein at least one function to be accessed over the secondary secure communication channel comprises unlocking the door lock.

7. The method as in claim 1 wherein establishing a primary secure communication channel between the IoT device and an IoT service using a primary set of keys comprises:

establishing communication between the IoT service and the IoT device through an IoT hub or a client device;

generating a service public key and a service private key by key generation logic of a first encryption engine on the IoT service;

generating a device public key and a device private key by key generation logic of a second encryption engine on the IoT device;

transmitting the service public key from the first encryption engine to the second encryption engine and transmitting the device public key from the second encryption engine to the first encryption engine;

generating a secret using the device public key and the service private key;

generating the same secret using the service public key and the device private key; and

encrypting and decrypting data packets transmitted between the first encryption engine and the second encryption engine using the secret or using data structures derived from the secret.

8. The method as in claim 7 wherein the key generation logic comprises a hardware security module (HSM).

9. The method as in claim 8 wherein the data structures derived from the secret comprise a first key stream generated by the first encryption engine and a second key stream generated by the second encryption engine.

10. The method as in claim 9 wherein a first counter is associated with the first encryption engine and a second counter is associated with the second encryption engine, the first encryption engine incrementing the first counter responsive to each data packet transmitted to the second encryption engine and the second encryption

engine incrementing the second counter responsive to each data packet transmitted to the first encryption engine.

11. The method as in claim 10 wherein the first encryption engine generates the first key stream using a current counter value of the first counter and the secret and the second encryption engine generates the second key stream using a current counter value of the second counter and the secret.

12. The method as in claim 11 wherein the first encryption engine comprises an elliptic curve method (ECM) module to generate the first key stream using the first counter value and the secret and the second encryption engine comprises an ECM module to generate the second key stream using the first counter value and the secret.

13. The method as in claim 11 wherein the first encryption engine encrypts a first data packet using the first key stream to generate a first encrypted data packet and transmits the first encrypted data packet to the second encryption engine along with a current counter value of the first counter.

14. The method as in claim 13 wherein the second encryption engine uses the current counter value of the first counter and the secret to generate the first key stream and uses the first key stream to decrypt the encrypted data packet.

15. A system comprising:

an IoT device to establish a primary secure communication channel with an IoT service using a primary set of keys;

the IoT device to perform a secondary key exchange using the primary secure communication channel;

a client device and the IoT device each being provided with a secondary set of keys following the secondary key exchange;

the IoT device and/or client device to detect that the primary secure communication channel is inoperative; and

the IoT device and/or client device to responsively establish a secondary secure wireless connection between the client device and the IoT device using the secondary set of keys;

the client device being provided with access to data and/or functions made available by the IoT device over the secondary secure wireless connection.

16. The system as in claim 15 wherein the access to data and/or functions over the secondary secure wireless connection comprises more limited access to the data and/or functions than when connected over the primary secure communication channel.

17. The system as in claim 15 further comprising:

an authentication module to store a passcode on the IoT device and to prompt a user to enter the passcode from the client device;

the authentication module providing access to the data and/or functions of the IoT device only if the user enters the correct passcode from the wireless device.

18. The system as in claim 17 wherein the passcode is initially received from an an app on the client device prior to storing the passcode on the IoT device, the user choosing the passcode and the passcode being transmitted to the IoT device over the primary secure communication channel.

19. The system as in claim 18 further comprising:

the app executed on the client device to prompt the user to enter the passcode upon establishing the secondary secure wireless connection, the passcode being transmitted from the app to the IoT device prior to the IoT device providing access to the data and/or functions.

20. The system as in claim 19 wherein the IoT device comprises a wireless door lock and wherein at least one function to be accessed over the secondary secure communication channel comprises locking or unlocking the door lock.

21. The system as in claim 15 wherein establishing a primary secure communication channel between the IoT device and an IoT service using a primary set of keys comprises:

the IoT service establishing communication with the IoT device through an IoT hub or a client device;

a first encryption engine on the IoT service comprising key generation logic to generate a service public key and a service private key;

a second encryption engine on the IoT device comprising key generation logic to generate a device public key and a device private key;

the first encryption engine to transmit the service public key to the second encryption engine and the second encryption engine to transmit the device public key to the first encryption engine;

the first encryption engine to use the device public key and the service private key to generate a secret;

the second encryption engine to use the service public key and the device private key to generate the same secret; and

wherein once the secret is generated, the first encryption engine and the second encryption engine encrypt and decrypt data packets transmitted between the first encryption engine and the second encryption engine using the secret or using data structures derived from the secret.

22. The system as in claim 21 wherein the key generation logic comprises a hardware security module (HSM).

23. The system as in claim 22 wherein the data structures derived from the secret comprise a first key stream generated by the first encryption engine and a second key stream generated by the second encryption engine.

24. The system as in claim 23 further comprising a first counter associated with the first encryption engine and a second counter associated with the second encryption engine, the first encryption engine incrementing the first counter responsive to each data packet transmitted to the second encryption engine and the second encryption engine incrementing the second counter responsive to each data packet transmitted to the first encryption engine.

25. A system comprising:

an Internet of Things (IoT) device comprising a wireless communication interface to establish communication with an IoT service;

the IoT device including an application to execute commands received from the IoT service and to responsively generate a response; and

messaging obfuscation logic to modify timing for transmitting the response to the IoT service.

26. The system as in claim 25 wherein the messaging obfuscation logic modifies the timing for transmitting the response by introducing a variable delay in the response.

27. The system as in claim 26 wherein the messaging obfuscation logic generates a random delay to be used for the variable delay for each response.

28. The system as in claim 25 further comprising:

an IoT hub or mobile device to communicatively couple the IoT device to the IoT service, the IoT device to establish a local wireless connection to the IoT hub or mobile device using the wireless communication interface and the IoT hub to establish a connection to the IoT service over the Internet.

29. The system as in claim 25 further comprising:

service-side messaging obfuscation logic executed on the IoT service, the service-side messaging obfuscation logic to transmit one or more obfuscation packets to the IoT device and, in response to the obfuscation packets, the messaging obfuscation logic on the IoT device to generate an obfuscation reply at a specified point in time.

30. The system as in claim 29 wherein each obfuscation packet transmitted by the service-side messaging obfuscation logic includes timing data indicating a point in time at which the obfuscation reply is to be sent.

31. The system as in claim 30 wherein the service-side messaging obfuscation logic comprises a set of obfuscation rules to determine when obfuscation packets are to be transmitted and to generate the timing data.

32. The system as in claim 31 wherein the service-side messaging obfuscation logic generates randomly-selected timing data within a specified range, the randomly-selected timing data resulting in randomly transmitted obfuscation replies from the IoT device.

33. The system as in claim 29 wherein the messaging obfuscation logic on the IoT device is to transmit one or more decoy advertisements responsive to one or more of the obfuscation packets transmitted from the service-side messaging obfuscation logic.

34. A system comprising:

an Internet of Things (IoT) device comprising a wireless communication interface to establish communication with an IoT service;

the IoT device including an application to execute commands received from the IoT service and to responsively generate a response; and

service-side messaging obfuscation logic executed on the IoT service, the service-side messaging obfuscation logic to transmit one or more obfuscation packets to the IoT device and, in response to the obfuscation packets, the IoT device to generate an obfuscation reply at a specified point in time.

35. The system as in claim 34 wherein each obfuscation packet transmitted by the service-side messaging obfuscation logic includes timing data indicating a point in time at which the obfuscation reply is to be sent.

36. The system as in claim 35 wherein the service-side messaging obfuscation logic comprises a set of obfuscation rules to determine when obfuscation packets are to be transmitted and to generate the timing data.

37. The system as in claim 36 wherein the service-side messaging obfuscation logic generates randomly-selected timing data within a specified range, the randomly-selected timing data resulting in randomly transmitted obfuscation replies from the IoT device.

38. The system as in claim 34 wherein the messaging obfuscation logic on the IoT device is to transmit one or more decoy advertisements responsive to one or more of the obfuscation packets transmitted from the service-side messaging obfuscation logic.

39. The system as in claim 36 wherein the obfuscation rules specify generating obfuscation packets and/or setting timing data based on current state variables associated with the IoT device.

40. The system as in claim 39 wherein the current state variables include a current battery level of the IoT device and/or an indication of an IoT device type.

41. The system as in claim 40 wherein for relatively lower battery levels and/or for certain types of IoT devices, the service-side messaging obfuscation logic is to transmit relatively fewer obfuscation packets.

42. A method comprising:

transmitting a command from an Internet of Things (IoT) service to an IoT device;

transmitting an obfuscation packet from the IoT service to the IoT device;

executing the command on the IoT device to generate a result;

transmitting the result from the IoT device to the IoT service; and

transmitting an obfuscation reply from the IoT device to the IoT service.

43. The method as in claim 42 further comprising:

determining a first amount of time to wait prior to transmitting the obfuscation reply; and

transmitting the obfuscation reply after waiting the first amount of time.

44. The method as in claim 43 wherein the first amount of time is specified within the obfuscation packet transmitted from the IoT service.

45. A system comprising:

an Internet of Things (IoT) device comprising a first wireless networking interface to establish communication with an IoT hub over a local wireless network channel, the first wireless networking interface implementing a first advertising interval between advertising packets; and

advertising interval selection logic to cause the first wireless networking interface to use a second advertising interval for advertising packets upon detecting that the IoT device has data to be transmitted to the IoT hub, the IoT hub to detect that the IoT device has data to be transmitted based on the change to the second advertising interval.

46. The system as in claim 45 wherein the first advertising interval comprises a first amount of time, T, and wherein the second advertising interval comprises a second amount of time, T/*n*, where *n* is a positive value.

47. The system as in claim 45 wherein the wireless networking interface comprises a Bluetooth Low Energy (BTLE) interface, the local wireless network channel comprises a BTLE channel, and wherein the first advertising interval comprises a standard BTLE advertising interval.

48. The system as in claim 45 wherein the IoT hub comprises a second wireless networking interface comprising advertising interval detection logic to detect the second advertising interval indicating that the IoT device has data to be transmitted.

49. The system as in claim 48 wherein, upon detecting the second advertising interval, the second wireless networking interface is to transmit an indication to the first wireless networking interface that it may transmit the data.

50. The system as in claim 49 wherein, upon receipt of the indication, the first wireless networking interface transmits the data to the second wireless networking interface.

51. The system as in claim 50 further comprising:

an IoT service communicatively coupled to the IoT hub over the Internet, the IoT service to establish a secure communication channel with the IoT device through the IoT hub, wherein the IoT hub transmits the data received from the IoT device to the IoT service.

52. The system as in claim 51 further comprising:

a first encryption engine on the IoT service comprising key generation logic to generate a service public key and a service private key;

a second encryption engine on the IoT device comprising key generation logic to generate a device public key and a device private key;

the first encryption engine to transmit the service public key to the second encryption engine and the second encryption engine to transmit the device public key to the first encryption engine;

the first encryption engine to use the device public key and the service private key to generate a secret;

the second encryption engine to use the service public key and the device private key to generate the same secret; and

wherein once the secret is generated, the first encryption engine and the second encryption engine encrypt and decrypt data packets transmitted between the first encryption engine and the second encryption engine using the secret or using data structures derived from the secret.

53. The system as in claim 52 wherein the key generation logic comprises a hardware security module (HSM).

54. The system as in claim 52 wherein the data structures derived from the secret comprise a first key stream generated by the first encryption engine and a second key stream generated by the second encryption engine.

55. The system as in claim 54 further comprising a first counter associated with the first encryption engine and a second counter associated with the second encryption engine, the first encryption engine incrementing the first counter responsive to each data packet transmitted to the second encryption engine and the second encryption engine incrementing the second counter responsive to each data packet transmitted to the first encryption engine.

56. The system as in claim 55 wherein the first encryption engine generates the first key stream using a current counter value of the first counter and the secret and the second encryption engine generates the second key stream using a current counter value of the second counter and the secret.

57. The system as in claim 56 wherein the first encryption engine comprises an elliptic curve method (ECM) module to generate the first key stream using the first counter value and the secret and the second encryption engine comprises an ECM module to generate the second key stream using the first counter value and the first secret.

58. The system as in claim 56 wherein the first encryption engine encrypts a first data packet using the first key stream to generate a first encrypted data packet and transmits the first encrypted data packet to the second encryption engine along with a current counter value of the first counter.

59. The system as in claim 58 wherein the second encryption engine uses the current counter value of the first counter and the secret to generate the first key stream and uses the first key stream to decrypt the encrypted data packet.

60. A method comprising:

selecting a first advertising interval for an Internet of Things (IoT) device, the first advertising interval specifying timing for the transmission of advertising packets;

detecting that the IoT device has data to transmit to an IoT hub;

dynamically modifying the advertising interval to a second advertising interval, the second advertising interval notifying the IoT hub that the IoT device has data to transmit;

receiving an indication from the IoT hub to transmit the data from the IoT device; and

transmitting the data from the IoT device.

61. The method as in claim 60 wherein the first advertising interval comprises a first amount of time, T, and wherein the second advertising interval comprises a second amount of time, T/*n*, where *n* is a positive value.

62. The method as in claim 60 wherein the first and second advertising intervals comprise Bluetooth Low Energy (BTLE) advertising intervals.

63. The method as in claim 60 wherein the IoT device comprises a first BTLE network interface to transmit advertising packets according to the first and second advertising intervals and the IoT hub comprises a second BTLE network interface to

detect the advertising packets transmitted according to the first and second advertising intervals.

64. The method as in claim 63 wherein, upon detecting the second advertising interval, the second wireless networking interface is to transmit an indication to the first wireless networking interface that it may transmit the data.

65. The method as in claim 64 wherein, upon receipt of the indication, the first wireless networking interface transmits the data to the second wireless networking interface.

66. The method as in claim 65 further comprising:

communicatively coupling an IoT service to the IoT hub over the Internet, the IoT service to establish a secure communication channel with the IoT device through the IoT hub, wherein the IoT hub transmits the data received from the IoT device to the IoT service.

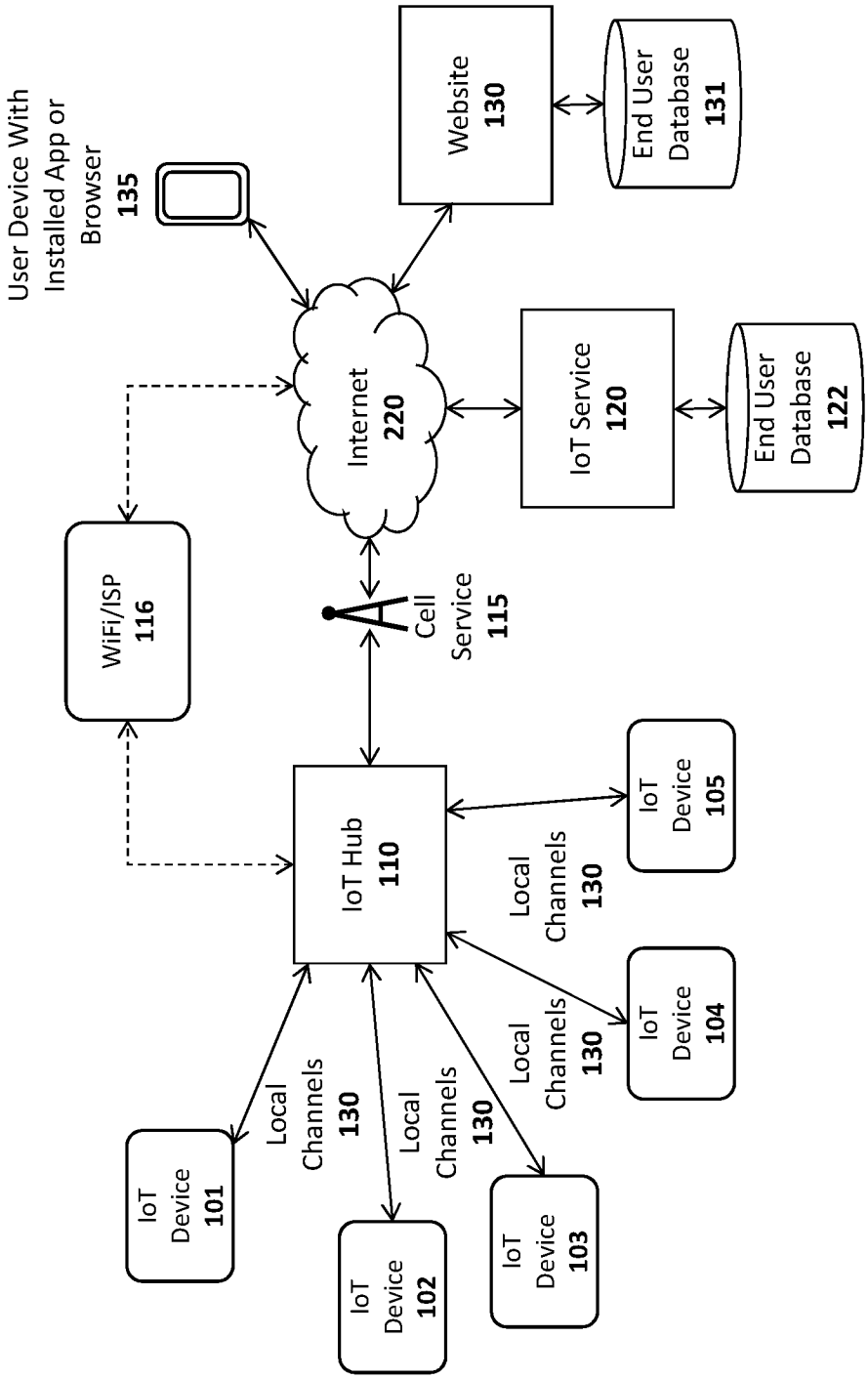
User Device With Installed App or Browser 135
Website 130
End User Database 131
Internet 220
IoT Service 120
End User Database 122
WiFi/ISP 116
Cell Service 115
IoT Hub 110
IoT Device 101
IoT Device 102
IoT Device 103
IoT Device 104
IoT Device 105
Local Channels 130
Local Channels 130
Local Channels 130
Local Channels 130

FIG. 1A

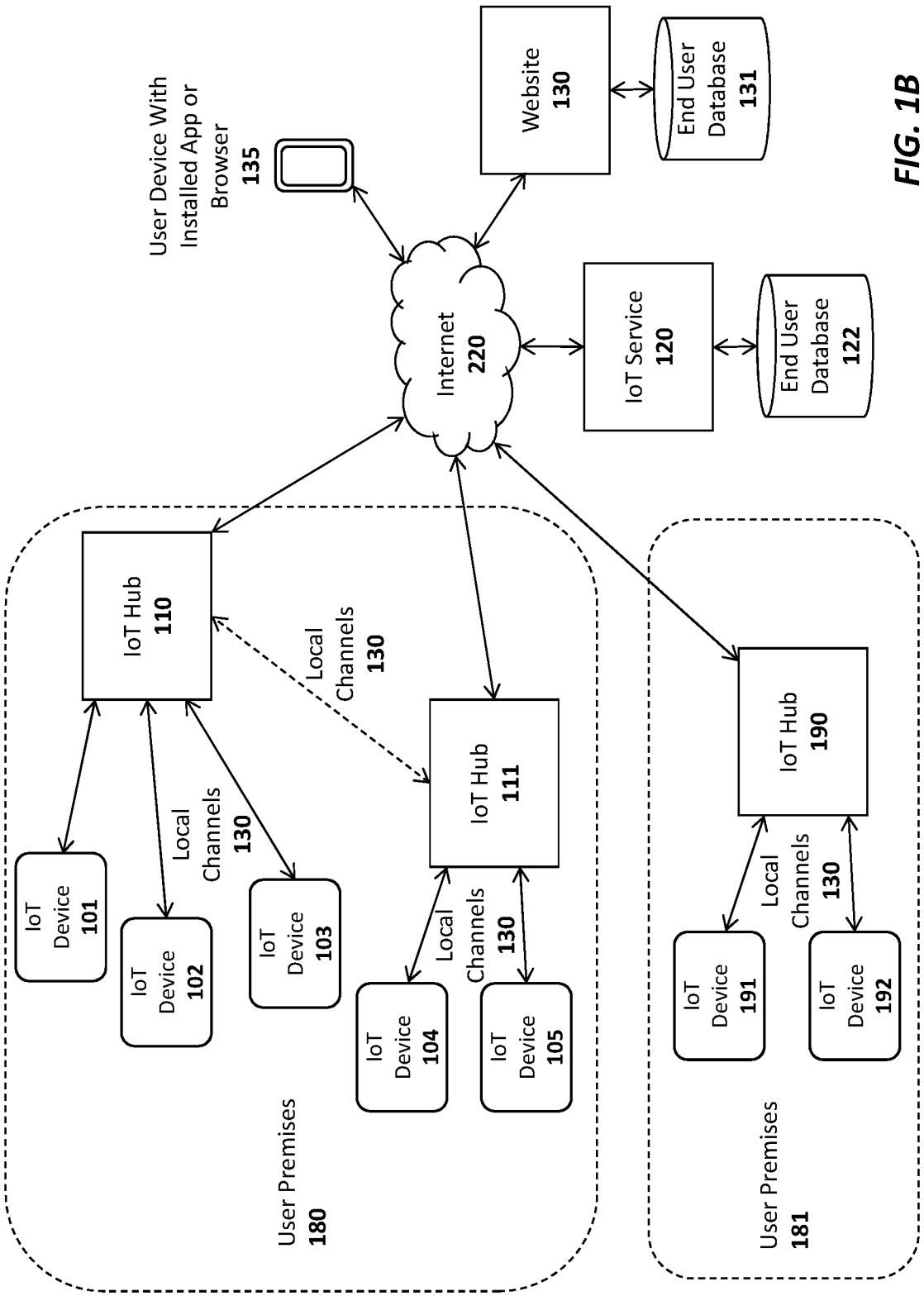
User Device With Installed App or Browser 135
Website 130
End User Database 131
Internet 220
IoT Service 120
End User Database 122
IoT Hub 110
Local Channels 130
IoT Hub 111
IoT Hub 190
IoT Device 101
IoT Device 102
IoT Device 103
IoT Device 104
IoT Device 105
IoT Device 191
IoT Device 192
User Premises 180
User Premises 181

FIG. 1B

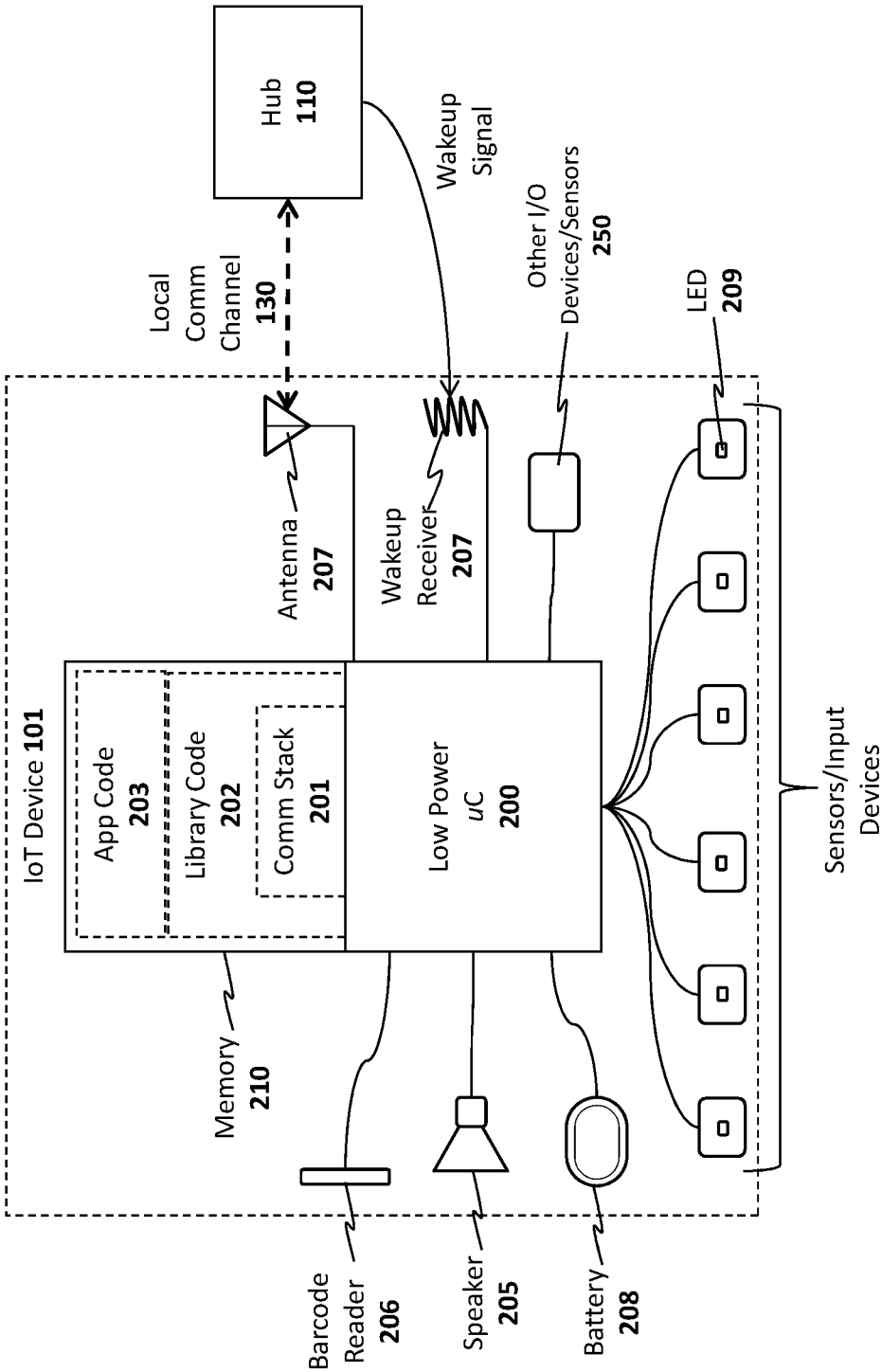
Hub
110
Wakeup
Signal
Local
Comm
Channel
130
Other I/O
Devices/Sensors
250
LED
209
Antenna
207
Wakeup
Receiver
207
IoT Device 101
App Code
203
Library Code
202
Comm Stack
201
Low Power
uC
200
Sensors/Input
Devices
210
Memory
210
Barcode
Reader
206
Speaker
205
Battery
208

FIG. 2

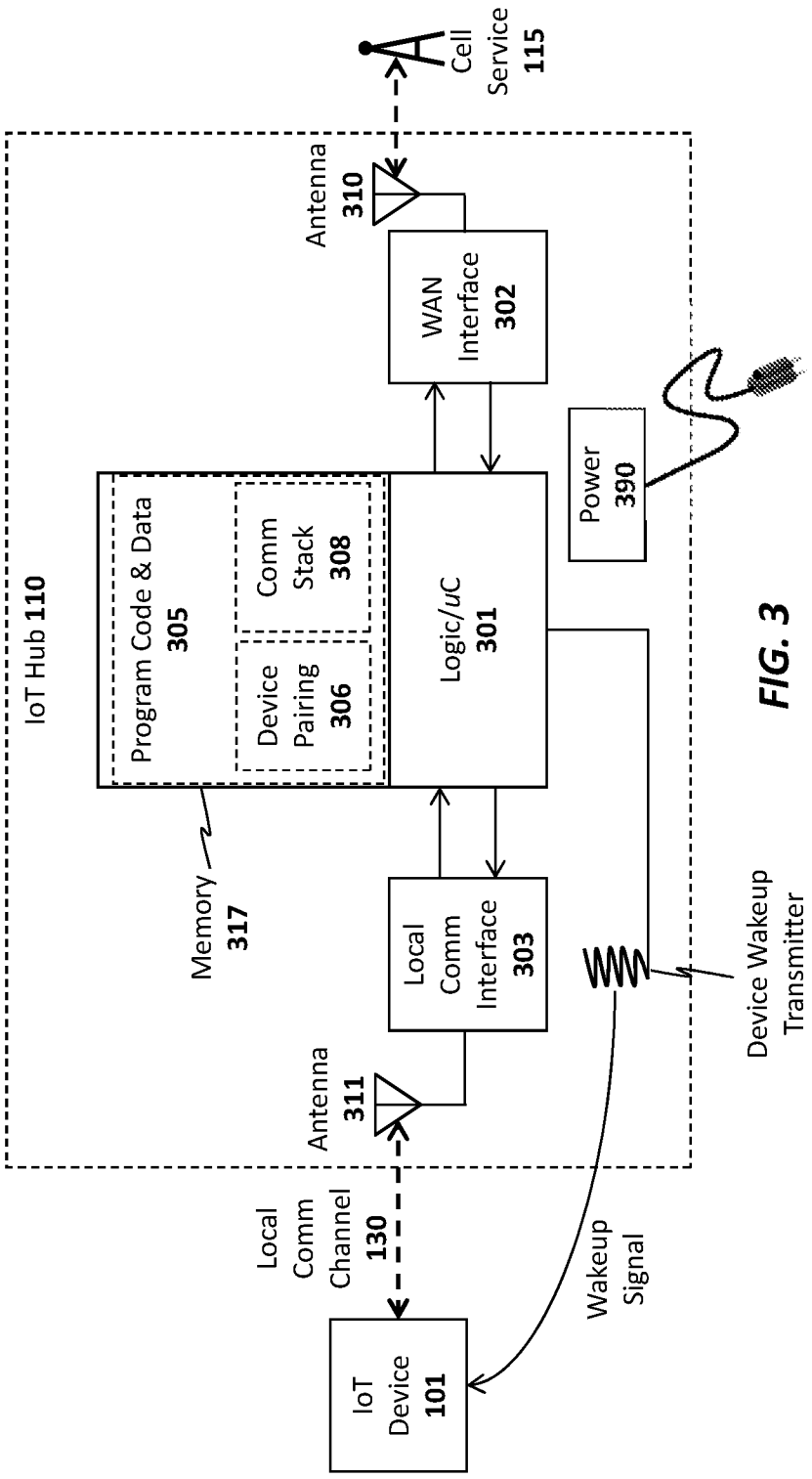
Cell Service 115
Antenna 310
WAN Interface 302
Power 390
IoT Hub 110
Program Code & Data 305
Comm Stack 308
Device Pairing 306
Logic/uC 301
Memory 317
Local Comm Interface 303
Device Wakeup Transmitter 307
Antenna 311
Local Comm Channel 130
Wakeup Signal
IoT Device 101

FIG. 3

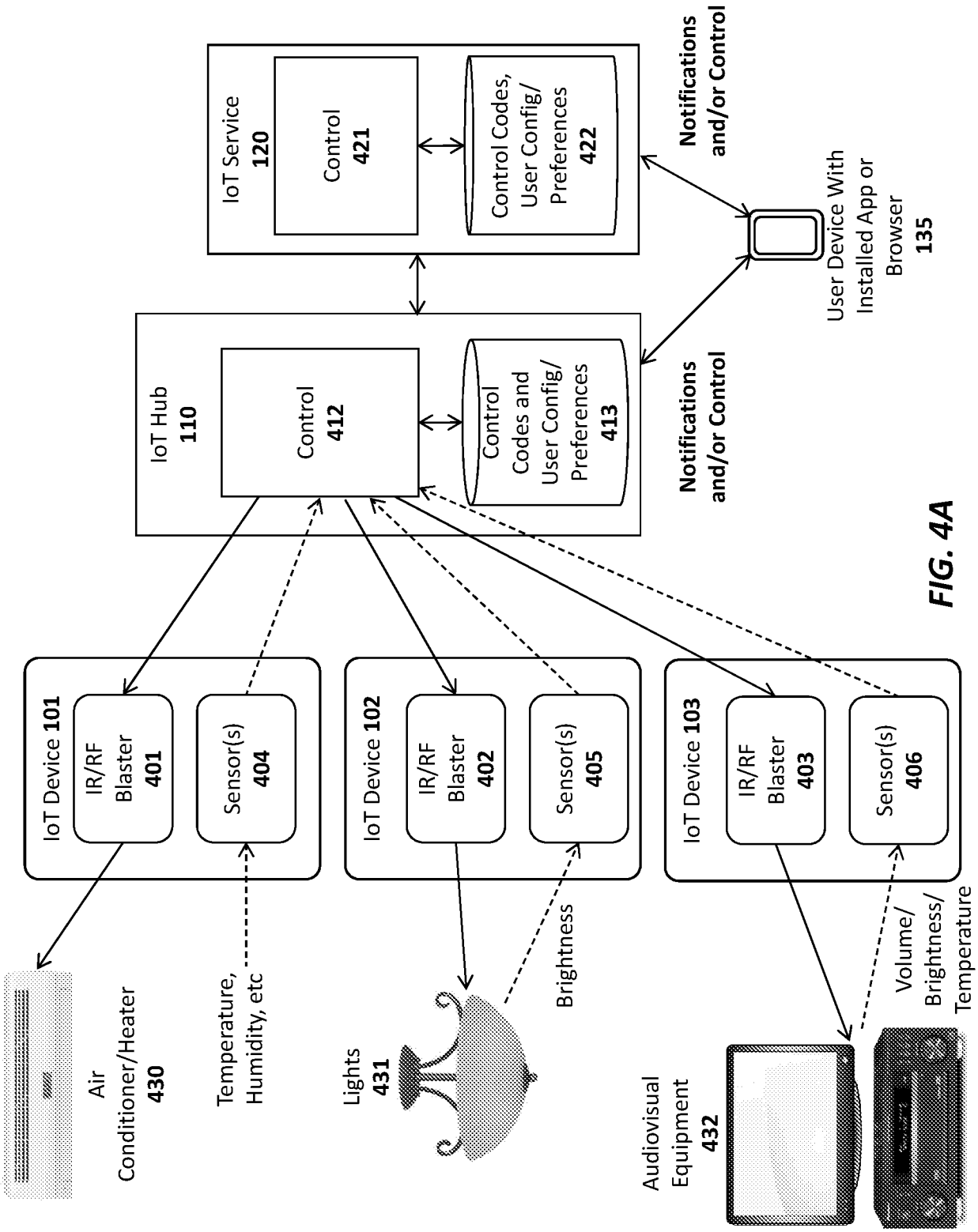
IoT Service
120
Control
421
Control Codes,
User Config/
Preferences
422
Notifications
and/or Control
User Device With
Installed App or
Browser
135
IoT Hub
110
Control
412
Control
Codes and
User Config/
Preferences
413
Notifications
and/or Control
IoT Device 101
IR/RF
Blaster
401
Sensor(s)
404
IoT Device 102
IR/RF
Blaster
402
Sensor(s)
405
IoT Device 103
IR/RF
Blaster
403
Sensor(s)
406
Air
Conditioner/Heater
430
Temperature,
Humidity, etc
Lights
431
Brightness
Audiovisual
Equipment
432
Volume/
Brightness/
Temperature

FIG. 4A

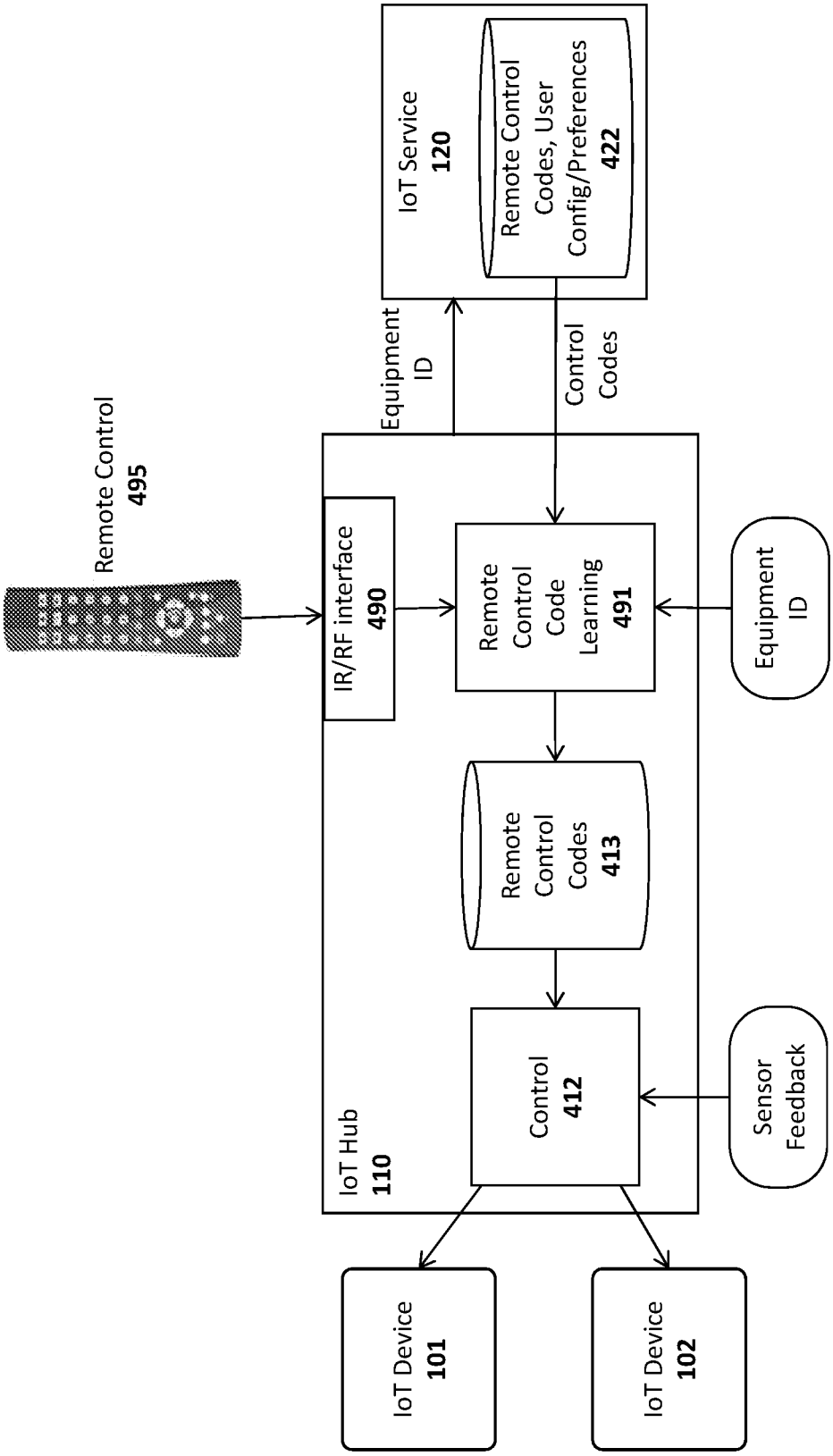
IoT Service
120
Remote Control Codes, User Config/Preferences
422
Equipment ID
Control Codes
Remote Control
495
IR/RF interface
490
Remote Control Code Learning
491
Equipment ID
Remote Control Codes
413
Control
412
Sensor Feedback
IoT Hub
110
IoT Device
101
IoT Device
102

FIG. 4B

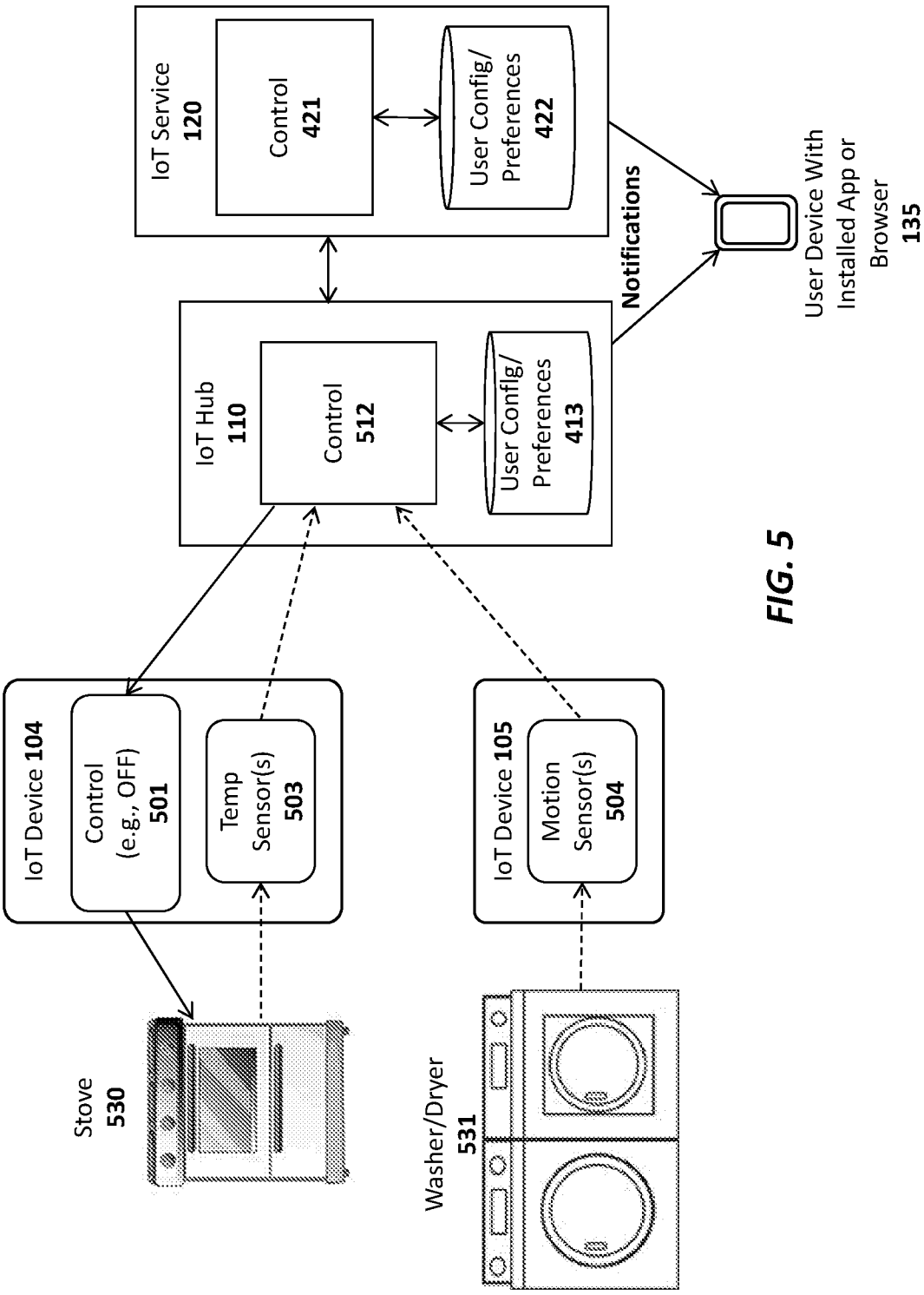
IoT Service
120
Control
421
User Config/
Preferences
422
Notifications
User Device With
Installed App or
Browser
135
IoT Hub
110
Control
512
User Config/
Preferences
413
IoT Device 104
Control
(e.g., OFF)
501
Temp
Sensor(s)
503
IoT Device 105
Motion
Sensor(s)
504
Stove
530
Washer/Dryer
531

FIG. 5

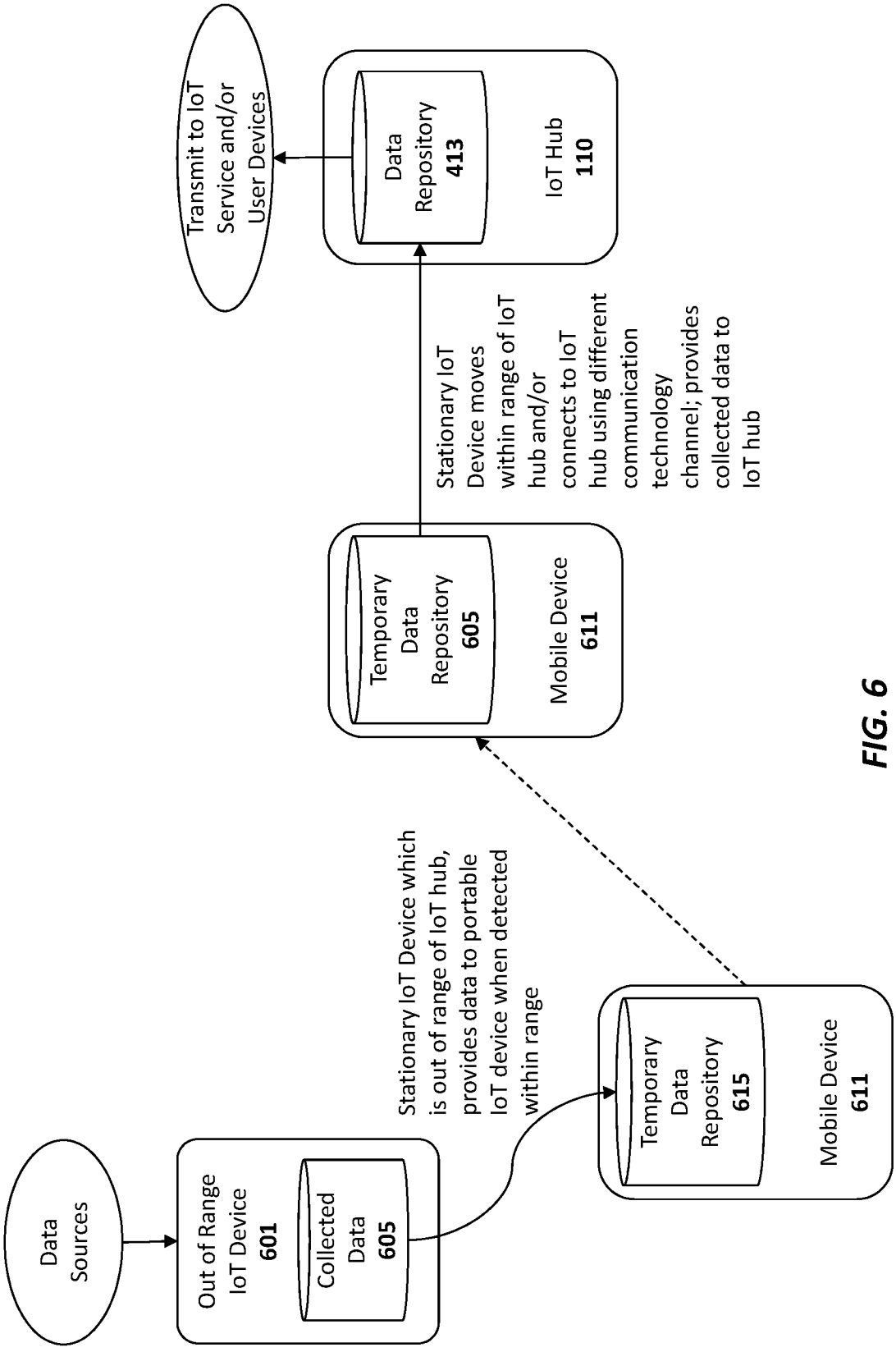
Data Sources
Out of Range IoT Device 601
Collected Data 605
Stationary IoT Device which is out of range of IoT hub, provides data to portable IoT device when detected within range
Temporary Data Repository 615
Mobile Device 611
Temporary Data Repository 605
Mobile Device 611
Stationary IoT Device moves within range of IoT hub and/or connects to IoT hub using different communication technology channel; provides collected data to IoT hub
Data Repository 413
IoT Hub 110
Transmit to IoT Service and/or User Devices

FIG. 6

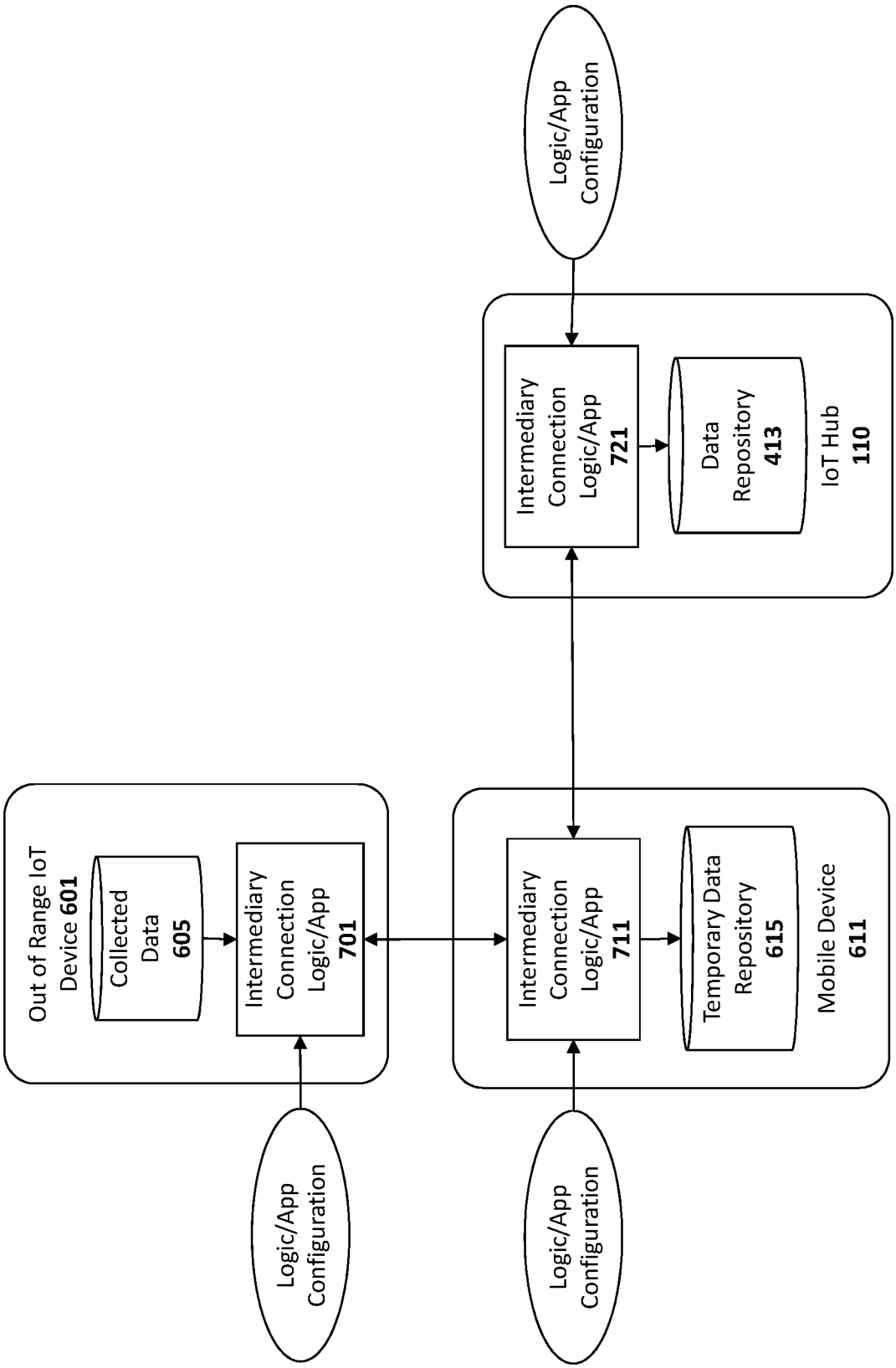
Logic/App Configuration
Intermediary Connection Logic/App 721
Data Repository 413
IoT Hub 110
Out of Range IoT Device 601
Collected Data 605
Intermediary Connection Logic/App 701
Intermediary Connection Logic/App 711
Temporary Data Repository 615
Mobile Device 611
Logic/App Configuration
Logic/App Configuration

FIG. 7

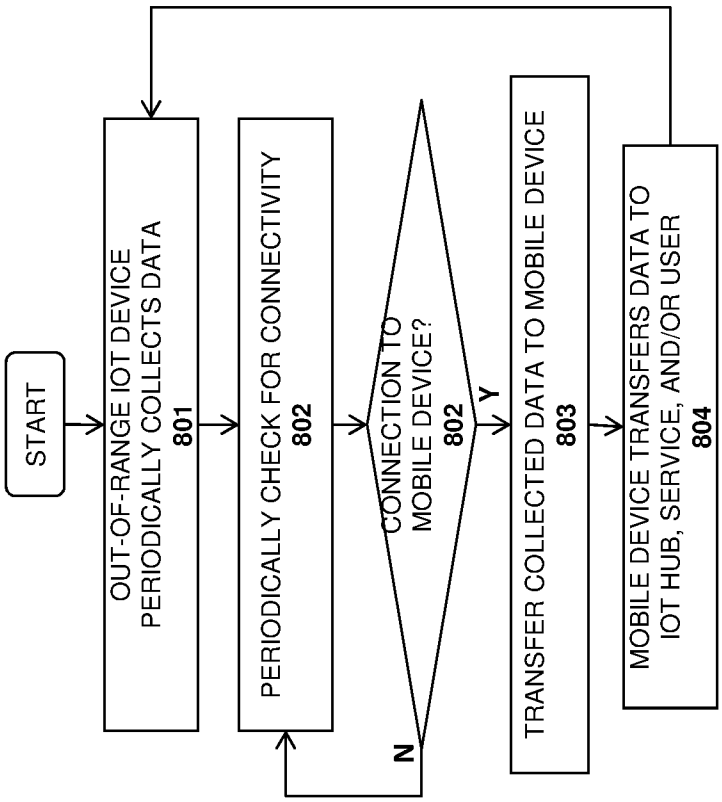
START
OUT-OF-RANGE IOT DEVICE PERIODICALLY COLLECTS DATA
801
PERIODICALLY CHECK FOR CONNECTIVITY
802
CONNECTION TO MOBILE DEVICE?
802
Y
N
TRANSFER COLLECTED DATA TO MOBILE DEVICE
803
MOBILE DEVICE TRANSFERS DATA TO IOT HUB, SERVICE, AND/OR USER
804

FIG. 8

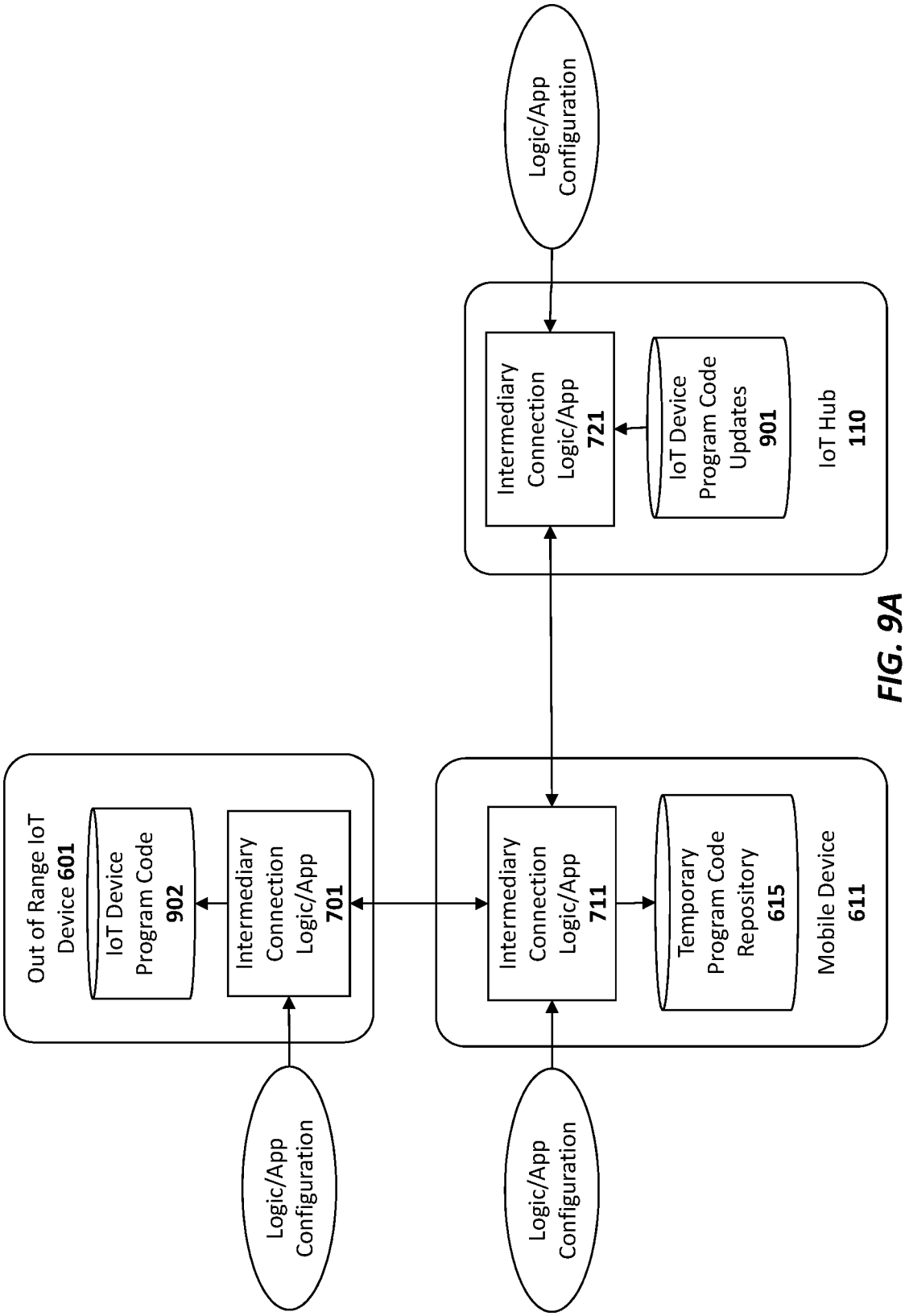
Logic/App Configuration
Intermediary Connection Logic/App 721
IoT Device Program Code Updates 901
IoT Hub 110
Out of Range IoT Device 601
IoT Device Program Code 902
Intermediary Connection Logic/App 701
Intermediary Connection Logic/App 711
Temporary Program Code Repository 615
Mobile Device 611
Logic/App Configuration
Logic/App Configuration

FIG. 9A

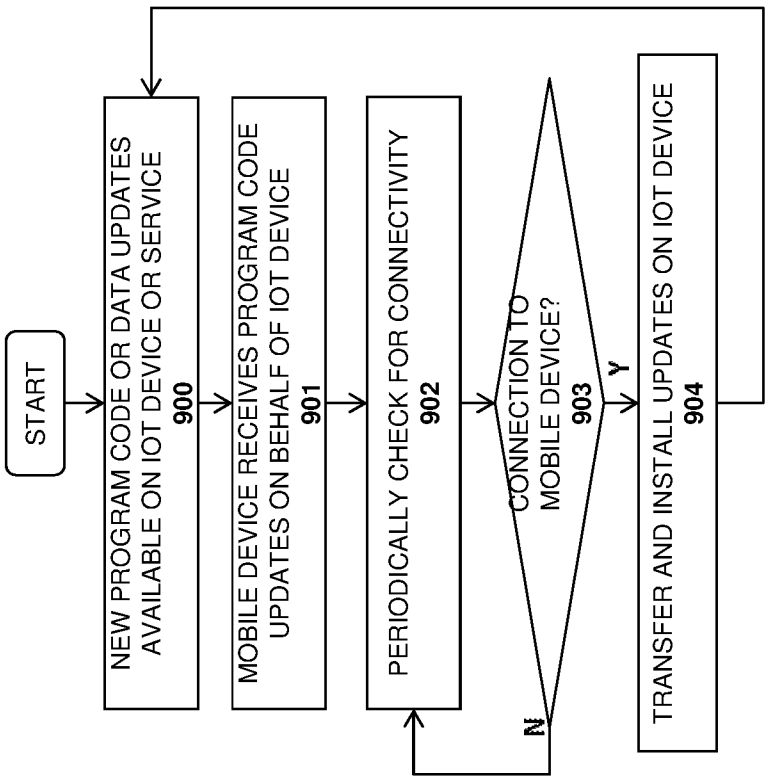
START
NEW PROGRAM CODE OR DATA UPDATES AVAILABLE ON IOT DEVICE OR SERVICE
900
MOBILE DEVICE RECEIVES PROGRAM CODE UPDATES ON BEHALF OF IOT DEVICE
901
PERIODICALLY CHECK FOR CONNECTIVITY
902
CONNECTION TO MOBILE DEVICE?
903
Y
N
TRANSFER AND INSTALL UPDATES ON IOT DEVICE
904

FIG. 9B

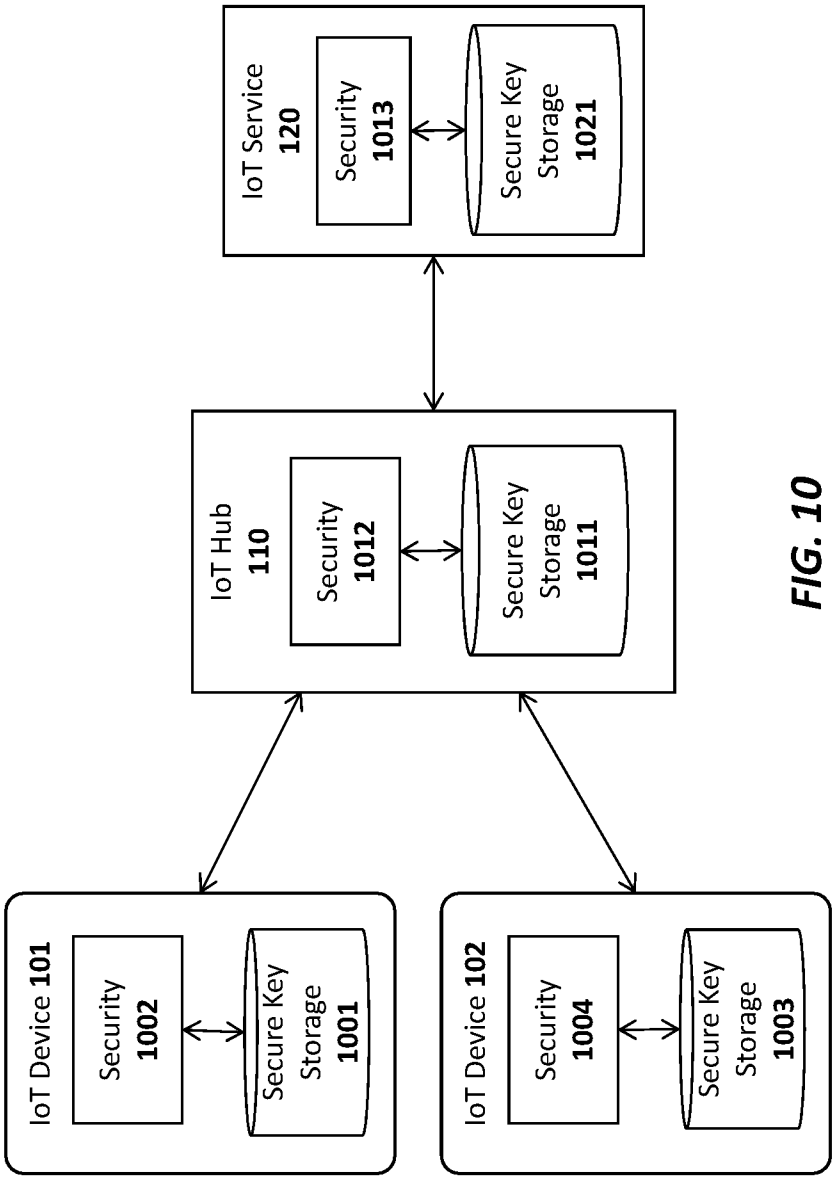
IoT Service
120
Security
1013
Secure Key
Storage
1021
IoT Hub
110
Security
1012
Secure Key
Storage
1011
IoT Device 101
Security
1002
Secure Key
Storage
1001
IoT Device 102
Security
1004
Secure Key
Storage
1003

FIG. 10

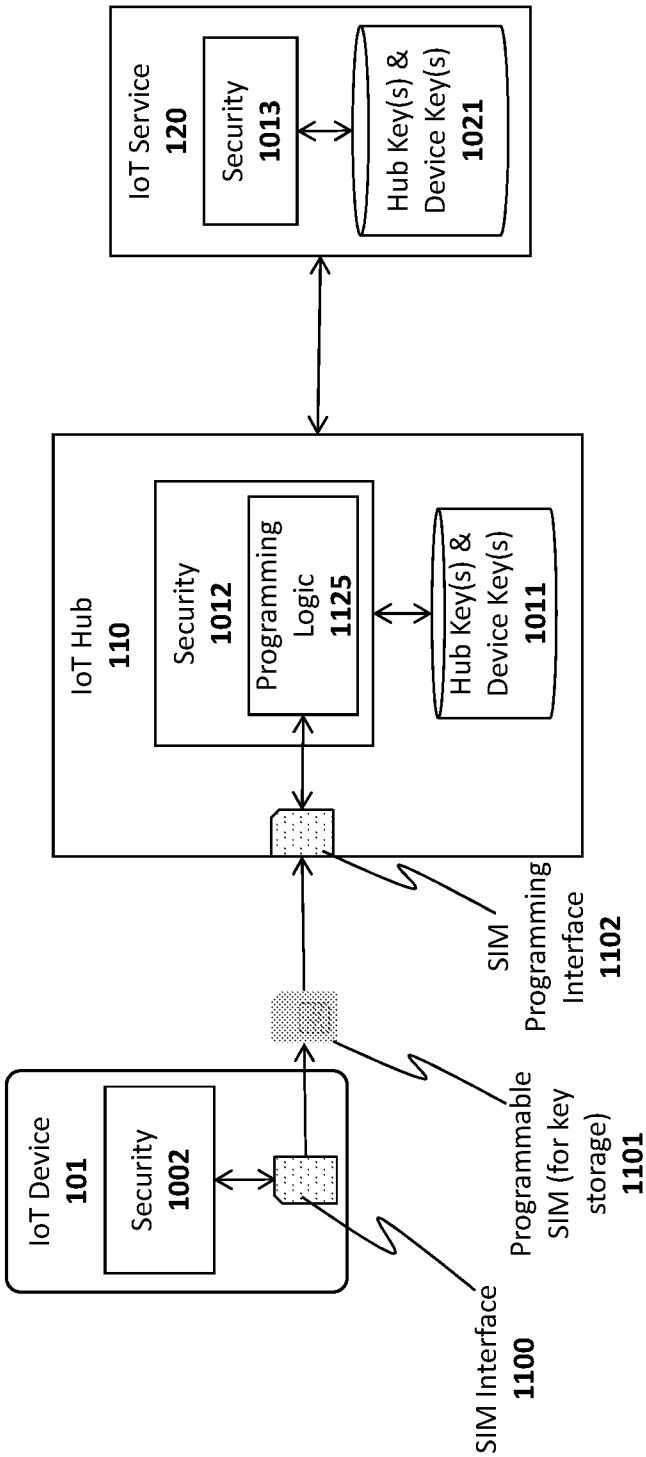
IoT Service
120
Security
1013
Hub Key(s) &
Device Key(s)
1021
IoT Hub
110
Security
1012
Programming
Logic
1125
Hub Key(s) &
Device Key(s)
1011
SIM
Programming
Interface
1102
IoT Device
101
Security
1002
Programmable
SIM (for key
storage)
1101
SIM Interface
1100

FIG. 11

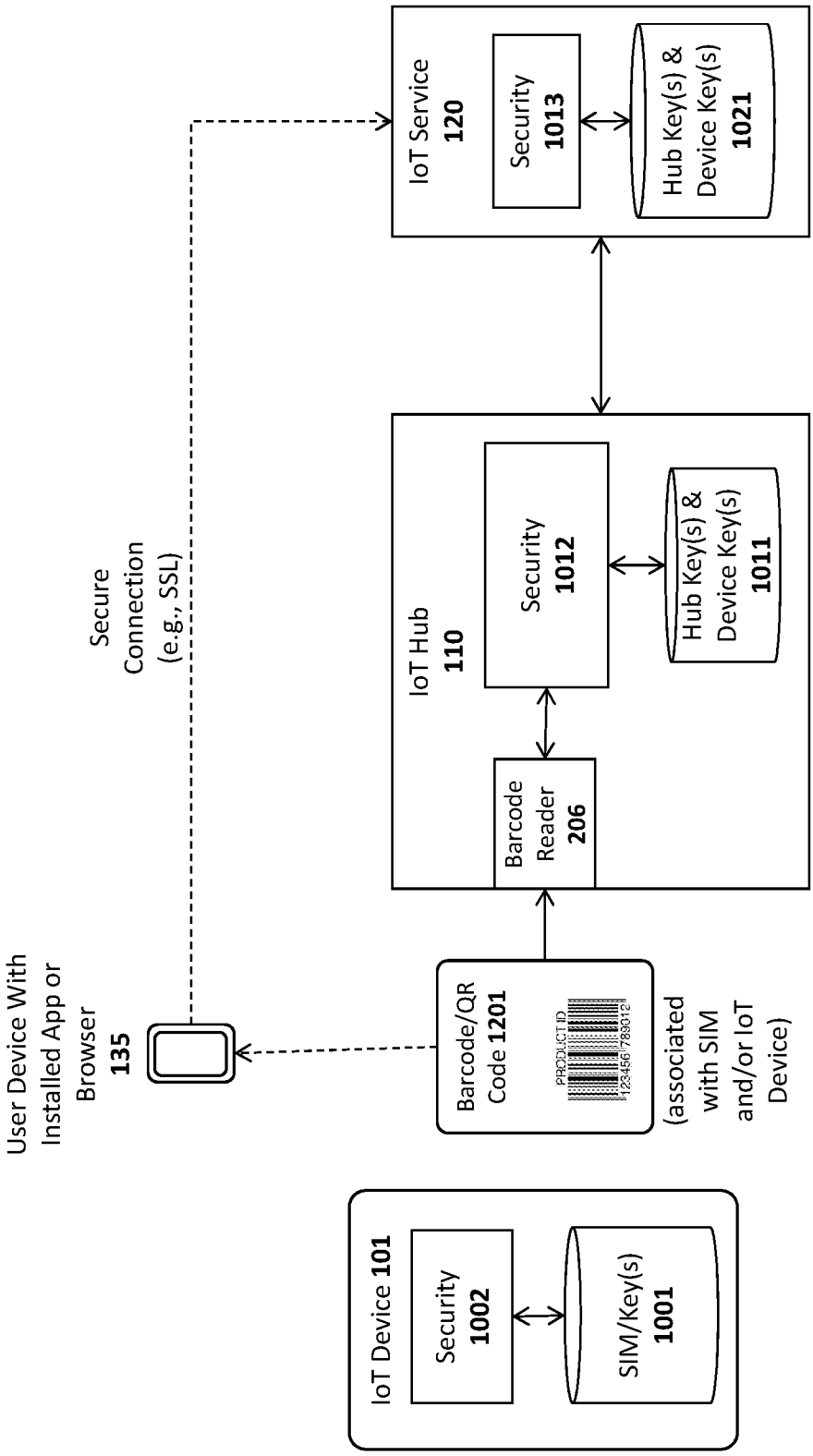
IoT Service
120
Security
1013
Hub Key(s) &
Device Key(s)
1021
IoT Hub
110
Security
1012
Hub Key(s) &
Device Key(s)
1011
Barcode
Reader
206
Secure
Connection
(e.g., SSL)
User Device With
Installed App or
Browser
135
Barcode/QR
Code 1201
PRODUCT ID
123456 789012
(associated
with SIM
and/or IoT
Device)
IoT Device 101
Security
1002
SIM/Key(s)
1001

FIG. 12A

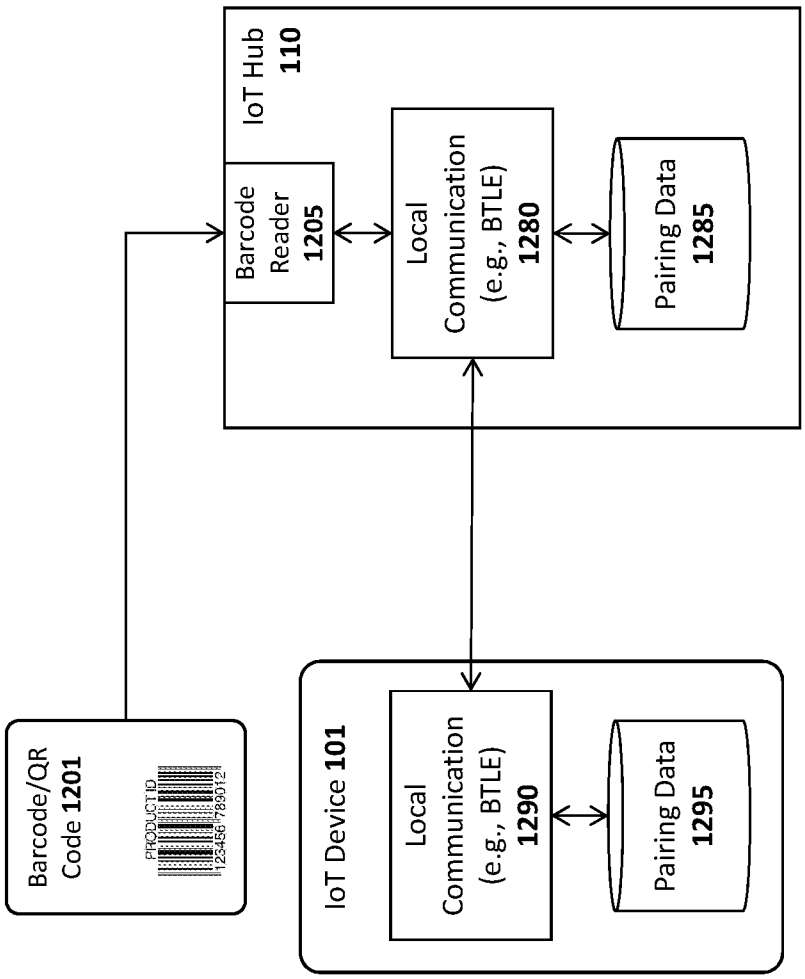
IoT Hub 110
Barcode Reader 1205
Local Communication (e.g., BTLE) 1280
Pairing Data 1285
Barcode/QR Code 1201
PRODUCT ID
123456789012
IoT Device 101
Local Communication (e.g., BTLE) 1290
Pairing Data 1295

FIG. 12B

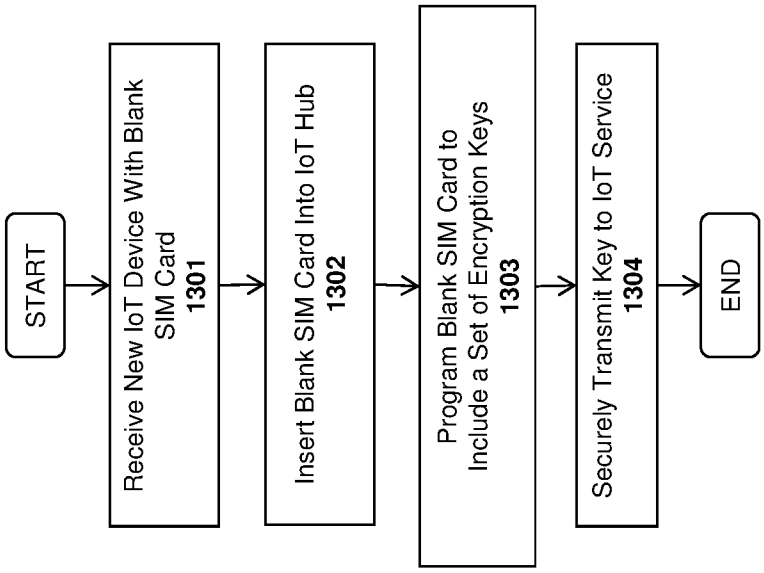
START
Receive New IoT Device With Blank SIM Card
1301
Insert Blank SIM Card Into IoT Hub
1302
Program Blank SIM Card to Include a Set of Encryption Keys
1303
Securely Transmit Key to IoT Service
1304
END

Fig. 13

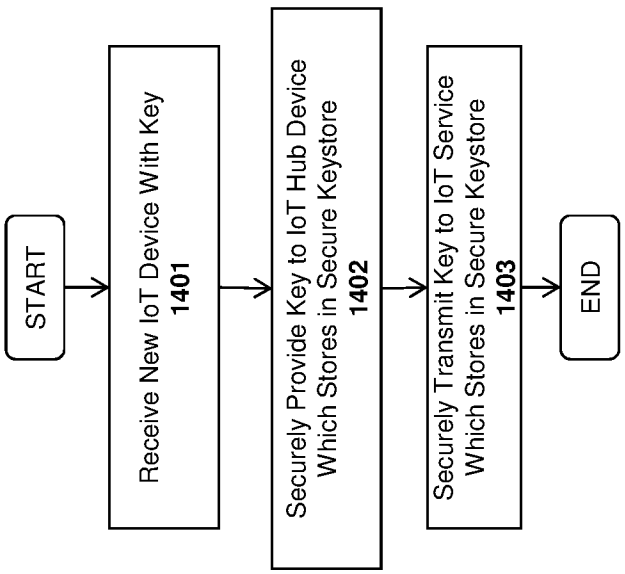
START
Receive New IoT Device With Key
1401
Securely Provide Key to IoT Hub Device
Which Stores in Secure Keystore
1402
Securely Transmit Key to IoT Service
Which Stores in Secure Keystore
1403
END

Fig. 14

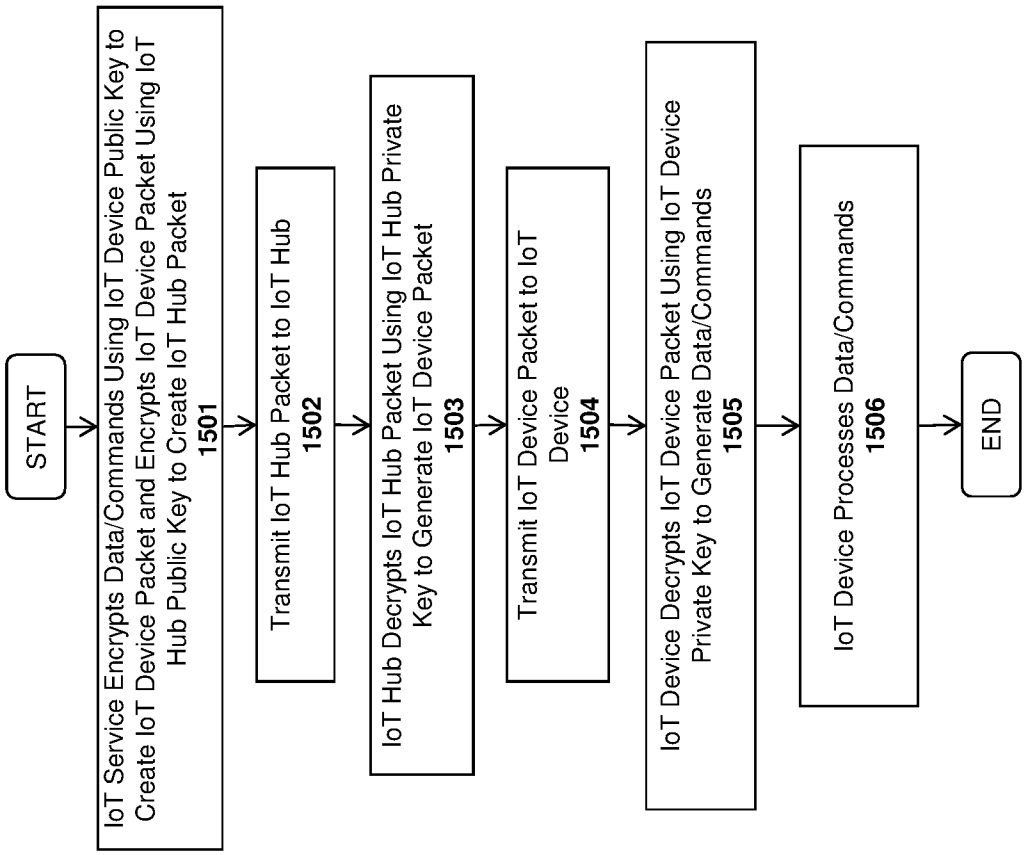
START
IoT Service Encrypts Data/Commands Using IoT Device Public Key to Create IoT Device Packet and Encrypts IoT Device Packet Using IoT Hub Public Key to Create IoT Hub Packet
1501
Transmit IoT Hub Packet to IoT Hub
1502
IoT Hub Decrypts IoT Hub Packet Using IoT Hub Private Key to Generate IoT Device Packet
1503
Transmit IoT Device Packet to IoT Device
1504
IoT Device Decrypts IoT Device Packet Using IoT Device Private Key to Generate Data/Commands
1505
IoT Device Processes Data/Commands
1506
END

Fig. 15

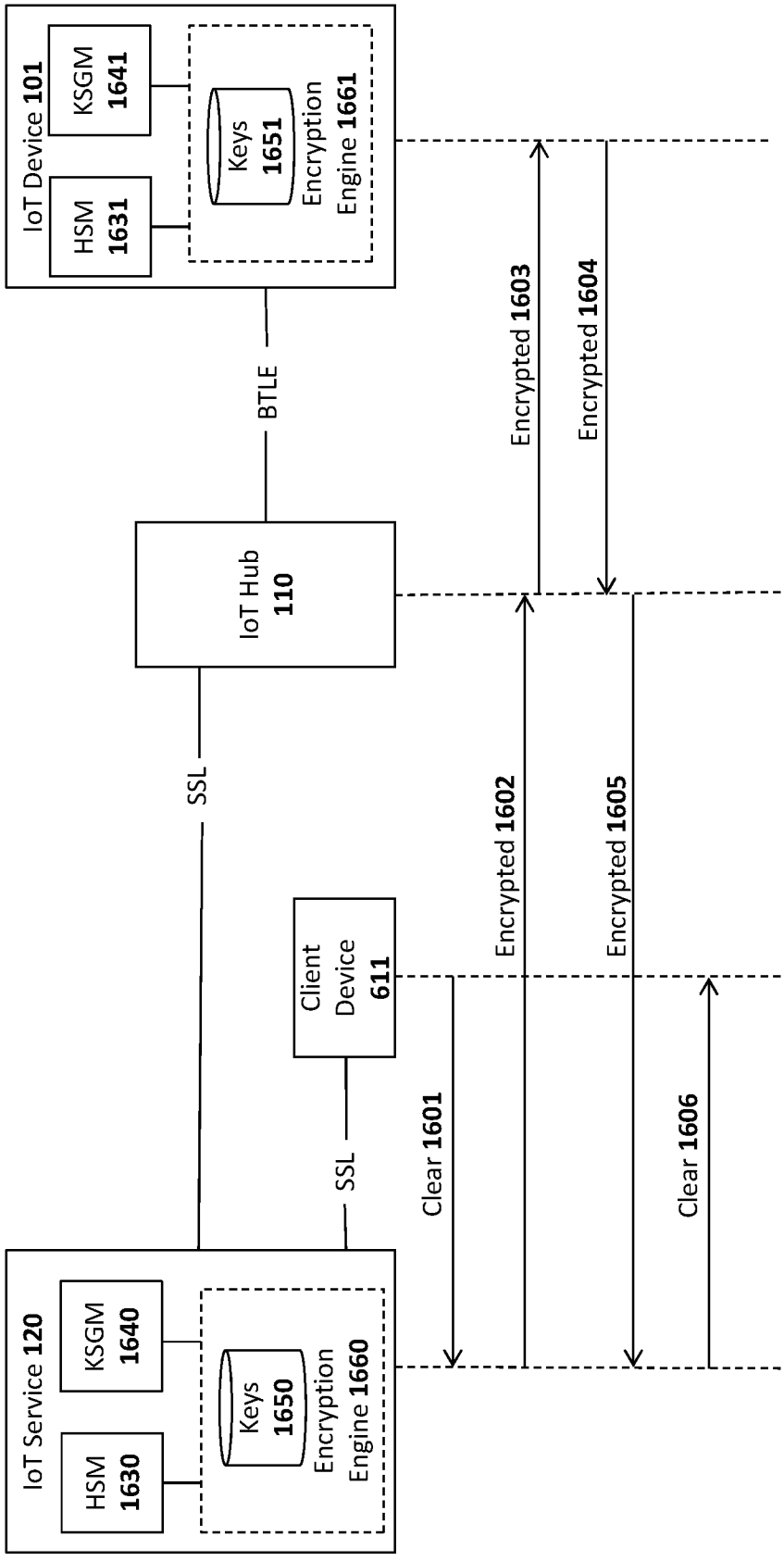
IoT Device 101
KSGM 1641
HSM 1631
Keys 1651
Encryption Engine 1661
BTLE
IoT Hub 110
SSL
Client Device 611
SSL
IoT Service 120
KSGM 1640
HSM 1630
Keys 1650
Encryption Engine 1660
Encrypted 1603
Encrypted 1604
Encrypted 1602
Encrypted 1605
Clear 1601
Clear 1606

Fig. 16A

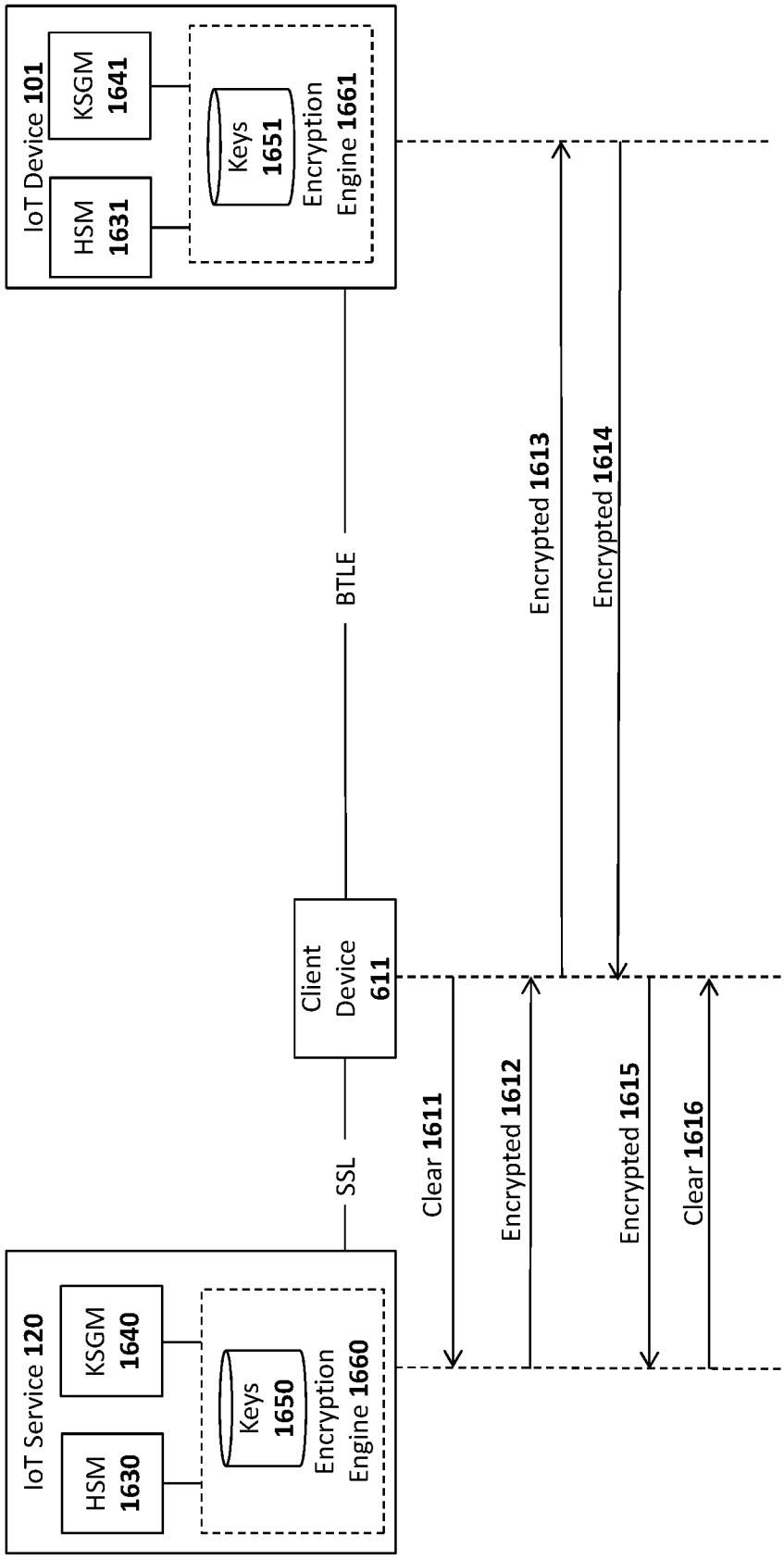
IoT Device 101
KSGM 1641
HSM 1631
Keys 1651
Encryption Engine 1661
BTLE
Client Device 611
SSL
IoT Service 120
KSGM 1640
HSM 1630
Keys 1650
Encryption Engine 1660
Clear 1611
Encrypted 1612
Encrypted 1613
Encrypted 1614
Encrypted 1615
Clear 1616

Fig. 16B

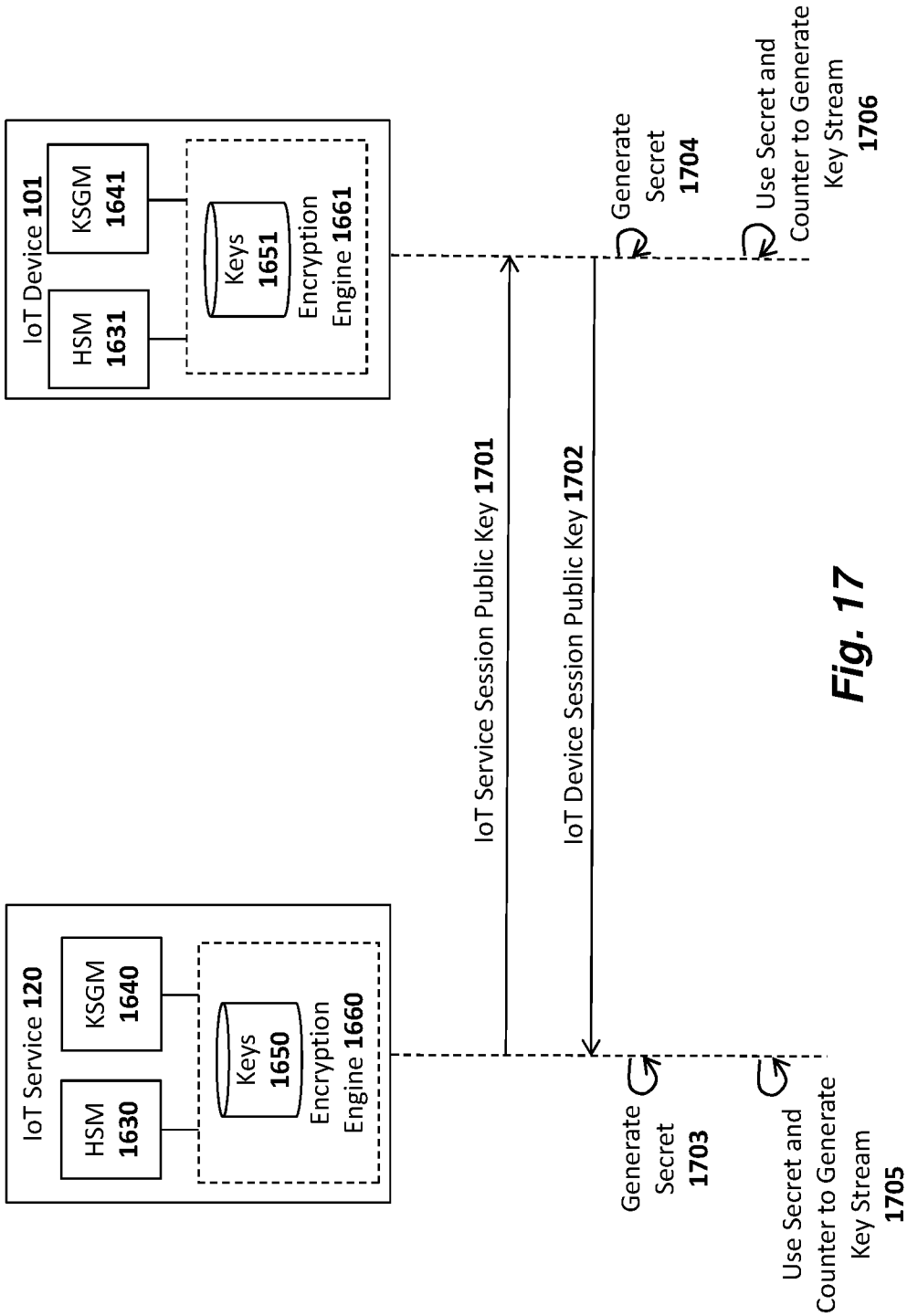
IoT Device 101
HSM 1631
KSGM 1641
Keys 1651
Encryption Engine 1661
IoT Service 120
HSM 1630
KSGM 1640
Keys 1650
Encryption Engine 1660
IoT Service Session Public Key 1701
IoT Device Session Public Key 1702
Generate Secret 1703
Use Secret and Counter to Generate Key Stream 1705
Generate Secret 1704
Use Secret and Counter to Generate Key Stream 1706

Fig. 17

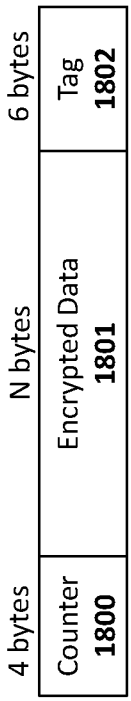
4 bytes
N bytes
6 bytes
Counter
1800
Encrypted Data
1801
Tag
1802

Fig. 18

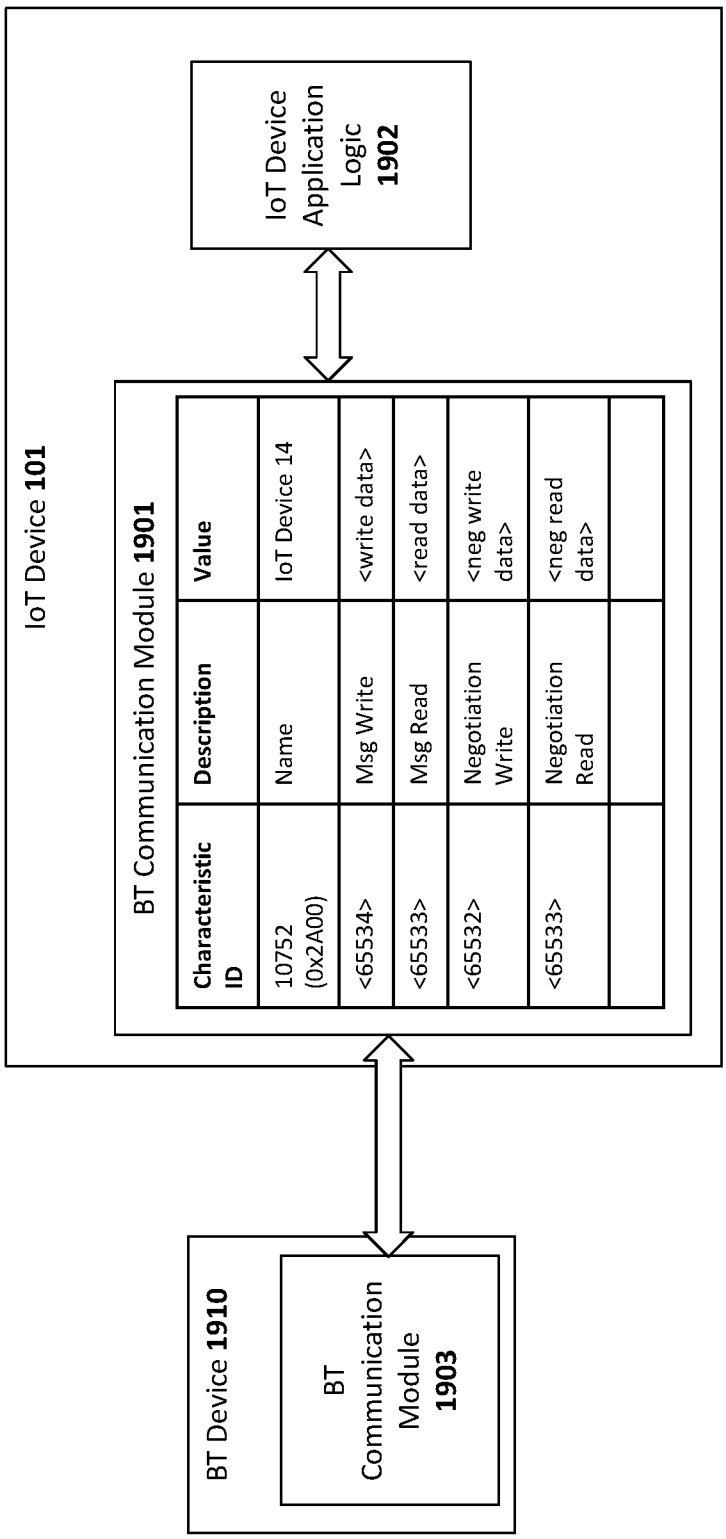
IoT Device 101
IoT Device Application Logic 1902
BT Communication Module 1901
Characteristic ID
Description
Value
10752 (0x2A00)
Name
IoT Device 14
<65534>
Msg Write
<write data>
<65533>
Msg Read
<read data>
<65532>
Negotiation Write
<neg write data>
<65533>
Negotiation Read
<neg read data>
BT Device 1910
BT Communication Module 1903

Fig. 19

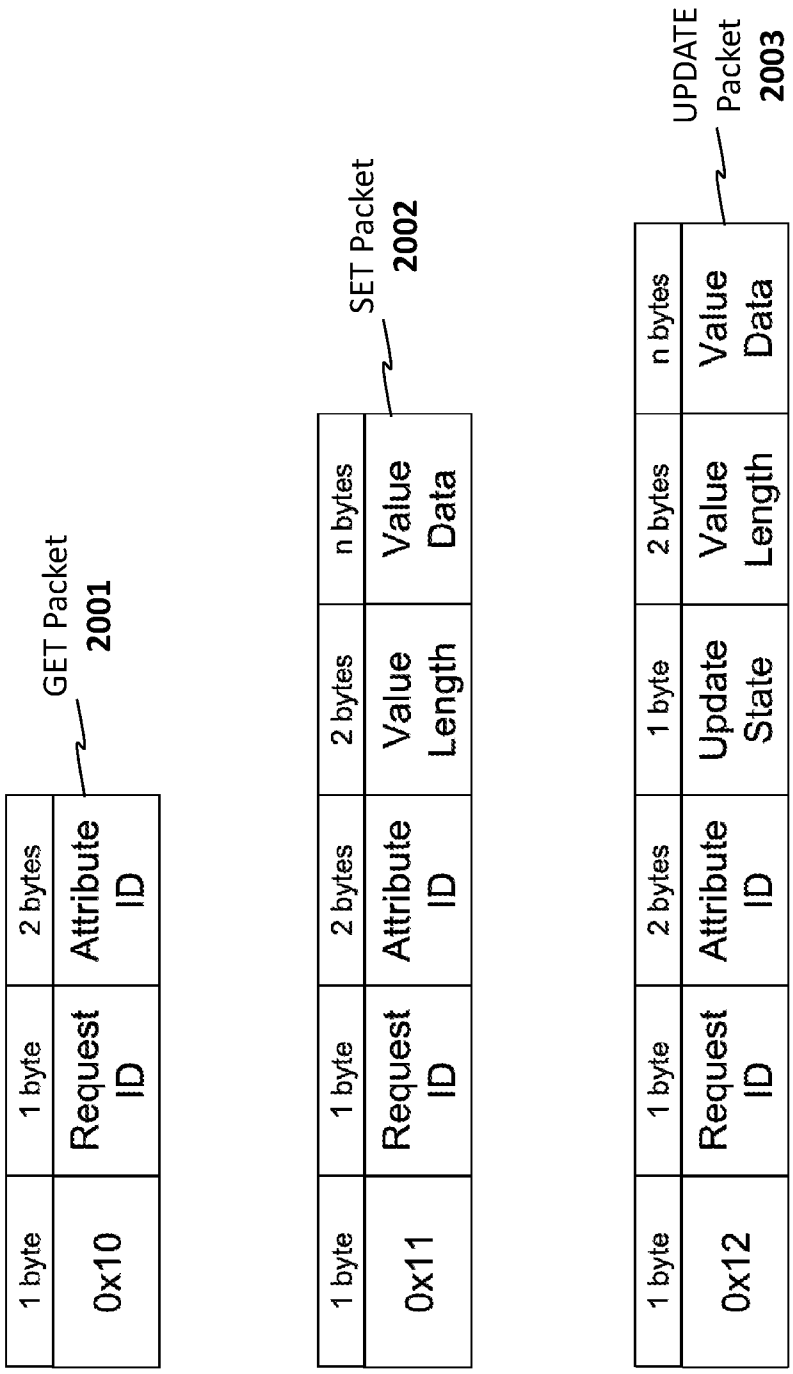
GET Packet
2001
1 byte
2 bytes
0x10
Request ID
Attribute ID
SET Packet
2002
1 byte
2 bytes
2 bytes
n bytes
0x11
Request ID
Attribute ID
Value Length
Value Data
UPDATE Packet
2003
1 byte
2 bytes
1 byte
2 bytes
n bytes
0x12
Request ID
Attribute ID
Update State
Value Length
Value Data

Fig. 20

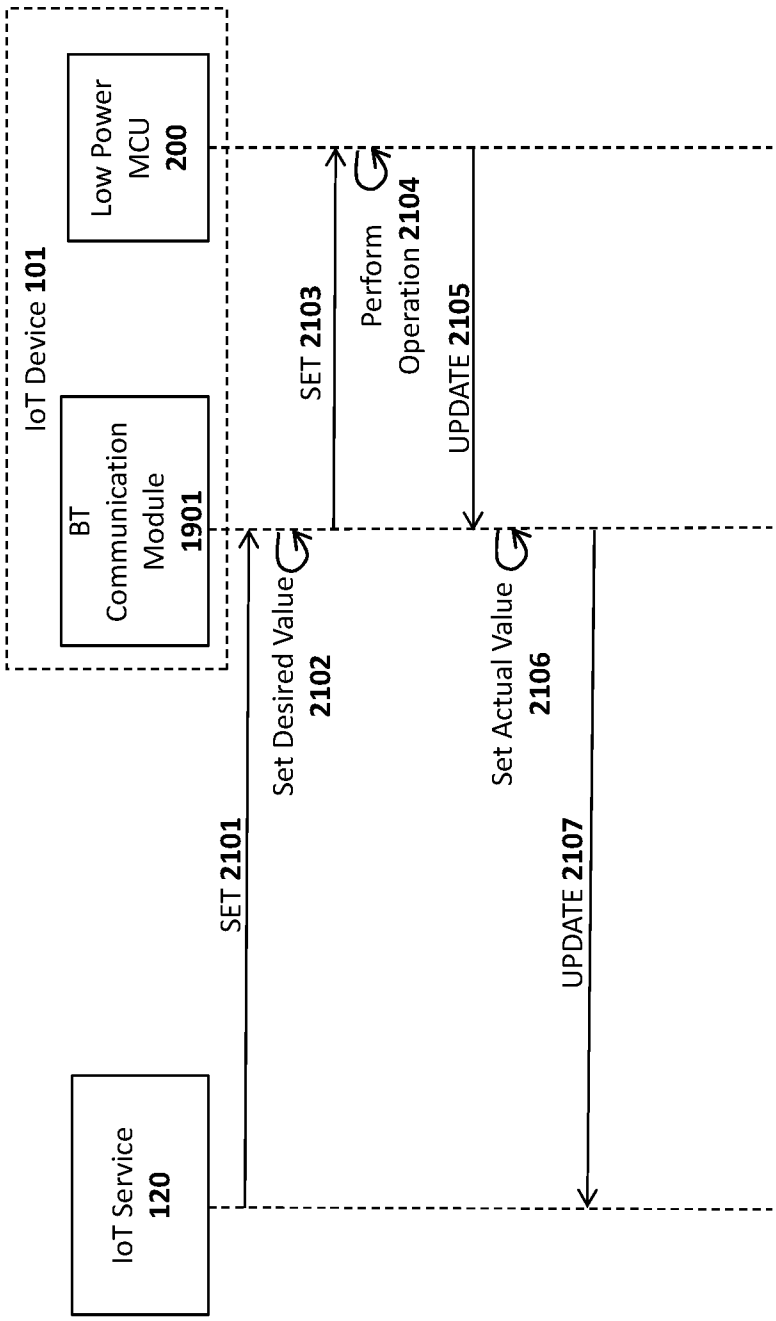
IoT Device 101
Low Power MCU 200
BT Communication Module 1901
IoT Service 120
SET 2101
Set Desired Value 2102
SET 2103
Perform Operation 2104
UPDATE 2105
Set Actual Value 2106
UPDATE 2107

Fig. 21

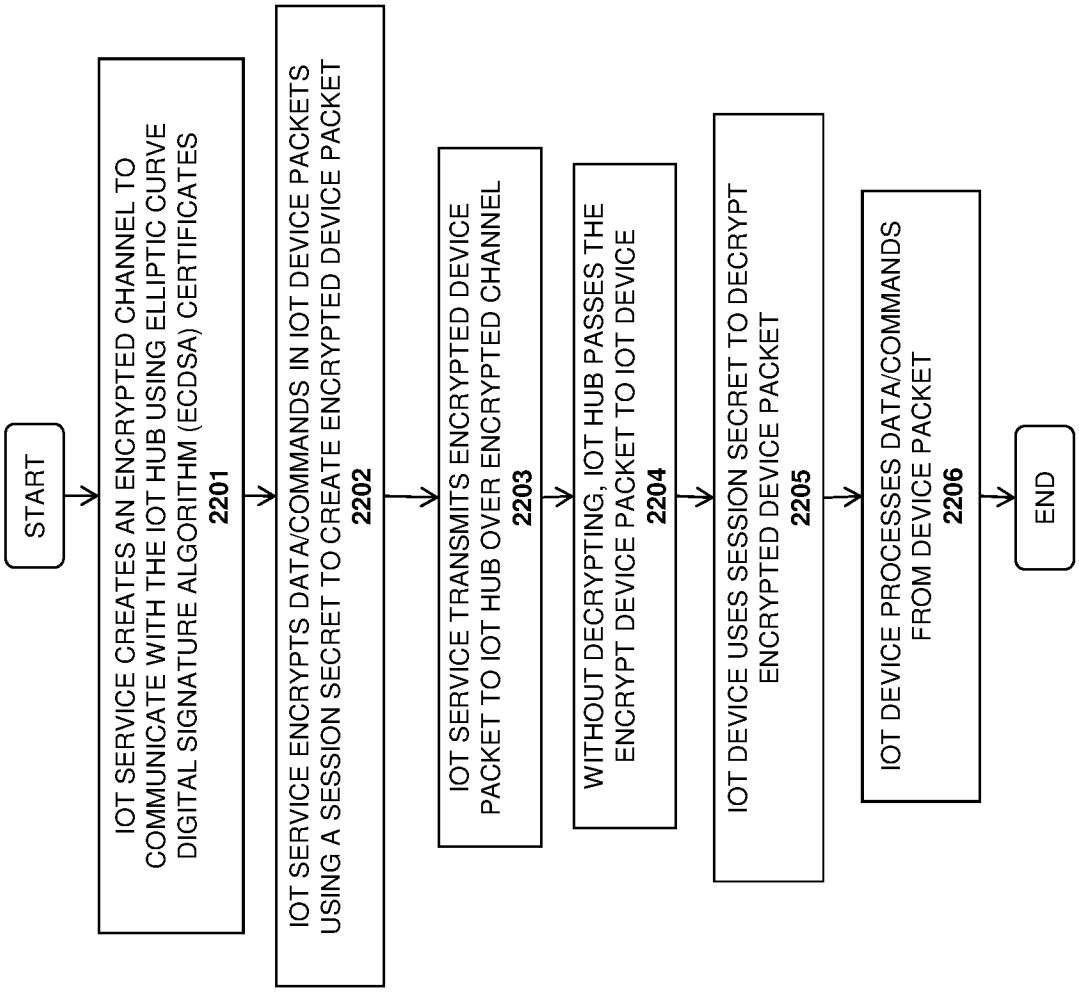
START
IOT SERVICE CREATES AN ENCRYPTED CHANNEL TO COMMUNICATE WITH THE IOT HUB USING ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA) CERTIFICATES
2201
IOT SERVICE ENCRYPTS DATA/COMMANDS IN IOT DEVICE PACKETS USING A SESSION SECRET TO CREATE ENCRYPTED DEVICE PACKET
2202
IOT SERVICE TRANSMITS ENCRYPTED DEVICE PACKET TO IOT HUB OVER ENCRYPTED CHANNEL
2203
WITHOUT DECRYPTING, IOT HUB PASSES THE ENCRYPT DEVICE PACKET TO IOT DEVICE
2204
IOT DEVICE USES SESSION SECRET TO DECRYPT ENCRYPTED DEVICE PACKET
2205
IOT DEVICE PROCESSES DATA/COMMANDS FROM DEVICE PACKET
2206
END

Fig. 22

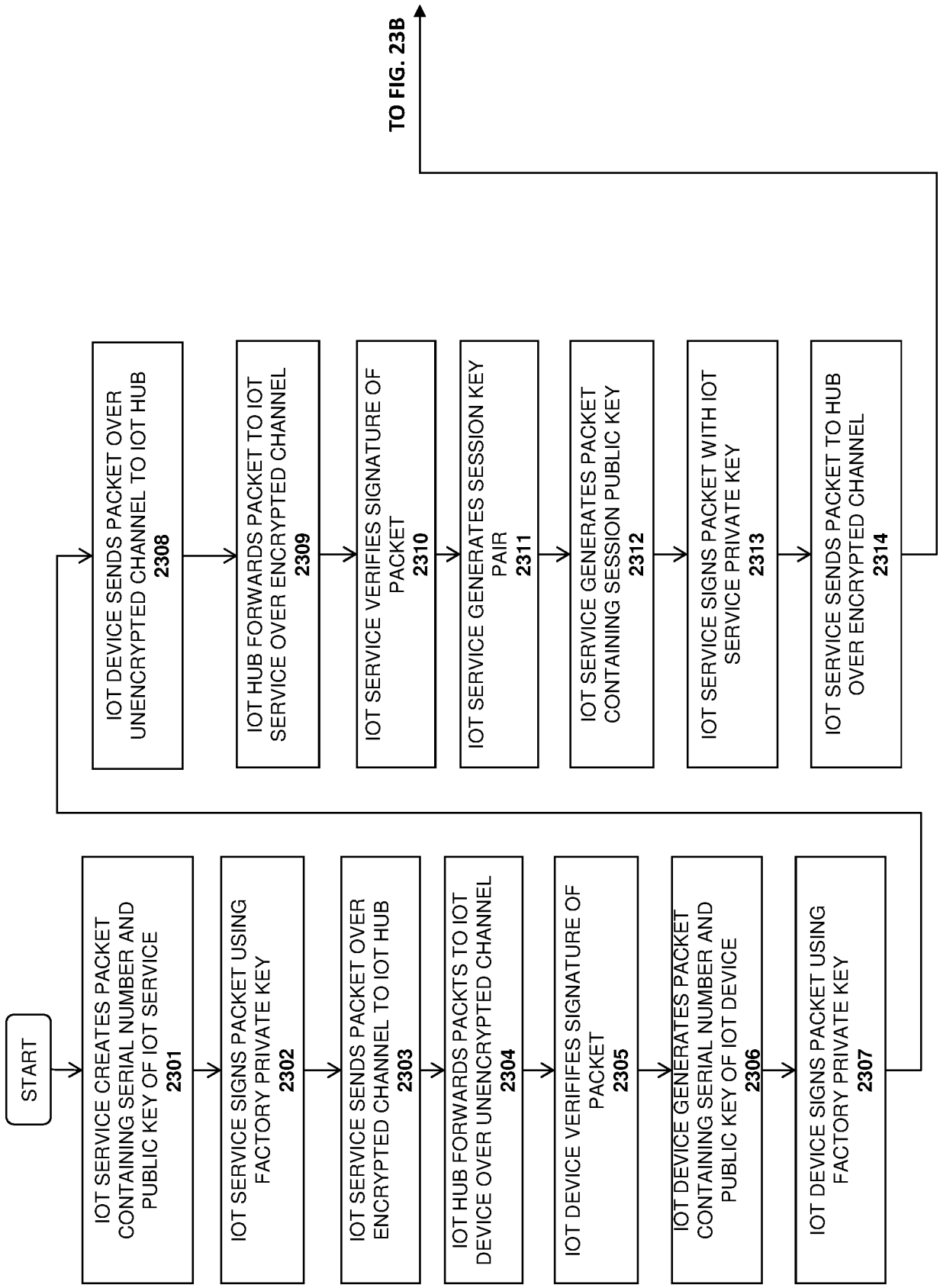
START
IOT SERVICE CREATES PACKET CONTAINING SERIAL NUMBER AND PUBLIC KEY OF IOT SERVICE 2301
IOT SERVICE SIGNS PACKET USING FACTORY PRIVATE KEY 2302
IOT SERVICE SENDS PACKET OVER ENCRYPTED CHANNEL TO IOT HUB 2303
IOT HUB FORWARDS PACKTS TO IOT DEVICE OVER UNENCRYPTED CHANNEL 2304
IOT DEVICE VERIFIES SIGNATURE OF PACKET 2305
IOT DEVICE GENERATES PACKET CONTAINING SERIAL NUMBER AND PUBLIC KEY OF IOT DEVICE 2306
IOT DEVICE SIGNS PACKET USING FACTORY PRIVATE KEY 2307
IOT DEVICE SENDS PACKET OVER UNENCRYPTED CHANNEL TO IOT HUB 2308
IOT HUB FORWARDS PACKET TO IOT SERVICE OVER ENCRYPTED CHANNEL 2309
IOT SERVICE VERIFIES SIGNATURE OF PACKET 2310
IOT SERVICE GENERATES SESSION KEY PAIR 2311
IOT SERVICE GENERATES PACKET CONTAINING SESSION PUBLIC KEY 2312
IOT SERVICE SIGNS PACKET WITH IOT SERVICE PRIVATE KEY 2313
IOT SERVICE SENDS PACKET TO HUB OVER ENCRYPTED CHANNEL 2314
TO FIG. 23B

Fig. 23A

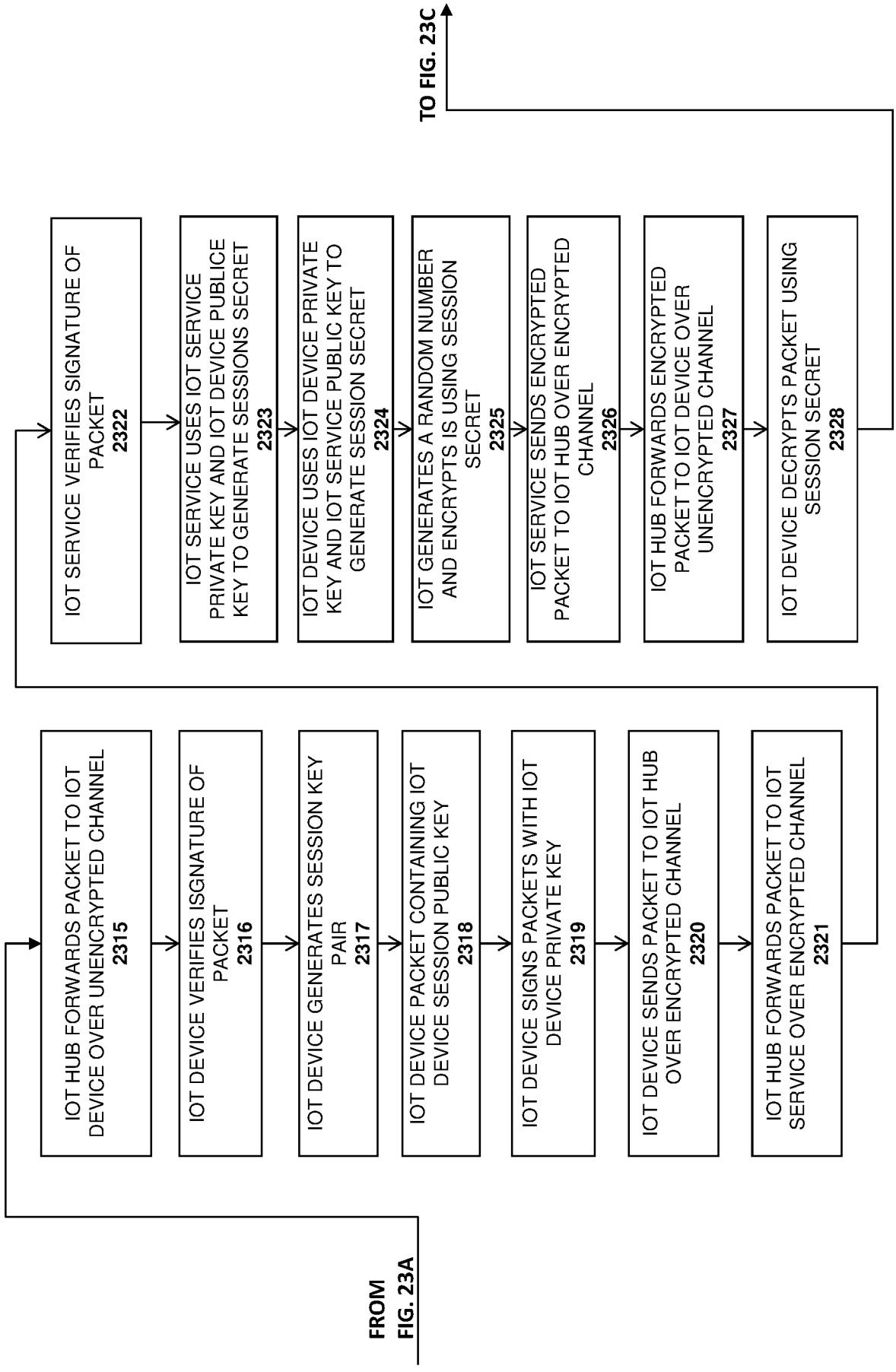
FROM FIG. 23A
IOT HUB FORWARDS PACKET TO IOT DEVICE OVER UNENCRYPTED CHANNEL 2315
IOT DEVICE VERIFIES ISGNATURE OF PACKET 2316
IOT DEVICE GENERATES SESSION KEY PAIR 2317
IOT DEVICE PACKET CONTAINING IOT DEVICE SESSION PUBLIC KEY 2318
IOT DEVICE SIGNS PACKETS WITH IOT DEVICE PRIVATE KEY 2319
IOT DEVICE SENDS PACKET TO IOT HUB OVER ENCRYPTED CHANNEL 2320
IOT HUB FORWARDS PACKET TO IOT SERVICE OVER ENCRYPTED CHANNEL 2321
IOT SERVICE VERIFIES SIGNATURE OF PACKET 2322
IOT SERVICE USES IOT SERVICE PRIVATE KEY AND IOT DEVICE PUBLICE KEY TO GENERATE SESSIONS SECRET 2323
IOT DEVICE USES IOT DEVICE PRIVATE KEY AND IOT SERVICE PUBLIC KEY TO GENERATE SESSION SECRET 2324
IOT GENERATES A RANDOM NUMBER AND ENCRYPTS IS USING SESSION SECRET 2325
IOT SERVICE SENDS ENCRYPTED PACKET TO IOT HUB OVER ENCRYPTED CHANNEL 2326
IOT HUB FORWARDS ENCRYPTED PACKET TO IOT DEVICE OVER UNENCRYPTED CHANNEL 2327
IOT DEVICE DECRYPTS PACKET USING SESSION SECRET 2328
TO FIG. 23C

Fig. 23B

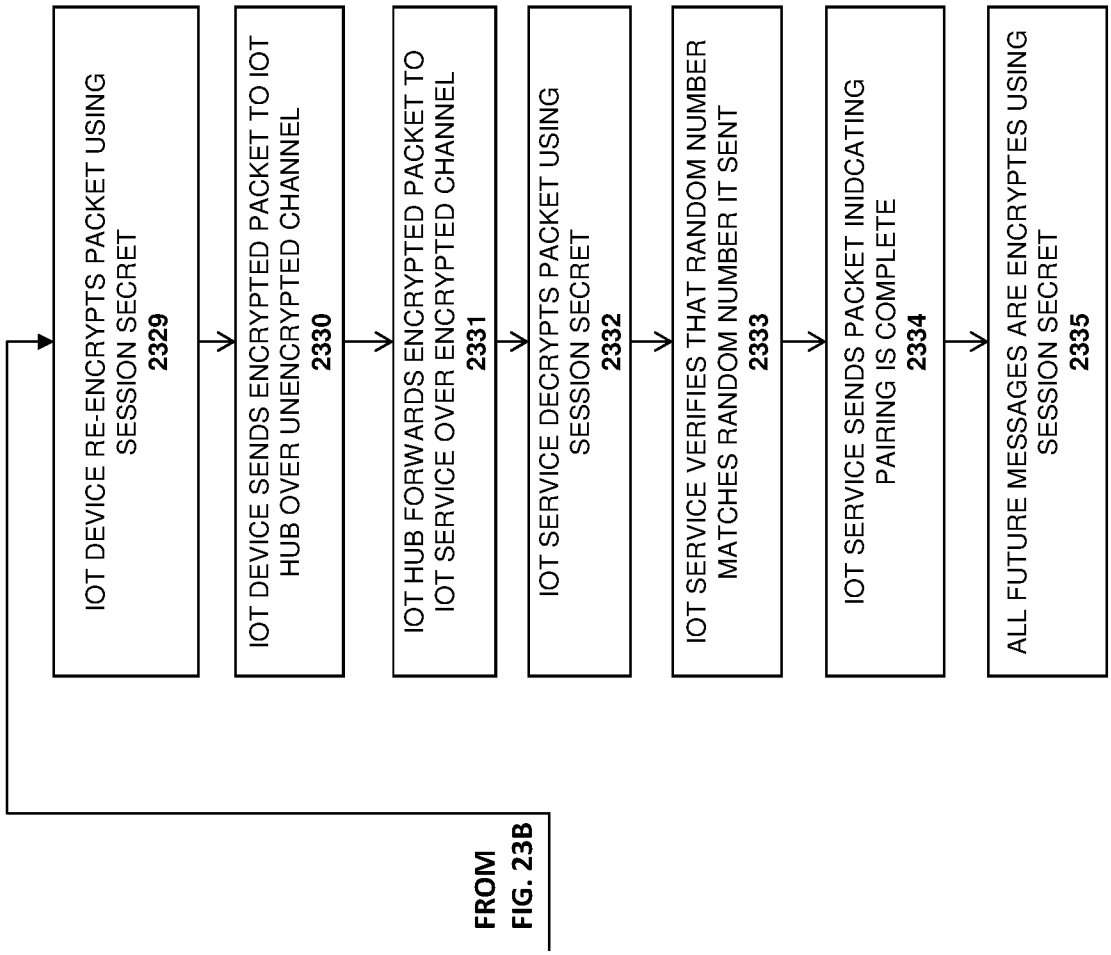
IOT DEVICE RE-ENCRYPTS PACKET USING SESSION SECRET
2329
IOT DEVICE SENDS ENCRYPTED PACKET TO IOT HUB OVER UNENCRYPTED CHANNEL
2330
IOT HUB FORWARDS ENCRYPTED PACKET TO IOT SERVICE OVER ENCRYPTED CHANNEL
2331
IOT SERVICE DECRYPTS PACKET USING SESSION SECRET
2332
IOT SERVICE VERIFIES THAT RANDOM NUMBER MATCHES RANDOM NUMBER IT SENT
2333
IOT SERVICE SENDS PACKET INIDCATING PAIRING IS COMPLETE
2334
ALL FUTURE MESSAGES ARE ENCRYPTES USING SESSION SECRET
2335
FROM FIG. 23B

Fig. 23C

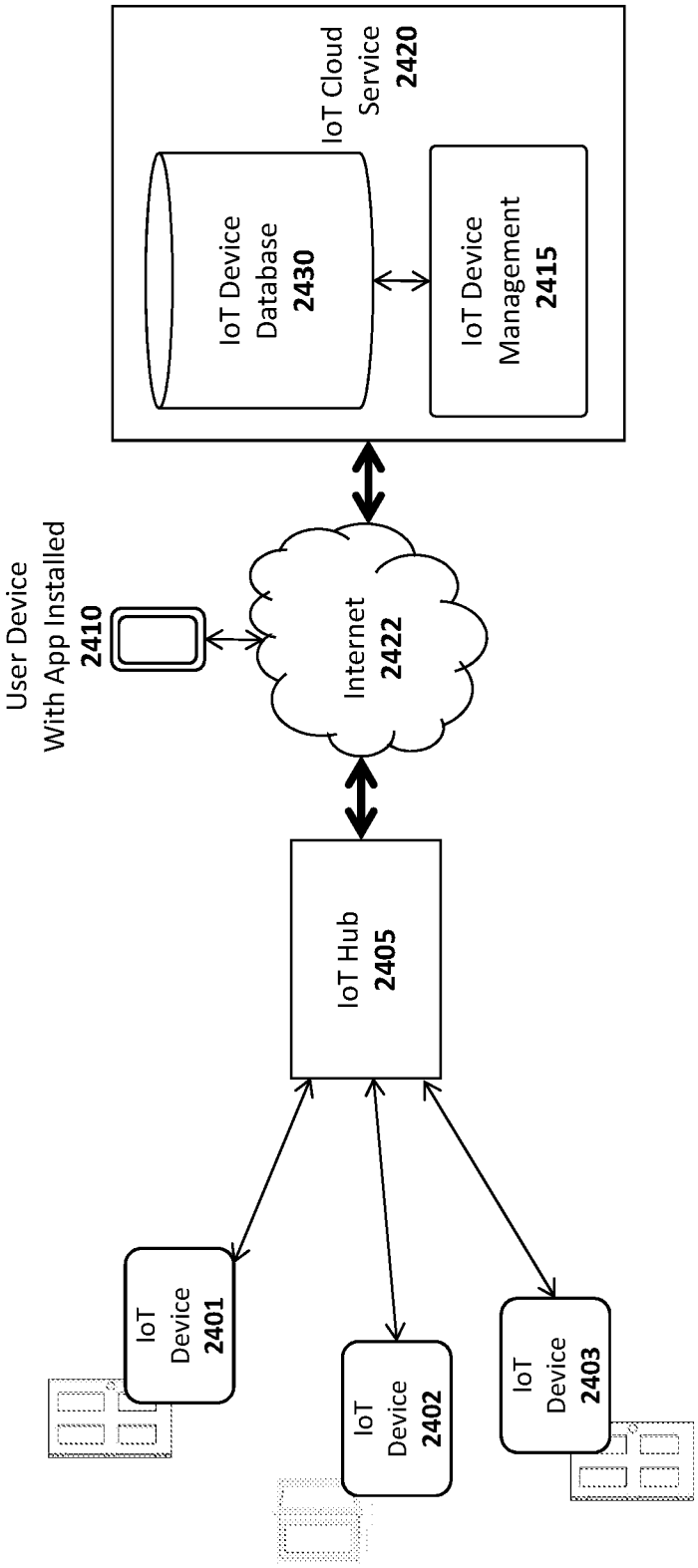
IoT Cloud Service 2420
IoT Device Database 2430
IoT Device Management 2415
User Device With App Installed 2410
Internet 2422
IoT Hub 2405
IoT Device 2401
IoT Device 2402
IoT Device 2403

FIG. 24

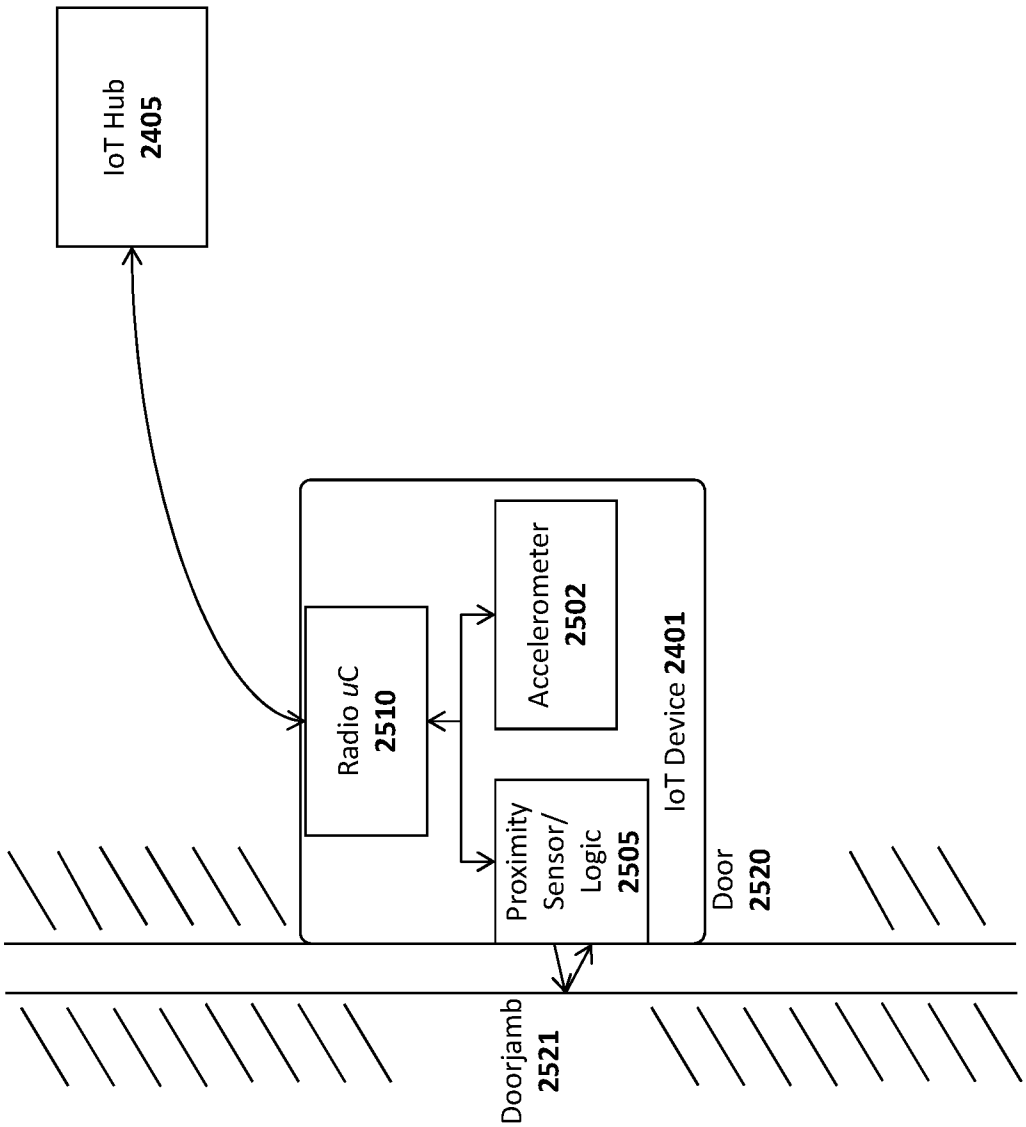
IoT Hub
2405
Radio uC
2510
Accelerometer
2502
Proximity
Sensor/
Logic
2505
IoT Device 2401
Door
2520
Doorjamb
2521

FIG. 25

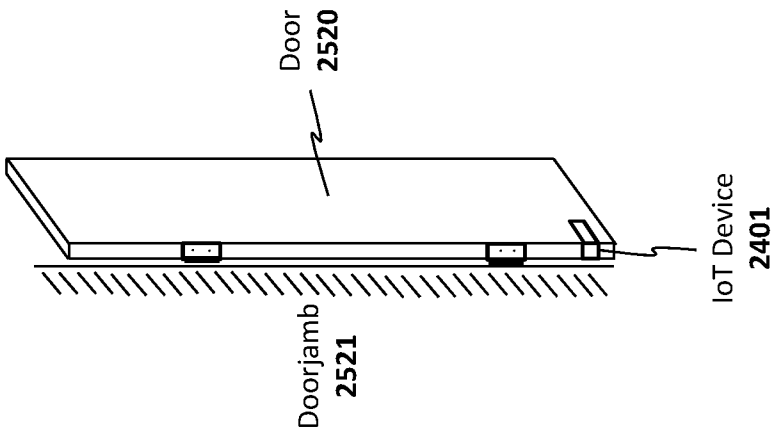

FIG. 26

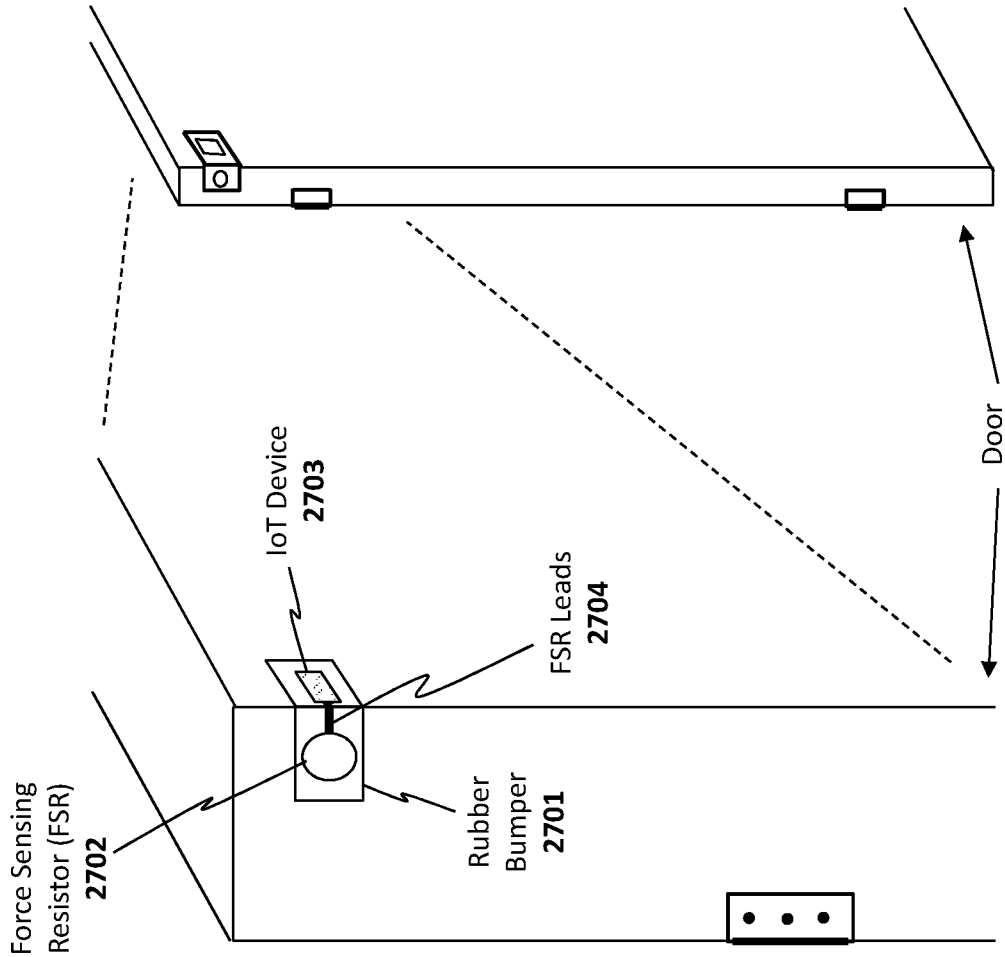

FIG. 27B

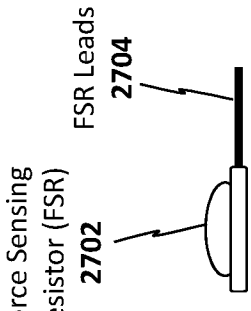

FIG. 27A

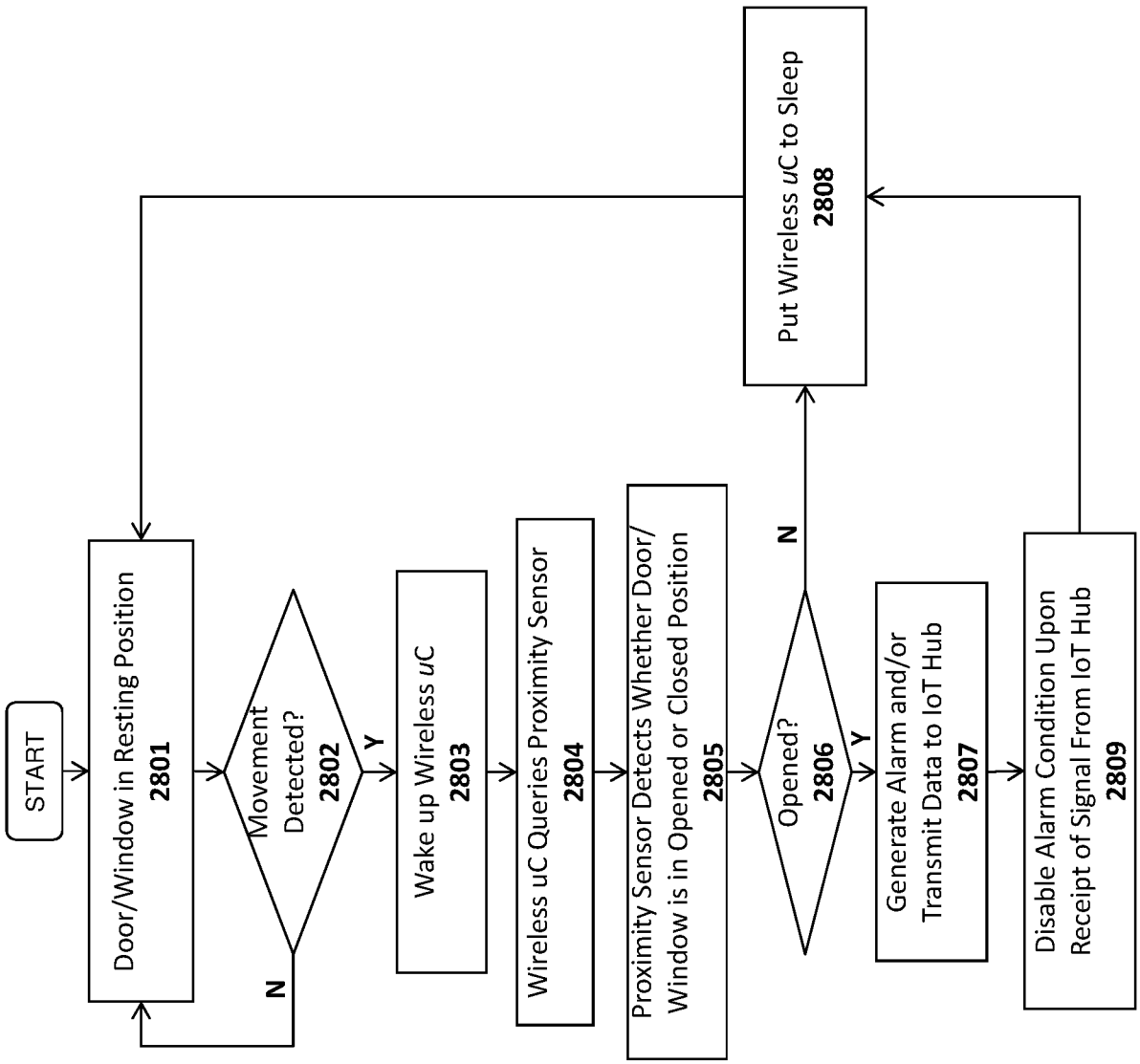
START
Door/Window in Resting Position
2801
Movement Detected?
2802
N
Y
Wake up Wireless uC
2803
Wireless uC Queries Proximity Sensor
2804
Proximity Sensor Detects Whether Door/ Window is in Opened or Closed Position
2805
Opened?
2806
N
Y
Generate Alarm and/or Transmit Data to IoT Hub
2807
Disable Alarm Condition Upon Receipt of Signal From IoT Hub
2809
Put Wireless uC to Sleep
2808

Fig. 28

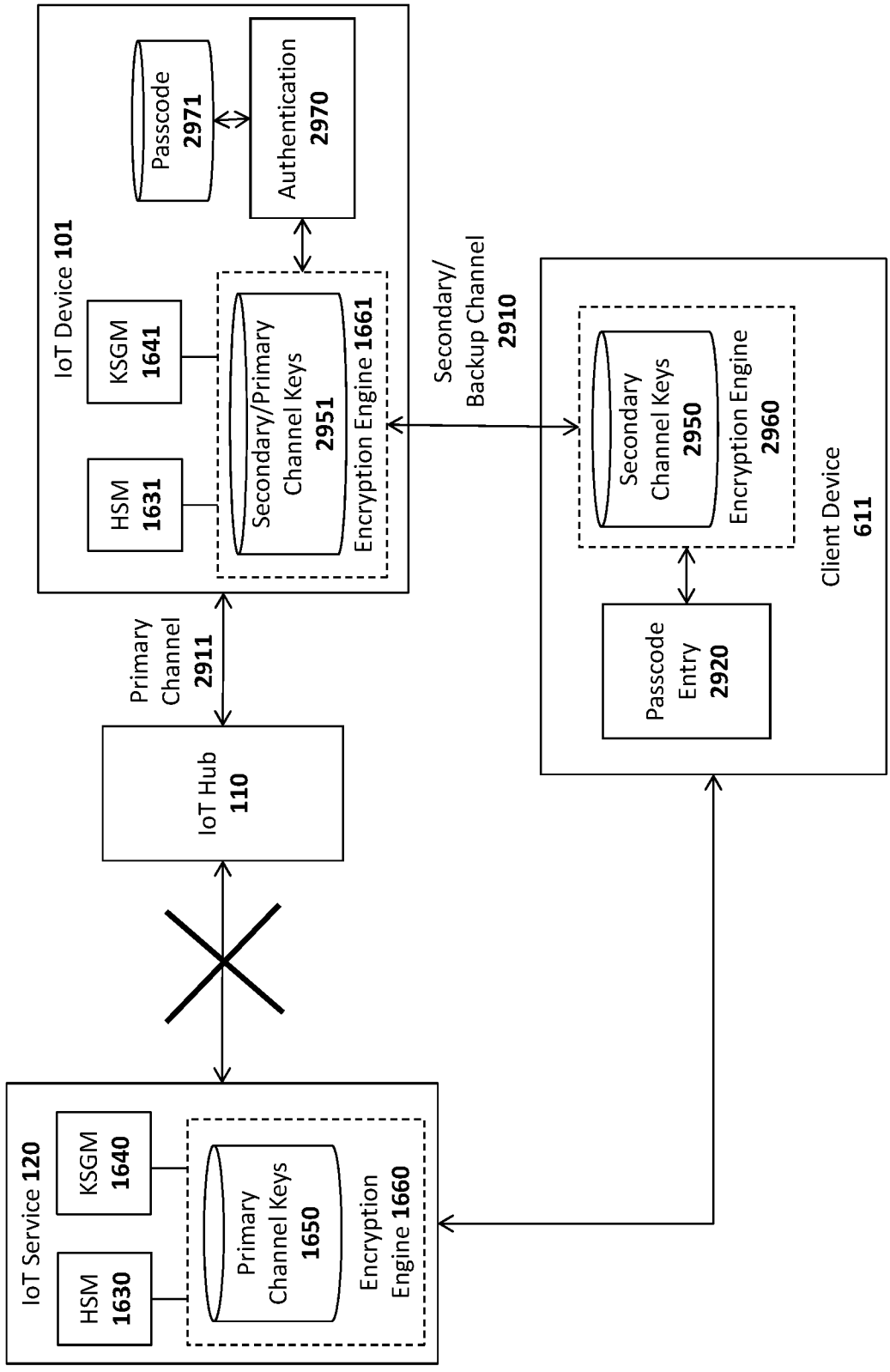
IoT Device 101
Passcode 2971
Authentication 2970
KSGM 1641
HSM 1631
Secondary/Primary Channel Keys 2951
Encryption Engine 1661
Secondary/ Backup Channel 2910
Primary Channel 2911
IoT Hub 110
Secondary Channel Keys 2950
Encryption Engine 2960
Client Device 611
Passcode Entry 2920
IoT Service 120
KSGM 1640
HSM 1630
Primary Channel Keys 1650
Encryption Engine 1660

Fig. 29

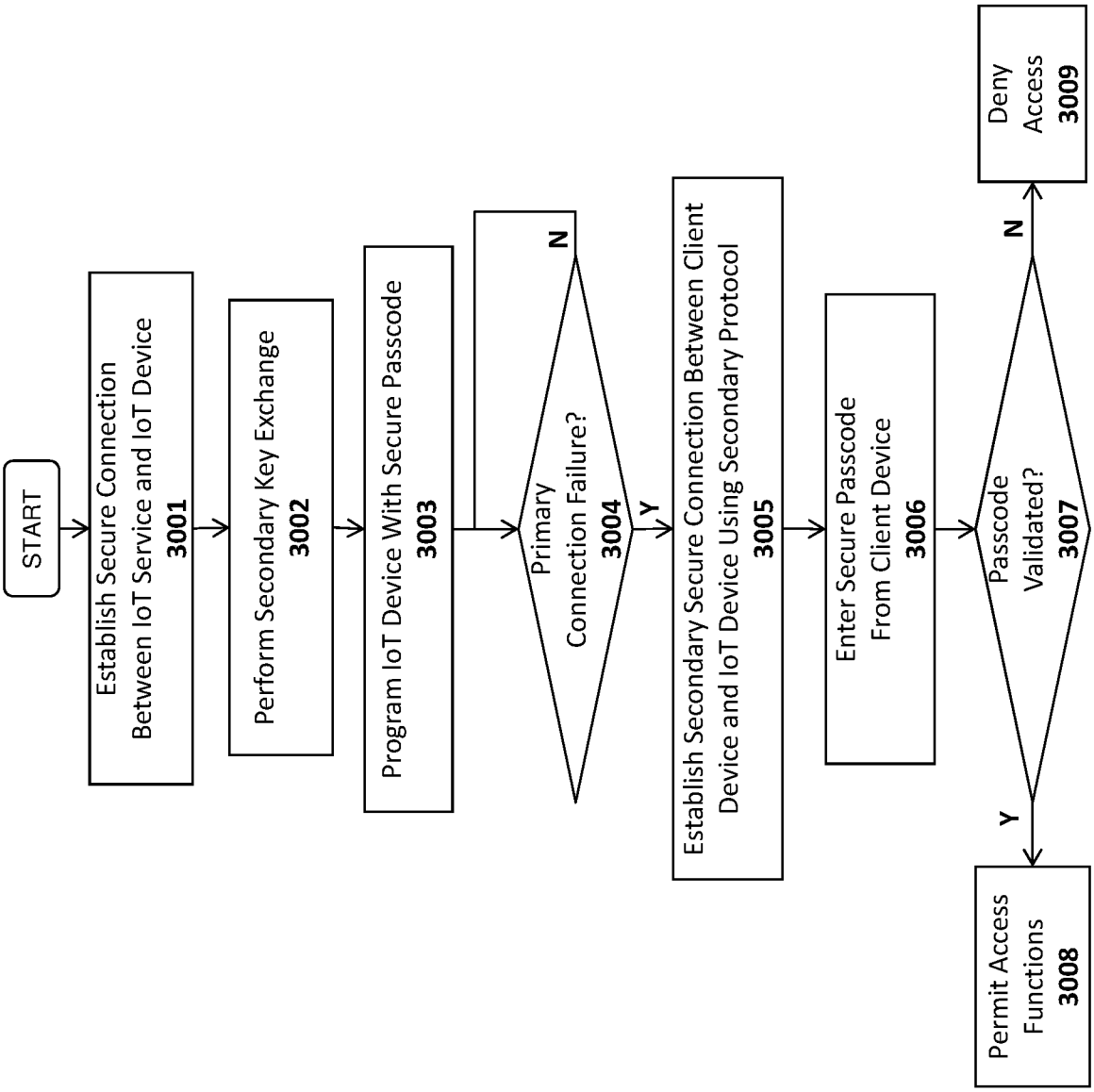
START
Establish Secure Connection Between IoT Service and IoT Device 3001
Perform Secondary Key Exchange 3002
Program IoT Device With Secure Passcode 3003
Primary Connection Failure? 3004
N
Y
Establish Secondary Secure Connection Between Client Device and IoT Device Using Secondary Protocol 3005
Enter Secure Passcode From Client Device 3006
Passcode Validated? 3007
N
Y
Deny Access 3009
Permit Access Functions 3008

Fig. 30

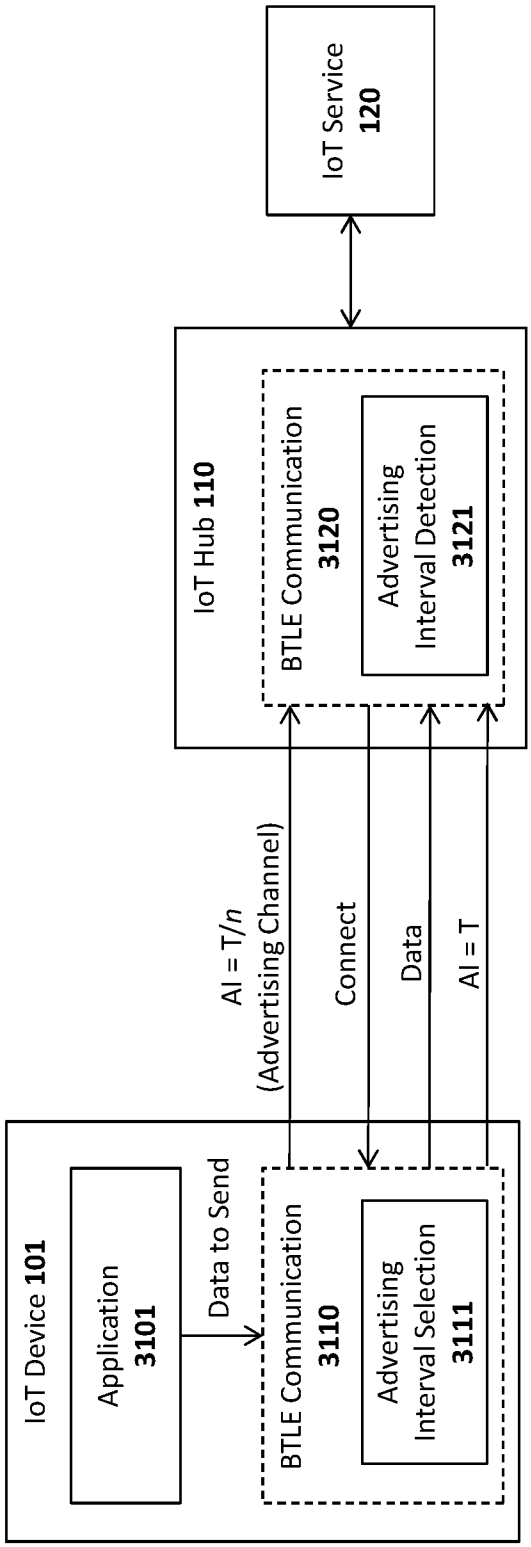
IoT Service
120
IoT Hub 110
BTLE Communication
3120
Advertising
Interval Detection
3121
AI = T/n
(Advertising Channel)
Connect
Data
AI = T
Normal Advertising
Interval (AI) = T
IoT Device 101
Application
3101
Data to Send
BTLE Communication
3110
Advertising
Interval Selection
3111

Fig. 31

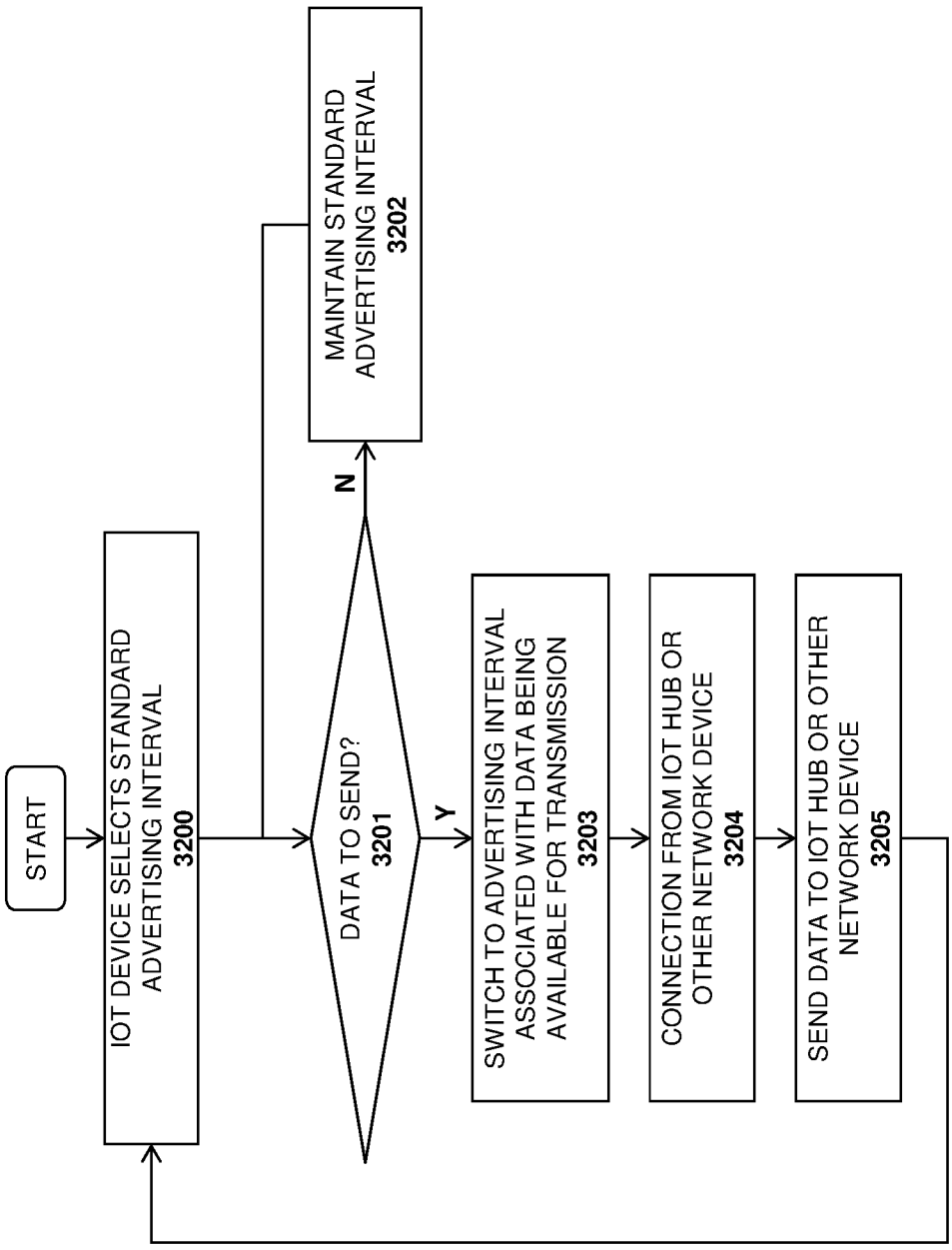
START
IOT DEVICE SELECTS STANDARD ADVERTISING INTERVAL
3200
DATA TO SEND?
3201
N
MAINTAIN STANDARD ADVERTISING INTERVAL
3202
Y
SWITCH TO ADVERTISING INTERVAL ASSOCIATED WITH DATA BEING AVAILABLE FOR TRANSMISSION
3203
CONNECTION FROM IOT HUB OR OTHER NETWORK DEVICE
3204
SEND DATA TO IOT HUB OR OTHER NETWORK DEVICE
3205

FIG. 32

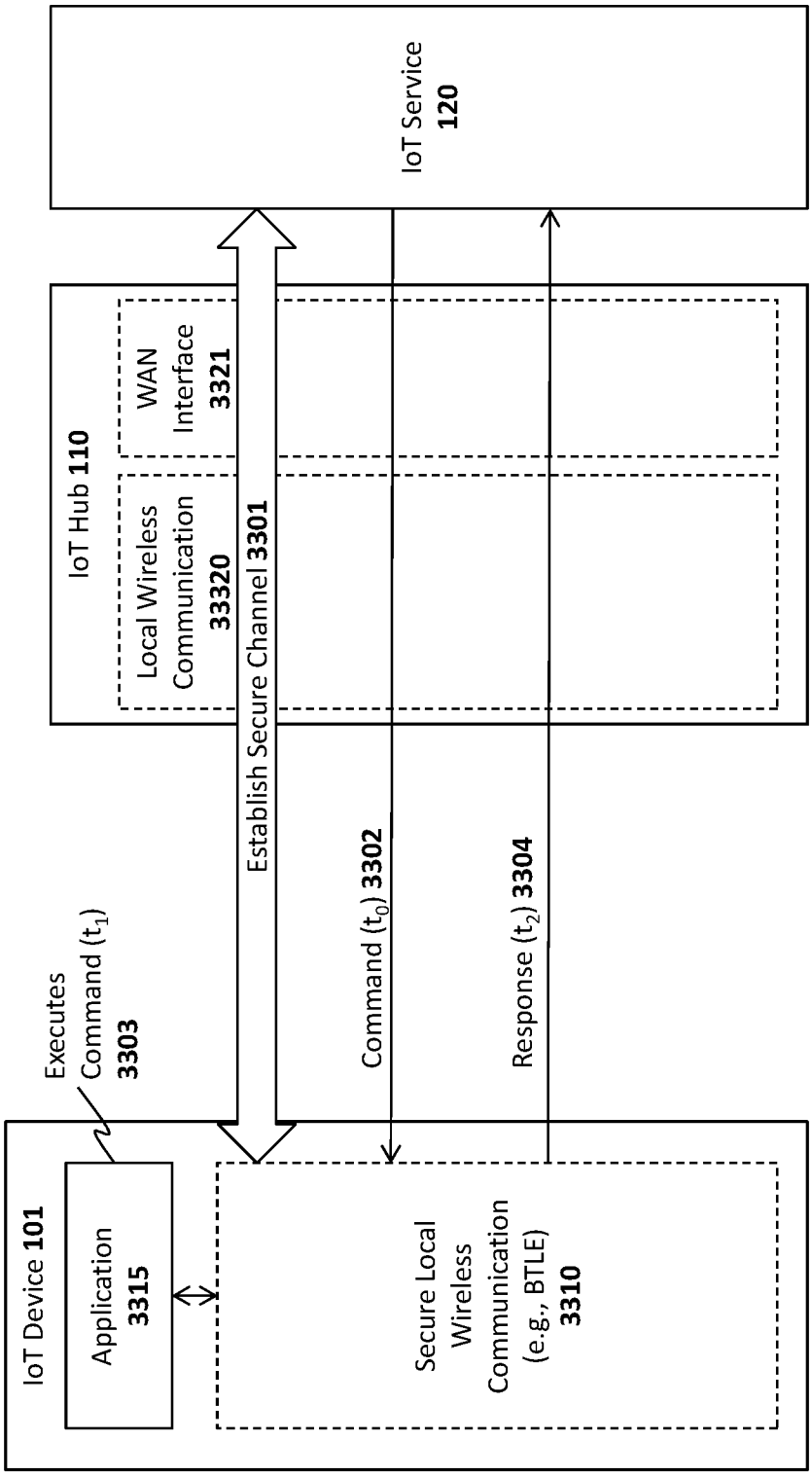
IoT Service
120
IoT Hub 110
WAN
Interface
3321
Local Wireless
Communication
33320
Establish Secure Channel 3301
Command (t_0) 3302
Response (t_2) 3304
Executes
Command (t_1)
3303
IoT Device 101
Application
3315
Secure Local
Wireless
Communication
(e.g., BTLE)
3310

Fig. 33

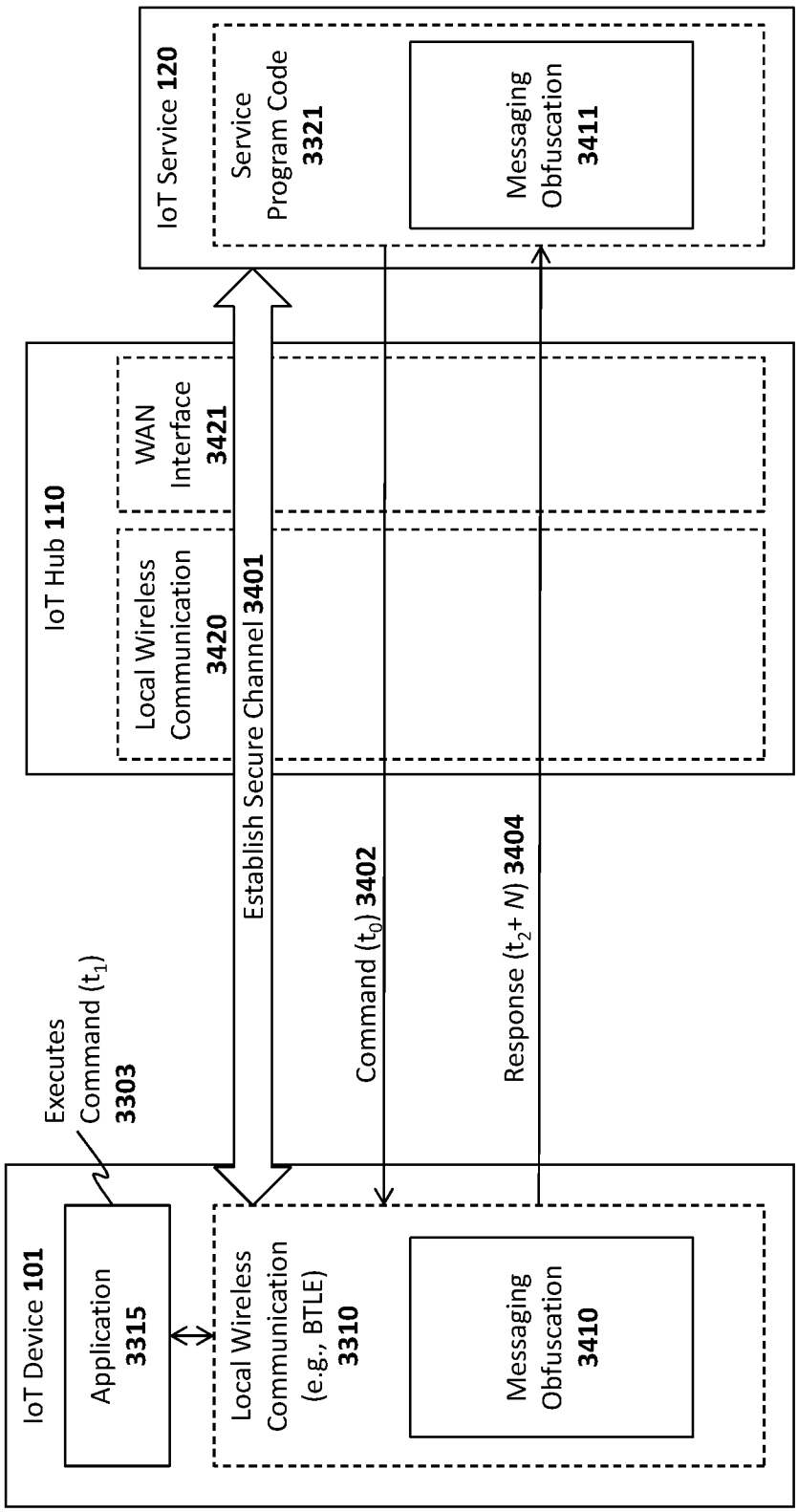
IoT Service 120
Service Program Code 3321
Messaging Obfuscation 3411
IoT Hub 110
WAN Interface 3421
Local Wireless Communication 3420
Establish Secure Channel 3401
Executes Command (t_1) 3303
Command (t_0) 3402
Response (t_2+ N) 3404
IoT Device 101
Application 3315
Local Wireless Communication (e.g., BTLE) 3310
Messaging Obfuscation 3410

Fig. 34

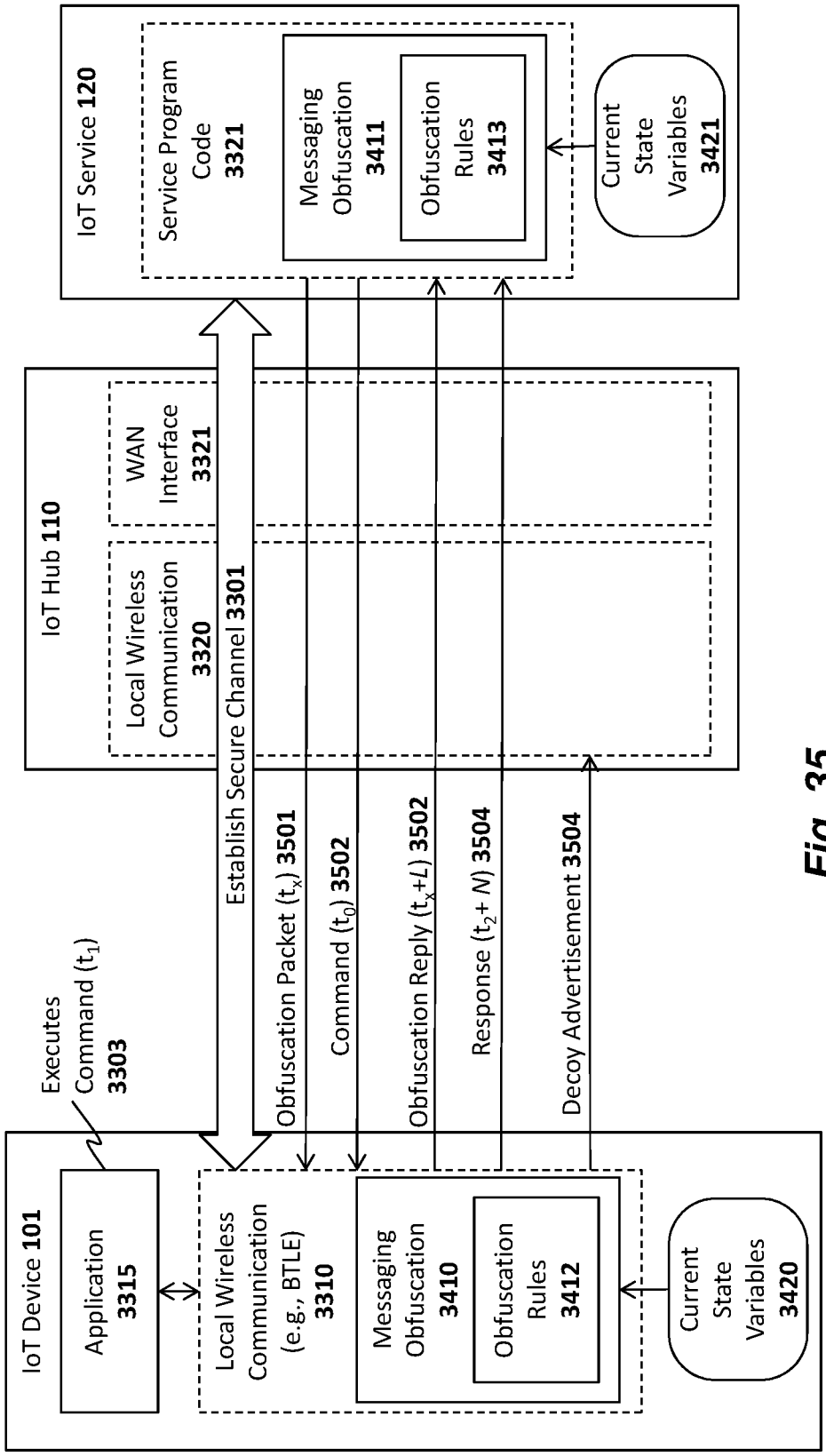
IoT Service 120
Service Program Code 3321
Messaging Obfuscation 3411
Obfuscation Rules 3413
Current State Variables 3421
IoT Hub 110
WAN Interface 3321
Local Wireless Communication 3320
Establish Secure Channel 3301
Executes Command (t_1) 3303
Obfuscation Packet (t_x) 3501
Command (t_0) 3502
Obfuscation Reply (t_x+L) 3502
Response (t_2+ N) 3504
Decoy Advertisement 3504
IoT Device 101
Application 3315
Local Wireless Communication (e.g., BTLE) 3310
Messaging Obfuscation 3410
Obfuscation Rules 3412
Current State Variables 3420

Fig. 35

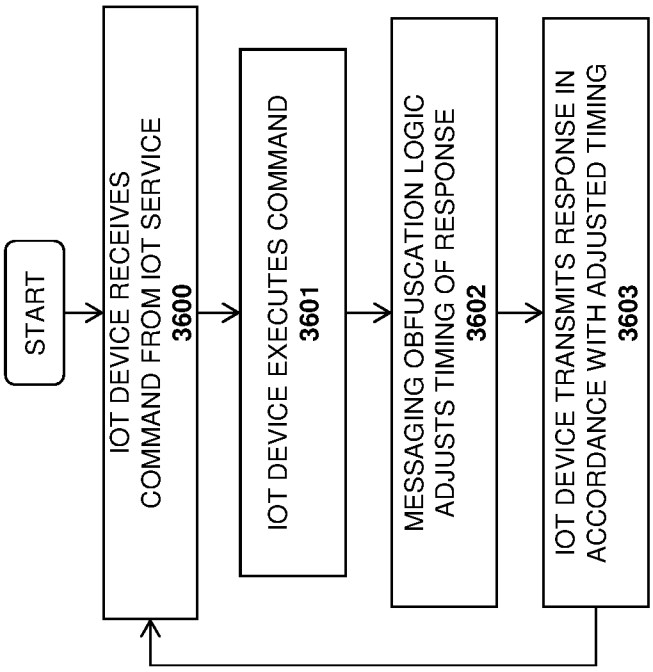
START
IOT DEVICE RECEIVES COMMAND FROM IOT SERVICE 3600
IOT DEVICE EXECUTES COMMAND 3601
MESSAGING OBFUSCATION LOGIC ADJUSTS TIMING OF RESPONSE 3602
IOT DEVICE TRANSMITS RESPONSE IN ACCORDANCE WITH ADJUSTED TIMING 3603

FIG. 36

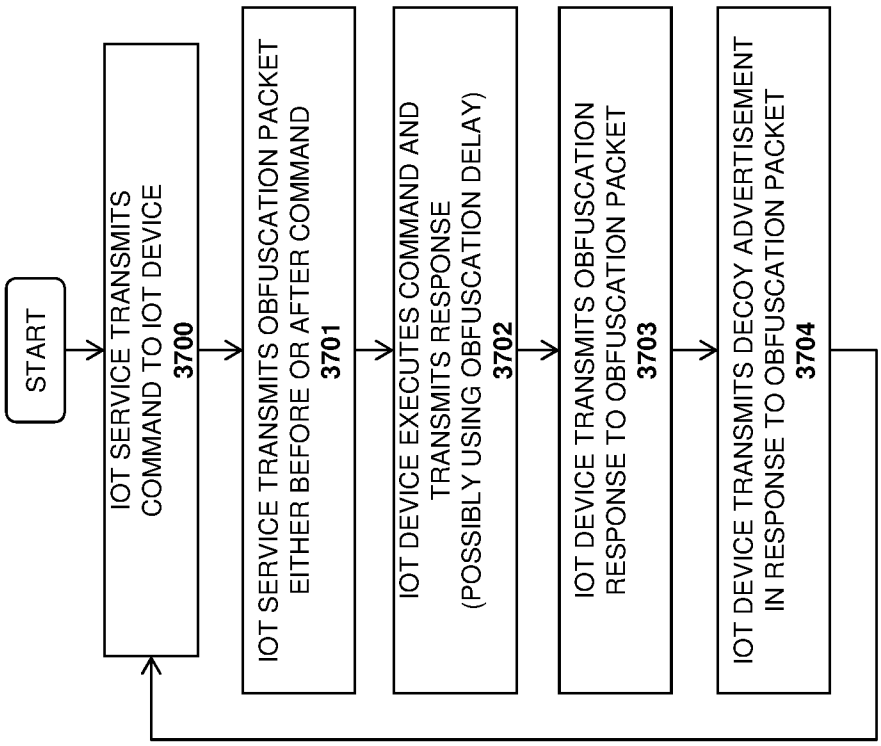
START
IOT SERVICE TRANSMITS COMMAND TO IOT DEVICE 3700
IOT SERVICE TRANSMITS OBFUSCATION PACKET EITHER BEFORE OR AFTER COMMAND 3701
IOT DEVICE EXECUTES COMMAND AND TRANSMITS RESPONSE (POSSIBLY USING OBFUSCATION DELAY) 3702
IOT DEVICE TRANSMITS OBFUSCATION RESPONSE TO OBFUSCATION PACKET 3703
IOT DEVICE TRANSMITS DECOY ADVERTISEMENT IN RESPONSE TO OBFUSCATION PACKET 3704

FIG. 37

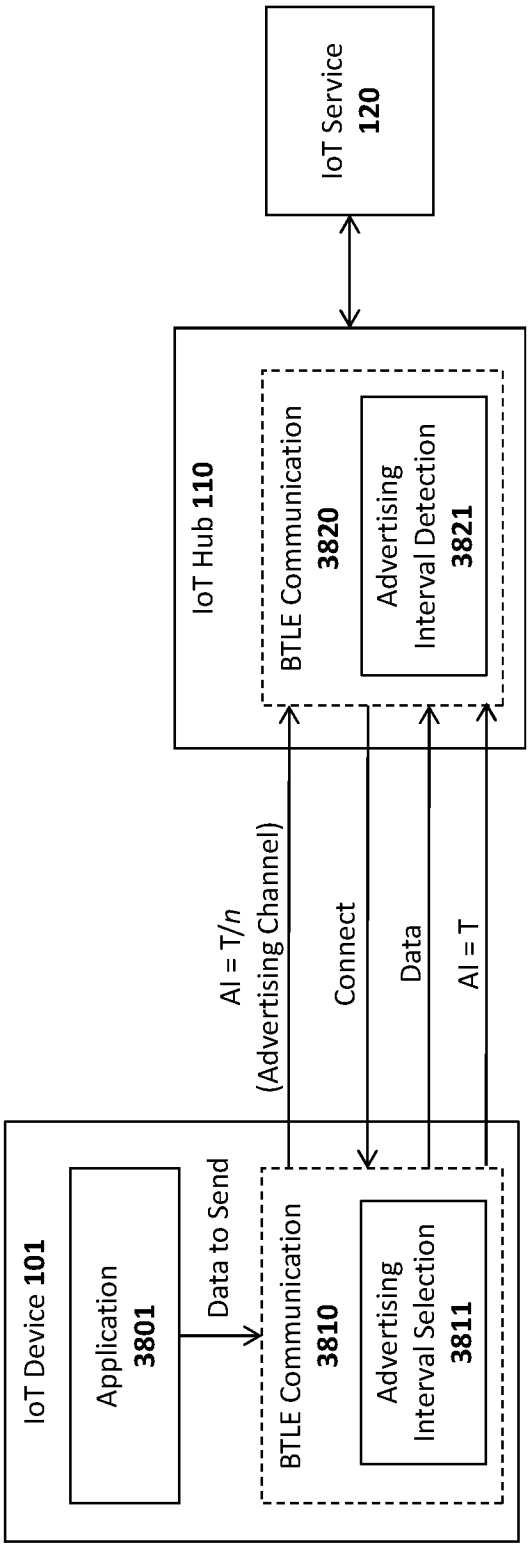
IoT Service
120
IoT Hub 110
BTLE Communication
3820
Advertising
Interval Detection
3821
AI = T/n
(Advertising Channel)
Connect
Data
AI = T
Normal Advertising
Interval (AI) = T
IoT Device 101
Application
3801
Data to Send
BTLE Communication
3810
Advertising
Interval Selection
3811

Fig. 38

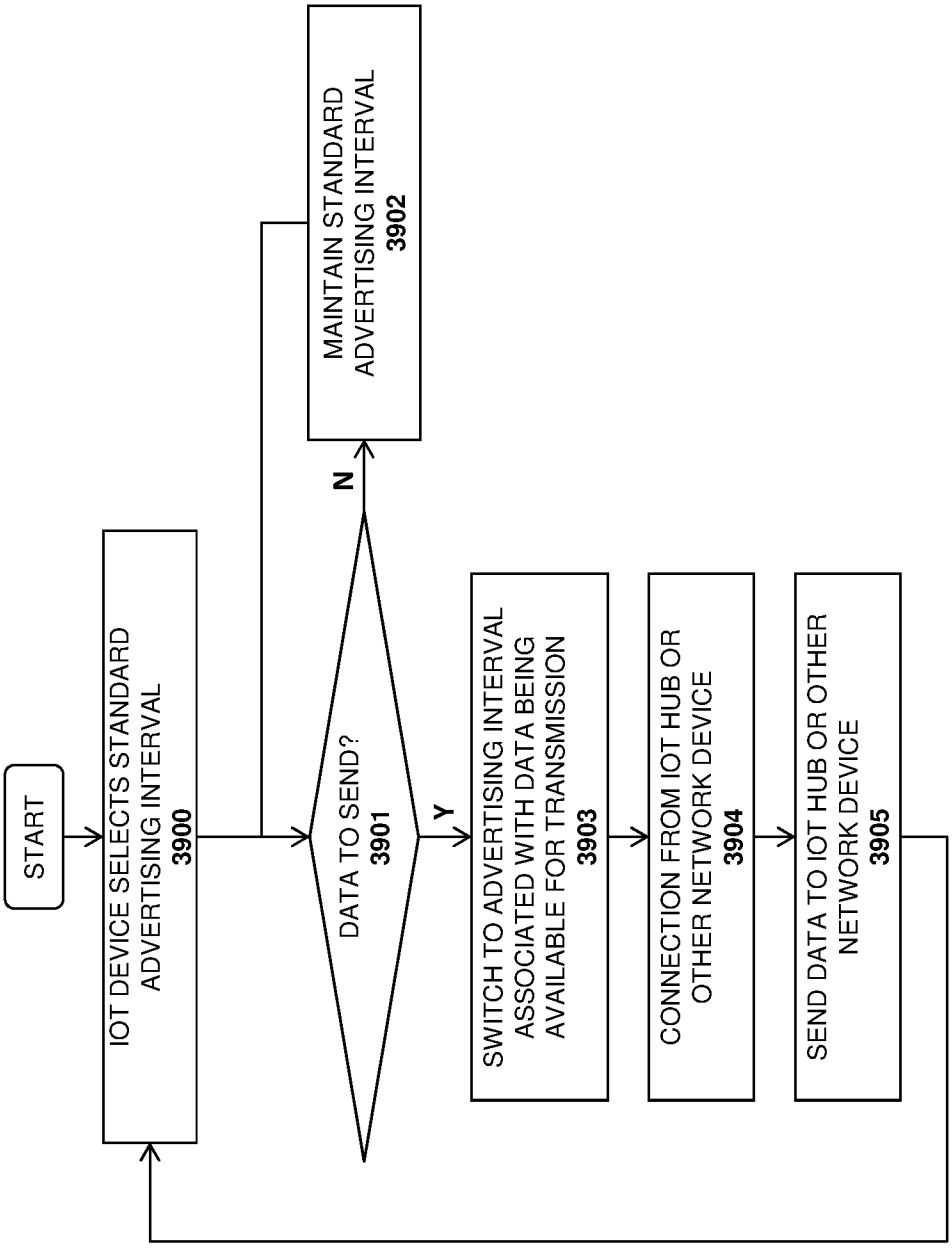
START
IOT DEVICE SELECTS STANDARD ADVERTISING INTERVAL 3900
DATA TO SEND? 3901
N
MAINTAIN STANDARD ADVERTISING INTERVAL 3902
Y
SWITCH TO ADVERTISING INTERVAL ASSOCIATED WITH DATA BEING AVAILABLE FOR TRANSMISSION 3903
CONNECTION FROM IOT HUB OR OTHER NETWORK DEVICE 3904
SEND DATA TO IOT HUB OR OTHER NETWORK DEVICE 3905

FIG. 39

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US16/66513

A. CLASSIFICATION OF SUBJECT MATTER
IPC - H04L9/08 (2017.01)
CPC - H04L9/006, H04L9/08, H04L9/14

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)
See Search History document

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 9,110,848 B1 (BELKIN INTERNATIONAL, INC.) 18 August 2015; entire document	1-24
A	US 2010/0306572 A1 (SALVARANI, A et al.) 02 December 2010; entire document	1-24
A	US 2009/0037998 A1 (ADHYA, S et al.) 05 February 2009; entire document	1-24
A	US 2014/0258405 A1 (PERKIN, S) 11 September 2014; entire document	1-24

☐ 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
29 March 2017 (29.03.2017)	17 APR 2017
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US16/66513

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
-***-Continued within extra sheet-***-

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
Group I: Claims 1-24

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US16/66513

-***-Continued from Box No. III - Observations where unity of invention is lacking-***-

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fee must be paid.

Group I: Claims 1-24 are directed towards a method to establish a secondary communication channel between an Internet of Things (IoT) device and a client device.
Group II: Claims 25-44 are directed towards systems and a method comprising obfuscation logic.
Group III: Claims 45-66 are directed towards a system and method comprising an advertising interval.

The inventions listed as Groups I-III do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons:

The special technical features of Group I include at least establishing a primary secure communication channel between the IoT device and an IoT service using a primary set of keys; performing a secondary key exchange using the primary secure communication channel, the client device and the IoT device each being provided with a secondary set of keys following the secondary key exchange; detecting that the primary secure communication channel is inoperative; and responsively establishing a secondary secure wireless connection between the client device and the IaT device using the secondary set of keys, the client device being provided with access to data and/or functions made available by the IoT device over the secondary secure wireless connection, which are not present in Groups II-III.

The special technical features of Group II include at least messaging obfuscation logic to modify timing for transmitting the response to the IoT service, which are not present in Groups I and III.

The special technical features of Group III include at least advertising interval selection logic to cause the first wireless networking interface to use a second advertising interval for advertising packets upon detecting that the IoT device has data to be transmitted to the IoT hub, the IoT hub to detect that the IoT device has data to be transmitted based on the change to the second advertising interval, which are not present in Groups I-II.

The common technical features shared by Groups I-III are an IoT device comprising a wireless communication interface to establish communication with an IoT service.

However, these common features are previously disclosed by US 2014/0241354 A1 to QUALCOMM INCORPORATED (hereinafter "Qualcomm"). Qualcomm discloses an IoT device comprising a wireless communication interface to establish communication with an IoT service (IoT devices organized into IoT device groups for wireless service discovery schemes; Abstract; Figs. 1A-1E; paragraphs [0031]).

Since the common technical features are previously disclosed by the Qualcomm reference, these common features are not special and so Groups I-III lack unity.