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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 August 2017 (31.08.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/146727 A1

(51) International Patent Classification:
H04W 12/02 (2009.01) *H04W 4/00* (2009.01)
H04K 3/00 (2006.01) *H04W 4/06* (2009.01)

(21) International Application Number:
PCT/US2016/019792

(22) International Filing Date:
26 February 2016 (26.02.2016)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP** [US/US]; 11445 Compaq Center Drive West, Houston, Texas 77070 (US).

(72) Inventors: **FAWAZ, Kassem**; 1501 Page Mill Rd., Palo Alto, California 94304-1100 (US). **KIM, Kyu-Han**; 1501 Page Mill Rd., Palo Alto, California 94304-1100 (US).

(74) Agents: **KWOK, Jonathan T.** et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79, Fort Collins, Colorado 80528 (US).

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

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

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

[Continued on next page]

(54) Title: DEVICE PRIVACY PROTECTION

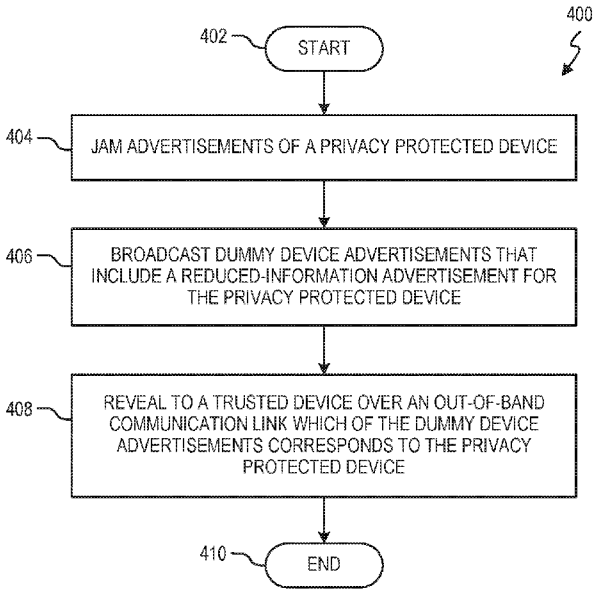

FIG. 4

(57) Abstract: Example implementations relate to advertisements of a privacy protected device. For example, advertisements of the privacy protected device are jammed. Additionally dummy device advertisements are broadcasted. The dummy device advertisements include a reduced-information advertisement for the privacy protected device.

WO 2017/146727 A1

Published:

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

DEVICE PRIVACY PROTECTION

Background

[0001] Devices may be equipped with sensors, actuators, electronics, software, and electronic communication technology. Such devices may collect data and may also exchange data with each other, with computing platforms, and/or with the Internet (e.g., a cloud-based platform, or more generally, the cloud). The device may broadcast electronic advertisements to announce its presence in order for a gateway to connect with it. Advertisements may contain data that identifies the device or a user of the device.

Brief Description of the Drawings

[0002] Various examples will be described below with reference to the following figures.

[0003] FIG. 1 depicts an example environment in which device privacy protection may be employed, according to an implementation.

[0004] FIG. 2 depicts a block diagram of an example apparatus that includes an advertisement jammer and an advertiser, according to an implementation.

[0005] FIG. 3 depicts a block diagram of an example apparatus that includes an advertisement jammer, an advertiser, and an access control manager, according to an implementation.

[0006] FIG. 4 is a flowchart of an example method for protecting the privacy of a device, according to an implementation.

[0007] FIG. 5 is a flowchart of an example method for protecting the privacy of a device, according to another implementation.

[0008] FIG. 6 is a block diagram of a gateway that includes a non-transitory, machine readable medium encoded with example instructions to

broadcast a jamming signal and broadcast dummy device advertisements, according to an implementation.

[0009] FIG. 7 is a block diagram of a gateway that includes a non-transitory, machine readable medium encoded with example instructions to set an advertisement interval and calculate a jamming duration, according to an implementation.

[0010] FIG. 8 depicts an example timing sequence of advertisement jamming and dummy device advertisements.

Detailed Description

[0011] Devices may be equipped with sensors, actuators, electronics, software, and electronic communication technology. Such devices may collect data and may also exchange data with each other, with computing platforms, and/or with the Internet (e.g., a cloud-based platform, or more generally, the cloud). Additionally, such devices may take the form of various objects, such as wearable devices, healthcare devices, vehicles, media devices, home automation devices, or appliances. This paradigm of interconnected devices may be referred to as the "Internet-of-Things" (IoT).

[0012] IoT devices may communicate with each other and with gateway devices by wireless communication technology, such as Bluetooth Low Energy (BLE), Bluetooth, Wi-Fi, ZigBee, near field communication, etc. Gateway devices, or "gateways", may include computers, smartphones, tablets, networking access points, or other electronic devices, and may act as a link between the IoT device and a user or between the IoT device and the cloud. For example, a user may utilize a gateway (e.g., a smartphone) to view data collected by an IoT device (e.g., a fitness tracker worn by the user). In another example, a gateway device (e.g., a smartphone or a networking access point) may collect data from an IoT device (e.g., a fitness tracker) and transmit the data to the cloud, for storage and/or analysis.

[0013] The IoT device may advertise its presence in order for a gateway to connect with it. For example, the BLE protocol defines the types of

advertisements to broadcast, how often advertisements are to be broadcast, and three advertising channels over which the advertisements are to be broadcast. Generally, an advertisement may be packet(s) of data that contain an address of the IoT device, along with other information, such as the IoT device's name, class or type, and offered services. A gateway can scan for these advertisements and initiate a connection to the advertising IoT device. However, advertisements reveal the IoT device's presence and may leak the aforementioned information, and with such knowledge, a third party observer may profile or identify a user (e.g., based on the type of devices carried), monitor a user's behavior, access or infer sensitive information, or attack the device (e.g., denial of service attacks).

[0014] More particularly, a user may be profiled from advertisement information in terms of health situation (e.g., presence of a glucose monitor may imply a diabetic condition), lifestyle (e.g., based on a presence of fitness trackers), preferences (e.g., based on brands of devices), personal interests (e.g., based on class of devices, such as toys, cameras, pet activity trackers, etc.), fingerprint of a home security system or security cameras, or user behavior (e.g., based on sensory values from a smart home environment).

[0015] Example techniques of the present disclosure may relate to jamming advertisements broadcasted by a privacy protected device and broadcasting dummy device advertisements, which include a reduced-information advertisement for the privacy protected device. By virtue of the foregoing, the systems and techniques of the present disclosure may be useful for hiding the privacy protected device from third party observers while allowing legitimate or trusted devices to discover the privacy protected device.

[0016] Referring now to the figures, FIG. 1 depicts an example environment 100 in which device privacy protection may be employed. A user 102 may possess or operate at least one device. In the example illustrated in FIG. 1, the user 102 possesses a device A 112, a device B 114, and a device C 116 (referred to generally or collectively as a device or devices 110). The devices 110 may have a combination of communication technology, sensor

and/or actuator capabilities, and hardware and/or software (e.g., machine readable instructions), and may be analogous to IoT devices discussed above. Examples of devices 110 may include wearable devices, healthcare devices, home automation or security devices, etc.

[0017] In some implementations, the devices 110 may communicate electronically with other devices (including e.g., gateway 120 and trusted device 160 to be described below) via wireless communication technology, such as Bluetooth, Bluetooth Low Energy (BLE), Wi-Fi, ZigBee, near field communication, etc. In particular, examples that follow may describe an implementation utilizing BLE, although the systems and techniques of the present disclosure may be applicable to other wireless communication technologies.

[0018] Devices 110 may send sensor data to, receive inputs or commands from, or otherwise interact with other devices (e.g., a computer, a smartphone, a tablet, the cloud) via the wireless communication technology. For example, a device 110 may communicate with a gateway 120 to present data to the user 102 (e.g., a computer or a smartphone serving as the gateway 120). Additionally or alternatively, a device 110 may connect through the gateway 120 (e.g., a computer, a smartphone, an access point) to communicate with the cloud 170. The cloud 170 may store and/or analyze data from the device 110, and the user 102 may access the cloud 170 via a web page, an application, or the like, to view the data and any related information.

[0019] In order to connect with other devices such as the gateway 120, the devices 110 may advertise their presence by wirelessly broadcasting advertisements. However, as discussed above, a third party 140 may observe and analyze the broadcasted advertisements, for example, by using a sniffer that captures and analyzes broadcasted data. The third party 140 may be untrustworthy or may be malicious (e.g., an adversary or attacker).

[0020] In some cases, the user 102 may wish to remain private as to possession of certain ones of devices 110 but not necessarily as to others of

devices 110. Which of the devices 110 the user 102 may deem sensitive and thus should be privacy protected may depend on the user's level of risk aversion. For example, device C 116 may be a healthcare or fitness related device, and the user 102 may thus desire privacy protection for device C 116.

[0021] The user 102 may configure the gateway 120 to protect the privacy of device C 116. For example, the gateway 120 may include a user interface or may be accessible via a web page, whereby the user 102 may specify which of the devices 110 is to be privacy protected (i.e., device C 116, in the present example). In some implementations, the gateway 120 may be a computer, a smartphone, a tablet, a computing device, a networking access point (e.g., a wireless access point, a router), etc.

[0022] Various implementations of the gateway 120 will be described further herein below with respect to FIGS. 2-7. In some implementations, the gateway 120 may protect the privacy of device C 116 by jamming advertisements broadcasted by device C 116 (e.g., by an advertisement jamming signal 122) without affecting advertisements 118 of other devices 112 and 114. By virtue of jamming the advertisements of device C 116, the presence of device C 116 may be effectively hidden.

[0023] The gateway 120 also broadcasts dummy device advertisements 124 that include advertisements for dummy devices (that is, fictitious devices made up by the gateway 120) as well as a reduced-information advertisement broadcast on behalf of device C 116, with identifying or sensitive information removed. By virtue of including a reduced-information advertisement for device C among advertisements for dummy device, the third party 140 has a lower certainty of identifying the real device C 116 or class of the device C 116.

[0024] For example, the third party 140 may observe visible devices 150 that include device A 152 corresponding to device A 112, and device B 154 corresponding to device B 114), by virtue of the advertisements 118 of those devices not being privacy protected. The third party 140 also observes dummy device C 156, dummy device D 158, and dummy device E 160, based

on the dummy device advertisements 124. Dummy device C 156 may be related (via the reduced-information advertisement) to device C 116 while dummy device D 158 and dummy device E 160 are made up by the gateway 120, but the third party 140 may not be able to distinguish those advertised devices because advertisements 124 are all broadcast from the same gateway 120 in similar format and fashion. Accordingly, the presence of privacy protected device C 116 is obfuscated among the dummy devices.

[0025] In some cases, the user 102 may trust other devices 160 to communicate with device C 116, such as the user's own devices or devices of trusted partners (e.g., friends, family, a healthcare provider, etc.). For example, a trusted device 160 may be a computer, a smartphone, etc. The trusted device 160 may connect with the gateway 120 over an out-of-band communication 126, such as Wi-Fi or any other different communication channel or technology different from the communication technology associated with the advertisements 118 (e.g., BLE). The gateway 120 can then reveal to the trusted device 160, over the out-of-band communication 126, which of the dummy device advertisements 124 correspond to the real device C 116.

[0026] By virtue of the foregoing, the presence of privacy protected devices may be hidden from third party observers while still permitting connection with trusted devices.

[0027] FIG. 2 depicts a block diagram of an example apparatus 200. In some implementations, the apparatus 200 may serve as or form part of the gateway 120 described above. The apparatus 200 may be useful for protecting the privacy of a privacy protected device 210 (also referred to as device 210). The privacy protected device 210 may be an IoT device, and may be similar to the device C 116 described above. The privacy protected device 210 includes communication technology (e.g., including a transceiver) to wirelessly broadcast recurring advertisements 212 to announce its presence and availability for connection with nearby electronic devices and to exchange data with those electronic devices upon successful connection.

The apparatus 200 may include the same or compatible communication technology utilized by the privacy protected device 210.

[0028] The apparatus 200 includes an advertisement jammer 202 and an advertiser 204, each of which may be any combination of hardware and programming to implement their respective functionalities as described herein. For example, the programming may be executable instructions stored on a non-transitory machine readable medium and the hardware for the components may include a processing resource to retrieve and/or execute those instructions. (The term "non-transitory" does not encompass transitory propagating signals.) For example, the processing resource may be a microcontroller, a microprocessor, central processing unit (CPU) core(s), application-specific integrated circuit (ASIC), a field programmable gate array (FPGA), and/or other hardware device suitable for retrieval and/or execution of instructions from the machine readable medium, and the machine readable medium may be random access memory (RAM), read-only memory (ROM), electrically erasable programmable read-only memory (EEPROM), flash memory, a hard disk drive, etc. Additionally or alternatively, the advertisement jammer 202 and the advertiser 204 may include one or more hardware devices including electronic circuitry or logic for implementing functionality described herein.

[0029] The apparatus 200 includes advertisement jammer 202 to jam (220) advertisements 212 broadcasted by the privacy protected device 210. Various jamming techniques may be utilized, and specific implementation details may depend on the communication technology utilized by the privacy protected device 210 to broadcast the advertisements 212. In some implementations, the advertisement jammer 202 may broadcast a jamming signal at a timing that coincides with advertising by the privacy protected device 210. In this manner, the jamming signal may jam, block, mask, corrupt or otherwise interfere with advertisements 212 broadcasted by the privacy protected device 210. Thus, the advertisements 212 may no longer be visible or observable by other electronic devices.

[0030] The apparatus 200 also includes an advertiser 204 to broadcast dummy device advertisements 230. The dummy device advertisements 230 are formatted and broadcasted according to the same communication technology that produced the advertisements 212. In some implementations, the advertiser 204 broadcasts the dummy device advertisements 230 and the advertisement jammer 202 broadcasts the jamming signal (e.g. 220) at different times. The dummy device advertisements 230 include advertisements for dummy devices and a reduced-information advertisement 232 on behalf of the privacy protected device 210, which will be described in turn.

[0031] The dummy device advertisements 230 include advertisements for dummy devices, that is, fictitious devices devised by the apparatus 200. Although fictitious, the dummy device advertisements 230 may be based on real-world devices (e.g., existing products as registered with an industry group responsible for standardization of the involved communication technology). The advertised dummy devices may fall under device classes (e.g., as defined by the industry group), where such classes may include a wearable device class, a toy device class, a health device class, a phone device class, an imaging device class, etc. In some implementations, the dummy device advertisements may include an advertisement for a dummy device within the same device class as the privacy protected device 210. Additionally or alternatively, the dummy device advertisements may include an advertisement for a dummy device in a different device class than the privacy protected device 210. By virtue of the foregoing, anonymity of the privacy protected device 210 may be preserved within the same device class and across device classes.

[0032] In some implementations, the apparatus 200 generates the reduced-information advertisement 232 by capturing an advertisement 212 of the privacy protected device 210 and modifying the advertisement 212 to remove sensitive information (e.g., user name, device name) while maintaining sufficient information to connect with the device 210 (e.g., a

device address). By virtue of including the reduced-information advertisement 232 among the dummy device advertisements 230, the presence of the privacy protected device 210 may be hidden among dummy devices, thus frustrating profiling attempts by a third party observer, while still allowing trusted devices to connect with the privacy protected device 210.

[0033] FIG. 3 depicts a block diagram of an example apparatus 300 for protecting the privacy of a privacy protected device 310 (also referred to as device 310). In some implementations, the apparatus 300 may serve as or form part of the gateway 120 described above. The apparatus 300 includes an advertisement jammer 302, a dummy device advertiser 304, and an access control manager 306, each of which will be described further herein below. The advertisement jammer 302, the advertiser 304, and the access control manager 306 may each be any combination of hardware (e.g., a processing resource, electronic circuitry, logic) and programming (e.g., instructions stored on a non-transitory machine readable medium) to implement their respective functionalities as described herein.

[0034] The privacy protected device 310 may be an IoT device, and may be similar to the device C 116 described above. The privacy protected device 310 includes communication technology to wirelessly broadcast recurring advertisements 312 to announce its presence and availability for connection with nearby electronic devices and to exchange data with those electronic devices upon successful connection. The apparatus 300 may include the same or compatible communication technology utilized by the privacy protected device 310. For example, the privacy protected device 310 may broadcast advertisements 312 and exchange data in a manner compatible with or in adherence to the BLE protocol. In such an implementation, the apparatus 300 also may include a BLE (or BLE-compatible) transceiver.

[0035] In view of privacy concerns related to advertisements 312, a user of the device 310 may want to protect the privacy of the device 310. The user may configure the apparatus 300 to protect the privacy of device 310, by way of an interface of the apparatus 300. For example, the apparatus 300 may be

in the form of a smartphone (or other computing device), in which case the interface may include a touch screen (or other input/output peripheral) to receive configuration data. In another example, the apparatus 300 may be in the form of networking equipment such as an access point, in which case the interface may be a web page or portal provided by the apparatus 300. The user may configure the apparatus 300 by specifying via the interface that the device 310 is to be privacy protected. In some implementations, the apparatus 300 may provide or display a list of detected devices, including device 310 as detected by virtue of advertisements 312, and the user may select device(s) from the list to configure the privacy protection to be provided by the apparatus 300.

[0036] The access control manager 306 may maintain (e.g., in storage or memory) a configurable list of privacy protected devices specified via the interface. In some implementations, the apparatus 300 may enter a learning period to learn about characteristics of device 310 and advertisements 312, in response to being configured to protect the privacy of the device 310. Some example aspects of learning by the apparatus 300 will be described further herein below.

[0037] With respect to the BLE protocol, advertisements 312 may be broadcast on any of three advertisement channels on the 2.4 GHz spectrum. Advertisements 312 are broadcast by the device 310 at a preset rate determined in the configuration of the device 310. More specifically, advertisements may occur at an interval between 20 milliseconds and 10.24 seconds, at increments of 0.625 milliseconds. Additionally, to avoid advertisements 312 from colliding with advertisements of other devices, the device 310 may wait a random delay between 0 and 10 milliseconds, on top of the advertisement interval, before advertising. Thus, the time between advertisements 312 may vary under the BLE protocol.

[0038] The advertisement jammer 302 jams (320) advertisements 312 broadcasted by the privacy protected device 310. In some implementations, the advertisement jammer 302 may broadcast a jamming signal on a wireless

advertising channel at a timing to coincide with advertising by the privacy protected device 310 to jam advertisements 312. The jamming signal may be broadcast periodically at an advertising interval (an interval between broadcast of jamming signals), and may be broadcast for a duration referred to as a jamming duration.

[0039] In the example implementation utilizing the BLE protocol, the advertisement jammer 302 may generate a jamming signal by commanding the BLE transceiver of the apparatus 300 to continuously transmit over one or more of the three BLE advertisement channels in a window of time. More particularly, the advertisement jammer 302 may issue a Host Controller Interface (HCI) transmission test command (e.g., 0x08 0x01e channel packet_length packet_type) to the BLE transceiver to initiate the continuous jamming transmission, and may issue another HCI command (e.g., 0x08 0x01f) to stop the jamming transmission.

[0040] In some implementations, the advertisement jammer 302 may learn the advertisement interval for broadcasting the jamming signal. For example, the advertisement jammer 302 may learn the advertising interval during the aforementioned learning period, or any other time after the learning period (e.g., by user command or by periodically). The learning may be based on multiple advertisements 312 observed by the apparatus 300 during the learning period. The time interval between successive observed advertisements 312 is referred to as an "observed time interval."

[0041] The advertisement jammer 302 may learn the advertisement interval as based on a minimum interval from among the observed time intervals. For BLE-based advertisements 312, the advertisement interval may be a minimum interval that is evenly divisible by 0.625 milliseconds, the BLE specification for advertisement interval increment.

[0042] As discussed above, BLE-based advertisements 312 may be broadcast after a random delay in a range of 0 to 10 milliseconds. Accordingly, to account for the random delay, the advertisement jammer 302 may broadcast the jamming signal for a long jamming duration of at least 10

milliseconds to cover the full possible range of delay and provide that advertisements 312 are jammed. In some implementations, to account for cumulative uncertainty in when successive advertisements 312 are actually broadcasted owing to the random delay, the jamming duration may be lengthened for each successive jamming signal broadcast. For example, if an advertisement interval is 1000 milliseconds and the jamming duration is 10 milliseconds, a first jamming signal may be broadcast at 0 seconds for 10 milliseconds duration, a second jamming signal may be broadcast at 1000 milliseconds for a 20 millisecond duration, a third jamming signal may be broadcast at 2000 milliseconds for a 30 millisecond duration, a fourth jamming signal may be broadcast at 3000 milliseconds for a 40 millisecond duration, and so forth.

[0043] In another implementation, the advertisement jammer 302 may learn the jamming duration (e.g., during the learning period, or any time thereafter), rather than defaulting to a 10 millisecond duration. Learning the jamming duration may be useful if the advertisements 312 are not utilizing the full range of delay (e.g., delays being generally shorter than 10 milliseconds), and thus jamming may be reduced to avoid interference with other transmissions, such as the broadcast of dummy device advertisements which will be described below. The advertisement jammer 302 may base the jamming duration on an empirical distribution (e.g., a histogram, an empirical density function, etc.) of arithmetic differences between the observed time intervals and the learned advertisement interval.

[0044] More particularly, the advertisement jammer 302 may select a percentile-rank (e.g., 75th percentile, 80th percentile, 90th percentile, etc.) of the distribution of arithmetic differences as the jamming delay. In this manner, the jamming signal will jam most, if not all, of the randomly varying broadcasts of advertisements 312. The learned jamming duration may also be lengthened for successive broadcasts of the jamming signal, in the manner described above. An example method of learning the advertising interval and the jamming duration will be described below with respect to FIG. 3.

[0045] The advertisement jammer 302 may listen for advertisements 312 in some implementations, including during the jamming duration. During active jamming, the advertisements 312 may be completely hidden or may be corrupted. The advertisement jammer 302 may be able to deduce that a corrupted advertisement 312 belongs to the privacy protected device 310, by virtue of contextual information, such as a signal power level associated with the corrupted advertisement 312 or certain identifying information in the corrupted advertisement 312 despite an invalid checksum. A detected advertisement 312, whether corrupted or otherwise, may be used by the advertisement jammer 302 as a new reference point for the jamming timing. The advertisement jammer 302 may broadcast a next jamming signal at an advertisement interval after the detected advertisement 312 and for the original jamming duration (i.e., a default value such as 10 milliseconds or a learned jamming duration).

[0046] The advertiser 304 broadcasts dummy device advertisements 330, which may be analogous in many respects to the dummy device advertisements 230. For example, the dummy device advertisements may include advertisements for dummy devices in the same device class and/or different device class than that of the privacy protected device 310. Additionally, the dummy device advertisements 330 include a reduced-information advertisement 332 for the privacy protected device 310, which may be analogous in many respects to the reduced-information advertisement 232 described above. In some implementations, the advertiser 304 may observe advertisements 312 during the aforementioned learning period and may generate the reduced-information advertisement 232 from those learning period advertisements 312 (e.g., by removing sensitive or identifying information).

[0047] In implementations where the advertisements 312 and jamming 320 are BLE-based, the dummy device advertisements 330 also are compatible with the BLE protocol. The advertiser 304 may broadcast the dummy device

advertisements 330 at a time when the advertisement jammer 302 is not broadcasting a jamming signal (e.g., outside the jamming duration).

[0048] The advertiser 304 may use the same data structure to generate the advertisements of the dummy devices and the reduced-information advertisement. The advertiser 304 may compute a schedule for advertising the dummy device advertisements 330. To send the dummy advertisements in a BLE environment, the advertiser 304 may utilize HCI commands to change the address of the BLE transceiver of the apparatus 300, set the advertisement data and scan response to match or simulate the dummy devices, and then broadcast on BLE advertising channels. By virtue of sending using the same logic and hardware (e.g., BLE transceiver) to broadcast advertisements from the apparatus 300, all of the dummy device advertisements 330 (including the reduced-information advertisement 332) will indistinguishably originate from the same hardware, confusing any third party observers.

[0049] A user may wish to connect a trusted device 340 to the privacy protected device 310. Although the advertisements 312 are jammed, the advertisement jammer 302 broadcasts the reduced-information advertisement 332 on behalf of the device 310, by which the trusted device 340 may connect to the device 310. However, because the reduced-information advertisement 332 is hidden among the other dummy device advertisements 330 to frustrate profiling by a third party, the trusted device 340 also may not correctly distinguish which dummy device advertisement 330 corresponds to the privacy protected device 310.

[0050] To connect the trusted device 340 and the privacy protected device 310, the trusted device 340 may first connect to the apparatus 300 (and in particular, the access control manager 306) over an out-of-band communication link. In some implementations, the trusted device 340 may connect to the apparatus 300 using, for example, a password, a certificate, or other security measure, to confirm its trusted status (i.e., that the user of the privacy protected device 310 approves connection between the privacy

protected device 310 and the trusted device 310). The out-of-band communication link may be a communication technology different from the communication technology by which the advertisements 312, 330 are broadcast. For example, in implementations where advertisements 312, 330 are BLE-based, the out-of-band communication link may utilize Wi-Fi.

[0051] Once connected, the access control manager 306 indicates (350) to the trusted device 340, over the out-of-band communication link, which of the dummy device advertisements 330 corresponds to the privacy protected device 310. For example, the access control manager 306 may share with the trusted device 340 the device address and/or other information (e.g., device type) included in the reduced-information advertisement 332. The access control manager 306 then schedules a future window of time to temporarily pause the jamming 320 by advertisement jammer 302, so that the trusted device 340 can negotiate a connection with the privacy protected device 310.

[0052] FIG. 4 is a flowchart of an example method 400 for protecting the privacy of a device, according to an implementation. Method 400 may be implemented in the form of executable instructions stored on a machine readable medium and executed by a processing resource and/or in the form of electronic circuitry. For example, method 400 is described below as being performed by a gateway device, such as the gateway 120 of FIG. 1. Various other devices may perform method 400 as well, such as, for example, the apparatuses 200 or 300 (or gateway 500 or 600 described below). In some implementations of the present disclosure, the blocks of method 400 may be executed substantially concurrently, may be ongoing, and/or may repeat.

[0053] The method 400 begins at block 402, and continues to block 404, where a gateway device jams advertisements of a privacy protected device. At block 406, the gateway device broadcasts dummy device advertisements that include a reduced-information advertisement for the privacy protected device. At block 408, the gateway device reveals, to a trusted device over an out-of-band communication link, which of the dummy device advertisements

corresponds to the privacy protected device. The method 400 ends at block 410.

[0054] FIG. 5 is a flowchart of an example method 500 for protecting the privacy of a device, according to another implementation. As with method 400, method 500 may be implemented in the form of executable instructions stored on a machine readable medium and executed by a processing resource and/or in the form of electronic circuitry. Method 500 is described below as being performed by a gateway device, such as the gateway 120 of FIG. 1. At least some portions of method 500 also may be performed by apparatuses 200 or 300 (or gateway 500 or 600 described below). In some implementations of the present disclosure, one or more blocks of method 500 may be executed substantially concurrently or in a different order than shown in FIG. 5. Some of the blocks of method 500 may, at times, be ongoing and/or may repeat. In some implementations of the present disclosure, method 500 may include more or fewer blocks than are shown in FIG. 5.

[0055] The method 500 begins at block 502, and continues to block 503, where the gateway device may receive configuration data from a user identifying a device that is to be privacy protected. For example, the gateway device may provide a list of detected devices, and the user may select from the list (via an interface of the gateway device) a device to receive privacy protection.

[0056] At block 504, the gateway device may observe an original (i.e., not jammed) advertisement broadcasted by a privacy protected device and generate a reduced-information advertisement by modifying the original advertisement of the privacy protected device to remove name information and maintain a device address of the privacy protected device. The reduced-information advertisement may also maintain a device type from the original advertisement, or other non-sensitive information. In some implementations, generating the reduced-information advertisement from the original advertisement includes zeroing out payload fields of the original

advertisement that carry sensitive information (e.g., user identification, device name, device brand, sensor data).

[0057] At block 506, the gateway device generates dummy device advertisements. The dummy device advertisements may include an advertisement for a dummy device in a different device class than the privacy protected device, an advertisement for a dummy device within the same device class as the privacy protected device, or a combination thereof.

[0058] At block 508, the gateway device learns a timing to broadcast a jamming signal to coincide with advertising by the privacy protected device. The timing may be described in terms of an advertisement interval and a jamming duration. The advertisement interval controls an interval between broadcast of consecutive jamming signals and the jamming duration controls a duration of the jamming signal.

[0059] In some implementations, the learning at block 508 includes observing a plurality of advertisements broadcasted by the privacy protected device and calculating time intervals between successive advertisements of the plurality of advertisements. The gateway device may then set the advertisement interval to be a minimum interval from among the calculated time intervals. The gateway device may also calculate the jamming duration from a distribution of arithmetic differences resulting from subtraction of the advertisement interval from the calculated time intervals. In some implementations, the jamming duration may be a percentile-rank of the distribution.

[0060] In some implementations, blocks 504, 506, 508 may be deemed to occur during a learning period. After block 508, method 500 may proceed in parallel, in some implementations, along a first path that includes blocks 510, 512 and a second path that includes blocks 516, 518. In some implementations, the first path and the second path may proceed asynchronously. The paths will be described in turn.

[0061] At block 510, the gateway device jams advertisements of a privacy protected device. The jamming may include broadcasting a jamming signal on a wireless advertising channel at a timing to coincide with advertising by the privacy protected device, using the advertisement interval and the jamming duration learned at block 508.

[0062] At block 512, the gateway device broadcasts dummy device advertisements. More particularly, the gateway device broadcasts the reduced-information advertisement generated at block 504 and the dummy device advertisements generated at block 506. After block 512, the method 500 proceeds to block 514, but before describing block 514, blocks 516 and 518 will first be described.

[0063] At block 516, the gateway device determines whether an out-of-band communication from a trusted device has been received. More particularly, the out-of-band communication may be a request by the trusted device to connect to the privacy protected device. Additionally, the trusted device may authenticate itself to the gateway device as part of the out-of-band communication (e.g., via password, certificate, etc.). If no out-of-band communication has been received ("NO" at block 516), the method 500 proceeds to block 514. If an out-of-band communication has been received ("YES" at block 516), the method proceeds to block 518, where the gateway device reveals over an out-of-band communication link, which of the dummy device advertisements corresponds to the privacy protected device. After block 518, the method proceeds to block 514.

[0064] At block 514, the gateway device may determine whether to continue privacy protection for the privacy protected device. If privacy protection is to continue ("NO" at block 514), the gateway device proceeds back to block 510 and/or block 516. If privacy protection is to end ("YES" at block 514), the gateway device proceeds to block 520 and the method 500 ends. In some implementations, some example cases for ending privacy protection include a user configuring the gateway device to cease privacy

protection or the privacy protected device exiting a transmission range of the gateway device.

[0065] FIG. 6 is a block diagram depicting an example gateway 600 that includes a processing resource 602 coupled to a non-transitory machine readable medium 604 storing (or encoded with) instructions 606, 608, 610, 612. The gateway 600 may form part of the gateway 120 described above.

[0066] In some implementations, the processing resource 602 may be a microcontroller, a microprocessor, CPU core(s), an ASIC, an FPGA, and/or other hardware device suitable for retrieval and/or execution of instructions stored on the machine readable medium 604. Additionally or alternatively, the processing resource 602 may include one or more hardware devices, including electronic circuitry, for implementing functionality described herein.

[0067] The machine readable medium 604 may be any medium suitable for storing executable instructions, such as RAM, ROM, EEPROM, flash memory, a hard disk drive, an optical disc, or the like. In some example implementations, the machine readable medium 604 may be a tangible, non-transitory medium. The machine readable medium 604 may be disposed within the gateway 600, as shown in FIG. 6, in which case the executable instructions may be deemed installed or embedded on the gateway 600. Alternatively, the machine readable medium 604 may be a portable (e.g., external) storage medium, and may be part of an installation package.

[0068] As described further herein below, the machine readable medium 604 may be encoded with a set of executable instructions 606, 608, 610, 612. It should be understood that part or all of the executable instructions and/or electronic circuits included within one box may, in alternate implementations, be included in a different box shown in the figures or in a different box not shown.

[0069] Instructions 608, when executed, cause the processing resource 602 to maintain a device privacy protection list that includes a privacy protected device. Instructions 610, when executed, cause the processing

resource 602 to broadcast a jamming signal on a wireless advertising channel at a timing to coincide with advertising by the privacy protected device. Instructions 612, when executed, cause the processing resource 602 to broadcast dummy device advertisements on the wireless advertising channel, the dummy device advertisements including a reduced-information advertisement for the privacy protection device. Instructions 614, when executed, cause the processing resource 602 to respond to a trusted device over an out-of-band communication link with an indication of which dummy device advertisement corresponds to the privacy protected device.

[0070] FIG. 7 is a block diagram depicting an example gateway 700 that includes a processing resource 702 coupled to a non-transitory machine readable medium 704 storing (or encoded with) instructions 706, 708, 710, 712. The processing resource 702 and the non-transitory machine readable medium 704 may be analogous in many respects to the processing resource 602 and the non-transitory machine readable medium 604, respectively. The gateway 700 may form part of the gateway 120 described above.

[0071] Instructions 706, when executed, cause the processing resource 702 to observe a plurality of advertisements broadcasted by a privacy protected device. Instructions 708, when executed, cause the processing resource 702 to calculate time intervals between successive advertisements of the plurality of advertisements. Instructions 710, when executed, cause the processing resource 702 to set an advertisement interval to be a minimum interval from among the calculated time intervals. Instructions 712, when executed, cause the processing resource 702 to calculate a jamming duration from an empirical distribution of arithmetic differences between the time intervals and the advertisement interval. The timing for broadcast of a jamming signal by e.g., instructions 610 described above may be based on the advertisement interval and the jamming duration, with the advertisement interval controlling an interval between broadcast of consecutive jamming signals and the jamming duration controlling a duration of the jamming signal.

[0072] FIG. 8 depicts an example timing sequence of broadcasts 800, including advertisement jamming and dummy device advertisements. For example, jamming signals and dummy device advertisements may be described below as being broadcast by a gateway, such as the gateway 120 of FIG. 1, but various other devices may perform broadcasting as well, such as, for example, the apparatuses 200 or 300 or the gateways 600 or 700. The timing sequence shown may be useful for jamming a privacy protected device that operates in accordance with a protocol, such as BLE, that broadcasts advertisements at a fixed interval plus a random delay (e.g., 0 to 10 milliseconds, under BLE). Accordingly, in some examples, the gateway and privacy protected device may operate a same or compatible communications technology, such as BLE.

[0073] A gateway (e.g., similar to 120) may first detect an advertisement 810-1 broadcasted by a privacy protected device (e.g., similar to 116), which is deemed a reference point. The gateway then waits an advertisement interval 802 from the reference point. For example, the advertisement interval 802 may be learned by the gateway in a manner analogous to that described above with respect to the advertisement jammer 302, block 508 of method 500, or instructions 706, 708, 710.

[0074] After waiting the advertisement interval 802, the gateway broadcasts a first jamming signal after the reference point (810-1) for a duration 804-1. The duration for the first jamming signal is a base duration that may be a default value (e.g., a maximum random delay value associated with the communication protocol of the privacy protected device, such as 10 milliseconds for BLE) or may be a duration learned by the gateway in a manner analogous to that described above with respect to advertisement jammer 302, block 508 of method 500, or instructions 712. Because the gateway may not know ahead of time when the privacy protected device will broadcast its advertisement owing to the random delay, the jamming signal may be broadcasted continuously for the base duration to account for cover most or all of the random delay in privacy protected device advertising.

[0075] The gateway then waits for another advertisement interval 802 (e.g., timed from the start of the first jamming signal, having duration 804-1) before broadcasting a second jamming signal after the reference point (810-1), the second jamming signal having a duration 804-2. Meanwhile, as the gateway waits between jamming signals, the gateway broadcasts the dummy device advertisements 806, which includes a reduced-information advertisement for the privacy protected device hidden among advertisements for dummy devices.

[0076] The uncertainty in random delay and thus in the actual timing of the privacy protected device advertising compounds with each successive advertisement interval. Accordingly, jamming duration 804-2 is longer than the duration 804-1 in order to provide jamming in view of that increased uncertainty. For example, the duration 804-2 may be the proceeding duration 804-1 plus the base duration. Similarly, a third jamming signal has a duration 804-3 that may be the duration 804-2 plus the base duration.

[0077] Occasionally, the gateway may detect advertisements broadcasted by the privacy protected device. For example, in FIG. 8, the gateway may detect advertisement 810-2 occurring during the N-th jamming signal after the detected advertisement 810-1. The advertisement 810-2 may occur during a jamming duration (e.g., 804-N), in which case the advertisement 810-2 may be corrupted due to the jamming but still attributable to the privacy protected device by virtue of contextual information. In some cases, the advertisement 810-2 may be outside a jamming duration.

[0078] The gateway may deem the newly detected advertisement 810-2 as a new reference point. For example, the gateway may wait an advertisement interval 802 from the new reference point (i.e., detected advertisement 810-2) and then broadcast a jamming signal with duration 804-(N+1), which may be the base duration. The second jamming signal after the new reference point (810-2) may have a duration 804-(N+2) that is the duration 804-(N+1) plus the base duration, and so on.

[0079] A trusted device (e.g., similar to device 160) may communicate with the gateway via an out-of-band communications link. For example, out-of-band communications 850 may be performed over Wi-Fi while communications 800 are performed over BLE. In response to a request 852 from the trusted device to connect to the privacy protected device, the gateway may temporarily stop jamming (e.g., represented by the dashed box for the jamming duration 804-(N+3)) and allow connection 812 via BLE between the privacy protected device and the trusted device. The temporary pause in jamming may be scheduled by the gateway, and may not necessarily happen in the next instance of jamming immediately following the request 852.

[0080] In view of the foregoing description, it can be appreciated that a gateway device (e.g., a networking access point, a smartphone, other computing device) may protect the privacy of a user and a user's device, such as an Internet-of-Things devices. More particularly, such privacy protection may be achieved without modifying the underlying communications technology or protocol of the device (e.g., BLE). Additionally, privacy protection may be provided irrespective of the device type or class (i.e., privacy protection is device agnostic). Also, the gateway device may provide access control functionality by virtue of revealing which dummy device advertisement corresponds to the privacy protected device just to trusted devices over an out-of-band communications link.

[0081] In the foregoing description, numerous details are set forth to provide an understanding of the subject matter disclosed herein. However, implementation may be practiced without some or all of these details. Other implementations may include modifications and variations from the details discussed above. It is intended that the following claims cover such modifications and variations.

What is claimed:

1. An apparatus comprising:

an advertisement jammer to jam advertisements broadcasted by a privacy protected device; and

an advertiser to broadcast dummy device advertisements, the dummy device advertisements including a reduced-information advertisement for the privacy protected device.

2. The apparatus of claim 1, further comprising an access control manager to:

maintain a configurable list of privacy protected devices, and

indicate, to a trusted device over an out-of-band communication link, which of the dummy device advertisements corresponds to the privacy protected device.

3. The apparatus of claim 1, wherein the advertisements broadcasted by the privacy protected device and the dummy device advertisements are compatible with a Bluetooth Low Energy protocol.

4. The apparatus of claim 1, wherein the dummy device advertisements include an advertisement for a dummy device in a different device class than the privacy protected device.

5. The apparatus of claim 1, wherein the dummy device advertisements include an advertisement for a dummy device within the same device class as the privacy protected device.

6. The apparatus of claim 1, wherein the advertisement jammer is to:

broadcast a jamming signal on a wireless advertising channel at a timing to coincide with advertising by the privacy protected device to jam advertisements broadcasted by the privacy protected device, and

learn an advertisement interval and a jamming duration for broadcasting of the jamming signal,

the advertisement interval being an interval between broadcast of jamming signals and being based on a minimum interval from among observed intervals between advertisements broadcasted by the privacy protected device, and

the jamming duration being a duration of the jamming signal and being based on an empirical distribution of arithmetic differences between the observed intervals and the advertisement interval.

7. The apparatus of claim 6, wherein the advertiser broadcasts the dummy device advertisements and the advertisement jammer broadcasts the jamming signal at different times.

8. A method comprising:

jamming, by a gateway device, advertisements of a privacy protected device;

broadcasting, by the gateway device, dummy device advertisements that include a reduced-information advertisement for the privacy protected device; and

revealing, by the gateway device to a trusted device over an out-of-band communication link, which of the dummy device advertisements corresponds to the privacy protected device.

9. The method of claim 8, further comprising generating the reduced-information advertisement by modifying an original advertisement of the privacy protected device to remove name information and to maintain a device address.

10. The method of claim 8, further comprising generating the dummy device advertisements, including an advertisement for a dummy device in a different device class than the privacy protected device or an advertisement

for a dummy device within the same device class as the privacy protected device.

11. The method of claim 8, wherein the jamming includes broadcasting, by the gateway device, a jamming signal on a wireless advertising channel at a timing to coincide with advertising by the privacy protected device.

12. The method of claim 11, further comprising learning the timing by the gateway device,

wherein the timing includes an advertisement interval that controls an interval between broadcast of consecutive jamming signals and a jamming duration that controls a duration of the jamming signal, and

the learning includes:

observing a plurality of advertisements broadcasted by the privacy protected device,

calculating time intervals between successive advertisements of the plurality of advertisements,

setting the advertisement interval to be a minimum interval from among the calculated time intervals, and

calculating the jamming duration from a distribution of arithmetic differences between the time intervals and the advertisement interval.

13. A non-transitory machine readable medium storing instructions executable by a processing resource of a gateway, the non-transitory machine readable medium comprising:

instructions to maintain a device privacy protection list that includes a privacy protected device;

instructions to broadcast a jamming signal on a wireless advertising channel at a timing to coincide with advertising by the privacy protected device; and

instructions to broadcast dummy device advertisements on the wireless advertising channel, the dummy device advertisements including a reduced-information advertisement for the privacy protection device.

14. The non-transitory machine readable medium of claim 13, further comprising:

instructions to observe a plurality of advertisements broadcasted by the privacy protected device;

instructions to calculate time intervals between successive advertisements of the plurality of advertisements;

instructions to set an advertisement interval to be a minimum interval from among the calculated time intervals; and

instructions to calculate a jamming duration from an empirical distribution of arithmetic differences between the time intervals and the advertisement interval,

wherein the timing is based on the advertisement interval and the jamming duration, the advertisement interval controlling an interval between broadcast of consecutive jamming signals and the jamming duration controlling a duration of the jamming signal.

15. The non-transitory machine readable medium of claim 13, further comprising:

instructions to respond to a trusted device over an out-of-band communication link with an indication of which dummy device advertisement corresponds to the privacy protected device.

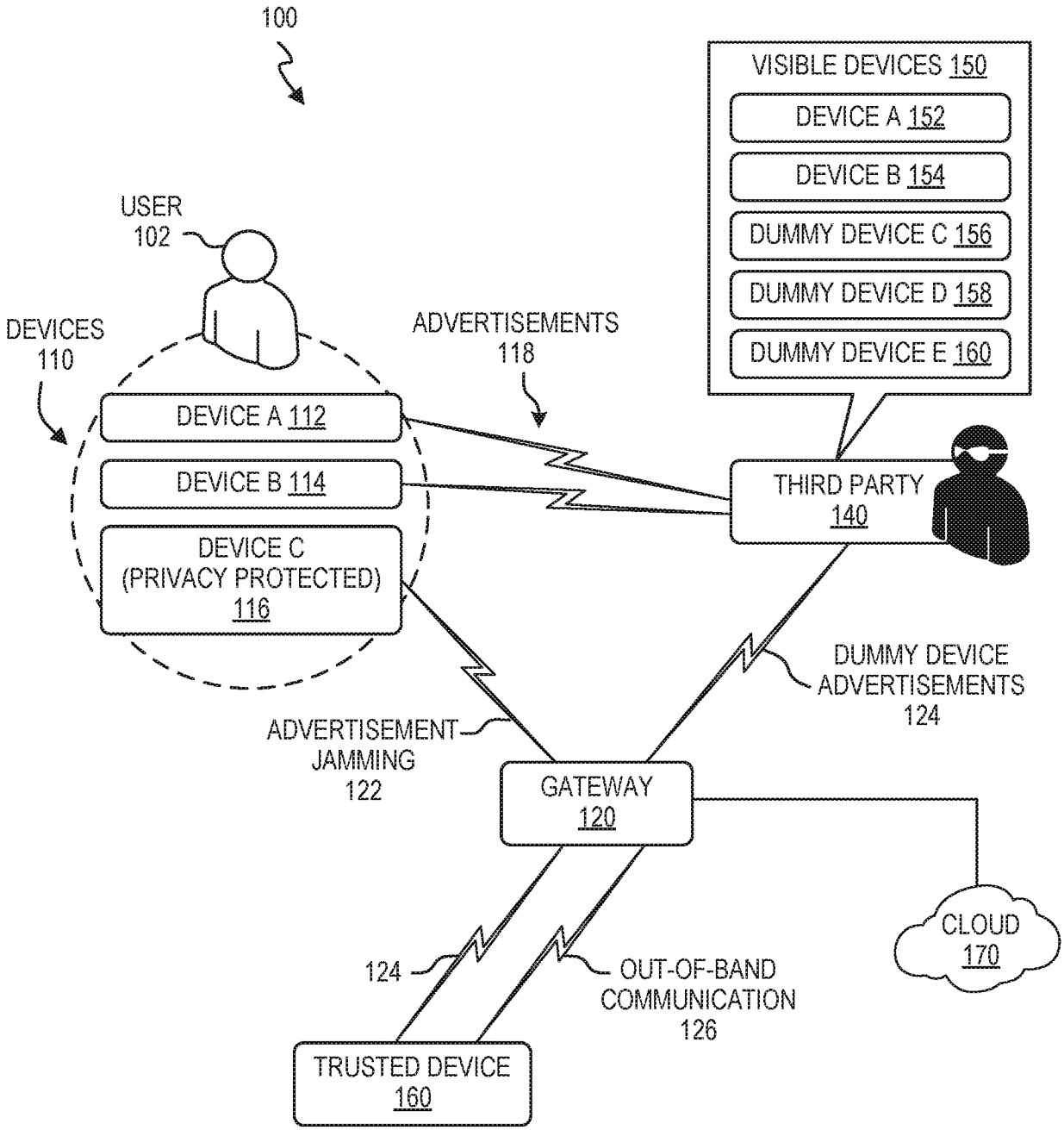
100
VISIBLE DEVICES 150
DEVICE A 152
DEVICE B 154
DUMMY DEVICE C 156
DUMMY DEVICE D 158
DUMMY DEVICE E 160
USER
102
DEVICES
110
ADVERTISEMENTS
118
DEVICE A 112
DEVICE B 114
DEVICE C
(PRIVACY PROTECTED)
116
THIRD PARTY
140
DUMMY DEVICE
ADVERTISEMENTS
124
ADVERTISEMENT
JAMMING
122
GATEWAY
120
CLOUD
170
124
OUT-OF-BAND
COMMUNICATION
126
TRUSTED DEVICE
160

FIG. 1

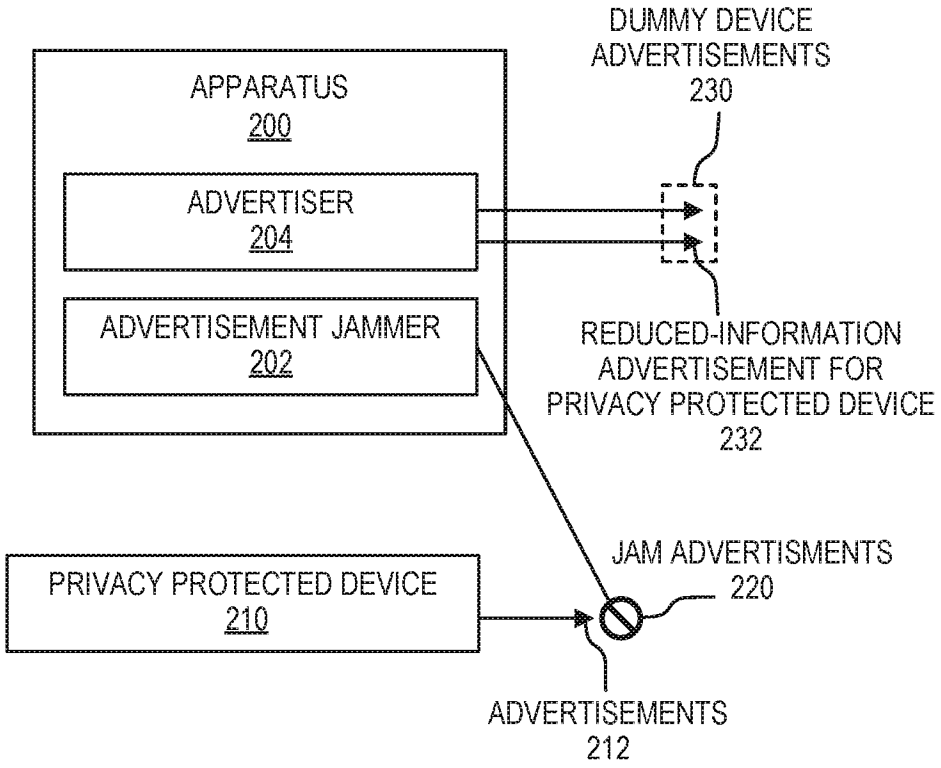
DUMMY DEVICE ADVERTISEMENTS 230
APPARATUS 200
ADVERTISER 204
ADVERTISEMENT JAMMER 202
REDUCED-INFORMATION ADVERTISEMENT FOR PRIVACY PROTECTED DEVICE 232
JAM ADVERTISMENTS 220
PRIVACY PROTECTED DEVICE 210
ADVERTISEMENTS 212

FIG. 2

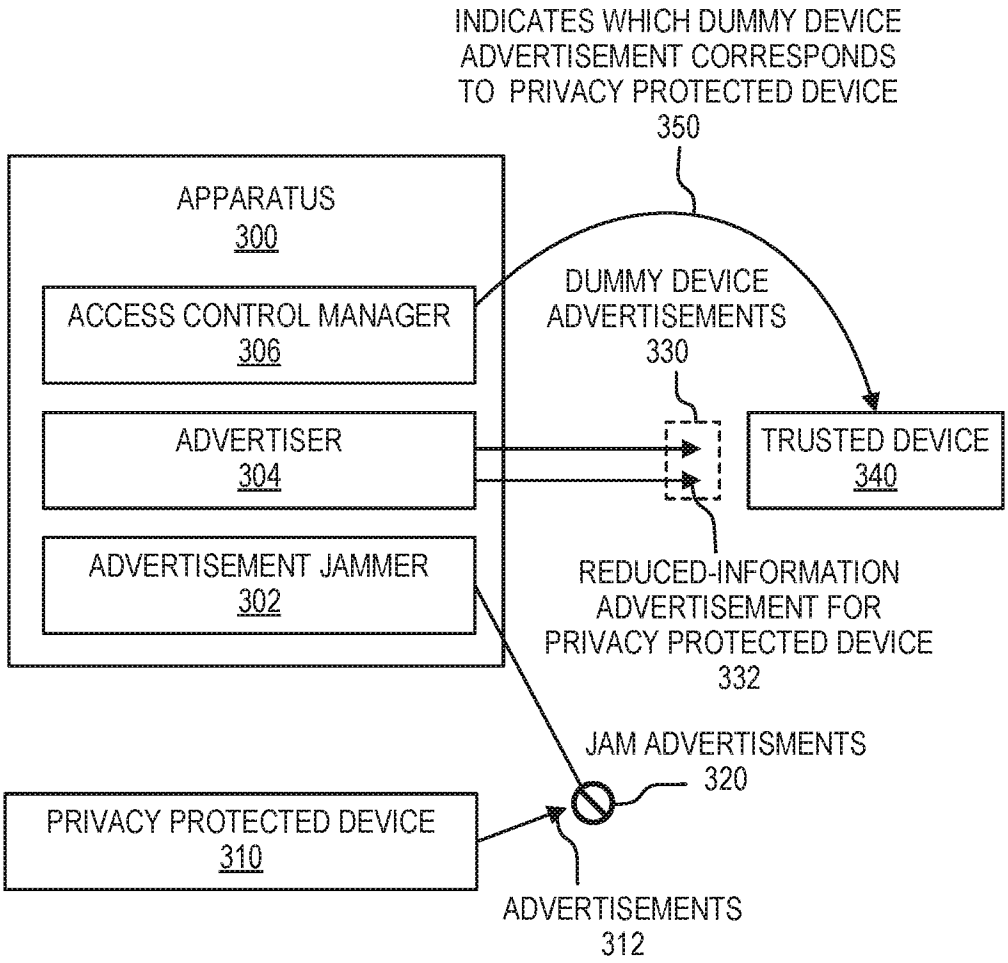
INDICATES WHICH DUMMY DEVICE ADVERTISEMENT CORRESPONDS TO PRIVACY PROTECTED DEVICE
350
APPARATUS
300
ACCESS CONTROL MANAGER
306
ADVERTISER
304
ADVERTISEMENT JAMMER
302
DUMMY DEVICE ADVERTISEMENTS
330
TRUSTED DEVICE
340
REDUCED-INFORMATION ADVERTISEMENT FOR PRIVACY PROTECTED DEVICE
332
JAM ADVERTISMENTS
320
PRIVACY PROTECTED DEVICE
310
ADVERTISEMENTS
312

FIG. 3

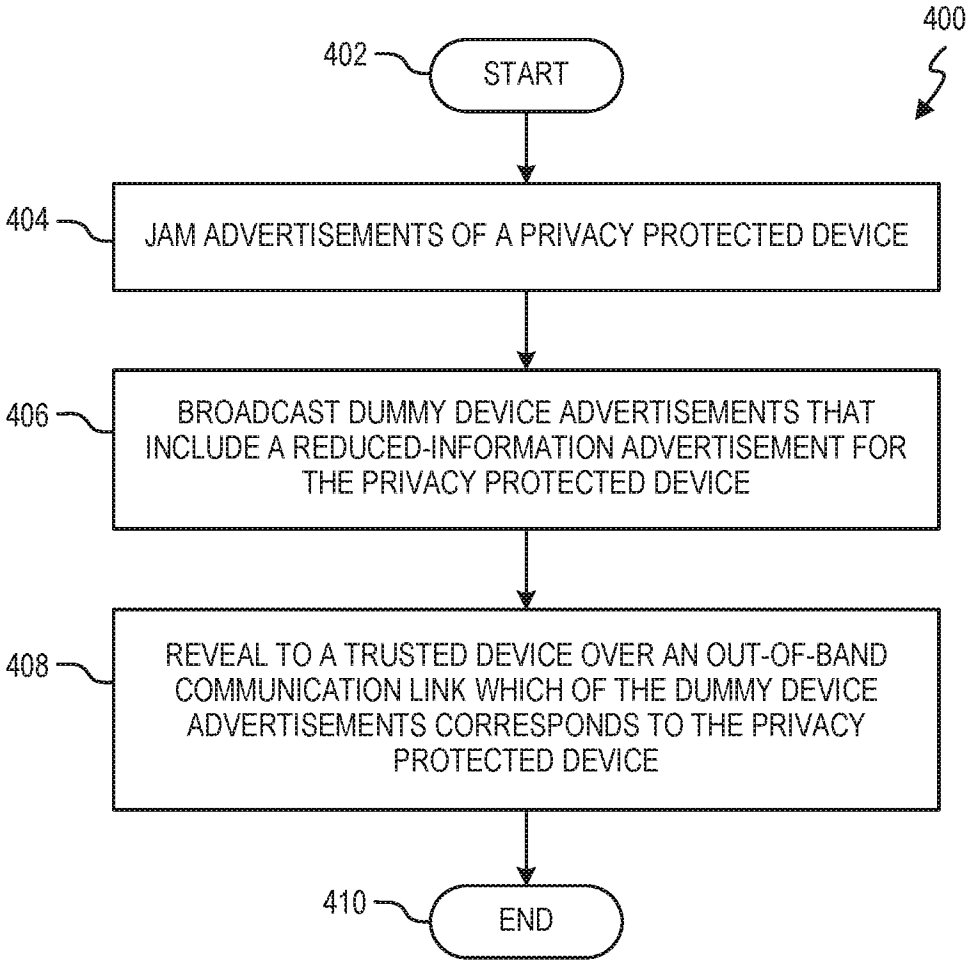
400
402
START
404
JAM ADVERTISEMENTS OF A PRIVACY PROTECTED DEVICE
406
BROADCAST DUMMY DEVICE ADVERTISEMENTS THAT INCLUDE A REDUCED-INFORMATION ADVERTISEMENT FOR THE PRIVACY PROTECTED DEVICE
408
REVEAL TO A TRUSTED DEVICE OVER AN OUT-OF-BAND COMMUNICATION LINK WHICH OF THE DUMMY DEVICE ADVERTISEMENTS CORRESPONDS TO THE PRIVACY PROTECTED DEVICE
410
END

FIG. 4

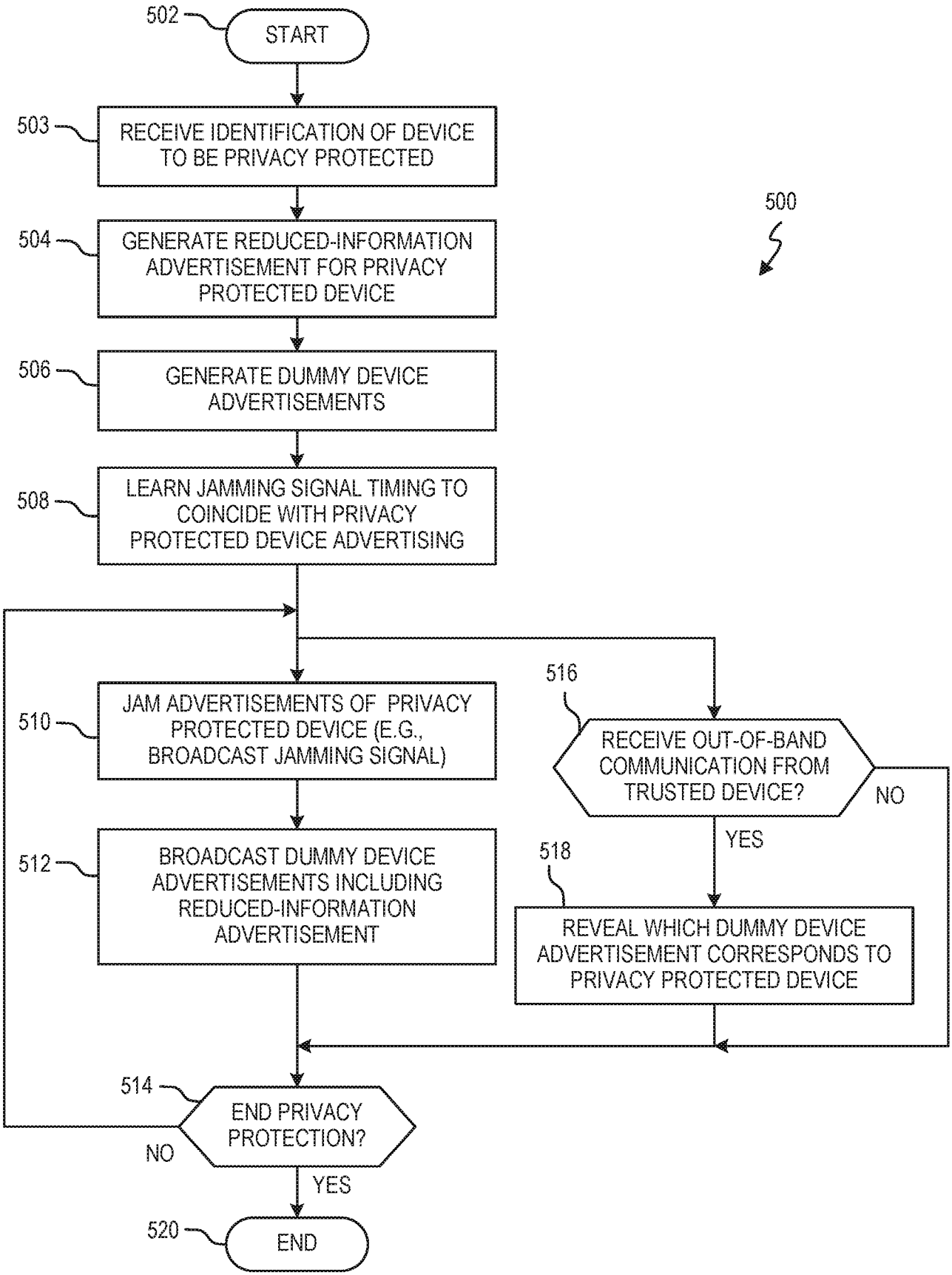
502
START
503
RECEIVE IDENTIFICATION OF DEVICE TO BE PRIVACY PROTECTED
500
504
GENERATE REDUCED-INFORMATION ADVERTISEMENT FOR PRIVACY PROTECTED DEVICE
506
GENERATE DUMMY DEVICE ADVERTISEMENTS
508
LEARN JAMMING SIGNAL TIMING TO COINCIDE WITH PRIVACY PROTECTED DEVICE ADVERTISING
510
JAM ADVERTISEMENTS OF PRIVACY PROTECTED DEVICE (E.G., BROADCAST JAMMING SIGNAL)
512
BROADCAST DUMMY DEVICE ADVERTISEMENTS INCLUDING REDUCED-INFORMATION ADVERTISEMENT
516
RECEIVE OUT-OF-BAND COMMUNICATION FROM TRUSTED DEVICE?
NO
YES
518
REVEAL WHICH DUMMY DEVICE ADVERTISEMENT CORRESPONDS TO PRIVACY PROTECTED DEVICE
514
END PRIVACY PROTECTION?
NO
YES
520
END

FIG. 5

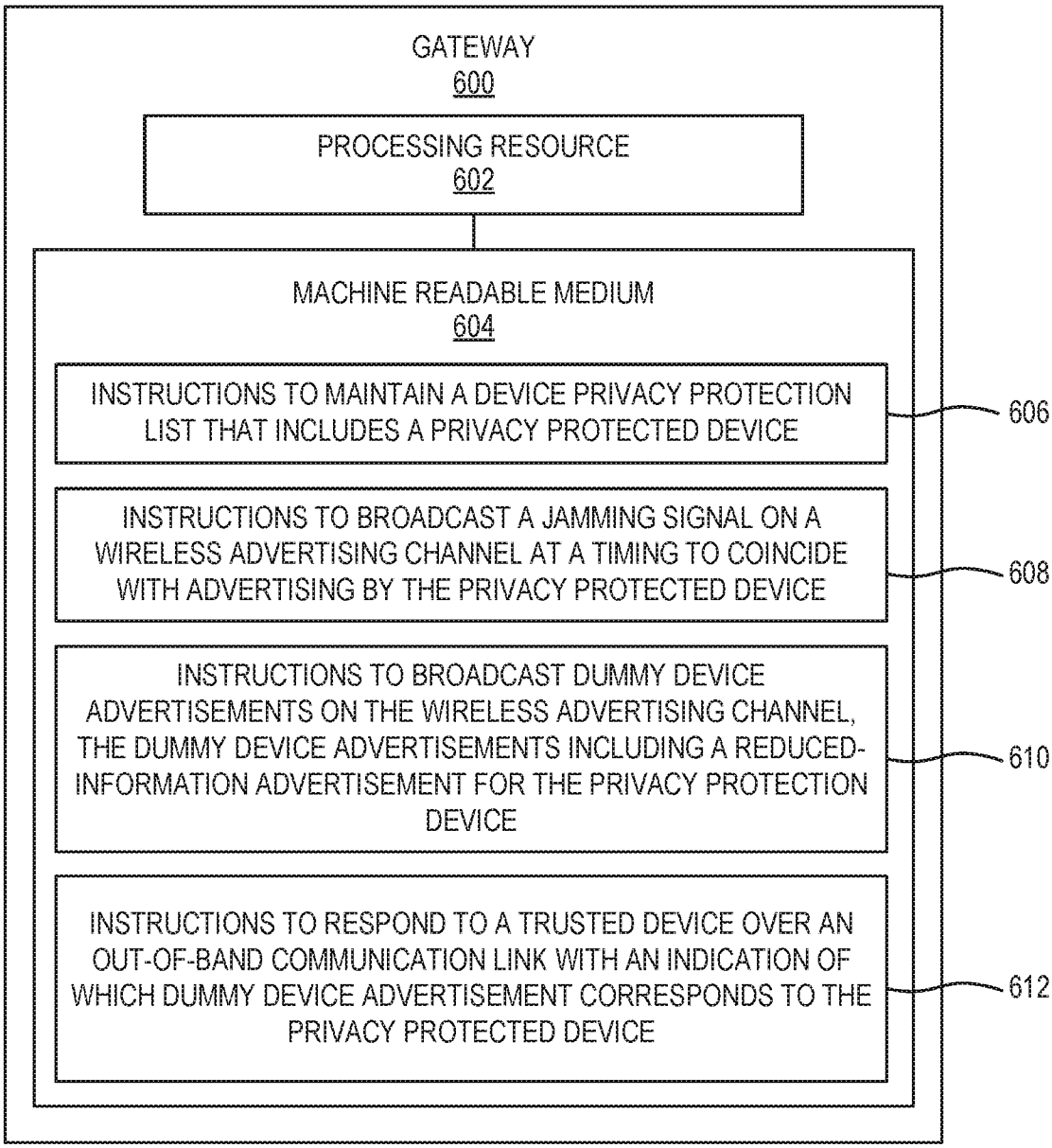
GATEWAY
600
PROCESSING RESOURCE
602
MACHINE READABLE MEDIUM
604
INSTRUCTIONS TO MAINTAIN A DEVICE PRIVACY PROTECTION LIST THAT INCLUDES A PRIVACY PROTECTED DEVICE
606
INSTRUCTIONS TO BROADCAST A JAMMING SIGNAL ON A WIRELESS ADVERTISING CHANNEL AT A TIMING TO COINCIDE WITH ADVERTISING BY THE PRIVACY PROTECTED DEVICE
608
INSTRUCTIONS TO BROADCAST DUMMY DEVICE ADVERTISEMENTS ON THE WIRELESS ADVERTISING CHANNEL, THE DUMMY DEVICE ADVERTISEMENTS INCLUDING A REDUCED-INFORMATION ADVERTISEMENT FOR THE PRIVACY PROTECTION DEVICE
610
INSTRUCTIONS TO RESPOND TO A TRUSTED DEVICE OVER AN OUT-OF-BAND COMMUNICATION LINK WITH AN INDICATION OF WHICH DUMMY DEVICE ADVERTISEMENT CORRESPONDS TO THE PRIVACY PROTECTED DEVICE
612

FIG. 6

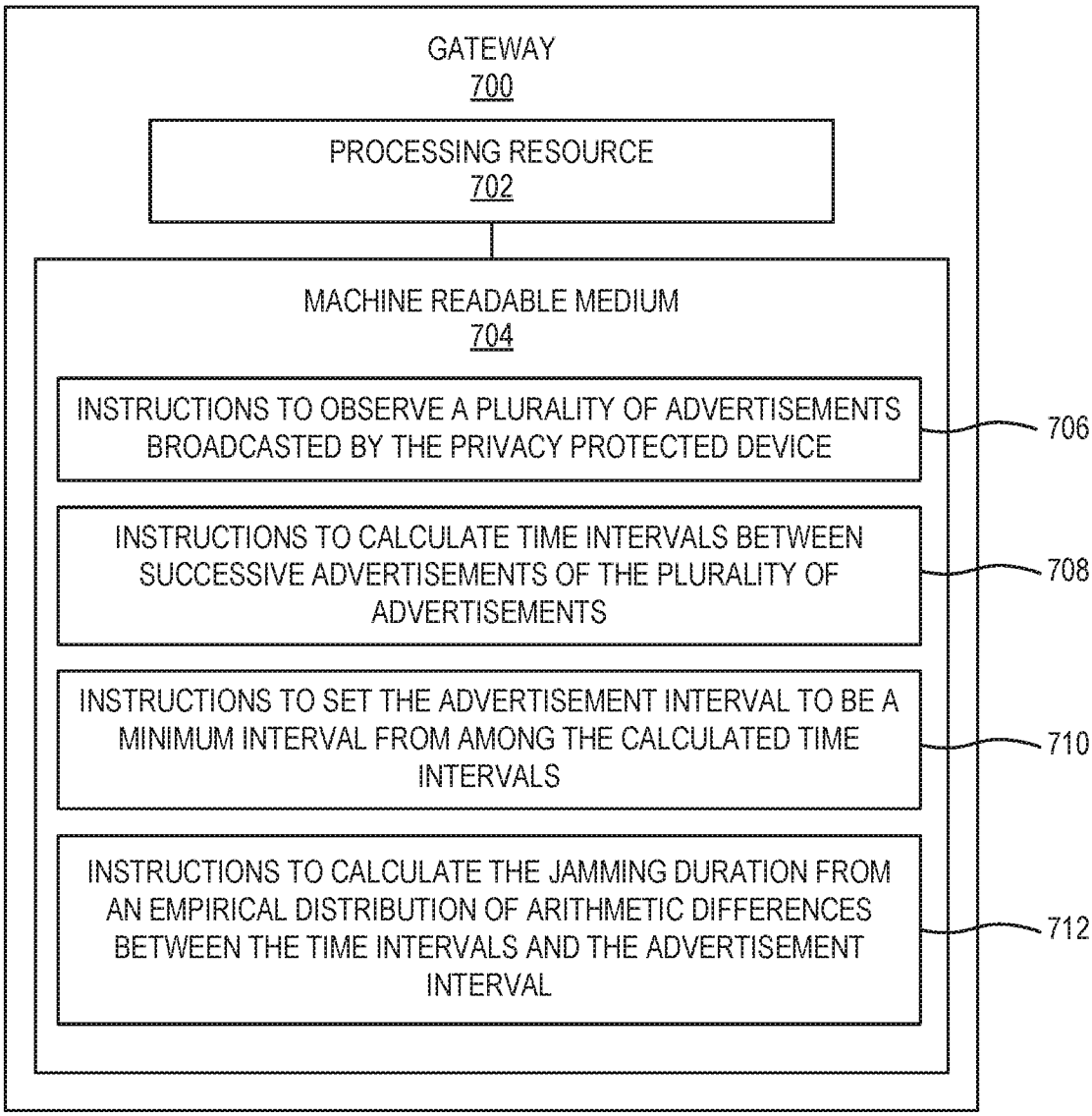
GATEWAY
700
PROCESSING RESOURCE
702
MACHINE READABLE MEDIUM
704
INSTRUCTIONS TO OBSERVE A PLURALITY OF ADVERTISEMENTS BROADCASTED BY THE PRIVACY PROTECTED DEVICE
706
INSTRUCTIONS TO CALCULATE TIME INTERVALS BETWEEN SUCCESSIVE ADVERTISEMENTS OF THE PLURALITY OF ADVERTISEMENTS
708
INSTRUCTIONS TO SET THE ADVERTISEMENT INTERVAL TO BE A MINIMUM INTERVAL FROM AMONG THE CALCULATED TIME INTERVALS
710
INSTRUCTIONS TO CALCULATE THE JAMMING DURATION FROM AN EMPIRICAL DISTRIBUTION OF ARITHMETIC DIFFERENCES BETWEEN THE TIME INTERVALS AND THE ADVERTISEMENT INTERVAL
712

FIG. 7

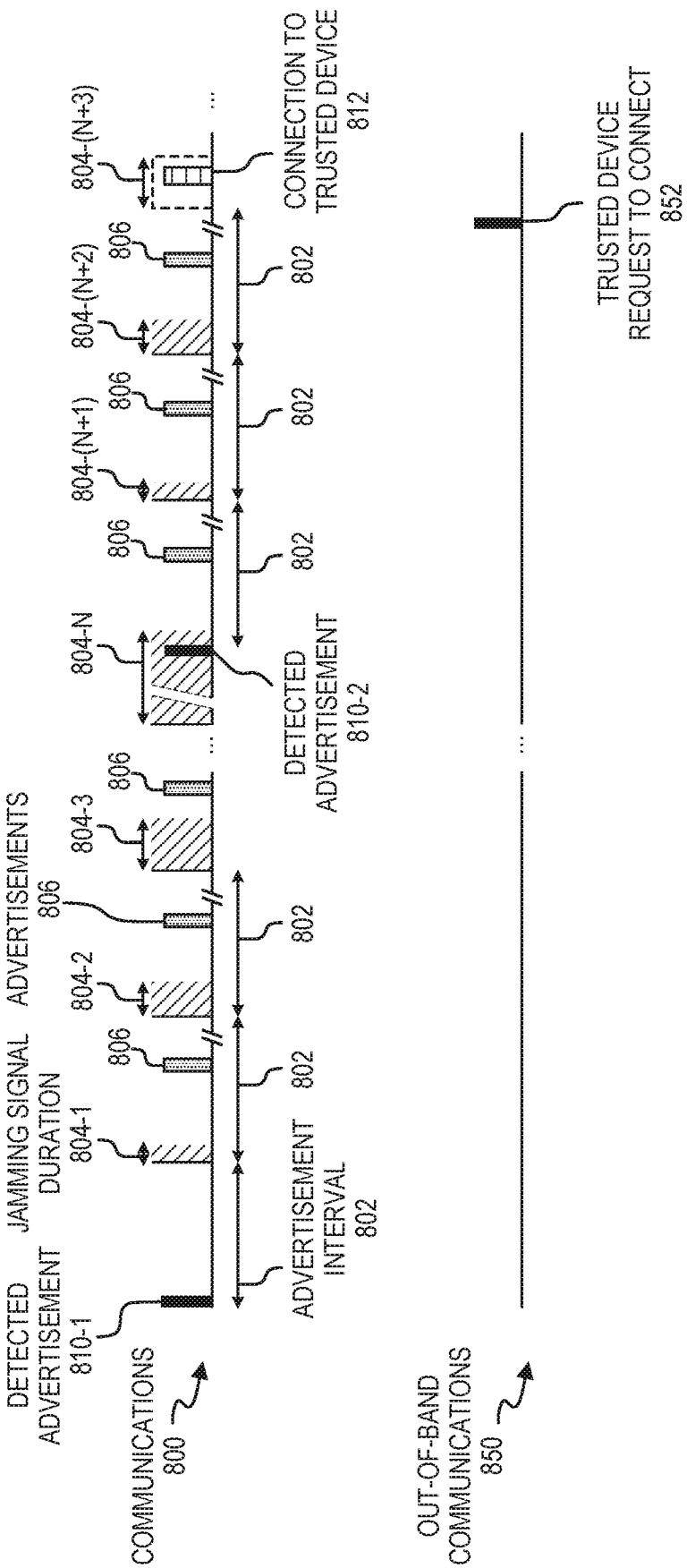
COMMUNICATIONS
800
DETECTED ADVERTISEMENT
810-1
JAMMING SIGNAL DURATION
804-1
DUMMY DEVICE ADVERTISEMENTS
806
804-2
804-3
804-N
804-(N+1)
804-(N+2)
804-(N+3)
ADVERTISEMENT INTERVAL
802
DETECTED ADVERTISEMENT
810-2
CONNECTION TO TRUSTED DEVICE
812
OUT-OF-BAND COMMUNICATIONS
850
TRUSTED DEVICE REQUEST TO CONNECT
852

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/019792

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/02(2009.01)i, H04K 3/00(2006.01)i, H04W 4/00(2009.01)i, H04W 4/06(2009.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W 12/02; H04K 3/00; H04L 29/06; H04L 9/00; H04W 4/02; H04W 4/00; H04W 4/06

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: advertisement, jam, broadcast, privacy, dummy

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2008-0298587 A1 (MARK Y. LUK et al.) 04 December 2008 See paragraphs [0086]-[0089]; and claims 6, 7.	1-15
A	US 2014-0099913 A1 (AT&T INTELLECTUAL PROPERTY I, L.P.) 10 April 2014 See paragraphs [0056]-[0061]; and claim 1.	1-15
A	US 2015-0118996 A1 (AT&T INTELLECTUAL PROPERTY I, L.P.) 30 April 2015 See paragraphs [0044]-[0046], [0064]; and claim 1.	1-15
A	WO 2010-135085 A1 (SYMBOL TECHNOLOGIES, INC.) 25 November 2010 See paragraphs [0027], [0079]; and claim 1.	1-15
A	US 7221900 B2 (WALTER C. READE et al.) 22 May 2007 See column 7, line 34 - column 8, line 39; and claim 1.	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

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

Date of the actual completion of the international search	Date of mailing of the international search report
16 November 2016 (16.11.2016)	**17 November 2016 (17.11.2016)**

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

Authorized officer
YANG, Jeong Rok
Telephone No. +82-42-481-5709

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2016/019792

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0298587 A1	04/12/2008	US 8150037 B2	03/04/2012
US 2014-0099913 A1	10/04/2014	US 2009-0047937 A1	19/02/2009
		US 2012-0034930 A1	09/02/2012
		US 2013-0171973 A1	04/07/2013
		US 8041817 B2	18/10/2011
		US 8402117 B2	19/03/2013
		US 8645505 B2	04/02/2014
US 2015-0118996 A1	30/04/2015	None	
WO 2010-135085 A1	25/11/2010	EP 2433439 A1	28/03/2012
		US 2010-0296496 A1	25/11/2010
		US 8694624 B2	08/04/2014
US 7221900 B2	22/05/2007	AU 2003-249180 A1	18/06/2004
		CA 2505413 A1	10/06/2004
		EP 1579381 A1	28/09/2005
		EP 1579381 B1	01/07/2009
		EP 2065838 A2	03/06/2009
		EP 2065838 A3	19/08/2009
		JP 04339261 B2	07/10/2009
		JP 2006-507599 A	02/03/2006
		KR 10-2005-0084664 A	26/08/2005
		MX PA05004837 A	22/07/2005
		US 2004-0100359 A1	27/05/2004
		WO 2004-049246 A1	10/06/2004
		ZA 200503648 A	26/03/2008