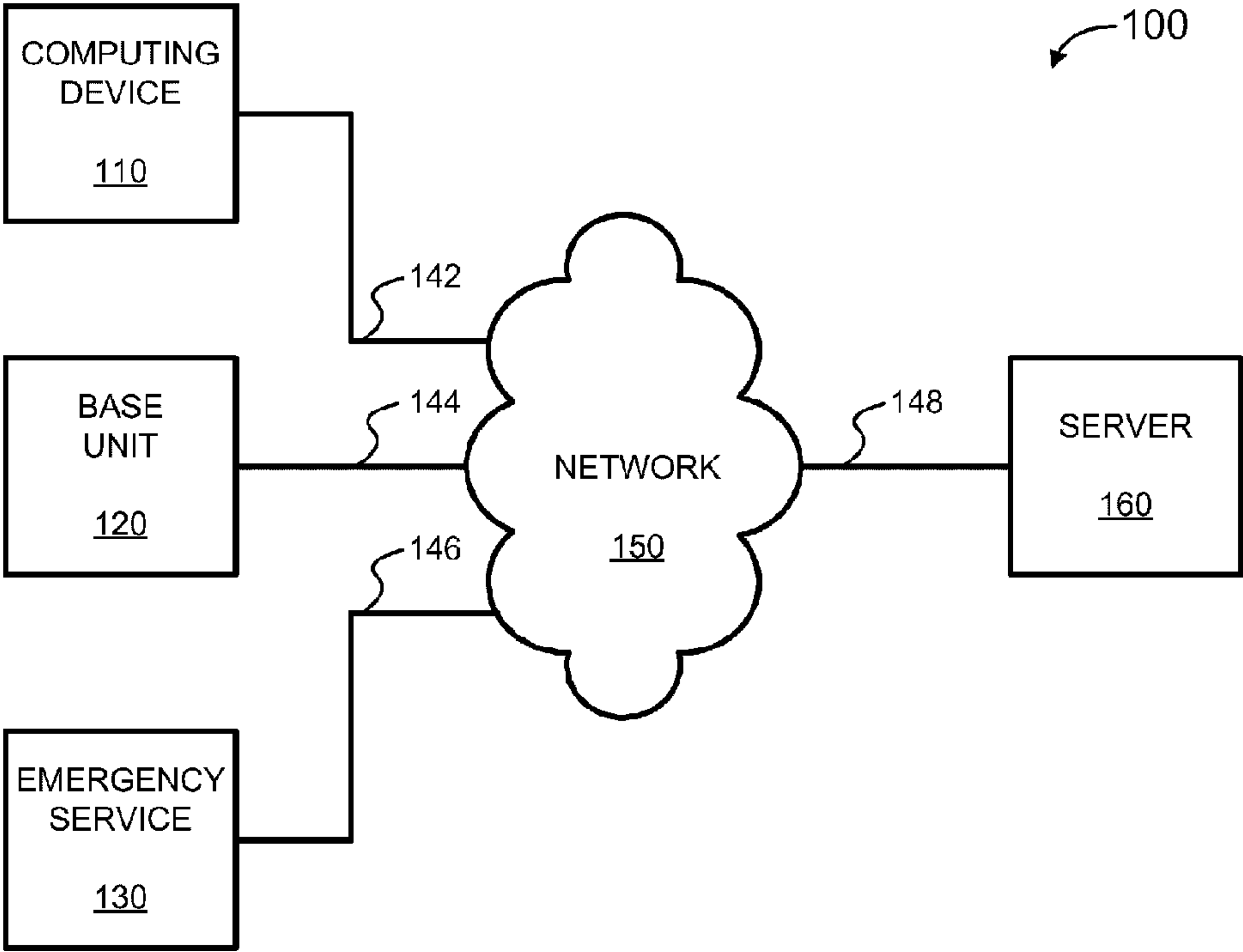




(86) Date de dépôt PCT/PCT Filing Date: 2015/05/04 (87) Date publication PCT/PCT Publication Date: 2015/11/26 (45) Date de délivrance/Issue Date: 2019/02/26 (85) Entrée phase nationale/National Entry: 2016/11/15 (86) N° demande PCT/PCT Application No.: US 2015/029109 (87) N° publication PCT/PCT Publication No.: 2015/179120 (30) Priorité/Priority: 2014/05/20 (US14/283,132)	(51) Cl.Int./Int.Cl. <i>G08B 29/18</i> (2006.01), <i>G08B 19/00</i> (2006.01), <i>G08B 25/00</i> (2006.01), <i>H04L 12/16</i> (2006.01) (72) Inventeurs/Inventors: FARRAND, TOBIN E., US; GILLON, WILLIAM M., US; SNOW, KEVIN D., US; KREIN, WILLIAM T., US; BRYAN, DAVID A., US (73) Propriétaire/Owner: OOMA, INC., US (74) Agent: SMART & BIGGAR
--	---

(54) **Titre : SURVEILLANCE ET COMMANDE DE SECURITE**
(54) **Title: SECURITY MONITORING AND CONTROL**



(57) **Abbrégé/Abstract:**
Systems, methods, and software for monitoring and controlling a security system for a structure are provided herein. An exemplary method may include receiving sensor data from at least one first peripheral, the sensor data associated with at least one of activity inside and activity outside of a structure; determining a critical event based in part on the sensor data; creating an alert based in part on the critical event; getting user preferences associated with at least one of a user and a base unit; determining a response based in part on the alert and user preferences; and activating at least one of a second peripheral and a service based in part on the response.

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

(19) World Intellectual Property
Organization
International Bureau

WIPO | PCT

(10) International Publication Number
WO 2015/179120 A1(43) International Publication Date
26 November 2015 (26.11.2015)(51) International Patent Classification:
G08B 13/00 (2006.01)(21) International Application Number:
PCT/US2015/029109(22) International Filing Date:
4 May 2015 (04.05.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/283,132 20 May 2014 (20.05.2014) US(71) Applicant: **OOMA, INC.** [US/US]; Ooma, Inc., 1880 Embarcadero Road, Palo Alto, California 94303 (US).(72) Inventors: **FARRAND, Tobin E.**; Ooma, Inc., 1880 Embarcadero Road, Palo Alto, California 94303 (US). **GILLON, William M.**; Ooma, Inc., 1880 Embarcadero Road, Palo Alto, California 94303 (US). **SNOW, Kevin D.**; Ooma, Inc., 1880 Embarcadero Road, Palo Alto, California 94303 (US). **KREIN, William T.**; Ooma, Inc., 1880 Embarcadero Road, Palo Alto, California 94303 (US). **BRYAN, David A.**; Ooma, Inc., 1880 Embarcadero Road, Palo Alto, California 94303 (US).(74) Agents: **KLINE, Keith** et al.; Carr & Ferrell LLP, 120 Constitution Drive, Menlo Park, California 94025 (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).

[Continued on next page]

(54) Title: SECURITY MONITORING AND CONTROL

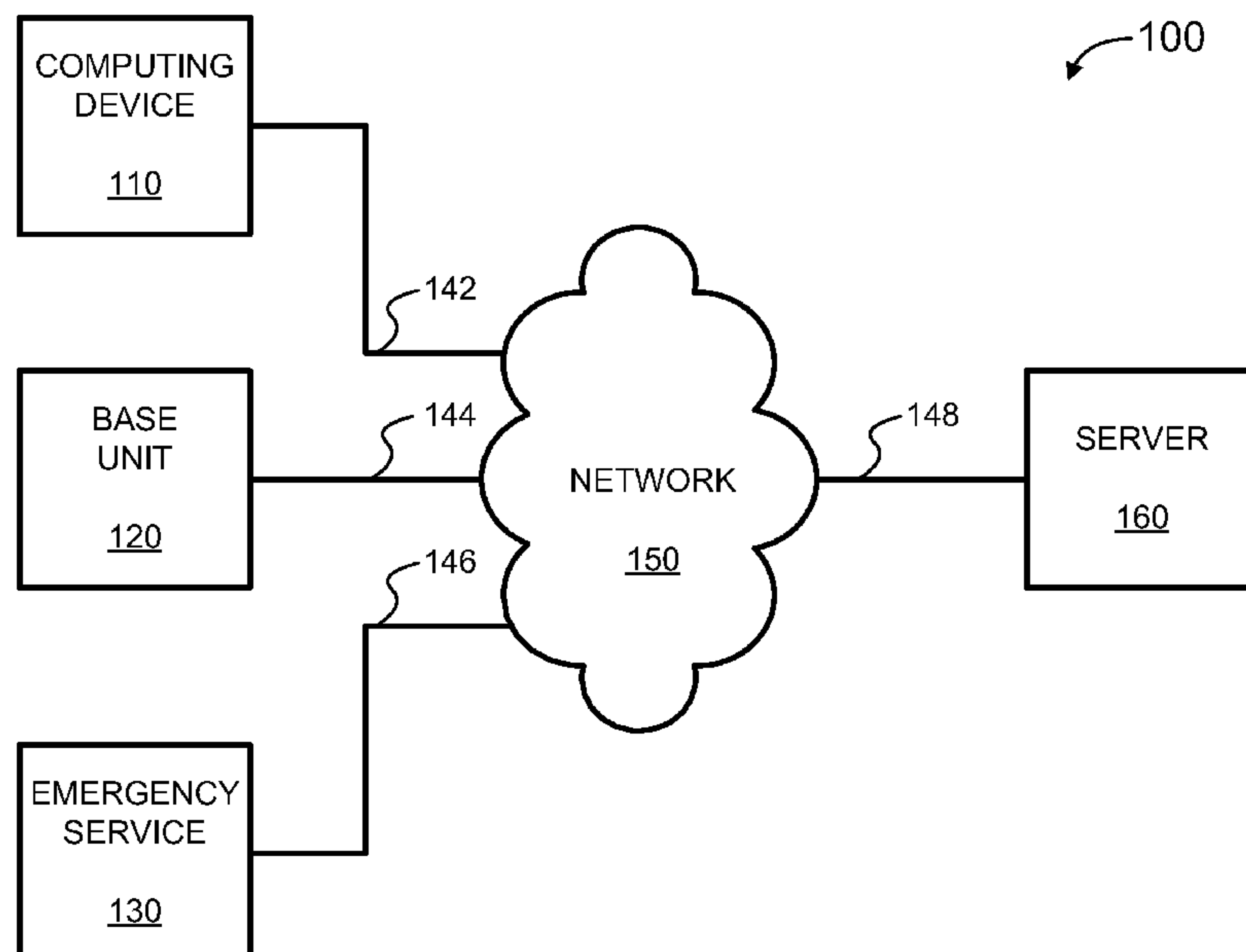


FIG. 1

(57) Abstract: Systems, methods, and software for monitoring and controlling a security system for a structure are provided herein. An exemplary method may include receiving sensor data from at least one first peripheral, the sensor data associated with at least one of activity inside and activity outside of a structure; determining a critical event based in part on the sensor data; creating an alert based in part on the critical event; getting user preferences associated with at least one of a user and a base unit; determining a response based in part on the alert and user preferences; and activating at least one of a second peripheral and a service based in part on the response.

WO 2015/179120 A1

Published:

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

SECURITY MONITORING AND CONTROL

Field of the Invention

[0001] The present technology pertains to monitoring and control, and more specifically to security monitoring and control for a structure.

Background of the Invention

[0002] Commercial and residential security systems detect intrusions and fire to prevent intruder and property damage. Present security systems suffer from false alarms and high monitoring costs. False alarms prevent first responders from being available to handle other in-progress or more urgent calls for service. In addition, first responders may levy fines for false alarms. Companies offer services to remotely monitor security systems. Some companies have trained staff to monitor their customers' security systems and call the appropriate authorities in the event an alarm signal is received. However, the cost and quality of these services vary by the provider, and can be beyond the reach of many families and organizations.

Summary of the Invention

[0003] In one embodiment, the present technology is directed to a method for security monitoring and control. The method may include receiving sensor data from at least one first peripheral, the sensor data associated with at least one of activity inside and activity outside of a structure; determining a critical event based in part on the sensor data; creating an alert based in part on the critical event; getting user preferences associated with at least one of a user and a base unit; determining a response based in part on the alert and user preferences; and activating at least one of a second peripheral and a service based in part on the response.

[0004] In one embodiment, the present technology is directed to a base unit. The base unit may include: a processor; and a memory coupled to the processor, the memory storing instructions executable by the processor to perform a method for security monitoring and control including: receiving sensor data from at least one first peripheral, the sensor data associated with at least one of activity inside and activity outside of a structure; determining a critical event based in part on the sensor data; creating an alert based in part on the critical event; getting user preferences associated with at least one of a user and a base unit; determining a response based in part on the alert and user preferences; and activating at least one of a second peripheral and a service based in part on the response.

[0005] In one embodiment, the present technology is directed to a non-transitory computer-readable storage medium having embodied thereon a program, the program being executable by a processor to perform a method for security monitoring and control. The method may include receiving sensor data from at least one first peripheral, the sensor data associated with at least one of activity inside and activity outside of a structure; determining a critical event based in part on the sensor data; creating an alert based in part on the critical event; getting user preferences associated

with at least one of a user and a base unit; determining a response based in part on the alert and user preferences; and activating at least one of a second peripheral and a service based in part on the response.

[0005a] According to another aspect of the present disclosure, there is provided a method for security monitoring and control comprising: receiving sensor data from at least one first peripheral, the sensor data associated with at least one of activity inside and activity outside of a structure; determining a critical event based in part on the sensor data; creating an alert based in part on the critical event; getting user preferences associated with at least one of a user and a base unit; determining a response based in part on the alert and user preferences; activating at least one of a second peripheral and a service based in part on the response; detecting a wireless device associated with an intruder; and determining one or more properties of the wireless device, the determining including detecting a digital fingerprint of the wireless device, the wireless device being an unpaired Bluetooth enabled device in discoverable mode, and the determining of one or more properties further includes at least one of executing software on, sending a chunk of data to, or sending a sequence of commands to the unpaired Bluetooth enabled device, so as to gain control of the unpaired Bluetooth enabled device.

[0005b] There is also provided a base unit comprising: a processor; and a memory coupled to the processor, the memory storing instructions executable by the processor to perform a method for security monitoring and control including: receiving sensor data from at least one first peripheral, the sensor data associated with at least one of activity inside and activity outside of a structure; determining a critical event based in part on the sensor data; creating an alert based in part on the critical event; getting user preferences associated with at least one of a user and a base unit; determining a response based in part on the alert and user preferences; activating at least one of a second peripheral and a service based in part on the response; detecting a wireless device associated with an intruder; and determining properties of the wireless device, the wireless device being an unpaired Bluetooth enabled device in discoverable mode, and the determining properties includes at least one of executing software on, sending a chunk of data to, or sending a sequence of commands to the

unpaired Bluetooth enabled device, so as to gain control of the unpaired Bluetooth enabled device.

[0005c] Another aspect of the present disclosure provides a non-transitory computer-readable storage medium having embodied thereon a program, the program being executable by a processor to perform a method for security monitoring and control, the method comprising: receiving sensor data from at least one first peripheral, the sensor data associated with at least one of activity inside and activity outside of a structure; determining a critical event based in part on the sensor data; creating an alert based in part on the critical event; getting user preferences associated with at least one of a user and a base unit; determining a response based in part on the alert and user preferences; activating at least one of a second peripheral and a service based in part on the response; detecting a wireless device associated with an intruder; and determining one or more properties of the wireless device, the wireless device being an unpaired Bluetooth enabled device in discoverable mode, and the determining of one or more properties includes at least one of executing software on, sending a chunk of data to, or sending a sequence of commands to the unpaired Bluetooth enabled device, so as to gain control of the unpaired Bluetooth enabled device.

Brief Description of the Drawings

[0006] The accompanying drawings, where like reference numerals refer to identical or functionally similar elements throughout the separate views, together with the detailed description below, are incorporated in and form part of the specification, and serve to further illustrate embodiments of concepts that include the claimed disclosure, and explain various principles and advantages of those embodiments. The methods and systems disclosed herein have been represented where appropriate by conventional symbols in the drawings, showing only those specific details that are pertinent to understanding the embodiments of the present disclosure so as not to obscure the disclosure with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein.

[0007] FIG. 1 is a simplified block diagram of a system for security monitoring and control, according to some embodiments of the present invention.

[0008] FIG. 2 is a simplified diagram of an environment of a structure, according to some embodiments.

[0009] FIG. 3 is a simplified block diagram of an architecture for customer-premises equipment (CPE), according to some embodiments.

[0010] FIG. 4 is a simplified flow diagram for a method for responding to sensor data, according to some embodiments.

[0011] FIG. 5 is a simplified flow diagram for a method for responding to a notification, according to some embodiments.

[0012] FIGS. 6-12 are simplified flow diagrams for wireless methods according to some embodiments.

[0013] FIG. 13 is a simplified block diagram for a computing system according to some embodiments.

Detailed Description

[0014] While this technology is susceptible of embodiment in many different forms, there is shown in the drawings and will herein be described in detail several specific embodiments with the understanding that the present disclosure is to be considered as an exemplification of the principles of the technology and is not intended to limit the technology to the embodiments illustrated. The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the technology. As used herein, the singular forms "a", "an," and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/ or "comprising," when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof. It will be understood that like or analogous elements and/or components, referred to herein, may be identified throughout the drawings with like reference characters. It will be further understood that several of the figures are merely schematic representations of the present technology. As such, some of the components may have been distorted from their actual scale for pictorial clarity.

[0015] According to various embodiments of the present invention, a base unit communicatively coupled to the Internet communicates with peripherals in and/or near a structure, for example, using wired and/or wireless communications. The peripherals may detect/sense conditions such as motion, glass breakage, smoke, heat, flooding, and the like. The peripherals may communicate the detected/sensed conditions to the base unit over any of several wired and/or wireless communications and/or networking mechanisms. The base unit may communicate the detected/sensed conditions over the Internet to a server. The base unit may also communicate with a web client (or other

client or software application) on a computing device (e.g., PC, tablet computer, smart phone, etc.).

[0016] A user operating the computing device may monitor and respond to detected/sensed conditions in and/or near the structure. Additionally or alternatively, the base unit may communicate with the computing device. In some embodiments, the base unit may, automatically and/or in response to at least one of instructions from a user and/or inputs from peripherals, control a peripheral and/or service. By way of example, the base unit may perform at least one of activate an internal or external siren, control lighting (e.g., flash, turn on, and turn off), activate audible and/or visual alarm in a smoke detector, launch a personal surveillance drone, lock and/or unlock door, move window coverings (e.g., open, close, and trim), post on social media, and the like.

[0017] FIG. 1 illustrates a system for security monitoring and control (system) 100, according to some embodiments. The system 100 includes computing device 110, base unit 120, emergency service 130, communications 142-148, network 150, and server 160.

[0018] Computing device 110 include at least one of a personal computer (PC), hand held computing system, telephone, mobile computing system, workstation, tablet, phablet, wearable, mobile phone, server, minicomputer, mainframe computer, or any other computing system. Computing device 110 is described further in relation to computing system 1300 in FIG. 13.

[0019] In some embodiments, computing device 110 may include a web browser (or similar software application) for communicating with base unit 120 and/or server 160. For example, computing device 110 is a PC running a web browser inside (or outside) a commercial or residential structure. Additionally or alternatively, computing device 110 is a smart phone running a client (or other software application).

[0020] In various embodiments, computing device 110 is used for telecommunications. For example, the user from his web or smartphone client upon

determining that the intruder alert is valid, could initiate a 911 call as if it were originating from the structure, rather than from the user's smartphone client. Normally a 911 call from a cell phone is directed to a public safety access point (PSAP) associated with the geographical location of the cell phone. For a user at a remote location who is alerted that his house is being invaded, dialing 911 from his cell phone could normally result in significant delay as he explains the situation to the PSAP serving the physical location of his smartphone (rather than that of the house that has been invaded), then waits for his call to be transferred to a PSAP in the area of his home and then takes the time to communicate the location of the house that is being invaded (which may even be in another state), and convinces the authorities to go to the invaded house.

[0021] In contrast, since base unit 120 may also provide VoIP service for the home, base unit 120 may already be provisioned to have its phone number associated with the appropriate physical address of the house, according to some embodiments. For example, the user operating his web or smartphone-based client, may initiate a 911 call as if it were originating from the invaded house. The call is directly connect to the PSAP that is local to the invaded house, with the proper address electronically passed to the PSAP as if the call had originated from the invaded house, bypassing the delays inherent in the prior art. Such 911 calls, from a location remote from the structure and/or "spoofing" the address presented to the PSAP (e.g., by provisioning the structure's address to the 911 service provider), may be used for other alert situations in the structure (e.g., smoke detector triggers, swimming pool monitor triggers, etc.).

[0022] In various embodiments, computing device 110 presents information, received from base unit 120 and/or server 160, graphically and/or textually, to at least one user (not shown in FIG. 1). The user may, for example, set up preferences, review sensor information (e.g., alarms) in real time, control peripherals, review logs, and the like using a web browser, client, or other software application.

[0023] Base unit 120 are disposed within or near to a commercial or residential structure (e.g., office building, house, townhouse, condominium, apartment, recreational vehicle, aircraft, yacht, and the like; not shown in FIG. 1) to be monitored and controlled. Base unit 120 controls and/or receives data from peripherals (not shown in FIG. 1) disposed in and about the commercial or residential structure. The peripherals are described further in relation to FIG. 2.

[0024] Emergency service 130 includes one or more of private security (e.g., security guard), law enforcement (e.g., police, sheriff, etc.), fire (e.g., fire and rescue service), emergency medical service (e.g., ambulance), and the like. In some embodiments, communication with emergency service 130 is through a public-safety answering point (PSAP), sometimes called "public-safety access point." A PSAP is a call center responsible for answering calls to an emergency telephone number for police, firefighting, ambulance services, etc. Telephone operators at the PSAP may be responsible for dispatching emergency service 130.

[0025] Communications 142-148 are wired and/or wireless communications (and combinations thereof) which communicatively couple computing device 110, base unit 120, and server 160 to each other and to network 150. For example, communications 142-148 may be at least one of plain old telephone service (POTS), cellular/mobile network (e.g., 1G, 2G, 3G, and 4G), and other voice communications network, dial up, digital subscriber line (DSL), cable internet, power-line internet, WiFi (e.g., IEEE 802.11), Bluetooth, Bluetooth low energy (BLE), WiMAX (e.g., IEEE 802.16), satellite broadband, mobile broadband (e.g., 2G, 3G, and 4G), and other broadband access. Although a single line is used to depict communications 142-148, there may be multiple computing devices 110, base units 120, emergency services 130, and servers 160, each of which may use different combinations of the wired and/or wireless communications described above.

[0026] Network 150 is a system of interconnected computer networks, such as the Internet. Additionally or alternatively, network 150 may be a private network, such as home, office, and enterprise local area networks (LANs).

[0027] Server 160 includes one or more systems (e.g., software and computer hardware) that respond to requests across network 150 to provide, or help to provide, a network service. Services, for example, include at least one of Voice over Internet Protocol (VoIP), Enhanced 911 (E911), Short Message Service (SMS), email, social media posting (e.g., Nextdoor, Facebook, Twitter, YouTube, Instagram, etc.), user preferences, notifications/alarms, and the like. In some embodiments, at least one service/function of server 160 may be performed alternatively by or in combination with base unit 120. Server 160 may be disposed in, near, or far away from the structure. Server 160 is described further in relation to computing system 1300 in FIG. 13.

[0028] In some embodiments, alerts for help in the event of an intruder, detection of an unauthorized pool entrance, fire, flood, or other emergency situation take new forms. Prior to the present technology, a user dialing 911 was the most effective response to an emergency. In contrast, in various embodiments the user via a web or smartphone-based client on computing device 110 may select from many more options for responding to an emergency quickly and conveniently. For example, with the selection of a button in a graphical user interface of the smartphone client, the web or smartphone client on computing device 110 can originate a 911 call through server 160, as if it came from the home location. By way of further example, a pre-programmed tweet can be posted to the user's account on Twitter and/or to a Nextdoor neighborhood group (e.g. "something's happening at my home (<address>), if you are nearby, please check it out"). By way of additional example, an automated message could be posted on the user's Facebook wall or a Facebook wall shared by a neighborhood watch group. In an emergency situation, quickly establishing broad awareness can be essential to successful resolution of the situation. Social networks

make possible such broad notifications to crowd-source home monitoring without the expense of professional monitoring services and/or to augment the professional monitoring services.

[0029] In various embodiments, when base unit 120 (and associated resources and services) are activated, the user may be given the option to be automatically added as a friend for a neighborhood watch Facebook page, join a Nextdoor neighborhood group, be added as a follower on a Twitter feed customized for her physical address, and the like. Such pages, posts, and feeds may be automatically accessible through the web or smartphone-based client on computing device 110 for posting in the event of an emergency, and advantageously provide neighbors and/or the community around a structure with awareness of emergency events taking place nearby, with a high degree of automation.

[0030] Moreover, social networking along with coordination of the services and devices described herein make possible new capabilities for bonding communities together to enhance their collective security. In some embodiments, when an intruder is detected based at least on his Bluetooth or cellular MAC address (as described below), the MAC address(s) may be communicated to other base units 120 on network 150, so that the movements of the intruder can be tracked. In various embodiments, when an intruder is detected in one house, all the other houses in the neighborhood who subscribe to the same service can be placed on a heightened state of readiness (e.g., lock down). For example, surveillance cameras on the house neighboring the house under attack are activated with the video being recorded. By way of further example, exterior lights under control of systems in other houses that subscribe to the same system are automatically turned on. By way of additional example, nearby homes are instructed to log any unusual Bluetooth "fingerprints," in case the intruder parked a vehicle a few doors down, but in range of another subscriber's home. When the occupant of a house that is being invaded receives a notification on his smartphone, for

example, a software application on computing device 110 communicates that there has been suspicious activity in another house in the neighborhood, thus increasing the probability that the occupant will not dismiss the alert as a false alarm. If an intrusion is detected in one home in the neighborhood, for example, then rather than just launching his own drone, all the surveillance drones in the neighborhood launch to try to identify the intruder, or begin performing a patrol circuit of their "home" building, both for video surveillance and deterrence. Given the expense of UAVs, a neighborhood as a whole may pool its resources, so that a single UAV serves an entire block, cul-de-sac, and other grouping of residents.

[0031] FIG. 2 illustrates an environment of a structure (environment) 200 according to some embodiments. Disposed in environment 200 is at least one of base unit 120, peripherals 202-210, and optionally smartphone 230 authorized by the system owner and potentially connected or paired with the base unit, and also optionally, additional non-owner (unpaired) devices 240.

[0032] Base unit 120 is communicatively coupled to network 150 using communications 144. Base unit 120 includes at least one network interface for wired and/or wireless communications. In some embodiments, base unit 120 includes at least one of an Ethernet adapter, cable modem, digital subscriber line (DSL) modem, wireless modem, cellular data connection, and the like (not shown in FIG. 2), for communication with network 150 over communications 144.

[0033] Base unit 120, may also include numerous network interfaces and/or modems/radios 220-225 (internal or externally coupled) to communicatively couple devices in environment 200. These may include, but are not limited to interfaces for DECT 220, WiFi 221, GSM/CDMA 222, Bluetooth 223, ZigBee 224 and Zwave 225.

[0034] By way of example, base unit 120 may include a DECT modem/radio 220 which may communicate with a DECT device, including handset 202. Integration of the DECT modem in base unit 120 offers the advantage of higher quality audio, because

integration eliminates loss of audio fidelity associated with passing audio through a band-limited Foreign Exchange Station (FXS) port to a separate DECT base device. Integration also offers the benefit of having fewer devices to manage, and allows interaction with DECT devices for other purposes, as detailed below.

[0035] By way of further example, base unit 120 includes Bluetooth modem 223. Bluetooth modem 223 may be paired with and communicate with devices such as a Bluetooth equipped smartphone 230 operated by the system user. In some embodiments, (telephone) calls may be directed from the smartphone so as to ring the smartphone and/or at least one DECT phone 202 in or near the structure. In some embodiments, DECT phone 202 is associated with a telephone service provisioned to a home or business. Base unit 120 is described further in relation to base unit 120 in FIG. 3 and computing system 1300 in FIG. 13.

[0036] In various embodiments, smartphone 230 and base unit 120 are Bluetooth paired. Incoming calls for smartphone 230 may be directed to base unit 120 and provided to the FXS port and/or DECT phone 202. Directing smartphone 230 calls in this way has the advantage of a more comfortable telephone experience, because DECT phone 202 may have superior ergonomics relative to smartphone 230. Additionally, incoming POTS and/or VOIP telephone calls may be directed from base unit 120 via Bluetooth to smartphone 230.

[0037] As another example of base unit 120 including various network interfaces, it may include microcell 222 (e.g., for CDMA, LTE, GSM, etc.) to provide (short-range) mobile/cellular service in and near the structure. Microcell 222 offers the advantage of improving reception of mobile/cellular signals, for example, when the structure is in an area where mobile/cellular coverage is marginal. Microcell 222 also offers the benefit of bypassing local mobile/cellular service and using the base unit 120 communication 144 to network 150 to backhaul calls originating from or terminating at smartphone 230. In this way, base unit may provide higher quality communications to smartphone 230.

[0038] As another example of base unit 120 including various interfaces, it may include a WiFi modem/radio 221 (e.g., IEEE 802.11). In addition, the structure may have a WiFi network which is accessible or delivered by base unit 120, and which may be used to communicate with at least one of peripherals 202-210.

[0039] In some embodiments, the various network interfaces (radios/modems) 220-225 may also serve as “sensors.” For example, in the case of Bluetooth, communication between base unit 120 and an unpaired Bluetooth-enabled device (including a phone or headset) 240 is possible. Many people (including intruders and other persons with nefarious objectives) have Bluetooth-enabled cell phones and/or Bluetooth peripherals and many people leave their cell phone Bluetooth radios turned on and in discoverable mode (all the time). For example, such people may typically leave their Bluetooth-enabled smartphones in discoverable mode, so that when they enter their car, their phones can automatically establish communication with the car’s audio system. Though data sharing with the car audio system requires a personal identification number and going through the pairing process, any cell phone with its Bluetooth turned on may be broadcasting information for which other Bluetooth devices can listen. In this way, Bluetooth-enabled cell phones may provide an “electronic fingerprint.” Similarly, other Bluetooth-enabled devices (e.g., headset, smart watch, fitness device, audio system of a car parked nearby, and other computing devices (e.g., tablet computer, phablet, notebook computer, etc.) in the car parked nearby), may also provide an “electronic fingerprint.”

[0040] In response to inputs from peripherals 202-210, base unit 120 may detect and record an electronic fingerprint associated with one or more unpaired Bluetooth-enabled devices 240 within its range. In this way, base unit 120 may record information (in one embodiment, a MAC address of one or more of an intruder’s unpaired Bluetooth-enabled device 240.) By logging such MAC addresses, the base unit 120 may help identify an intruder’s unpaired Bluetooth-enabled device 240, for example, at the

time of a break in. By further example, base unit 120 may be configured to record the fingerprint of any unknown device or any device seen at an unexpected time, or even to respond in a programmatic way as discussed below. (see also Figures 10, 11 and 12) .

[0041] By logging electronic fingerprint(s) such MAC addresses, the base unit 120 may help identify an intruder's unpaired Bluetooth-enabled device 240, for example, at the time of a break in. To aid an investigation, authorities such as law enforcement may determine information such as a manufacturer of unpaired Bluetooth-enabled device 240 based on the detected electronic fingerprint(s). After the intruder is apprehended, authorities may "match" the detected electronic fingerprint (and determined information) to unpaired Bluetooth-enabled device 240 in the suspect's possession. Additionally or alternatively, authorities can identify the specific owner of the unpaired Bluetooth-enabled device 240 based on the associated electronic fingerprint by contacting the cellular provider, manufacturer, etc. The utility of this technique may depend on at least the settings of unpaired Bluetooth-enabled device 240 (selected by the intruder), the manufacturer of the cell phone, and the provider of the Bluetooth software.

[0042] In addition, unpaired Bluetooth-enabled device 240 in discoverable mode may be vulnerable to a variety of exploits that can extract information such as a media access control (MAC) address. In some embodiments, base unit 120 may run software, send a chunk of data, send a sequence of commands, and the like that takes advantage of a bug, glitch, or vulnerability in order to gain control of unpaired Bluetooth-enabled device 240.

[0043] By way of further example, the Bluetooth modem 223 is configured such that base unit 120 may gather a range of data about the intruder's unpaired Bluetooth-enabled device 240 (referred to as "Bluesnarfing"), and/or take control of the intruder's unpaired Bluetooth-enabled device 240 (referred to as "Bluebugging"). For example, a user using a web or client on computing device 110 is given the option to have the base unit

collect the MAC address of the intruder's cell phone and/or attempt to take control of the intruder's unpaired Bluetooth-enabled device 240, to perform at least one of determining its phone number, downloading the intruder's address book and/or other identifying information. Base unit 120 may (surreptitiously) place a 911 call from the intruder's unpaired Bluetooth-enabled device 240, resulting in the intruder's unpaired Bluetooth-enabled device 240 leading authorities directly to him, even after he leaves the structure.

[0044] Similarly, Microcell 222 may also identify cell phones within range to obtain "electronic fingerprints" from device 240, for example, at the time of an intrusion into the structure. Microcell 222 may typically provide greater range and more certain connection with the intruder's cell phone than Bluetooth. Similar to Bluetooth, Microcell 222 may determine identifying information from the intruder's cell phone, without creating a permanent or authorized connection.

[0045] Similarly, WiFi radio 221 may be used to obtain "fingerprints" from device 250, for example at the time of an intrusion into the structure. WiFi radio 221 may determine a MAC addresses associated with a computing device carried by the intruder (that comes within range of WiFi radio 221).

[0046] Further, in some embodiments, base unit 120 may log all MAC addresses it encounters from any source using any wireless protocol to which it has access using any of the internal network interfaces or modems 220-225.

[0047] In various embodiments, a database is maintained by the Bluesnarfing process (or alternately by cellular, WiFi, or other protocol device monitoring processes) recording a date, time, MAC address, device name, manufacturer, model, etc. Event records may include an arrival time, departure time, and other (passively) collected activity information. One or more of device 240 detected using such mechanisms may have additional data associated with them by a user. For example, additional data may include one or more of a name, group, and notes. Groups, for example, include family,

friend, nanny, babysitter, house sitter, housekeeper, gardener, repair person, and the like.

[0048] The above database may be monitored. For example, events are generated based at least on default rules and/or rules configured by the user. The events may also be recorded in the database and may be used to trigger notifications. Notifications, for example, are at least one of an email, SMS text message, automated telephone call, and the like. Non-limiting examples of events which trigger a notification include: when a particular device appears (e.g., child home from school); when a device disappears (e.g., child leaves for school, teenager sneaks out of the house, etc.); when a device appears and disappears (e.g., monitor the arrival, departure, and/or length of stay of the housekeeper); and when a previously unknown device appears; when a non-family group device appears/disappears between 9PM and 5AM (e.g., teenager entertains guests after curfew).

[0049] As would be readily appreciated by one of ordinary skill in the art, the database and notification processes described herein can be performed by base unit 120 and/or on server 160. For example, to prevent loss of information in the event that base unit 120 is removed from the structure, base unit 120 may provide a log to server 160 periodically, as well as anytime a potentially triggering event occurs (e.g., a glass break sensor or any of the other peripherals 202-210 triggering an event).

[0050] Base unit 120 is also communicatively coupled to at least one of peripherals 202-210 using at least one of wired and wireless communications interfaces 220-225. By way of example and not limitation, wireless communications may be one or more of Digital Enhanced Cordless Telecommunications Ultra Low Energy (DECT ULE) 220 (e.g., according to the European Telecommunications Standards Institute (ETSI)), WiFi 221 (e.g., IEEE 802.11), cellular/mobile network 222 (e.g., GSM, CDMA, etc.), Bluetooth and/or BLE 223 (e.g., according to the Bluetooth Special Interest Group),

ZigBee 224(e.g., IEEE 802.15), and ZWave (e.g., according to the Z-Wave Alliance), and the like.

[0051] As shown in FIG. 2, base unit 120 may have various combinations of wireless interfaces (e.g., based on a diversity of interfaces of various devices found in the structure). DECT ULE 220 provides excellent range, operation in a licensed band, and good energy efficiency for long battery life, but unlike Bluetooth, CDMA, LTE, and GSM, DECT ULE may not typically found in cell phones and may have lower bandwidth than WiFi. ZWave 225 is widely adopted in a range of devices. ZigBee 224 is widely used in utility meters. As would be readily appreciated by one of ordinary skill in the art, specific wireless communications (e.g. DECT ULE) – described in relation to various embodiments – may be other wireless communications (e.g., WiFi, Bluetooth, Bluetooth LE, ZWave, ZigBee, etc.). In addition, different protocols may be used, each having associated performance characteristics. Some embodiments include base unit 120 which supports all of the standards suggested by FIG. 2. Some cost effective embodiments include various subsets of all of the standards suggested by FIG. 2. For example, base unit 120 includes DECT ULE (or WiFi) as a backbone network to connect to devices that route to at least one (short-range) standard (e.g., ZWave, ZigBee and Bluetooth). By way of further example, base unit 120 includes a DECT ULE modem and communicates with a plug-in ZWave adapter disposed on or near a front door, to take advantage of the wide range of ZWave-enabled door locks.

[0052] ZWave includes a single “Primary Controller” and optionally additional “Secondary Controllers.” ZWave may also have any number of slave devices. The Primary Controller includes and/or excludes slave nodes from the network, so it is a node having (guaranteed to have) a complete ZWave routing table. In some embodiments, a DECT ULE to ZWave bridge may be used to bridge DECT ULE to a ZWave Primary Controller, since the ZWave Primary Controller preferably accesses all the slave devices. This may imply ZWave devices are added to the DECT ULE network

piecemeal, rather than allowing DECT ULE to tap into an existing network. As devices are included in a ZWave segment of the network, the bridge develops a routing table (e.g., according to the ZWave specification). Changes to the routing table, (e.g., from addition and/or removal of ZWave nodes) is reflected back to the main DECT ULE controller, so that it may too have a complete topology for that segment and can integrate the complete topology into the overall topology of the combined DECT ULE and ZWave network in the structure.

[0053] In some embodiments, the DECT ULE to ZWave bridge may be configured in at least two different ways, depending at least on whether the system has knowledge of the ZWave controller node in the DECT ULE bridge or not. For example, if the system (or its software or APIs) knows that the ZWave controller exists and is tightly coupled to the DECT ULE to ZWave bridge, then the ZWave messages may be encapsulated. In other words, a command (or command string) that would traditionally have been presented to the ZWave controller via a direct interface (e.g., serial, Universal Serial Bus (USB), I2C, SPI, etc.) may be encapsulated in a datagram, and set to the DECT ULE to ZWave bridge with an indication (e.g., in the datagram or in the transfer mechanism) of the encapsulation. The bridge may then act in a “dumb” manner, and presents the command directly to the ZWave controller (e.g., via Serial, USB, I2C, SPI, or other connection).

[0054] For example, if the system or software is not aware of (or wishes to disregard) the bridging functionality, then the DECT ULE to ZWave bridge may handle all of the translation. The DECT ULE to ZWave bridge may issue commands to the ZWave controller to retrieve at least one of the ZWave network topology, the list of nodes/devices, and the capability of each node/device. The DECT ULE to ZWave bridge may create “pseudo-devices” within itself, and notify the ULE master to update its directory. When an entity in the system wishes to communicate with a device on the ZWave bus, the bridge may take the commands from the entity, transcode from

standard DECT ULE forms/APIs into standard ZWave forms/APIs, and issue the appropriate commands to the ZWave controller.

[0055] The DECT ULE to ZWave bridge may handle routing translation between busses. The DECT ULE controller treats the ZWave segment nodes as multiple endpoints within the DECT ULE->ZWave bridge node. Similarly, any secondary controller may treat DECT ULE nodes for which it has been made aware as additional functional units within the bridge device.

[0056] ZWave messages may not necessarily be transmitted directly to a destination node, but instead may pass through up to four routing nodes. ZWave nodes may not receive a message while sleeping (e.g., to conserve battery power), delivery time may be unbounded. The DECT ULE to ZWave bridge may run (essentially) asynchronously, with (only) an immediate response to a message request being an indication of the destination's validity. Subsequently, at least one of an ACK/NACK and a Timeout may be returned to the DECT ULE controller, depending on the ZWave device's capabilities.

[0057] ZigBee may be said to resemble Zwave in that it is also a mesh network which may need a DECT ULE to ZigBee bridge to act as a primary controller for the ZigBee network of devices.

[0058] An potential issue with bridging to Bluetooth Low Energy (BLE) is encapsulating Generic Attribute Profile (GATT) attribute fragments into Internet Protocol (IP) packets and transferring them back to the DECT ULE master. The DECT ULE master may un-encapsulates the GATT attribute fragments from the Internet Protocol (IP) packets, and may pass each of the GATT attribute fragments to the engine as an event. The DECT ULE - BLE bridge may track a segment topology and all of the paired nodes. The segment topology and all of the paired nodes may be presented as sub functions of the DECT ULE - BLE bridge. The DECT ULE - BLE bridge may optionally provide a generic BLE-gateway to the Internet via encapsulation.

[0059] As would be readily appreciated by one of ordinary skill in the art, base unit 120 providing such bridging capabilities is not limited to the protocols described in the example above, but could be any pair of protocols either directly supported by the base unit 120 or by an external device connected to base unit 120 (not shown in FIG. 2), including as a way to bridge existing systems with protocols not yet defined by way of additional peripherals connected to 120 to provide additional network connections and using the capabilities of 120 to provide translation.

[0060] Wired and wireless communications as described herein may be used to efficiently monitor and control devices. For example, base unit 120 may use an ULE channel to monitor and control thousands of sensor and/or actuators 203-210 (in addition to audio devices such as DECT phone 202).

[0061] DECT phone 202 may be a portable unit, such as a cordless telephone and optionally a base unit (e.g., to charge the portable unit). DECT phone 202 may originate and receive telephone calls, for example, using POTS, VOIP, and the like.

[0062] In some embodiments, DECT phone 202 also performs monitoring and/or control functions. In typical operation, an incoming call may cause DECT phone 202 to ring. A microphone and speaker of DECT phone 202 may be activated in response to a user pressing a button (or similar input), indicating that he wishes to answer the incoming call. In various embodiments, when a (remote) user has been notified that there may be an intruder in the home, the operation of DECT phone 202 is modified. With the appropriate firmware, for example, DECT phone 202 can be directed by the base unit 120 to silently connect to base unit 120 and activate its microphone (leaving the speaker muted). For example, a handset sitting on a table or otherwise innocuously disposed within the structure “listens in” on what is going on in the room, without ringing or providing any other indication that it is active. By way of further example, any or all of the handsets in the home are activated in this manner, such that multiple locations in the structure are simultaneously monitored for any audible activity.

[0063] In some embodiments, when an intruder has entered the home, the user's web or smartphone-based client on computing device 110 (FIG. 1) is notified of the intrusion and the user can choose to signal the base to activate some or all of the handsets in the home to silently "listen in" on activity in the home. By monitoring the structure in this way, the user may determine if the intruder alert is valid or a false alarm. From his smartphone, the user may choose to listen in to handsets one by one, or he may choose to listen to a mix (performed by the base or server infrastructure) of all of the handsets at once. The base or server infrastructure or client may record any or all of the audio streams coming from the activated handset(s), or other connected devices in the home such as a video door camera, for example, to provide evidence for use in an investigation and/or against the intruder during legal proceedings such as a trial.

[0064] In some embodiments, DECT phone 202 is used to communicate with the intruder. For example, after evaluating the state of the sensors in the home and perhaps listening in to the activity of the intruder through the silently activated DECT handsets, the user can engage the intruder directly. In various embodiments of the invention, the user may use his web or smartphone client on computing device 110 to direct one or more of DECT phone 202 to enter intercom mode which engages the speaker and microphone of any or all of the DECT phone 202 in the structure to tell the intruder to "Stop what you are doing. Leave the house!" This type of direct engagement may be more effective than calling the police or neighbor to investigate.

[0065] Some embodiments of the present invention include special/custom firmware in DECT phone 202 (e.g., in base and/or handset) to enable DECT phone 202 to activate silently, enter listen in mode, and change to intercom mode under the control of the remote client. As would be readily appreciated by one of ordinary skill in the art, the operation described herein does not correspond to standard DECT behaviors. In fact, present DECT handsets are activated individually. In contrast, a network of DECT

handsets, ideally with speakerphones, can all connect to the base simultaneously and, engaging their speakerphones, blare out a warning to the intruder to scare him off, according to some embodiments. For example, the warning is pre-recorded and streamed from server 160. In some embodiments, there is more than one message and each message is used in response to one or more specific sensed events. For example, in response to an intruder being detected in the living room or smoke being detected in the kitchen, "Motion in living room!" or "Smoke in the kitchen!" is respectively announced from all the handsets in the structure.

[0066] By way of further example, when a handset is in this monitoring announcement mode and its firmware senses the handset is removed from the cradle or activated, the announcement stops to allow a user to attempt to place a phone call (e.g., to 911). In some embodiments, the software application on computing device 110 (e.g., smartphone client, web client, etc.) is based on a Session Initiation Protocol (SIP) (e.g., according to Internet Engineering Task Force (IETF) RFC 3261) platform. PJ SIP, for example, includes a signaling protocol (SIP), a multimedia framework, and NAT traversal functionality into a high-level multimedia communication application programming interface (API). In some embodiments, the SIP platform is directed by the software application to initiate a VoIP session using server 160. Server 160 may direct base unit 120 to open the intercom channel to DECT phones 202 and the call is completed at any or all of DECT phone 202 operating in intercom mode (e.g., no action by the intruder is required for the call to be connected).

[0067] Sensor 203 may include at least one of a motion sensor, door/window sensor, glass breakage sensor, flood sensor, smoke detector, heat sensor, carbon monoxide sensor, and the like.

[0068] Smoke and/or carbon monoxide alarm sensors 203 senses the atmosphere and sounds a siren when smoke and/or carbon monoxide (respectively) are detected. In some embodiments, these alarms are connected to the base through DECT ULE (or

other wireless communication). Such network connectivity enables several new modes of operation for these alarms. For example, the function of the siren in the detector may be separately triggered (e.g., under firmware control) using DECT ULE signals, which has the advantage of better coordination between multiple detectors in the structure. In response to detecting smoke in one room or zone, rather than just a particular smoke detector sounding its siren, the particular smoke detector communicates the triggering event to base unit 120. Base unit 120, after optionally communicating with server 160 to determine any user preferences, may trigger some or all of the smoke and/or carbon monoxide detectors in the structure. A fire in the kitchen downstairs, for example, immediately results in the siren sounding in the bedroom area upstairs.

[0069] In some embodiments, at least some functions of the smoke or carbon monoxide alarm (e.g., testing the smoke alarm, disabling a false alarm, etc.) may be controlled by computing device 110 (e.g., smartphone 230). In various embodiments, when an intruder's penetration of the structure is detected by peripherals 202-210 and a (remote) user monitors the situation from his smartphone, the remote user activates the blaring siren of all the detectors to sound throughout the structure, absent any fire. Configuration and operation of the alarms in this manner offers the benefit of reinforcing the sound of a separate siren or the opportunity to eliminate the cost associated with a separate siren device, which would otherwise be required to effect such an audible intruder alarm.

[0070] Active device 204 includes at least one of an electrical switch, siren, speaker, locking mechanism (e.g., door handle lock, dead bolt lock, electromagnetic lock, etc.), light fixture, and the like. These active devices can be controlled by base unit 120 to programmatically respond to input from the user (via computing device 110), from various sensors 230, or other events as discussed.

[0071] Camera 205 may be one or more of a video camera and still image camera. For example, camera 205 may be a closed-circuit television (CCTV) camera. By

way of further example, camera 205 may be an internet protocol camera (IP camera). Camera 205 may be disposed at any of a variety of locations inside and/or outside the structure (e.g., for viewing persons arriving at a front door). One or more of camera 205 may be independently controlled (e.g., by a user through computing device 110), activated when UAV 206 (see below) follows an intruder into an area covered by one of camera 205, when a sensor 203 detects activity near one of camera 205, etc.

[0072] Hazard sensor 209 is used to prevent injury or death in hazards associated with the structure. For example, many pools, hot tubs, and other hazards are fitted with sensors that generate an alert in the event a child or pet falls into (or otherwise obtains access to) the pool, hot tub, and other hazard. Hazard sensor 209 may include at least one of gate sensor (e.g., detects when a gate providing access to the hazard is opened), motion sensor in the pool area, and sensor which detects disruption to the water surface.

[0073] Unmanned aerial vehicle (UAV) 206 may be a quadcopter or other drone. UAV 206 may include an electronic control system and electronic sensors to stabilize the aircraft. UAV 206 may also include one or more sensors, such as a video camera. UAV 206 may be operated inside and/or outside the structure. In some embodiments, UAV 206 is a terrestrial and/or aquatic vehicle, such as an unmanned ground vehicle (UGV), autonomous surface vehicles (ASV), autonomous underwater vehicle (AUV), and the like.

[0074] For example, when hazard sensor 209 detects an unsafe condition (for example the surface of a pool or hot tub being disturbed, perhaps by a child entering) or a sensor 203 detects a security situation (motion sensor activated, glass break sensor activated), a (remote) user monitoring the situation in the structure using computing device 110 may instruct UAV 206 to launch and follow a pre-programmed flight path to video the outside of the structure (e.g., a pool area) or location of the security situation. UAV 206 may maintain a connection to base unit 120 through the WiFi network for its

entire flight path and provide live video of the exterior of the structure to base unit 120. Base unit 120 may stream the live video to computing device 110 (e.g., smartphone 230). The user may also modify the flight path in response to the (observed) situation, communicating the flight path changes from computing device 110, through network 150, to base unit 120. Base unit 120 may control UAV 206 through the structure's WiFi network.

[0075] In some embodiments UAV 206 may be programmed to (follow waypoints on a path to a certain location and) hover near a certain location (e.g., a front door to awaiting the intruder's exit, a pool to verify a child has fallen in, etc.). In various embodiments, UAV 206 may take video of license plates of nearby cars in case one of them belongs to the intruder, while flying down a street (e.g., under real-time control from the user using computing device 110, following a pre-programmed route, etc.). In various embodiments, when UAV 206 flies out of range of the WiFi network, the video may be stored locally in UAV 206. In response to UAV 206 again being within range of the WiFi network (e.g., on its way back to its landing pad), the video may be uploaded through the WiFi network. In this way, UAV 206 may advantageously convince a would-be intruder – upon seeing UAV 206 circling the structure at the slightest provocation – to try a softer target.

[0076] In various embodiments, UAV 206 is employed in additional or alternative ways. UAV 206 may perform periodic patrols (e.g., following programmed routes around the property on which the structure is disposed). UAV 206 may include sensors (e.g., motion sensor, infrared cameras, additional Bluetooth sensors, etc.) for monitoring (e.g., to detect an unfamiliar car, a pedestrian, and the like within the property's perimeter). UAV 206 may communicate through WiFi with base unit 120 (e.g., to initiate a notification of the user via computing device 110). The user can then monitor the situation and direct further action. UAV 206 may also launch to perform a

pre-programmed mission in response to input received from at least one of peripherals 202-210, without intervention by the user.

[0077] In some embodiments, UAV 206 may be located outdoors (e.g., on the roof of the structure). UAV 206 may be stored in a shelter (not shown in FIG. 2) which protects UAV 206 from exposure to the elements and which does not interfere with UAV's 206 flight capabilities. The shelter may include a charging system. For example, the shelter includes a wireless charging system, so that launch of UAV 206 may be performed without disconnecting charging wires. By way of further example, the shelter also includes a mechanism to facilitate launch (e.g., to move the UAV out of the shelter for launch, open the roof of the shelter to allow the UAV to achieve aerodynamic lift, etc.).

[0078] Speaker 207 may be a loudspeaker. Two or more of speaker 207 may be disposed in and/or about the structure for purposes such as structure wide music reproduction, audio effects (e.g., multichannel surround sound), and coverage for public address system (PA system). Base unit 120 and/or a home entertainment system (not shown in FIG. 2) may provide ambient music both inside (e.g., through ceiling mounted speakers) and outside (e.g., for music on patios, in pool areas, etc.) the structure. In some embodiments, audio from the base unit's 120 voice communications may be provided through one or more of (high quality) speaker 207. In conjunction with at least one of DECT phone 202 or smartphone 230 to provide a microphone (or an external microphone not shown in FIG 2 connected to base unit 120) base unit 120 may use speaker 207 to provide a much higher quality speakerphone experience.

[0079] Speaker 207 may also be used in a manner similar to DECT phone 202 (e.g., to play announcements, messages, and to replace or augment alarm sirens), smoke alarm and/or carbon monoxide detector of sensor 203 (e.g., to replace or augment a separate alarm siren), and dedicated alarm sirens (not shown in FIG. 2) (e.g., to replace or augment a separate alarm siren).

[0080] Thermostat 208 senses an ambient temperature and controls a structure's heating and/or air conditioning system according to a desired temperature. Thermostat 208 may control the temperature of the structure according to a predetermined schedule, such as setting a lower temperature at night. Thermostat 208 may be a "smart" thermostat which, for example, learns when the structure is likely to be occupied and when it is likely to be empty (e.g., to automatically pre-heat or pre-cool the structure). Additionally or alternatively, more than one of thermostat 208 is disposed in the structure to control temperature in individual rooms or zones.

[0081] For example, thermostat 208 may include a motion sensor to determine occupancy and adjust temperature accordingly. In some embodiments, the thermostat is connected to base unit 120 via DECT ULE 220 (or other wireless communication). The motion sensor of thermostat 208 may be used as an additional sensor to detect intruders. In this way, a motion sensor of thermostat 208 provides the advantages of augmenting a separate motion sensor of sensor 203 and/or eliminating a separate motion sensor (and its associated costs, reducing the overall cost of the system). Additionally or alternatively, thermostat 208 may provide temperature information to base unit 120. In this way, dangerous conditions (e.g., high temperatures associated with a heat wave, fire, etc.) may be detected.

[0082] Baby monitor 210 includes audio and/or video sensors (e.g., microphone, video camera, etc.), for example to remotely monitor a baby from outside the baby's room. Baby monitor 210 may optionally include at least one of a night light, motion sensors (e.g., to sound an alarm if the baby stops moving for a predetermined amount of time), and night vision technology (e.g., infrared light emitting diodes and a charge-coupled device (CCD) sensor sensitive to infrared light) to enable viewing of a darkened room. When communicatively coupled to base unit 120, baby monitor 210 may also be used to provide audio or video for security monitoring, augmenting alert sounds, communicating with intruders etc., as described above.

[0083] Smartphone 230 is a mobile phone with more advanced computing capability and connectivity than, for example, basic feature phones. In some embodiments, smartphone 230 is one of computing device 110 (FIG. 1). As described herein, smartphone 230 may be used to monitor and control peripherals 202-210. For example, a web client (or other software application) on smartphone 230 may trigger actions designed to intimidate the intruder, include activating a siren (including those incorporated into sensors 203, DECT phones 202, speakers 207, baby monitors 210, etc.) in the house, by using actuators 203 to cause the lights to flash, lock doors, and the like. For example, such actions can be performed using communications between base unit 120 and at least one peripheral 202-210, via DECT ULE.

[0084] In various embodiments, smartphone 230 also serves a role similar to peripherals 202-210. For example, data from sensors (e.g., front and/or rear facing cameras, microphone(s), Global Positioning System (GPS) radio, WiFi modem, Bluetooth modem, etc.) of smartphone 230 is provided to base unit 120, received by base unit 120, and used by base unit 120 in a manner similar to peripherals 202-210, as described herein.

[0085] The present invention offers the user additional choices to respond to the intruder that leverage the VoIP capabilities of the server infrastructure. From his web or smartphone client, the user, upon determining that the intruder alert is valid, could initiate a 911 call as if it were originating from the house, rather than from the user's smartphone client. Normally a 911 call from a cell phone is directed to a public safety access point (PSAP) associated with the geographical location of the cell phone. For a user at a remote location who is alerted that his house is being invaded, dialing 911 from his cell phone would result in significant delay as he explains the situation to the PSAP serving the physical location of his smartphone (rather than that of the house that has been invaded), then waits for his call to be transferred to a PSAP in the area of his home and then takes the time to communicate the location of the house that is being

invaded (which may even be in another state), and convinces the authorities to go to the invaded house. In the present invention, since the base unit in the house also provides VoIP service for the home, it is already provisioned to have its phone number associated with the appropriate physical address of the house. In the present invention, the user, operating his web or smartphone-based client, may initiate a 911 call from the user running the app as if it were originating from the invaded house. The call will then directly connect to the PSAP that is local to the invaded house, with the proper address electronically passed to the PSAP as if the call had originated from the invaded house, bypassing the delay of the earlier scenario.

[0086] As would readily be appreciated by one of ordinary skill in the art, various combinations and permutations of inputs from peripherals 202-210 are received by base unit 120, actions taken by base unit 120 based at least in part on the inputs, and options offered to a user via a software application on computing device 110 (FIG. 1) are possible. By way of example, water/moisture sensors alert the owner to possible leak situations via a smartphone interface on computing device 110, UAV 206 is dispatched to observe the impacted area. By way of further non-limiting example, similar responses are provided for alerts from freeze sensors, power failure sensors, humidity sensors, and numerous other sensors, again with embodiments to play announcements, contact the user, share on social media, dispatch a drone, etc.

[0087] FIG 3. illustrates a simplified architecture of customer-premises equipment (CPE) 300, according to some embodiments. CPE 300 includes at least one of base unit 120 and external bridge 350. In some embodiments, base unit 120 includes CPU 310, RAM 320, and Flash Storage 330. Additionally, base unit 120 may include at least one of DECT radio 355, WiFi Radio 340, and wired interfaces for Local Area Network (LAN) 390, Wide Area Network (WAN) 392, and FXS interface to the phone system 394, all shown communicatively coupled to network 150. Additionally, base

unit 120 may include external USB connectivity (e.g., to peripherals as described in relation to FIGs. 2 and 13) via interface 396.

[0088] External bridge unit 350 includes bridge 360, which connects interfaces for one or more other protocols, for example, Bluetooth/BLE (361), ZigBee (362), ZWave (363), DECT (364) and other Wireless Interfaces (365). Bridge unit 350 may be connected to base unit 120 via one of the bridge interfaces (361-365) connecting to the base unit's WiFi Radio (340) or DECT Radio (355), via a USB connection from the base unit USB interface 396 to a USB connection on the bridge (not shown), via a wired network connection through network 150 to a wired connection on the bridge (not shown), or through another wired or wireless network connection.

[0089] FIG 4. shows a method 400 for operating base unit 120 (FIGS. 1 and 2) according to some embodiments. At step 410, sensor data is received from peripherals 202-210 by base unit 120. In some embodiments, sensor data is received from peripherals 202-210 (FIG. 2) through wired communications and/or wireless communications 220-225.

[0090] At step 415, a critical event such as an intruder entering the structure is determined from at least the received sensor data. For example, the intruder trips a motion sensor of sensor 203 which is interpreted as a critical event.

[0091] At step 420, an alert is created based at least on the critical event. For example, the alert includes information about the critical event (e.g., glass breakage detected in the family room, smoke detected in the kitchen, etc.)

[0092] At step 425, base unit 120 optionally provides the alert to server 160 (FIG. 1). For example, base unit 120 optionally sends the alert to server 160 through communications 144, network 150, and communications 148 (FIG. 1). In some embodiments where the apparatus and methods of server 160 are incorporated into base unit 120, the alert is not provided to server 160, but instead used internally by base unit 120.

[0093] At step 430, server 160 optionally receives the alert provided at step 425. In some embodiments where the apparatus and methods of server 160 are incorporated into base unit 120, the alert is not received by server 160, but instead used internally by base unit 120.

[0094] At step 435, user preferences associated with base unit 120 and/or a user of base unit 120 are retrieved (e.g., read from a database not shown in FIG. 2) and analyzed. At step 440, a response is determined based at least on the user preferences and the nature of the alert. For example, the determined response is to send a notification including a form of notification (e.g., send a notification through software application, SMS text message, etc.). At step 445, the notification is optionally provided. For example, base unit 120 and/or server 160, after analyzing at least one of the sensor data, critical event, alert, and the user preferences, communicate the notification to a software application on computing device 110 (e.g., user's smartphone) through a push notification. In response to receiving the notification, the software application attracts the user's attention (e.g., providing an audible tone, flashing screen, etc.) and apprises the user of the situation at the structure (e.g., through at least one of displayed text, displayed graphics (including video), and audible tones and/or voice). As another example, the notification is an SMS text message sent to smartphone 230. In some embodiments, the software application is not used when the notifications are SMS text messages.

[0095] Steps 435-445 may be performed at base unit 120, server 160, and combinations thereof. In some embodiments where the apparatus and methods of server 160 are incorporated into base unit 120, steps 435-445 are performed by base unit 120.

[0096] The software application on computing device 110 may use data from a GPS radio to determine a present location. Based at least on the present location, the software application will process the alert. For example, in response to the software

application determining the user is not presently in the structure (and therefore not under threat by a possible intruder), the software application displays the nature of the notification and presents multiple options for responding to the notification. The options presented to the user may be based in part on the capabilities of computing device 110 (smartphone, phablet, tablet computer, notebook computer, desktop computer, etc.), features supported by base unit 120 and/or server 160 (e.g., place telephone call, send an SMS text message, etc.), and availability of peripherals 202-210 (e.g., presence of siren, camera, etc.). The operation of computing device 110 and software application are described further in relation to FIG. 5.

[0097] At step 450, optionally an instruction is received. For example, the software application on computing device 110 may send an instruction generated based at least on a user selection from options presented. In some embodiments, a predetermined course of action may be taken (automatically without receipt of the instruction) in response to a particular determined critical event.

[0098] At step 455, a peripheral and/or service is activated. As described in greater detail herein, peripherals and/or services such as an internal and/or external siren, lighting (e.g., flash, turn on, and turn off), audible and/or visual alarm in a smoke detector, a personal surveillance drone, door locks, window coverings (e.g., open, close, and trim), postings to social media, and the like may be controlled or performed. In some embodiments where instructions are not received from the user, the activation may be automatic and/or based on the determined response (step 440).

[0099] FIG. 5. depicts a method 500 for operating computing device 110 (FIG. 1) according to various embodiments. At step 510 a notification is received. For example, a response is determined and a notification provided by base unit 120 (steps 440 and 445 in FIG. 4) is received by computing device 110. The notification may include information about the critical event.

[00100] At step 515, a user interface is provided by computing device 110, for example, in response to receipt of the notification. In some embodiments, the user interface at least notifies the user graphically and/or textually that a notification has been received. For example, the software application launches its user interface and offers the user the opportunity to activate a menu of alert responses (i.e., choices).

[00101] At step 520, a location of computing device 110 (and hence a user of computing device 110) is determined, for example, based in part on information received from a GPS radio of computing device 110.

[00102] At step 525, the presence of the user in the structure is evaluated based on the determined location. For example, if the client software application determines that the user is physically in the structure where the intruder has been detected, then it is possible that the user is not in a safe position to interact with the software application. In response to the user not being in the structure, the method proceeds to step 530. In response to the user being in the structure, the method proceeds to step 535.

[0103] At step 535, a reaction from the user responsive to the user interface is evaluated. For example, when the user does not respond (no response) to the appearance of the user interface and/or opportunity to activate the menu of alert responses, then the user may not be free to operate the software application (e.g., since he may be in dangerous proximity to the intruder). In response to the user responding, the method proceeds to step 530. In response to the user not responding, the method proceeds to step 540.

[0104] At step 540, an incoming communication (e.g., telephone call, text message, email, etc.) from base unit 120 and/or server 160 is received. For example, when the user does not respond to the user interface, the software application sends a message to base unit 120 and/or server 160 that causes a call to be placed to the smartphone. In some embodiments, the incoming call may verbally ask a challenge

question for at least one of a keyword, key phrase, personal identification number (PIN), and the like to cancel alarm condition (e.g., the alert).

[0105] At step 545, user input is received. User input is, for example, a verbal response to the challenge question or no response. At step 550, the user input (or lack thereof) is evaluated to determine if the user input is satisfactory. For example, satisfactory input is the expected predetermined keyword, key phrase, or personal identification number (PIN). For example, unsatisfactory input is the user does not answer the call (no response), the user fails to respond to the call with the proper keyword or PIN to disable the monitoring system, the user responds with a pre-arranged panic keyword or PIN, and the like. In response to the user providing a satisfactory response, the method proceeds to step 530. In response to the user not providing a satisfactory response, the method proceeds to step 555.

[0106] At step 555, a user status is provided to base unit 120 and/or server 160. For example, a user status indicates the user did not provide a satisfactory response. In response to receipt of the user status, base unit 120 and/or server 160 may be programmed to presume the user is under duress or otherwise in danger. For example, base unit 120 and/or server 160 may initiate a 911 call originating from the structure's address. The 911 call placed may have an automated message that describes the situation (e.g., based on sensor data, critical event, lack of user response, etc.), so that authorities can have the best opportunity to safely handle the situation, even when the user himself is not in a safe position to speak with the authorities. In this way, the user is given ample opportunity to disable the alarm condition (e.g., alert), but not at the expense of ultimately notifying the authorities.

[0107] At step 530, options are presented. For example, computing device 110 may present a menu of alert responses. Alert responses may include activating the microphone in one or more of DECT phone 202, hit a (virtual) "panic button," and the like. Further examples of alert response are described above.

[0108] At step 560, a selection from the alert responses is received from the user.

[0109] At step 565, an instruction associated with the received selection is provided to base unit 120 and/or server 160. For example, if the user hits the virtual panic button, then an instruction to initiate a 911 call is sent to base unit 120 and/or server 160.

[0110] In the absence of communication with the user or lack of response from the user at any stage, pre-programmed actions may be determined and performed by the base unit 120 or the server 160 .

[0111] FIGS. 6-12 illustrate methods for wireless operation according to various embodiments. FIG. 6 illustrates the process 600 of monitoring for devices in range of the various network interfaces 220-225 (in the example Bluetooth 223) and taking actions. FIG. 7 illustrates one embodiment 700 of actions based on rules taken in response to the various connected devices. FIG. 8 illustrates a mechanism 800 an embodiment could use to force scanning and record events, and then push them to the cloud in the case of an alarm event. FIG. 9 illustrates an embodiment 900 where notifications are generated as various devices 230 and 240 enter the range of various network interfaces 220-225. FIG 10 illustrates a mechanism 1000 an embodiment might use to process actions in response to a new device 230 or 240, not previously seen, entering the range of one of the various network interfaces 220-225. FIG. 11 illustrates one embodiment 1100 where notifications are generated based on the time that a device 230 or 240 is detected as being in range to one of various network interfaces 220-225. FIG 12 illustrates the process 1200 used by one embodiment to generate an alert when a particular "flagged" device 230 or 240 is detected to have come within range of one of the various network interfaces 220-225. These figures are provided by way of example and not limitation.

[0112] FIG. 13 illustrates an exemplary computing system 1300 that is used to implement some embodiments of the present systems and methods. The computing system 1300 of FIG. 13 is implemented in the contexts of the likes of computing devices,

networks, web servers, databases, or combinations thereof. The computing device 1300 of FIG. 13 includes a processor 1310 and memory 1320. Memory 1320 stores, in part, instructions and data for execution by processor 1310. Memory 1320 stores the executable code when in operation. The computing system 1300 of FIG. 13 further includes a mass storage 1330, portable storage 1340, output devices 1350, input devices 1360, a display system 1370, and peripherals 1380. The components shown in FIG. 13 are depicted as being connected via a single bus 1390. The components are connected through one or more data transport means. Processor 1310 and memory 1320 may be connected via a local microprocessor bus, and the mass storage 1330, peripherals 1380, portable storage 1340, and display system 1370 may be connected via one or more input/output (I/O) buses.

[0113] Mass storage 1330, which may be implemented with a magnetic disk drive, solid-state drive (SSD), or an optical disk drive, is a non-volatile storage device for storing data and instructions for use by processor 1310. Mass storage 1330 can store the system software for implementing embodiments of the present technology for purposes of loading that software into memory 1320.

[0114] Portable storage 1340 operates in conjunction with a portable non-volatile storage medium, such as a floppy disk, compact disk or digital video disc, to input and output data and code to and from the computing system 1300 of FIG. 13. The system software for implementing embodiments of the present technology may be stored on such a portable medium and input to the computing system 1300 via the portable storage 1340. Portable storage 1340 operates in conjunction with a portable non-volatile storage medium, such as a floppy disk, compact disk or digital video disc, to input and output data and code to and from the computing system 1300 of FIG. 13. The system software for implementing embodiments of the present technology may be stored on such a portable medium and input to the computing system 1300 via the portable storage 1340.

[0115] Input devices 1360 provide a portion of a user interface. Input devices 1360 may include an alphanumeric keypad, such as a keyboard, for inputting alphanumeric and other information, or a pointing device, such as a mouse, a trackball, stylus, or cursor direction keys. Additionally, the system 1300 as shown in FIG. 13 includes output devices 1350. Suitable output devices include speakers, printers, network interfaces, and monitors.

[0116] Display system 1370 includes a liquid crystal display (LCD) or other suitable display device. Display system 1370 receives textual and graphical information, and processes the information for output to the display device.

[0117] In addition to peripherals 102-107 (FIG. 2), peripherals 1380 may include any type of computer support device to add additional functionality to the computing system. Peripherals 1380, for example, include a modem and/or a router.

[0118] The components contained in the computing system 1300 of FIG. 13 are those typically found in computing systems that may be suitable for use with embodiments of the present technology and are intended to represent a broad category of such computer components that are well known in the art. Thus, the computing system 1300 can be a personal computer, hand held computing system, telephone, mobile phone, smartphone, tablet, phablet, wearable technology, mobile computing system, workstation, server, minicomputer, mainframe computer, or any other computing system. The computer can also include different bus configurations, networked platforms, multi-processor platforms, etc. Various operating systems can be used including UNIX, LINUX, WINDOWS, MACINTOSH OS, IOS, ANDROID, CHROME, and other suitable operating systems.

[0119] Some of the above-described functions may be composed of instructions that are stored on storage media (e.g., computer-readable medium). The instructions may be retrieved and executed by the processor. Some examples of storage media are memory devices, tapes, disks, and the like. The instructions are operational when

executed by the processor to direct the processor to operate in accord with the technology. Those skilled in the art are familiar with instructions, processor(s), and storage media.

[0120] In some embodiments, the computing system 1300 may be implemented as a cloud-based computing environment, such as a virtual machine operating within a computing cloud. In other embodiments, the computing system 1300 may itself include a cloud-based computing environment, where the functionalities of the computing system 1300 are executed in a distributed fashion. Thus, the computing system 1300, when configured as a computing cloud, may include pluralities of computing devices in various forms, as will be described in greater detail below.

[0121] In general, a cloud-based computing environment is a resource that typically combines the computational power of a large grouping of processors (such as within web servers) and/or that combines the storage capacity of a large grouping of computer memories or storage devices. Systems that provide cloud-based resources may be utilized exclusively by their owners or such systems may be accessible to outside users who deploy applications within the computing infrastructure to obtain the benefit of large computational or storage resources.

[0122] The cloud is formed, for example, by a network of web servers that comprise a plurality of computing devices, such as the computing system 1300, with each server (or at least a plurality thereof) providing processor and/or storage resources. These servers manage workloads provided by multiple users (e.g., cloud resource customers or other users). Typically, each user places workload demands upon the cloud that vary in real-time, sometimes dramatically. The nature and extent of these variations typically depends on the type of business associated with the user.

[0123] It is noteworthy that any hardware platform suitable for performing the processing described herein is suitable for use with the technology. The terms “computer-readable storage medium” and “computer-readable storage media” as used

herein refer to any medium or media that participate in providing instructions to a CPU for execution. Such media can take many forms, including, but not limited to, non-volatile media, volatile media and transmission media. Non-volatile media include, for example, optical, magnetic, and solid-state disks, such as a fixed disk. Volatile media include dynamic memory, such as system RAM. Transmission media include coaxial cables, copper wire and fiber optics, among others, including the wires that comprise one embodiment of a bus. Transmission media can also take the form of acoustic or light waves, such as those generated during radio frequency (RF) and infrared (IR) data communications. Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, a hard disk, magnetic tape, any other magnetic medium, a CD-ROM disk, digital video disk (DVD), any other optical medium, any other physical medium with patterns of marks or holes, a RAM, a PROM, an EPROM, an EEPROM, a FLASH memory, any other memory chip or data exchange adapter, a carrier wave, or any other medium from which a computer can read.

[0124] Various forms of computer-readable media may be involved in carrying one or more sequences of one or more instructions to a CPU for execution. A bus carries the data to system RAM, from which a CPU retrieves and executes the instructions. The instructions received by system RAM can optionally be stored on a fixed disk either before or after execution by a CPU.

[0125] Computer program code for carrying out operations for aspects of the present technology may be written in any combination of one or more programming languages, including an object oriented programming language such as JAVA, SMALLTALK, C++ or the like and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter

scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

[0126] The corresponding structures, materials, acts, and equivalents of all means or step plus function elements in the claims below are intended to include any structure, material, or act for performing the function in combination with other claimed elements as specifically claimed. The description of the present technology has been presented for purposes of illustration and description, but is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the invention. Exemplary embodiments were chosen and described in order to best explain the principles of the present technology and its practical application, and to enable others of ordinary skill in the art to understand the invention for various embodiments with various modifications as are suited to the particular use contemplated.

[0127] Aspects of the present technology are described above with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to embodiments of the invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0128] These computer program instructions may also be stored in a computer readable medium that can direct a computer, other programmable data processing apparatus, or other devices to function in a particular manner, such that the instructions stored in the computer readable medium produce an article of manufacture including instructions which implement the function/act specified in the flowchart and/or block diagram block or blocks.

[0129] The computer program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatus or other devices to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0130] The flowchart and block diagrams in the Figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present technology. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified

functions or acts, or combinations of special purpose hardware and computer instructions.

[0131] While the present technology has been described in connection with a series of preferred embodiment, these descriptions are not intended to limit the scope of the technology to the particular forms set forth herein. It will be further understood that the methods of the technology are not necessarily limited to the discrete steps or the order of the steps described. To the contrary, the present descriptions are intended to cover such alternatives, modifications, and equivalents as may be included within the spirit and scope of the technology as defined by the appended claims and otherwise appreciated by one of ordinary skill in the art.

CLAIMS:

1. A method for security monitoring and control comprising:

receiving sensor data from at least one first peripheral, the sensor data associated with at least one of activity inside and activity outside of a structure;

determining a critical event based in part on the sensor data;

creating an alert based in part on the critical event;

getting user preferences associated with at least one of a user and a base unit;

determining a response based in part on the alert and user preferences;

activating at least one of a second peripheral and a service based in part on the response;

detecting a wireless device associated with an intruder; and

determining one or more properties of the wireless device, the determining including detecting a digital fingerprint of the wireless device, the wireless device being an unpaired Bluetooth enabled device in discoverable mode, and the determining of one or more properties further includes at least one of executing software on, sending a chunk of data to, or sending a sequence of commands to the unpaired Bluetooth enabled device, so as to gain control of the unpaired Bluetooth enabled device.

2. The method of claim 1 wherein the first peripheral includes at least one of a cordless phone, door/gate sensor, window sensor, glass breakage sensor, flood sensor, pool sensor, and baby monitor.

3. The method of claim 1 further comprising:

providing the alert to a server,

wherein the user preferences are received from the server.

4. The method of claim 1 further comprising:

providing a notification to the user based at least on the response; and

receiving instructions from the user,

wherein the activating is further based on the instructions.

5. The method of claim 1 wherein

the second peripheral includes an unmanned aircraft, and the

activating the second peripheral includes:

sending the unmanned aircraft to an area of interest, the area of interest determined based at least on the critical event;

sensing at least one of video and audio, the sensing using at least one of video and audio sensors disposed on the unmanned aircraft; and

providing the at least one of video and audio.

6. The method of claim 1 wherein

the second peripheral includes at least one cordless phone, and the

activating the second peripheral includes:

silently turning on a microphone of the at least one cordless phone;

sensing audio using the microphone; and

providing the audio.

7. The method of claim 6 wherein the activating the second peripheral further includes playing a selected recorded announcement using a speaker of the at least one cordless phone, the selection of the recorded announcement based at least on the response.

8. The method of claim 1 wherein the activating the service includes posting to social media to alert neighbors based at least on the response.

9. A base unit comprising:

a processor; and

a memory coupled to the processor, the memory storing instructions executable by the processor to perform a method for security monitoring and control including:

receiving sensor data from at least one first peripheral, the sensor data associated with at least one of activity inside and activity outside of a structure;

determining a critical event based in part on the sensor data;

creating an alert based in part on the critical event;

getting user preferences associated with at least one of a user and a base unit;

determining a response based in part on the alert and user preferences;

activating at least one of a second peripheral and a service based in part on the response;

detecting a wireless device associated with an intruder; and

determining properties of the wireless device, the wireless device being an unpaired Bluetooth enabled device in discoverable mode, and the determining properties includes at least one of executing software on, sending a chunk of data to, or sending a sequence of commands to the unpaired Bluetooth enabled device, so as to gain control of the unpaired Bluetooth enabled device.

10. The base unit of claim 9 wherein the first peripheral includes at least one of a cordless phone, door/gate sensor, window sensor, glass breakage sensor, flood sensor, camera, smart thermostat, pool sensor, and baby monitor.

11. The base unit of claim 9 wherein the method further comprises:

providing the alert to a server,

wherein the user preferences are received from the server.

12. The base unit of claim 9 wherein the method further comprises:

providing a notification to the user based at least on the response; and

receiving instructions from the user,

wherein the activating is further based on the instructions from the user.

13. The base unit of claim 9 wherein

the second peripheral includes an unmanned aircraft, and the

activating the second peripheral includes:

sending the unmanned aircraft to an area of interest, the area of interest determined based at least on the critical event;

sensing at least one of video and audio, the sensing using at least one of video and audio sensors disposed on the unmanned aircraft; and

providing the at least one of video and audio.

14. The base unit of claim 9 wherein

the second peripheral includes at least one cordless phone, and the

activating the second peripheral includes:

silently turning on a microphone of the at least one cordless phone;

sensing audio using the microphone; and

providing the audio.

15. The base unit of claim 14 wherein the activating the second peripheral further includes playing a selected recorded announcement using a speaker of the at least one cordless phone, the selection of the recorded announcement based at least on the response.

16. The base unit of claim 9 wherein the activating the service includes posting to social media to alert neighbors based at least on the alert.

17. A non-transitory computer-readable storage medium having embodied thereon a program, the program being executable by a processor to perform a method for security monitoring and control, the method comprising:

receiving sensor data from at least one first peripheral, the sensor data associated with at least one of activity inside and activity outside of a structure;

determining a critical event based in part on the sensor data;

creating an alert based in part on the critical event;

getting user preferences associated with at least one of a user and a base unit;

determining a response based in part on the alert and user preferences;

activating at least one of a second peripheral and a service based in part on the response;

detecting a wireless device associated with an intruder; and

determining one or more properties of the wireless device, the wireless device being an unpaired Bluetooth enabled device in discoverable mode, and the determining of one or more properties includes at least one of executing software on, sending a chunk of data to, or sending a sequence of commands to the unpaired Bluetooth enabled device, so as to gain control of the unpaired Bluetooth enabled device.

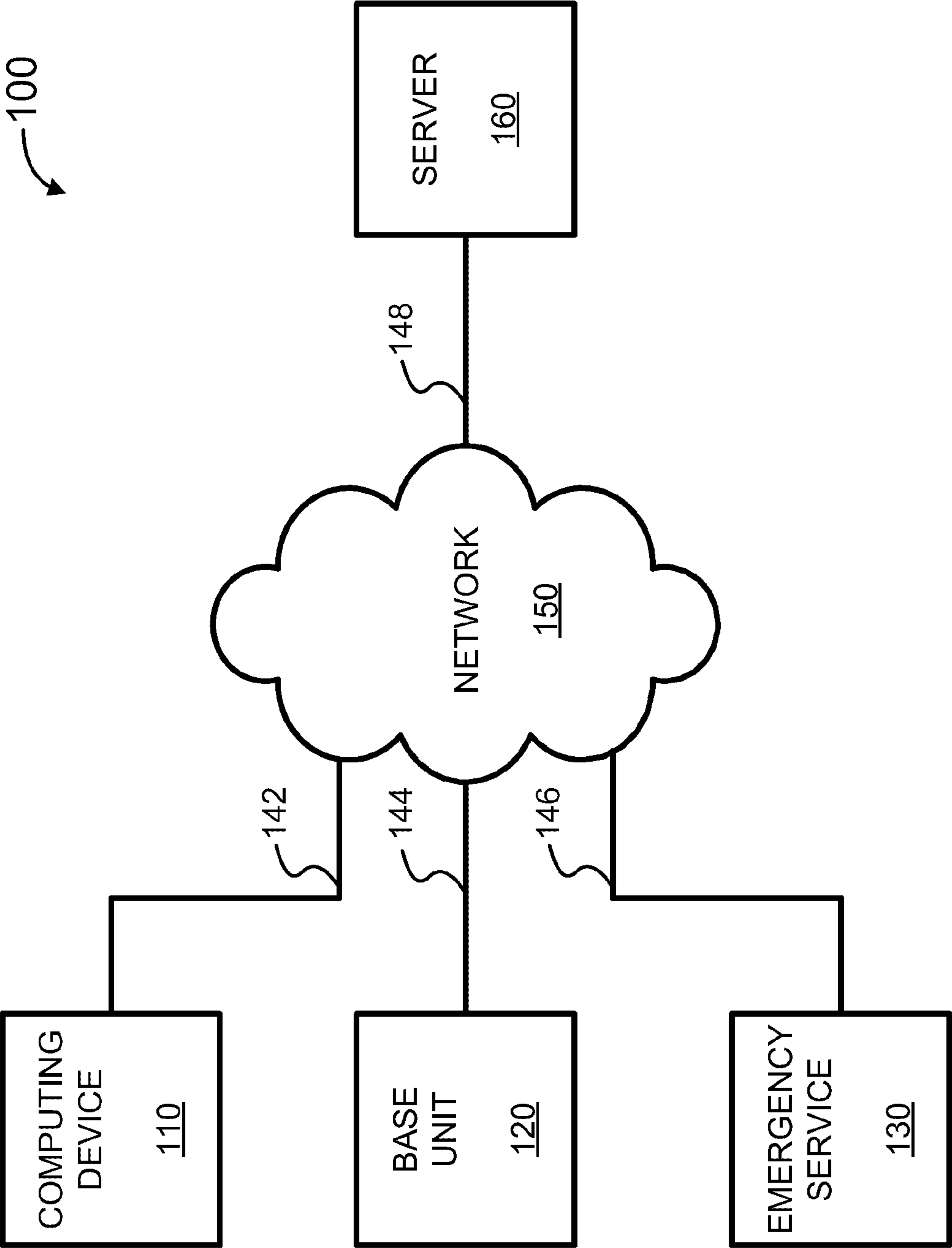


FIG. 1

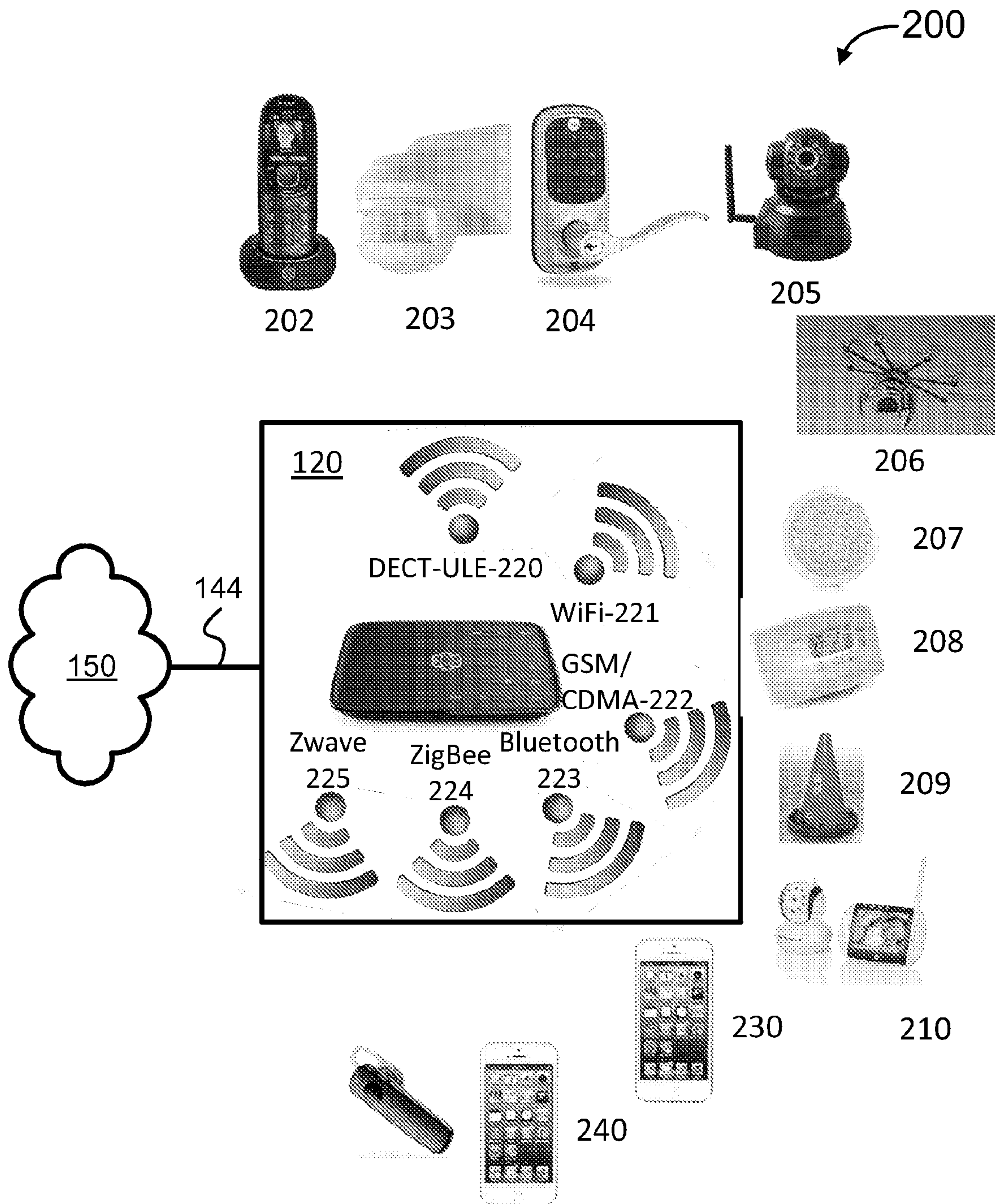


FIG. 2

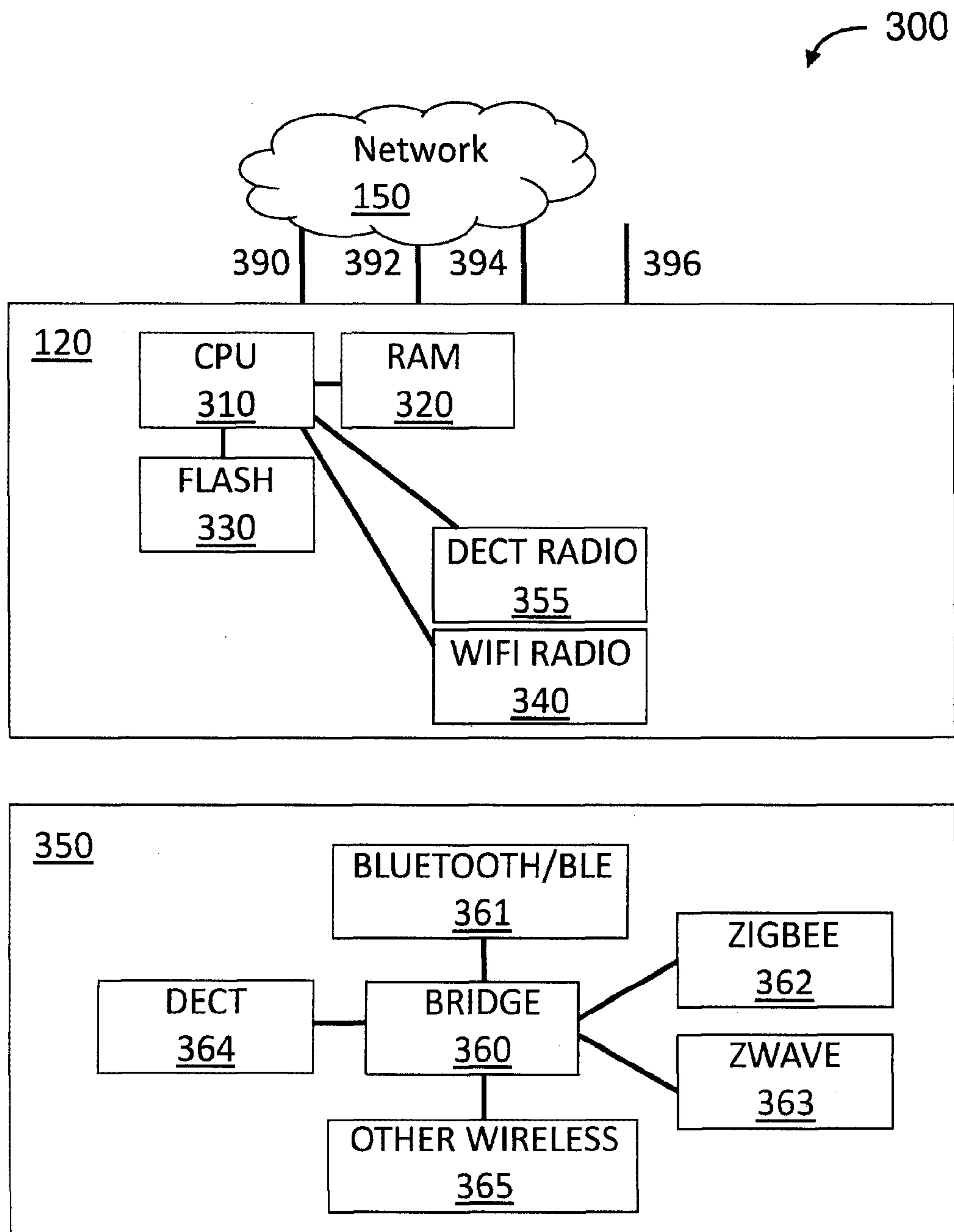


FIG. 3

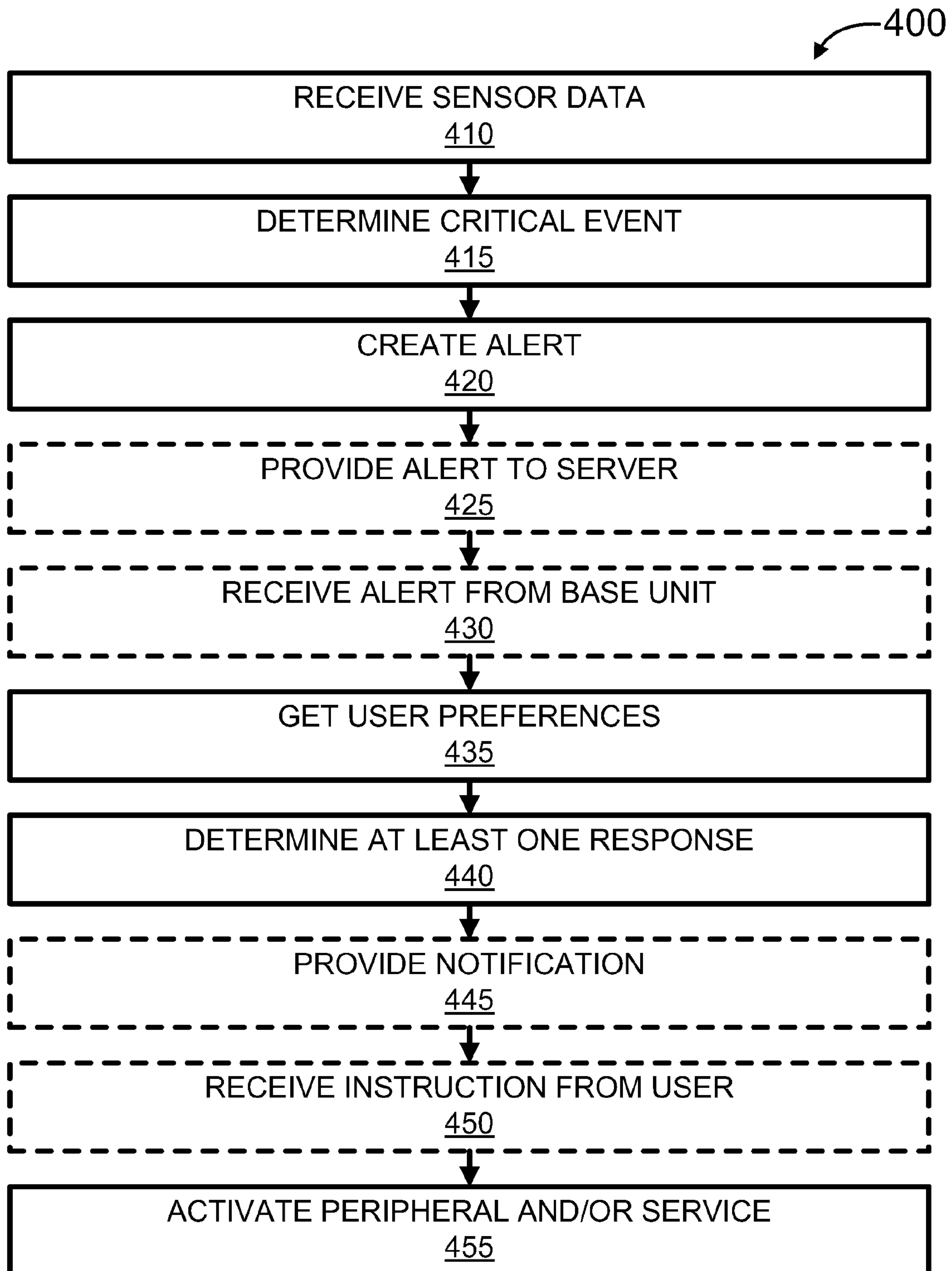


FIG. 4

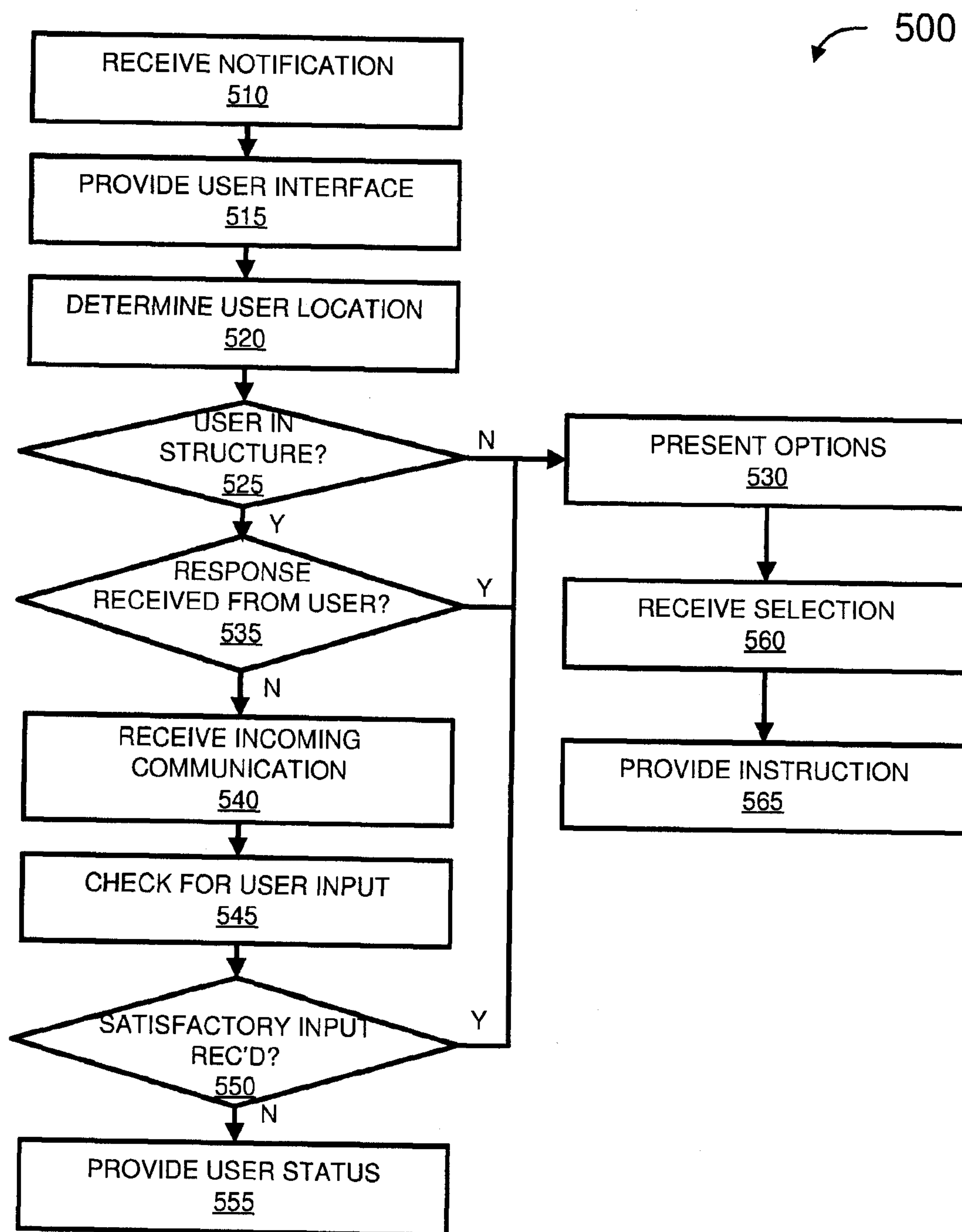


FIG. 5

5/13

600

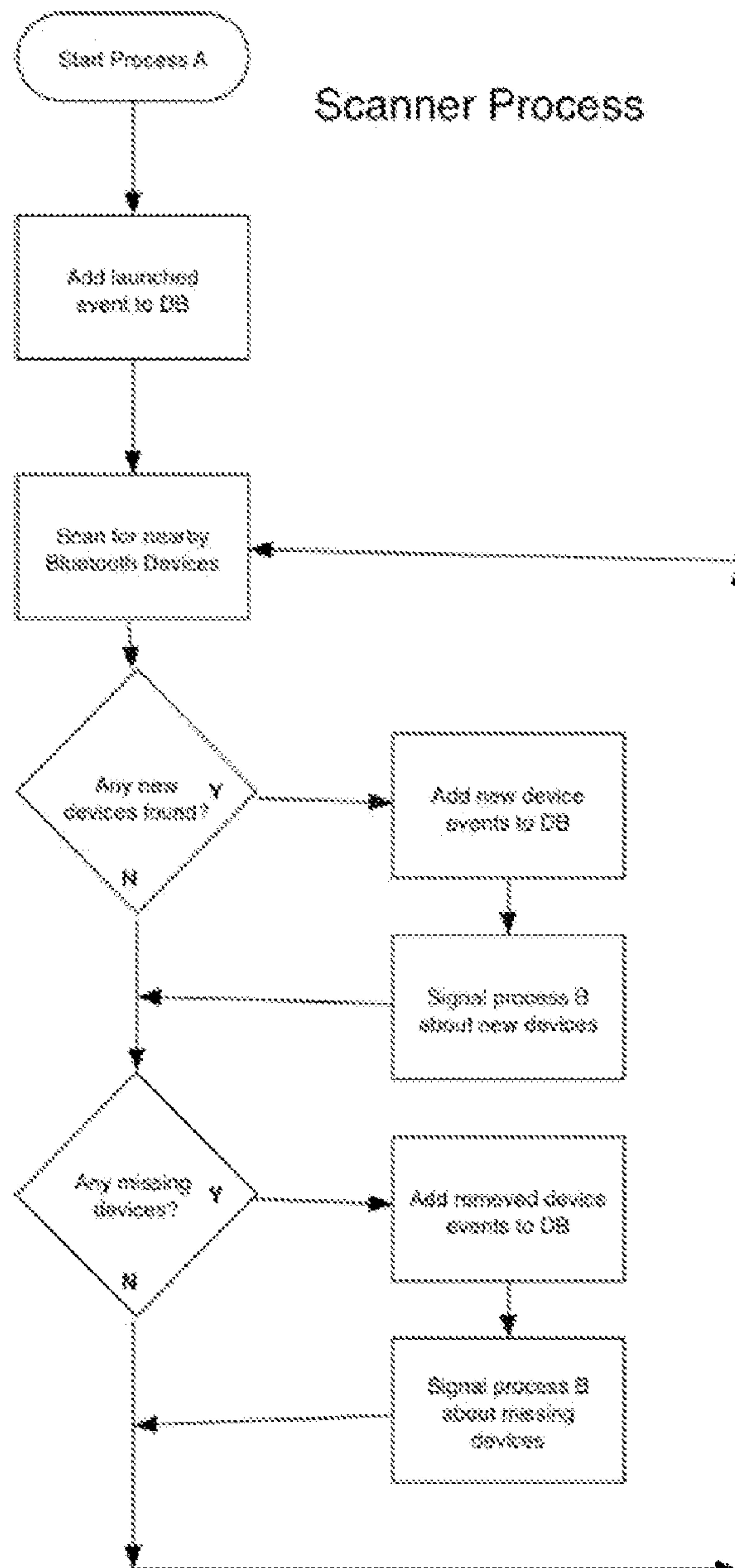


FIG. 6

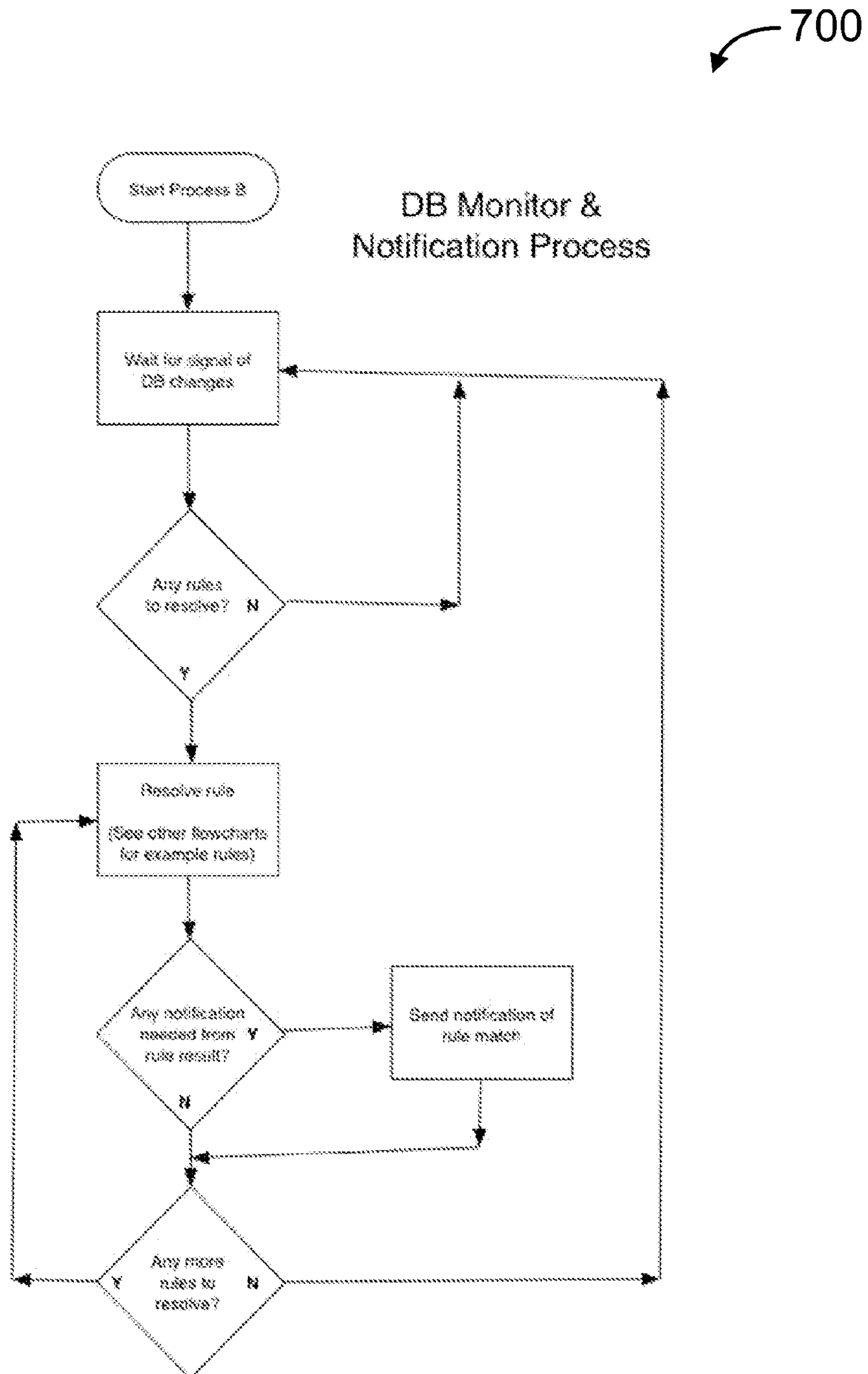


FIG. 7

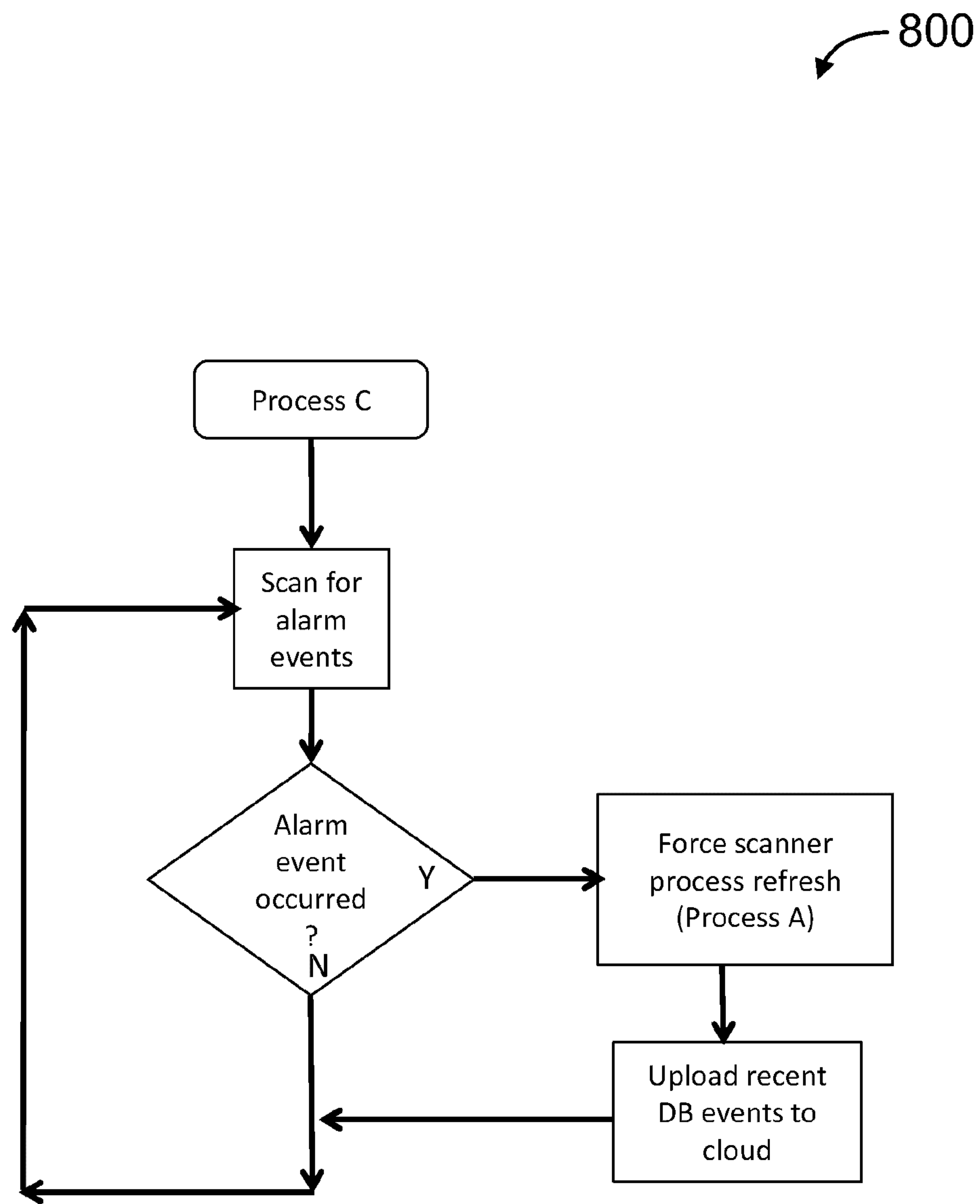


FIG. 8

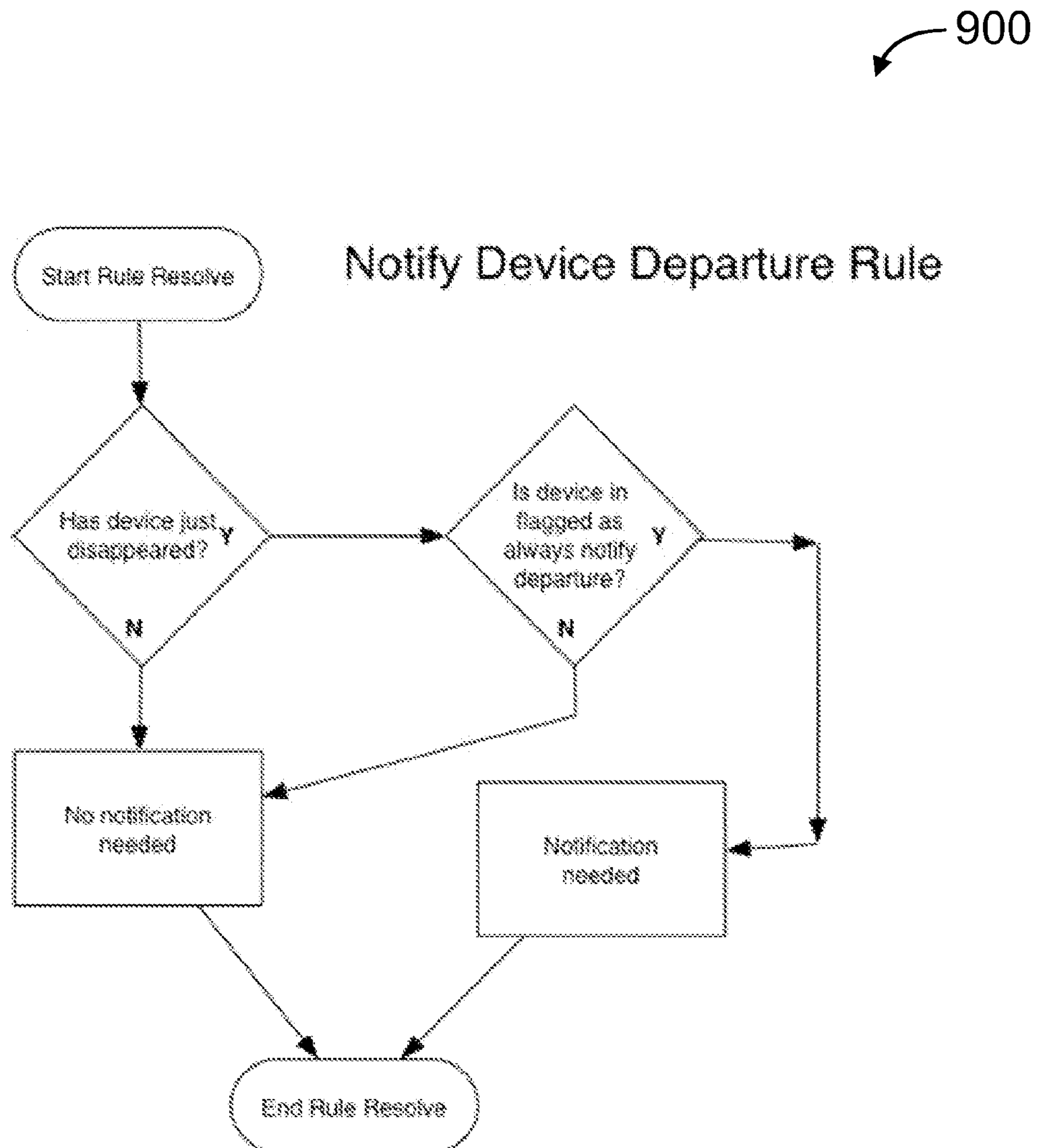


FIG. 9

1000

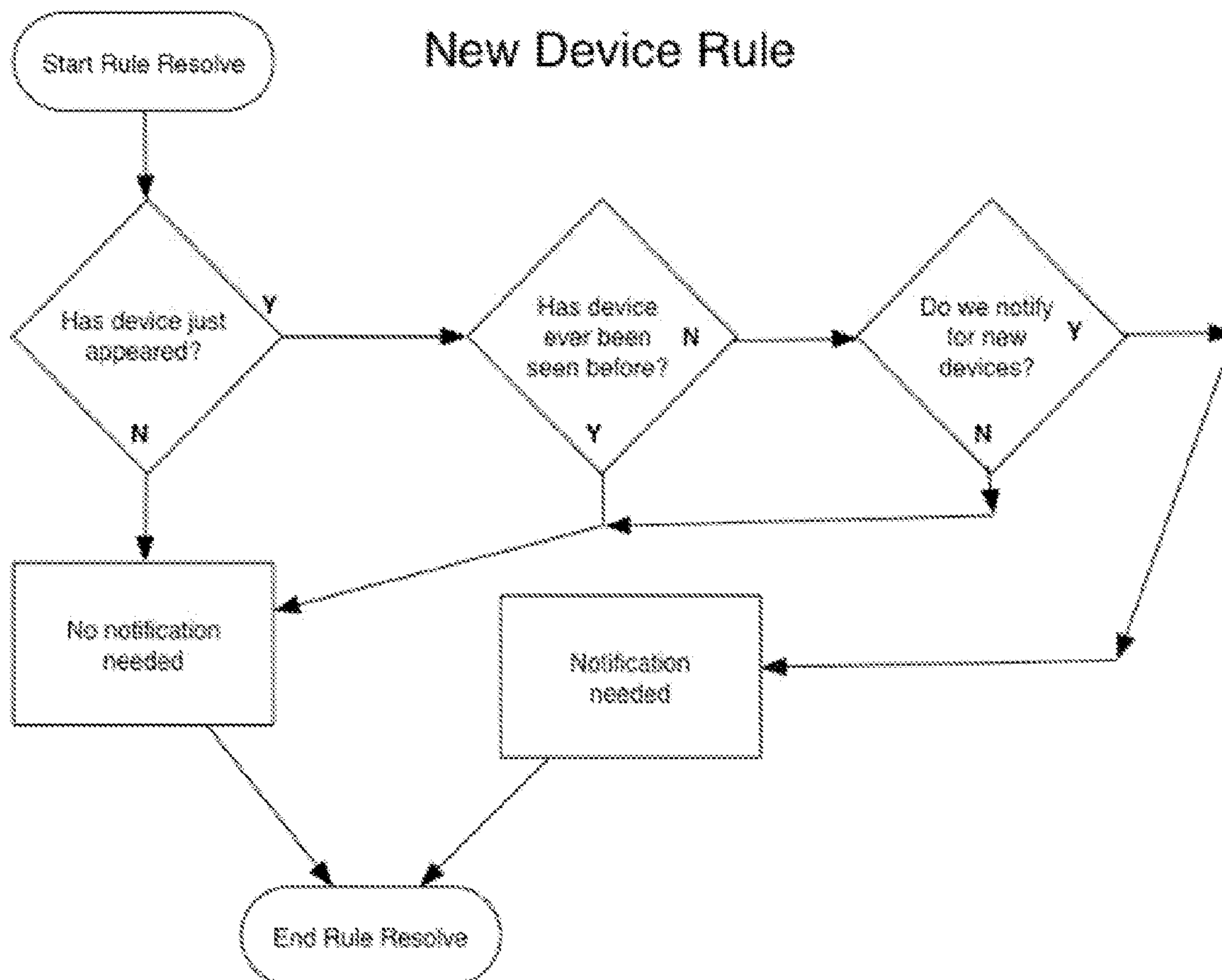


FIG. 10

1100

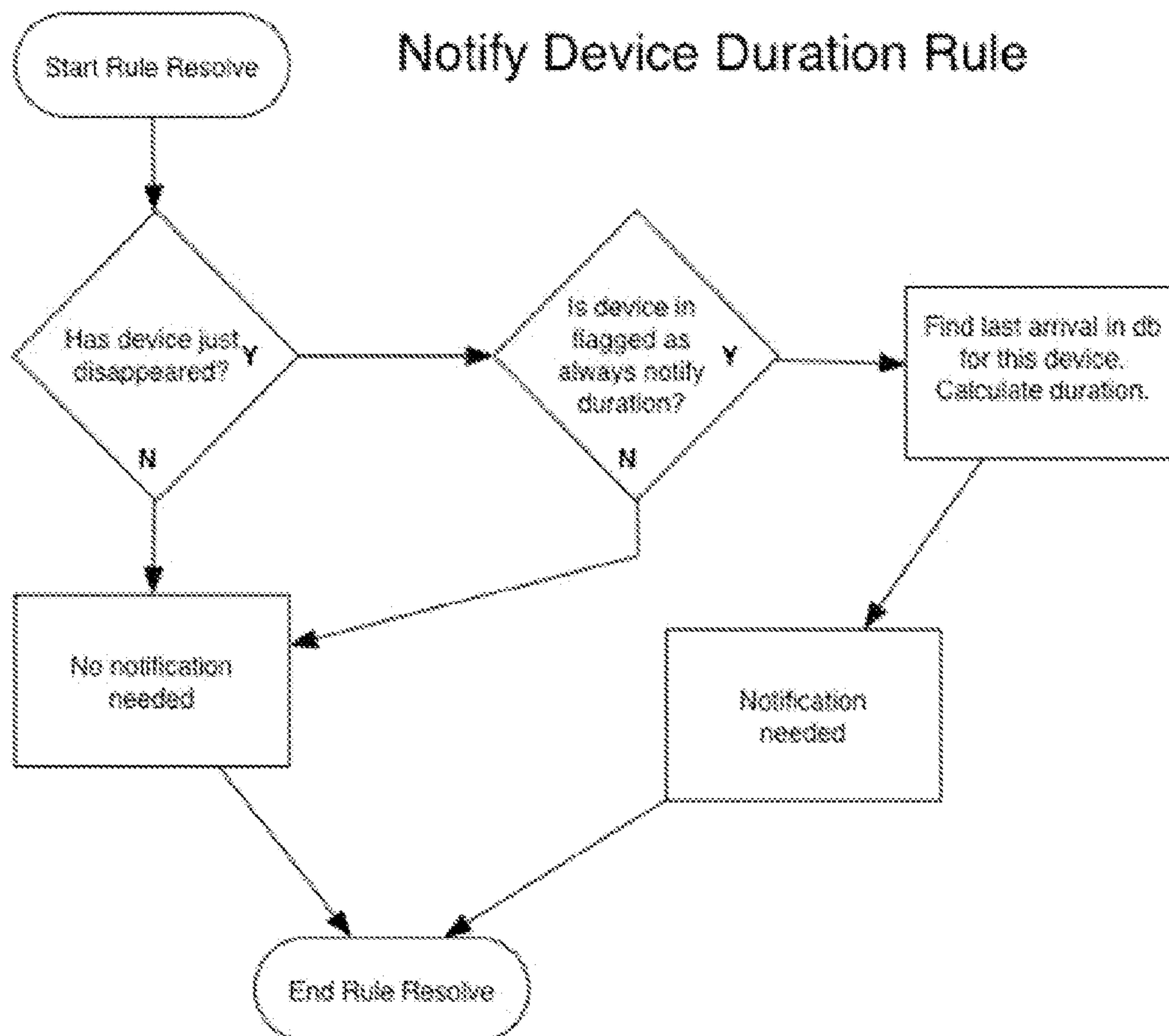


FIG. 11

1200

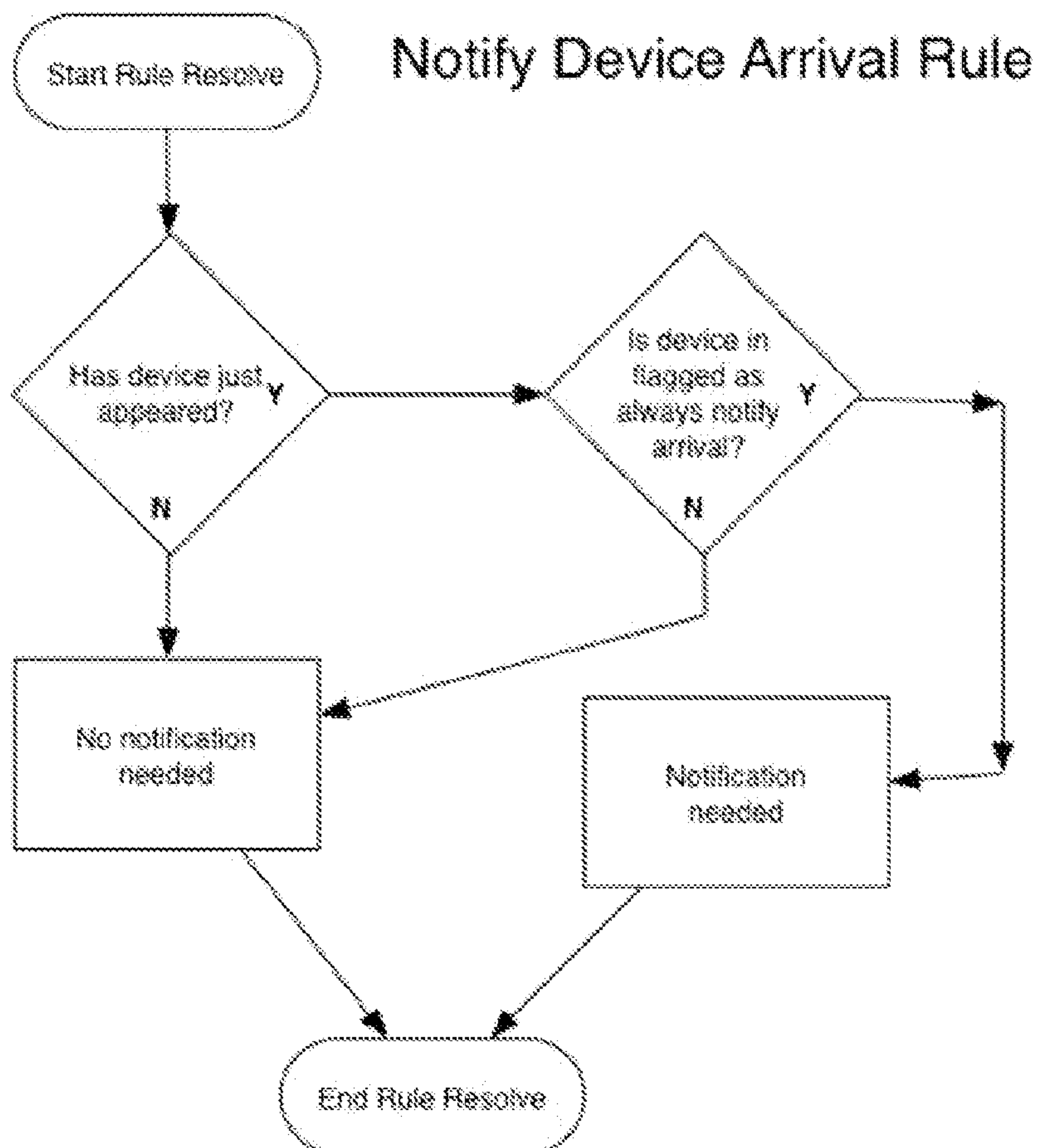


FIG. 12

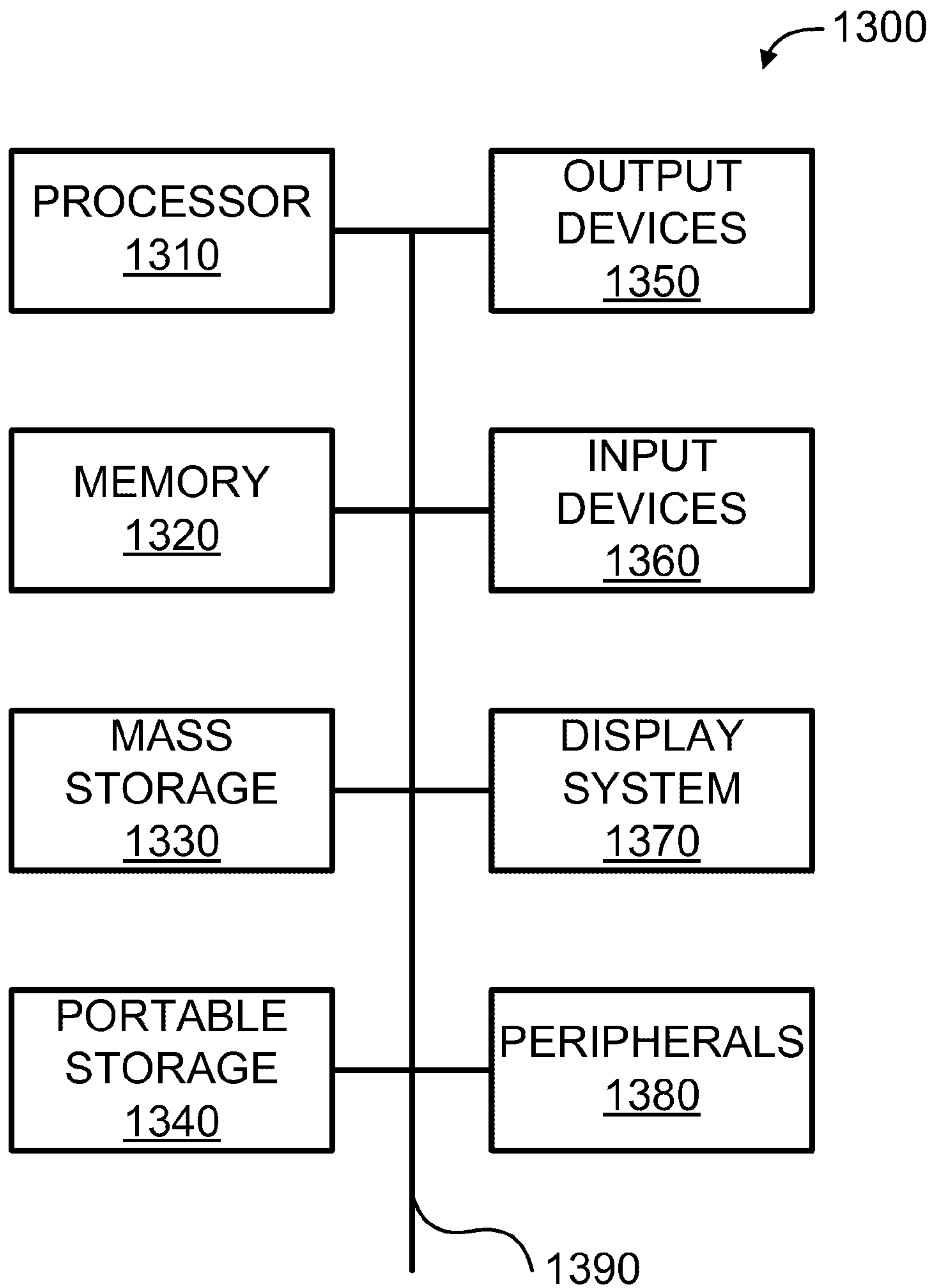


FIG. 13

