



(19) **United States**
(12) **Patent Application Publication**
Proud

(10) **Pub. No.: US 2014/0247148 A1**
(43) **Pub. Date: Sep. 4, 2014**

(54) **MONITORING DEVICE WITH WIRELESS COMMUNICATION USING CDMA**

(60) Provisional application No. 61/772,265, filed on Mar. 4, 2013, provisional application No. 61/823,502, filed on May 15, 2013.

(71) Applicant: **Hello Inc.**, San Francisco, CA (US)

Publication Classification

(72) Inventor: **James Proud**, San Francisco, CA (US)

(51) **Int. Cl.**
A61B 5/00 (2006.01)
G08C 17/02 (2006.01)

(73) Assignee: **Hello Inc.**, San Francisco, CA (US)

(52) **U.S. Cl.**
CPC *A61B 5/0024* (2013.01); *G08C 17/02* (2013.01); *A61B 5/0026* (2013.01)
USPC **340/870.02**

(21) Appl. No.: **13/967,094**

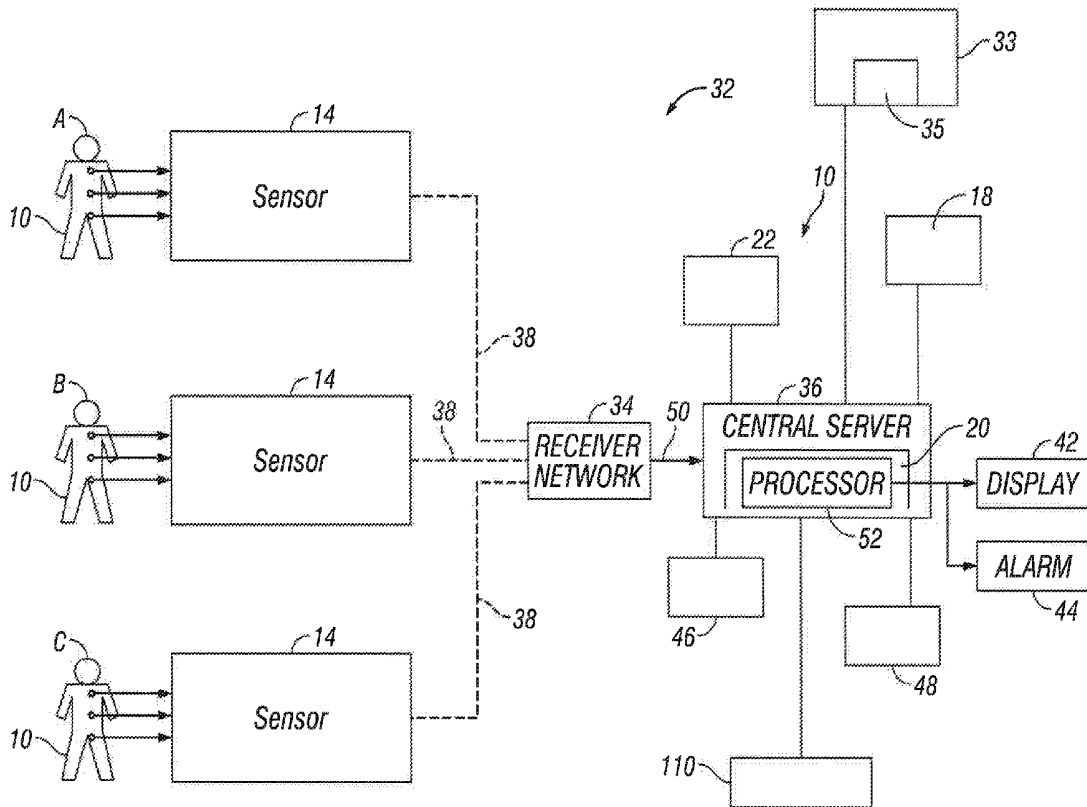
(22) Filed: **Aug. 14, 2013**

(57) **ABSTRACT**

Related U.S. Application Data

One or more sensors are coupled to a monitoring device that has a unique user ID, the one or more sensors acquiring user information selected from one of at least one of, a user's activities, behaviors and habit information. ID circuitry is at the monitoring device. Also included is ID storage, a communication system that reads and transmits the unique ID from an ID storage, a power source and a pathway system to route signals through the circuitry. A telemetry system includes a database of user ID's. The telemetry system is in communication with the monitoring device and analyzes data from monitoring device based on at least one of, user's activities, behaviors and habit information and creating personalized information about the user, and a controller transmits a set of data frames relative to the monitoring device. A set of data frames is transmitted from the monitoring device.

(63) Continuation-in-part of application No. 13/923,909, filed on Jun. 21, 2013, Continuation-in-part of application No. 13/923,637, filed on Jun. 21, 2013, Continuation-in-part of application No. 13/923,614, filed on Jun. 21, 2013, Continuation-in-part of application No. 13/923,809, filed on Jun. 21, 2013, Continuation-in-part of application No. 13/923,750, filed on Jun. 21, 2013, Continuation-in-part of application No. 13/923,583, filed on Jun. 21, 2013, Continuation-in-part of application No. 13/923,560, filed on Jun. 21, 2013, Continuation-in-part of application No. 13/923,543, filed on Jun. 21, 2013, Continuation-in-part of application No. 13/923,937, filed on Jun. 21, 2013.



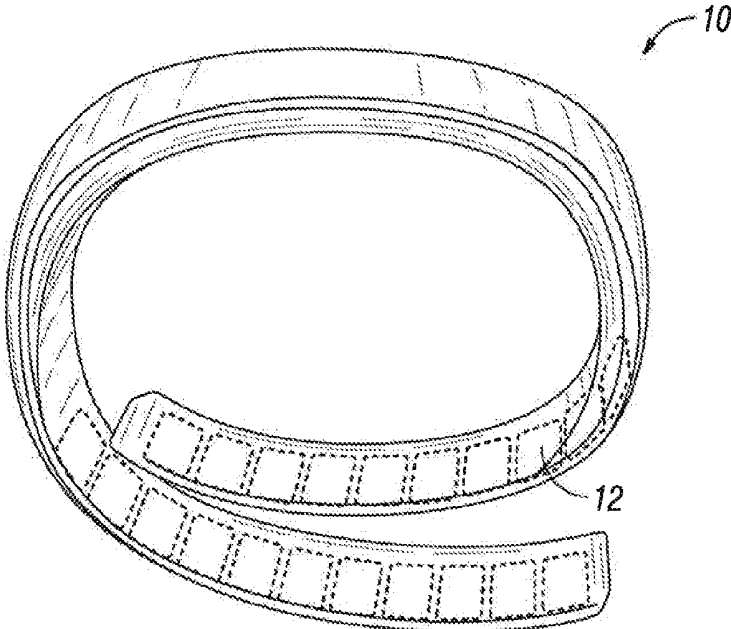


FIG. 1A

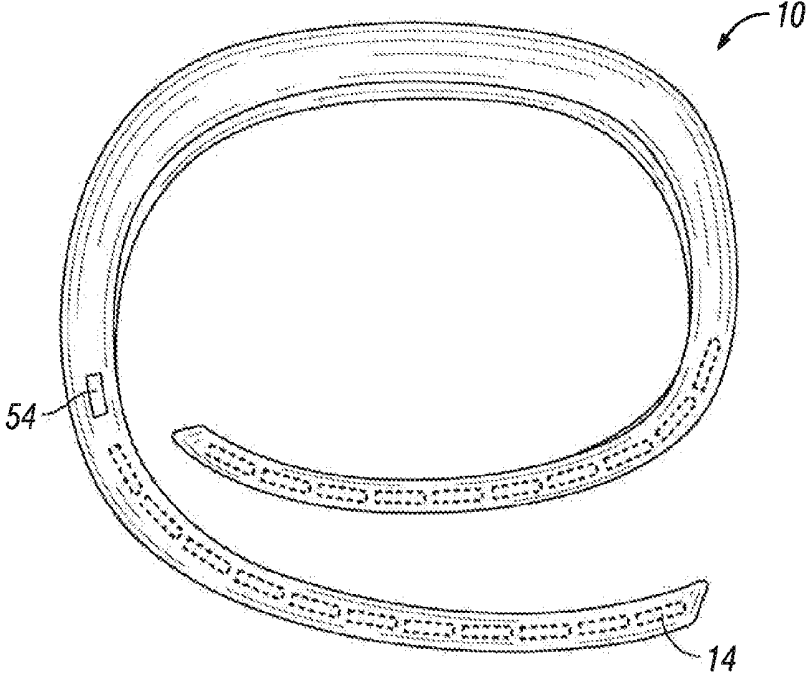


FIG. 1B

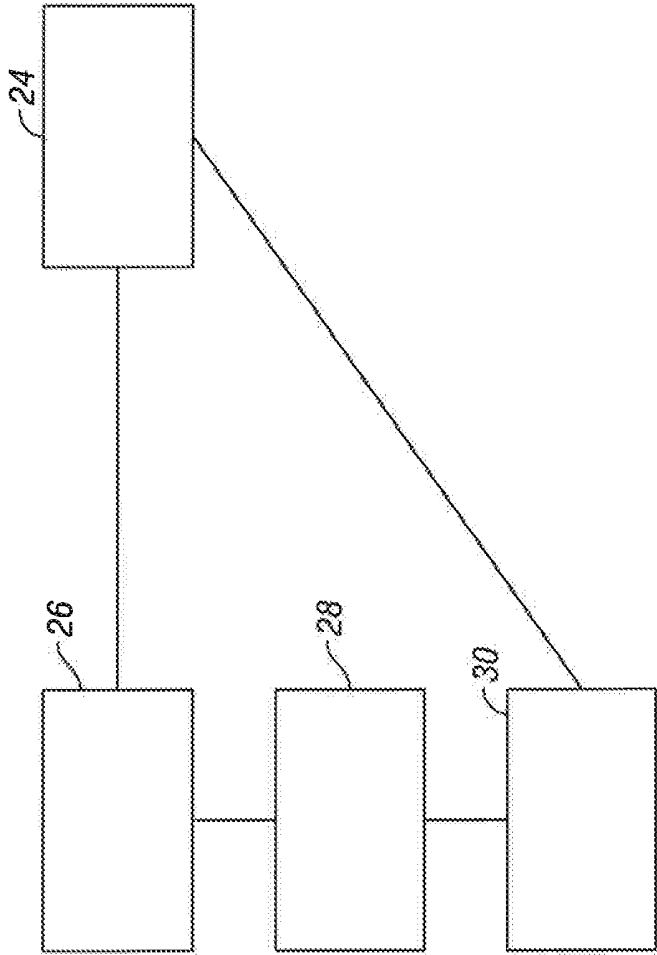


FIG. 2

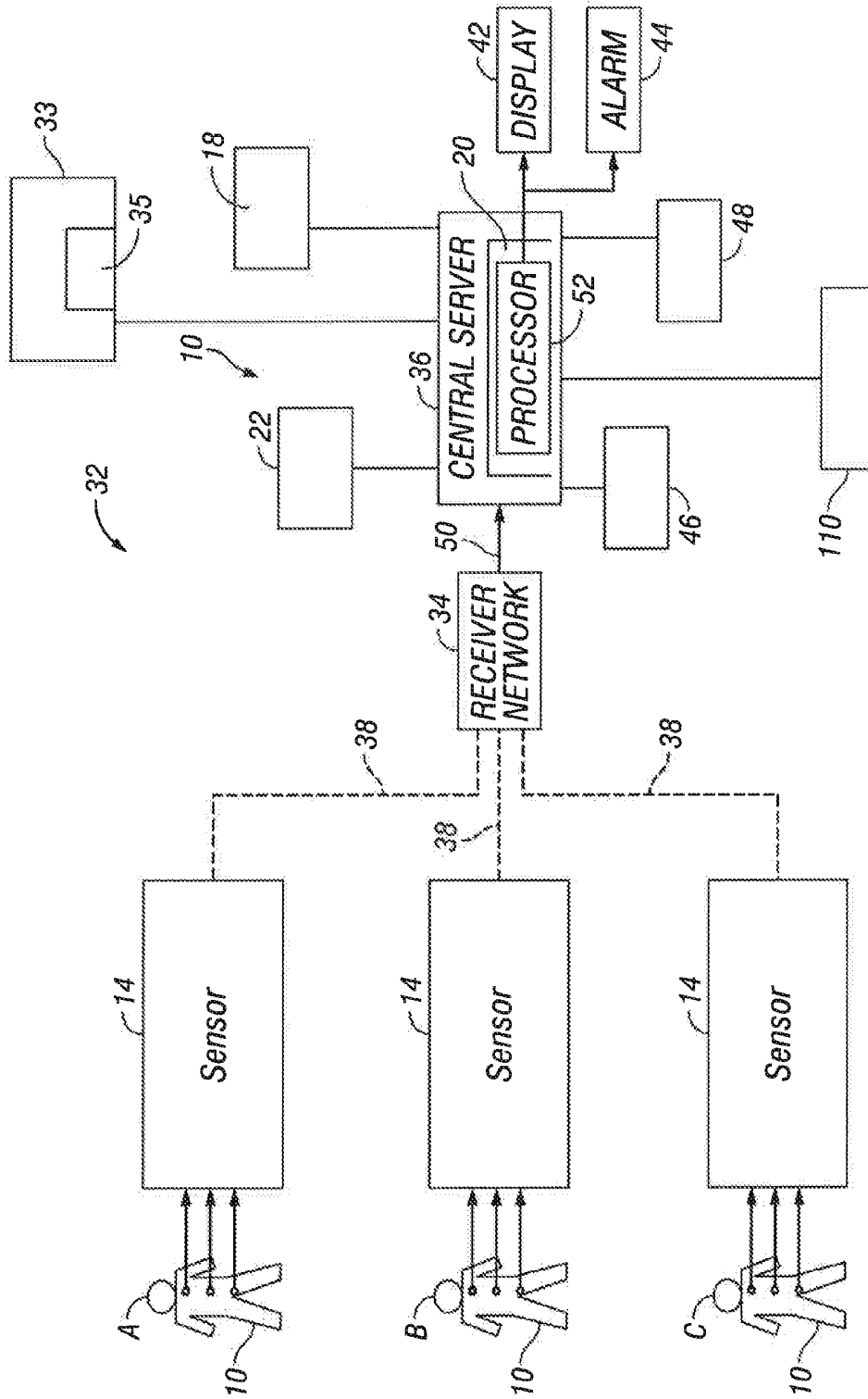


FIG. 3

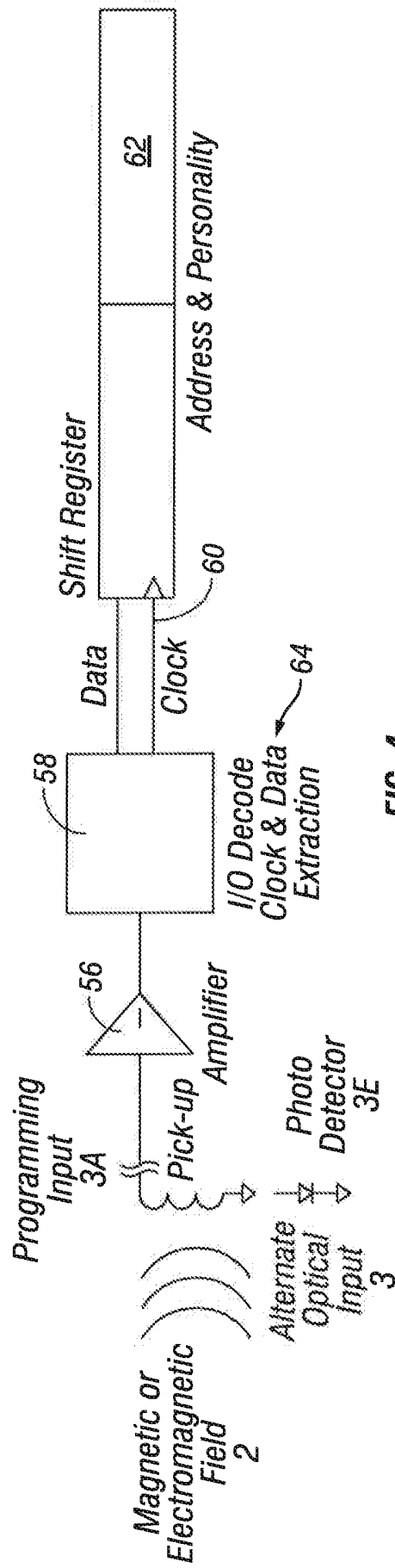


FIG. 4

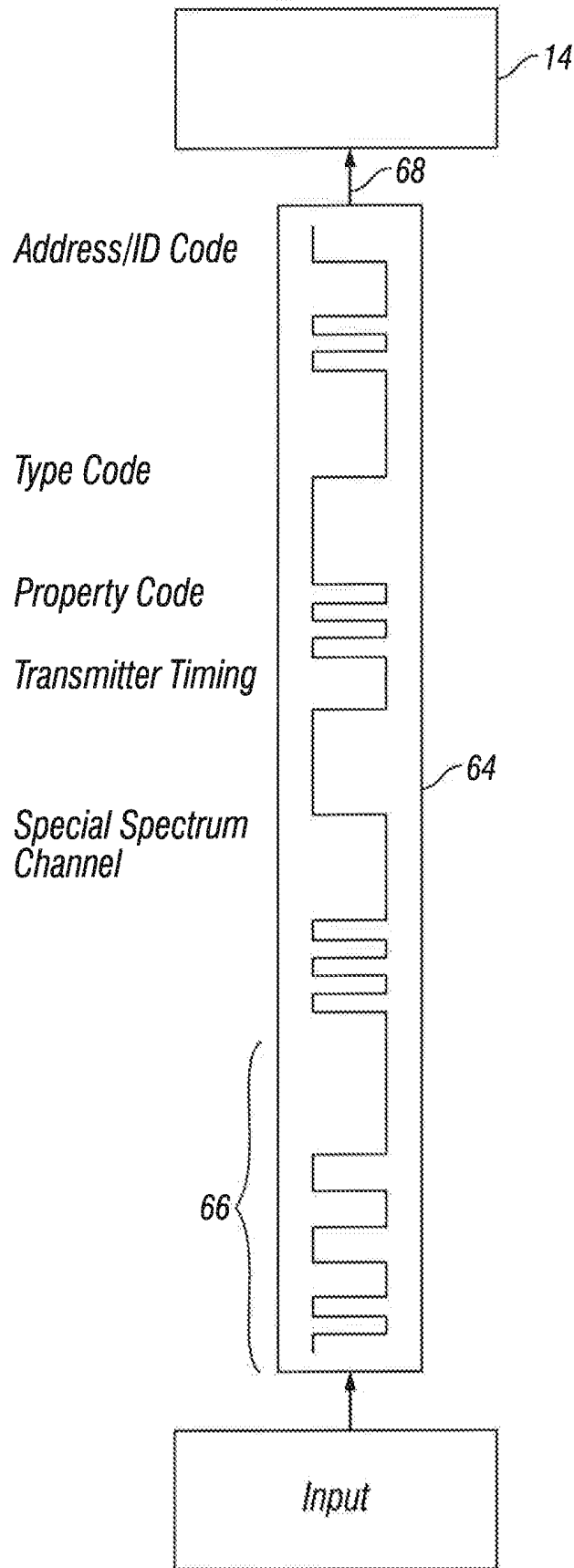


FIG. 6

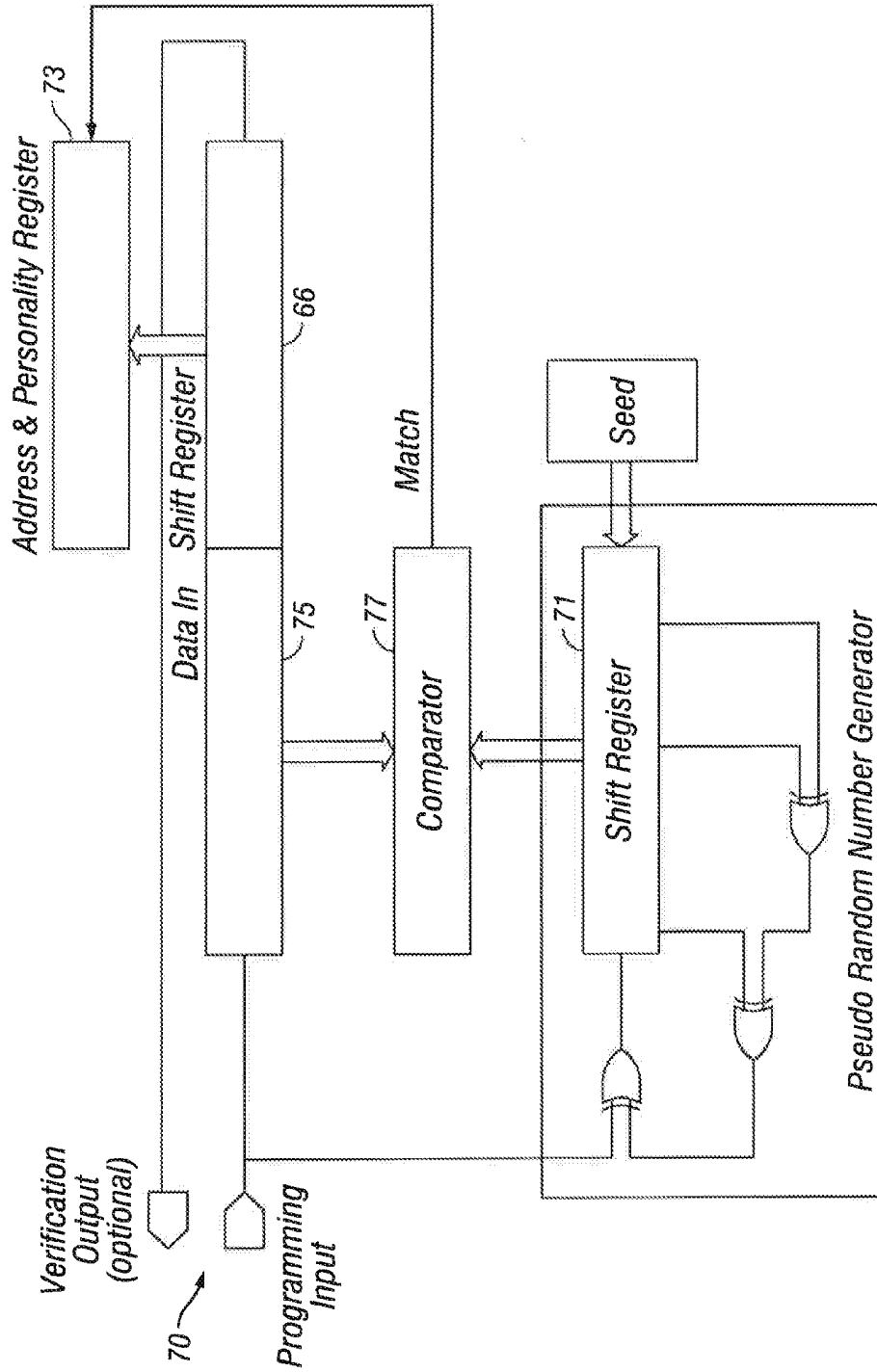


FIG. 7

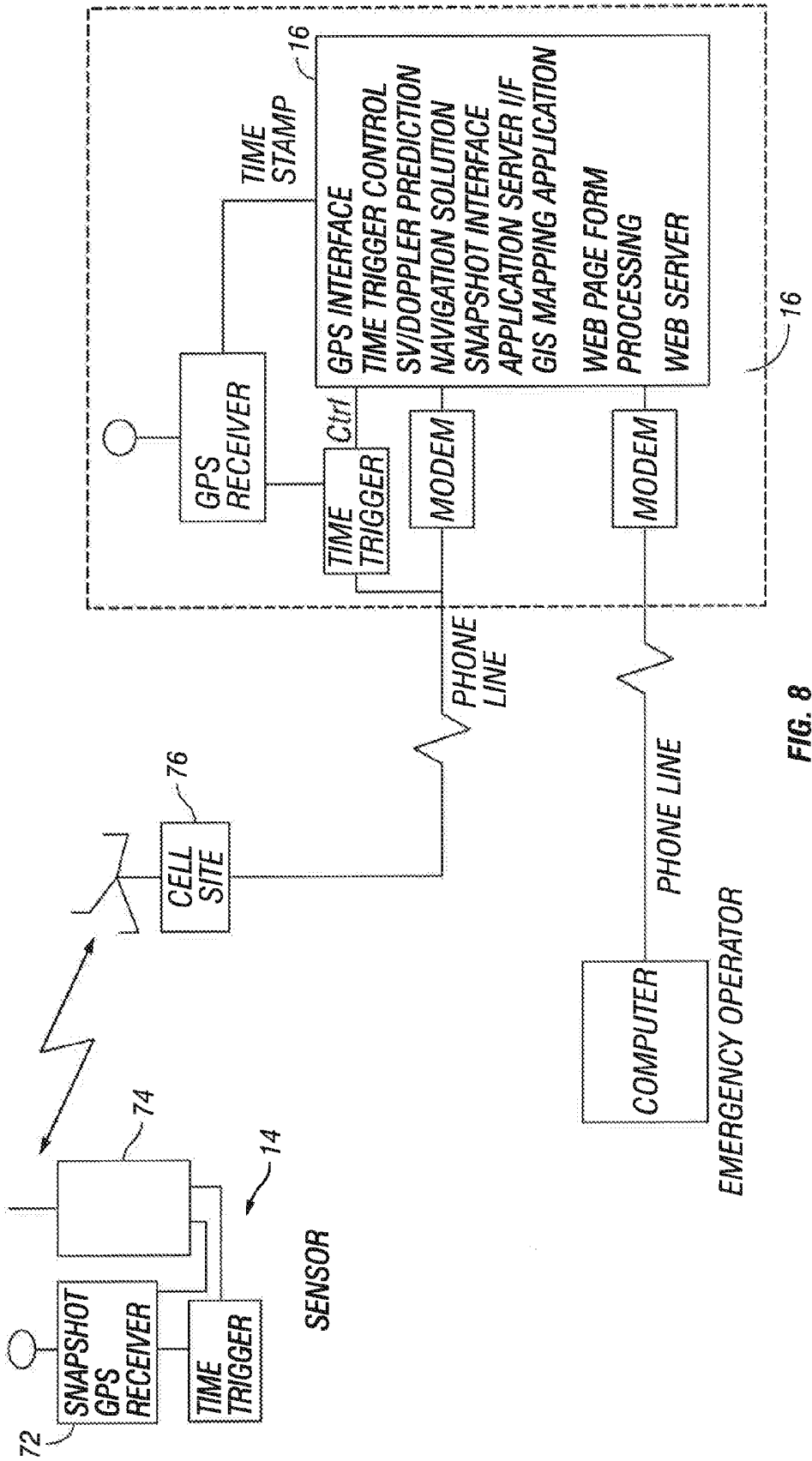


FIG. 8

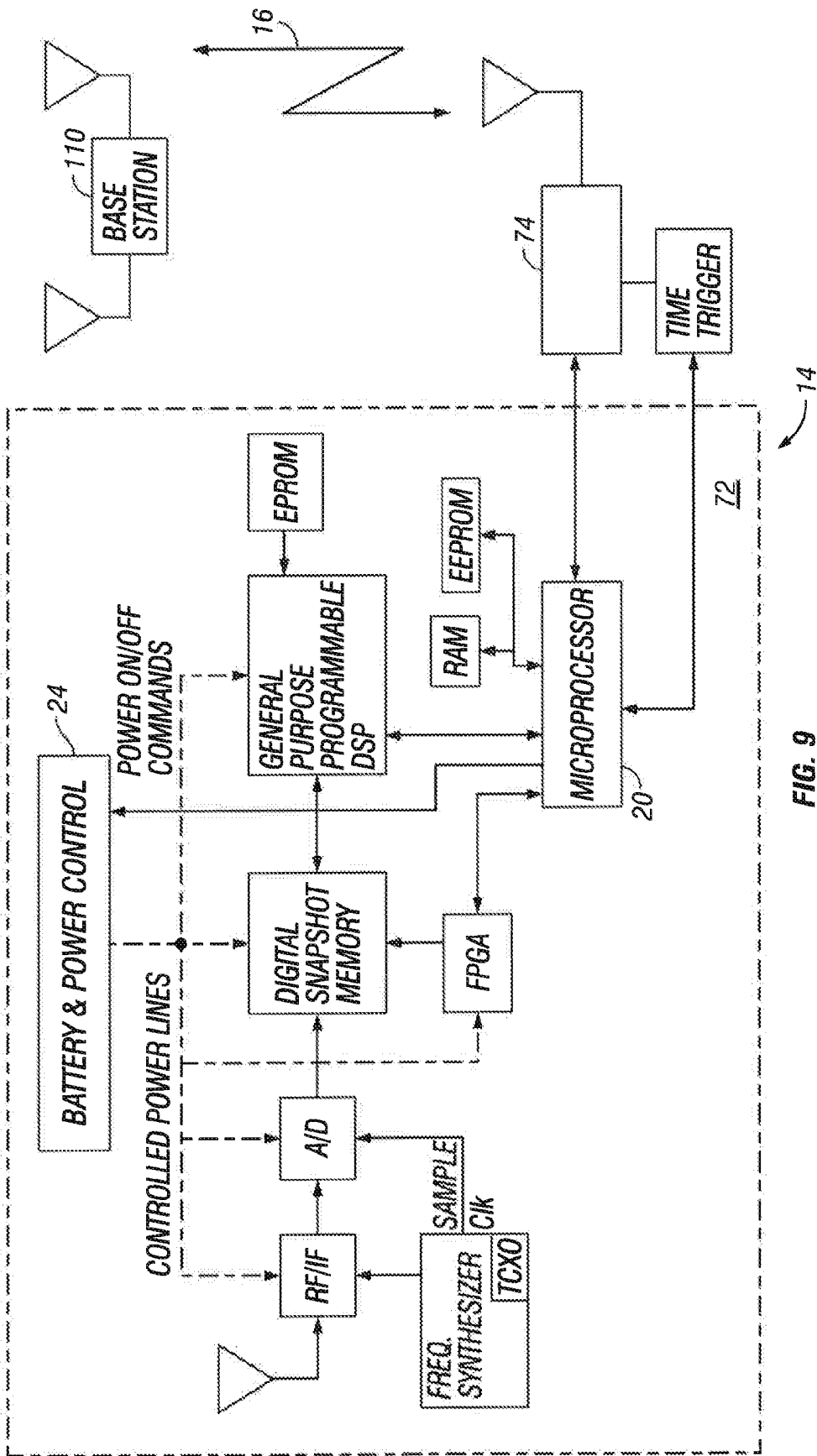
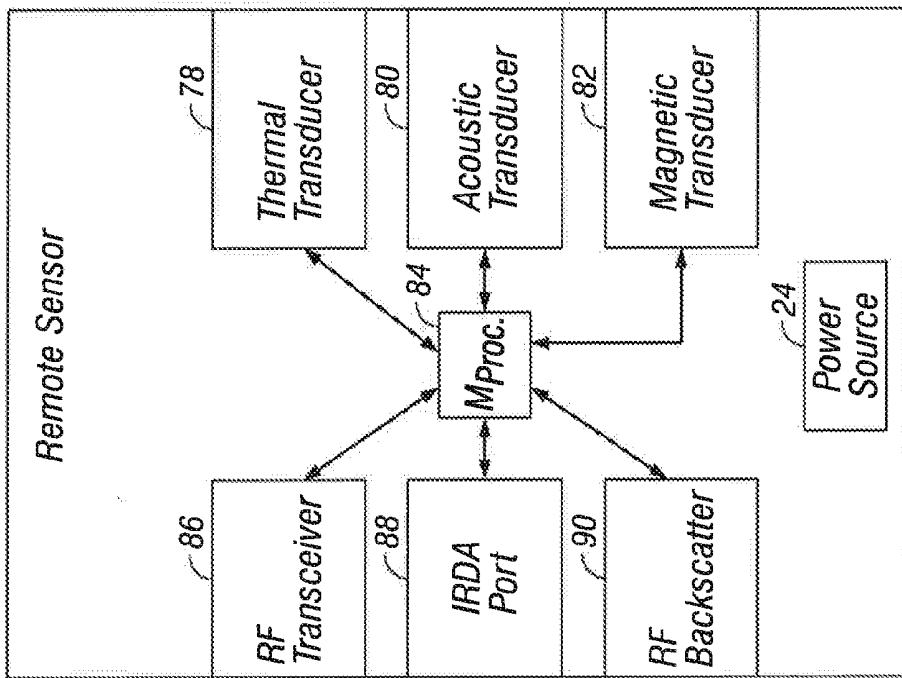


FIG. 9



14

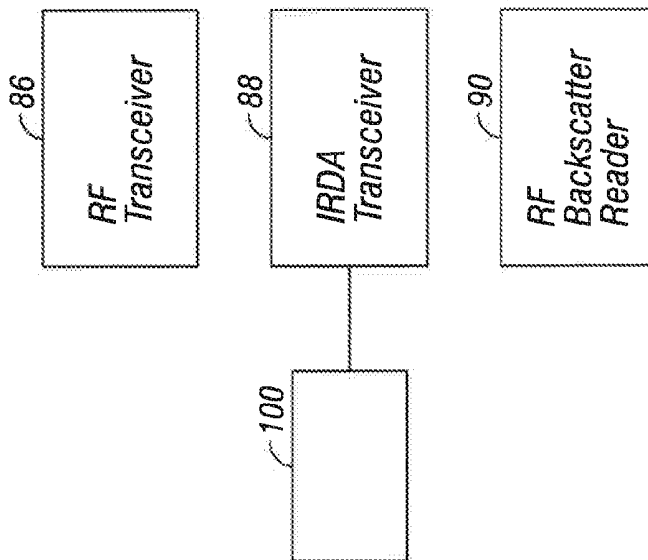


FIG. 10

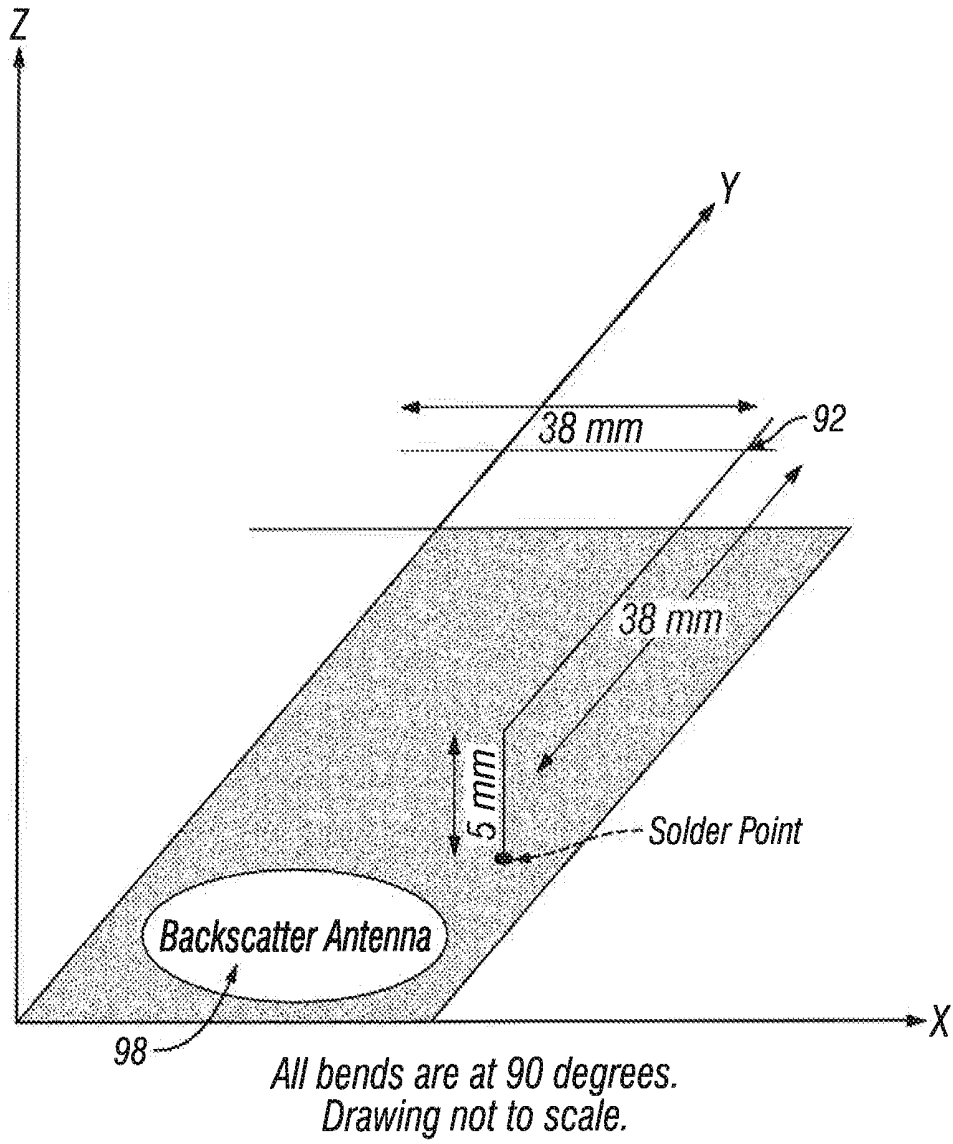


FIG. 11

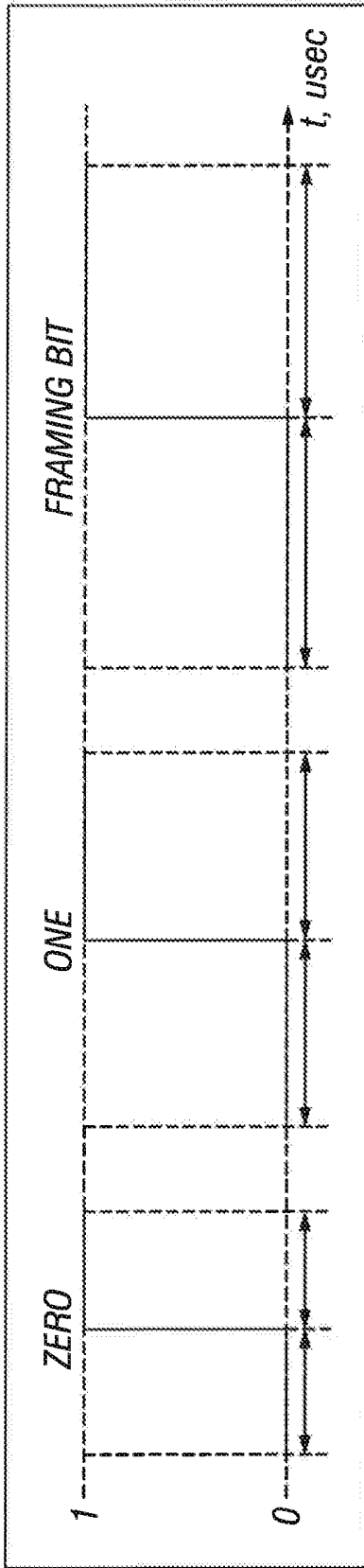


FIG. 12

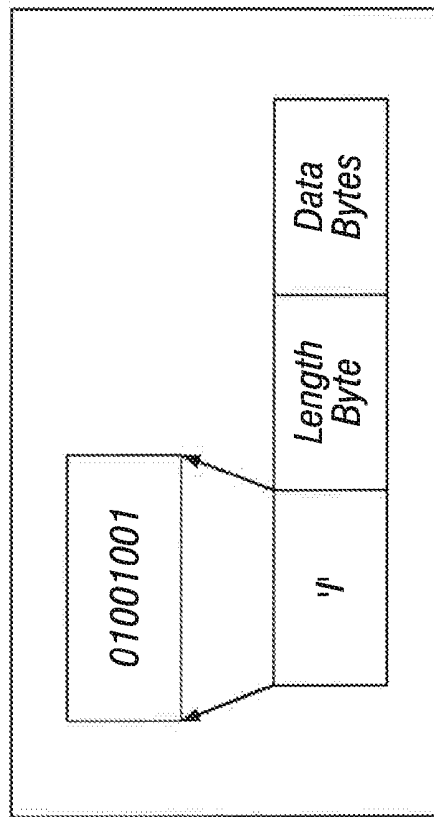


FIG. 13

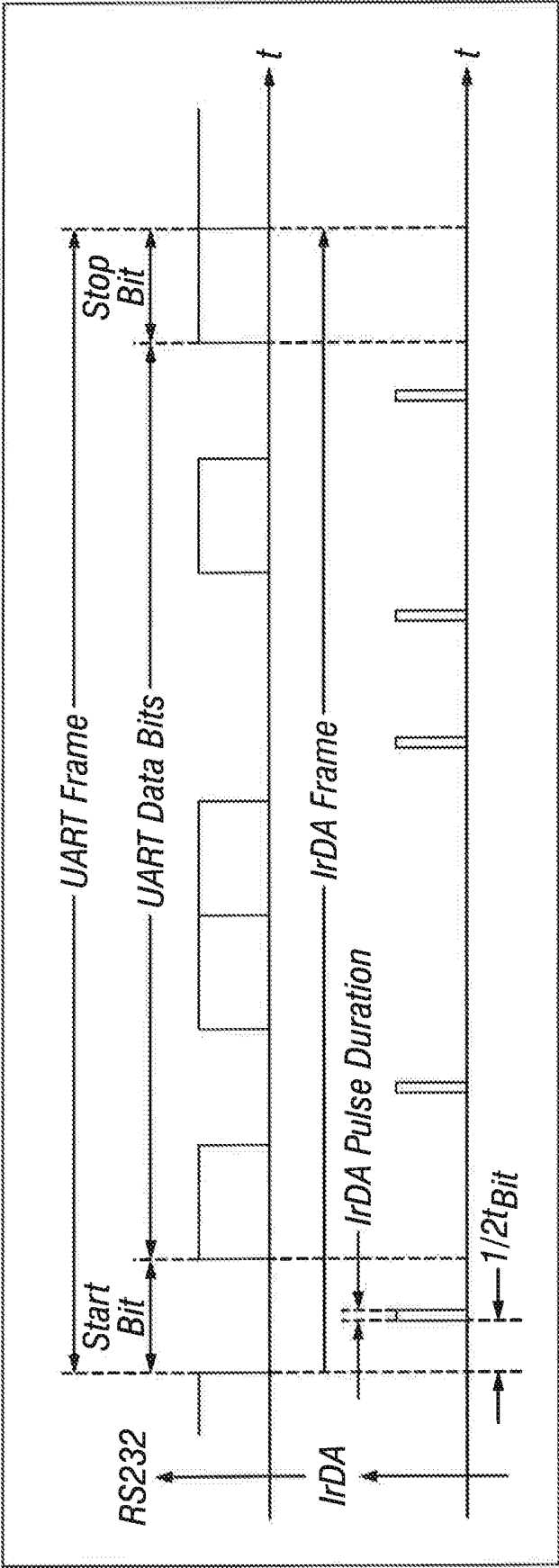


FIG. 14

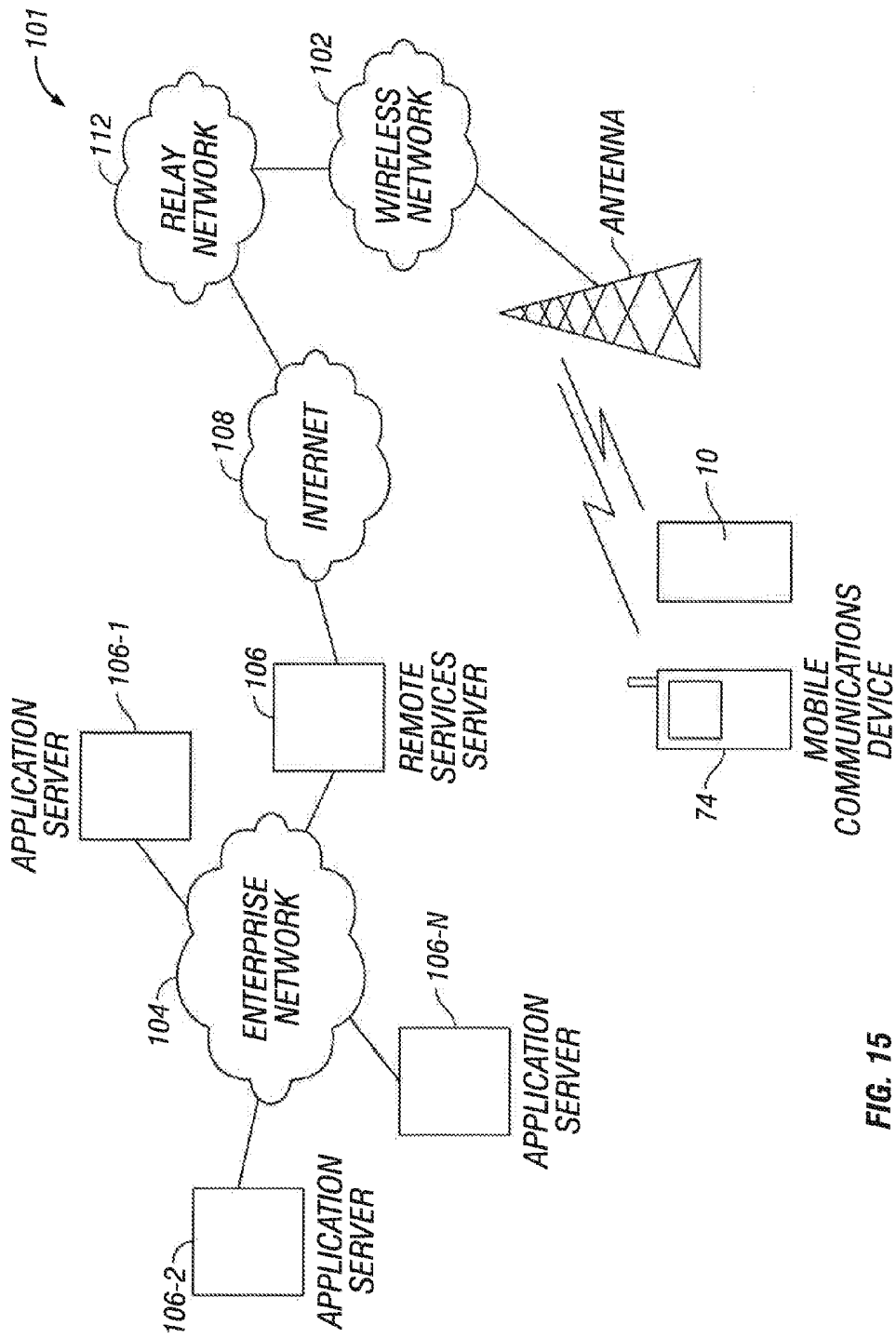


FIG. 15

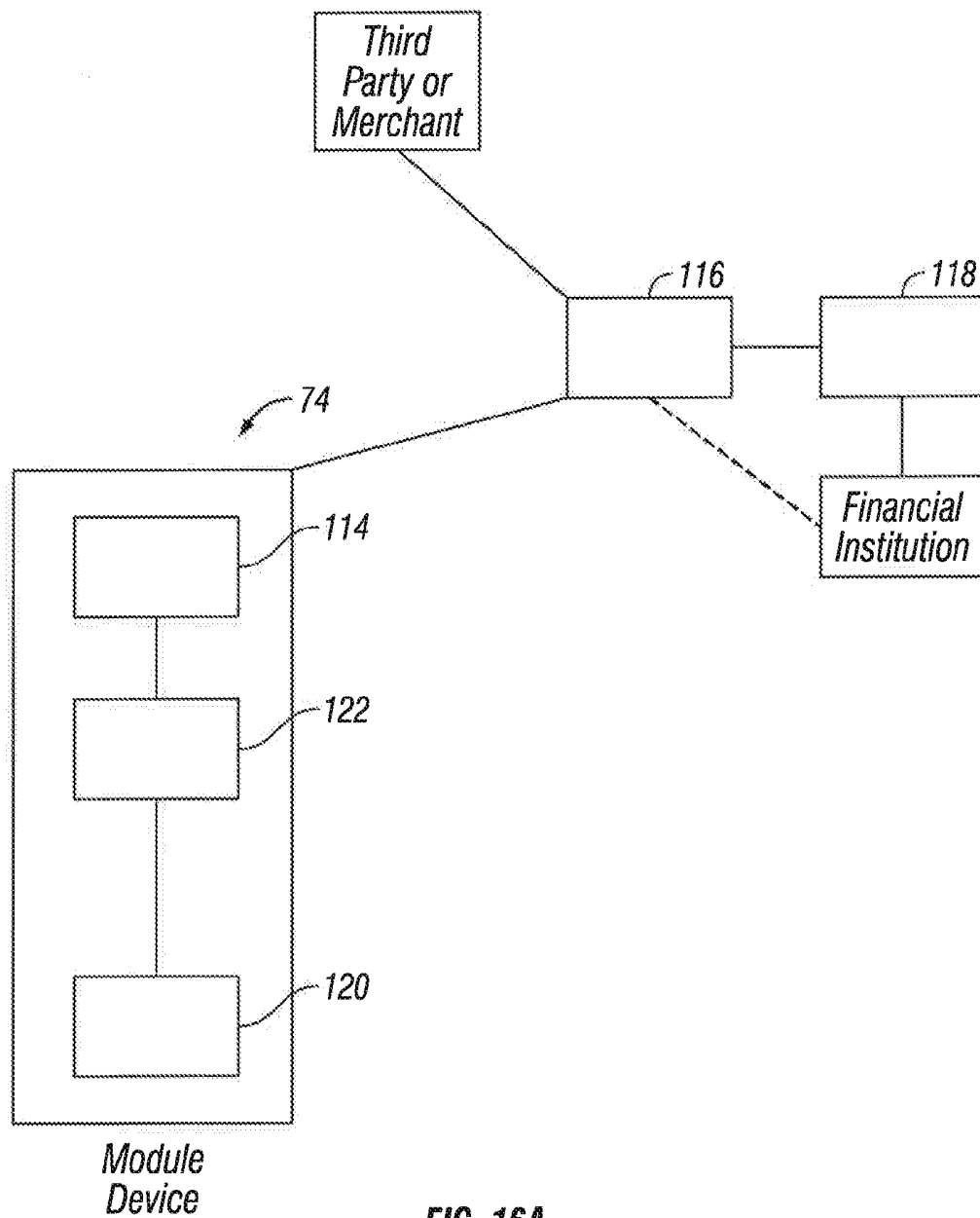


FIG. 16A

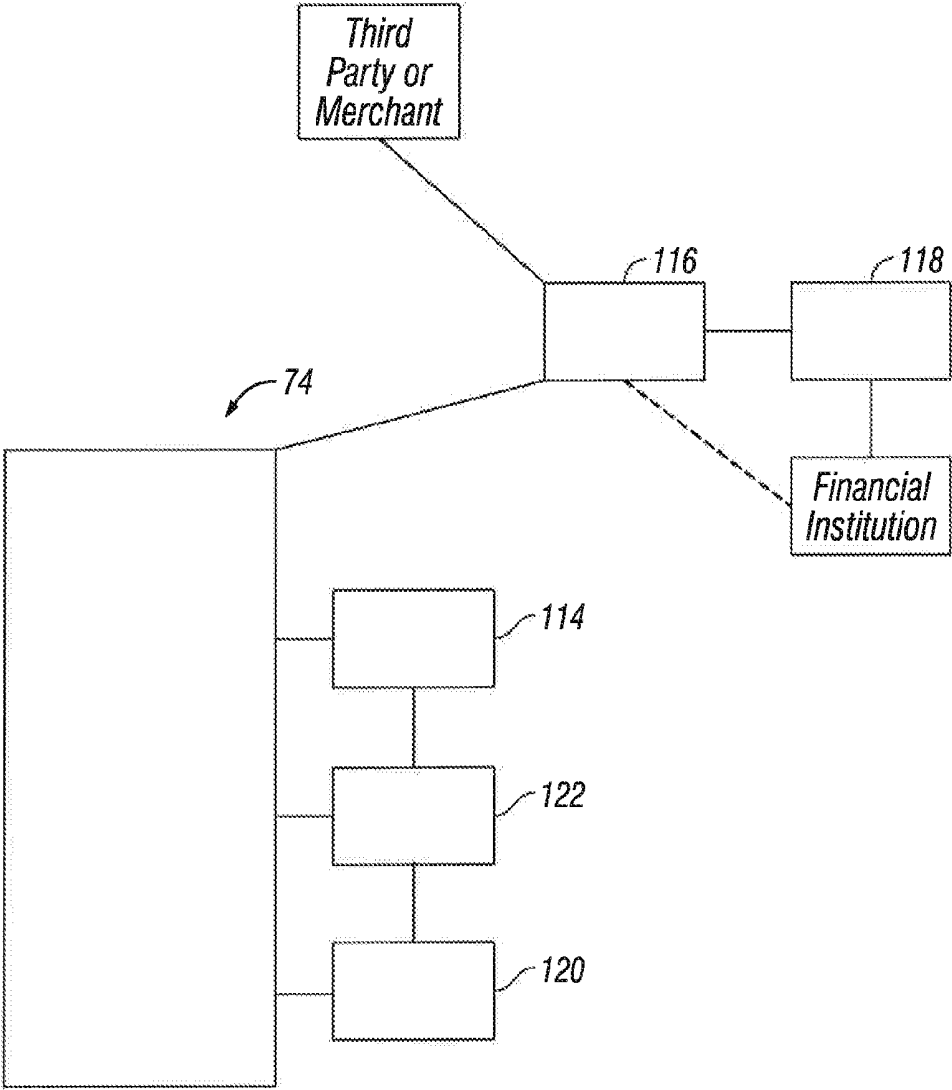


FIG. 16B

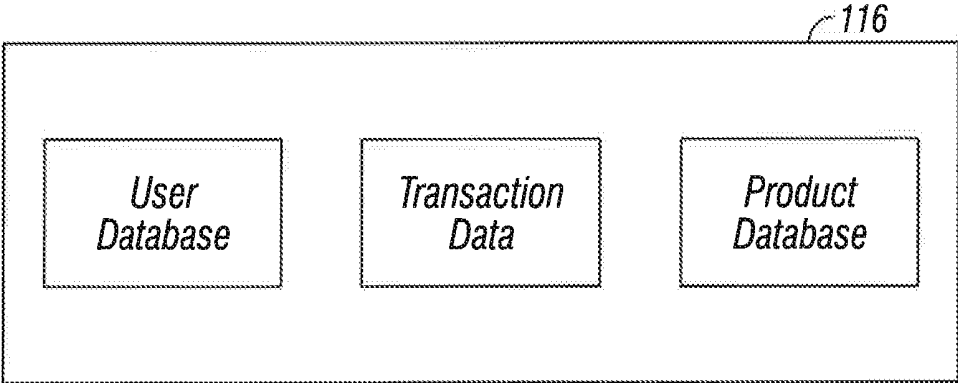


FIG. 16C

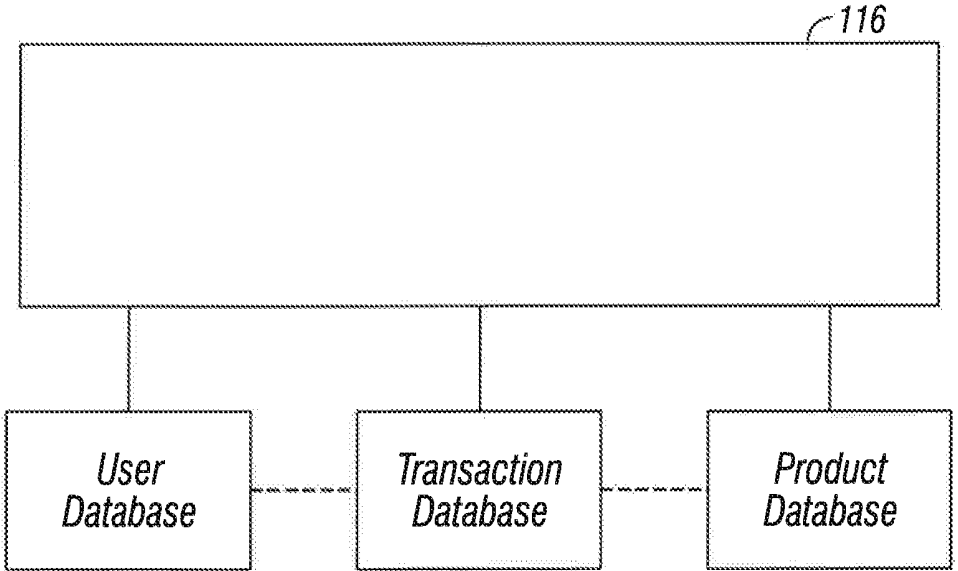


FIG. 16D

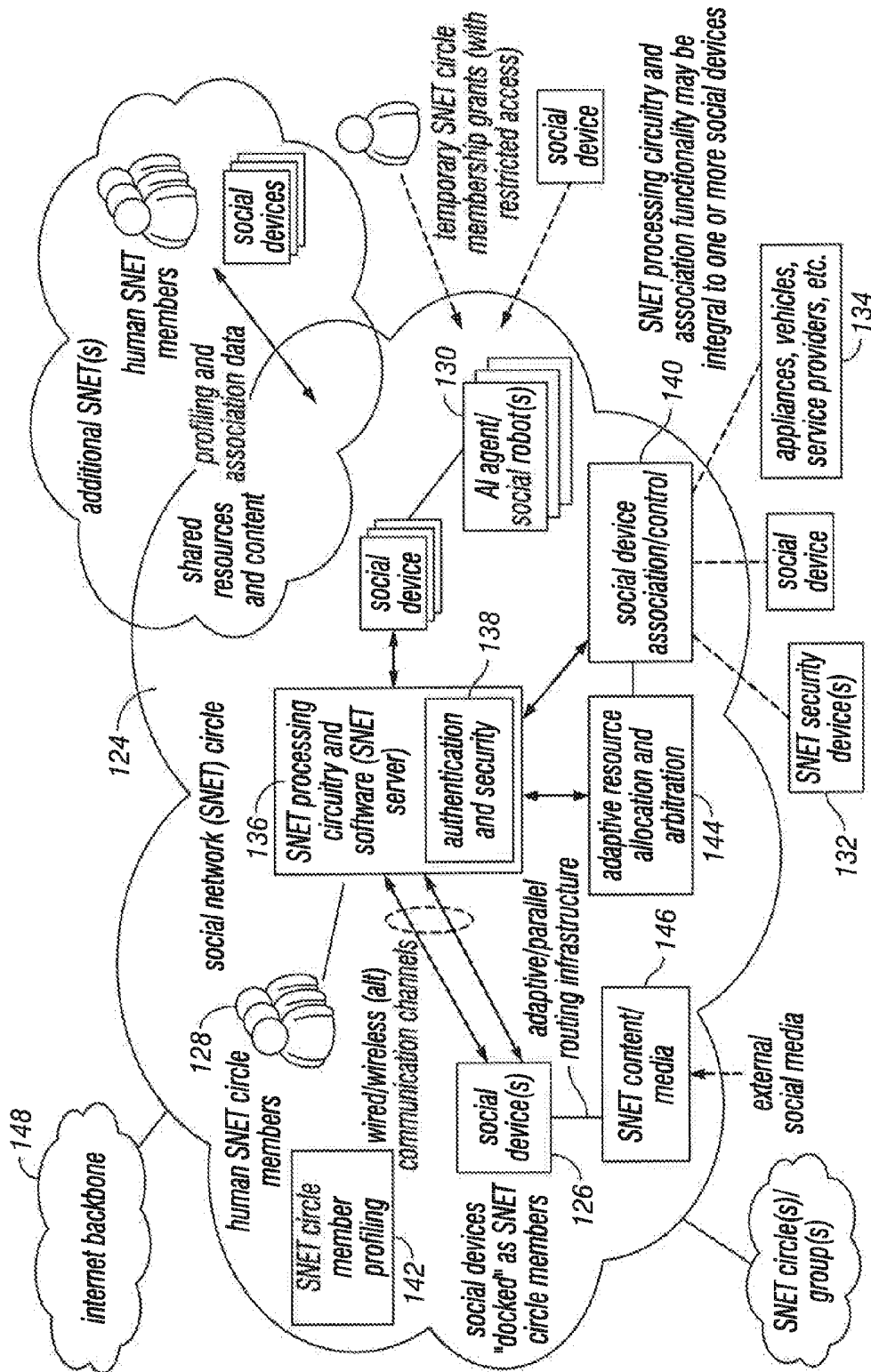


FIG. 17

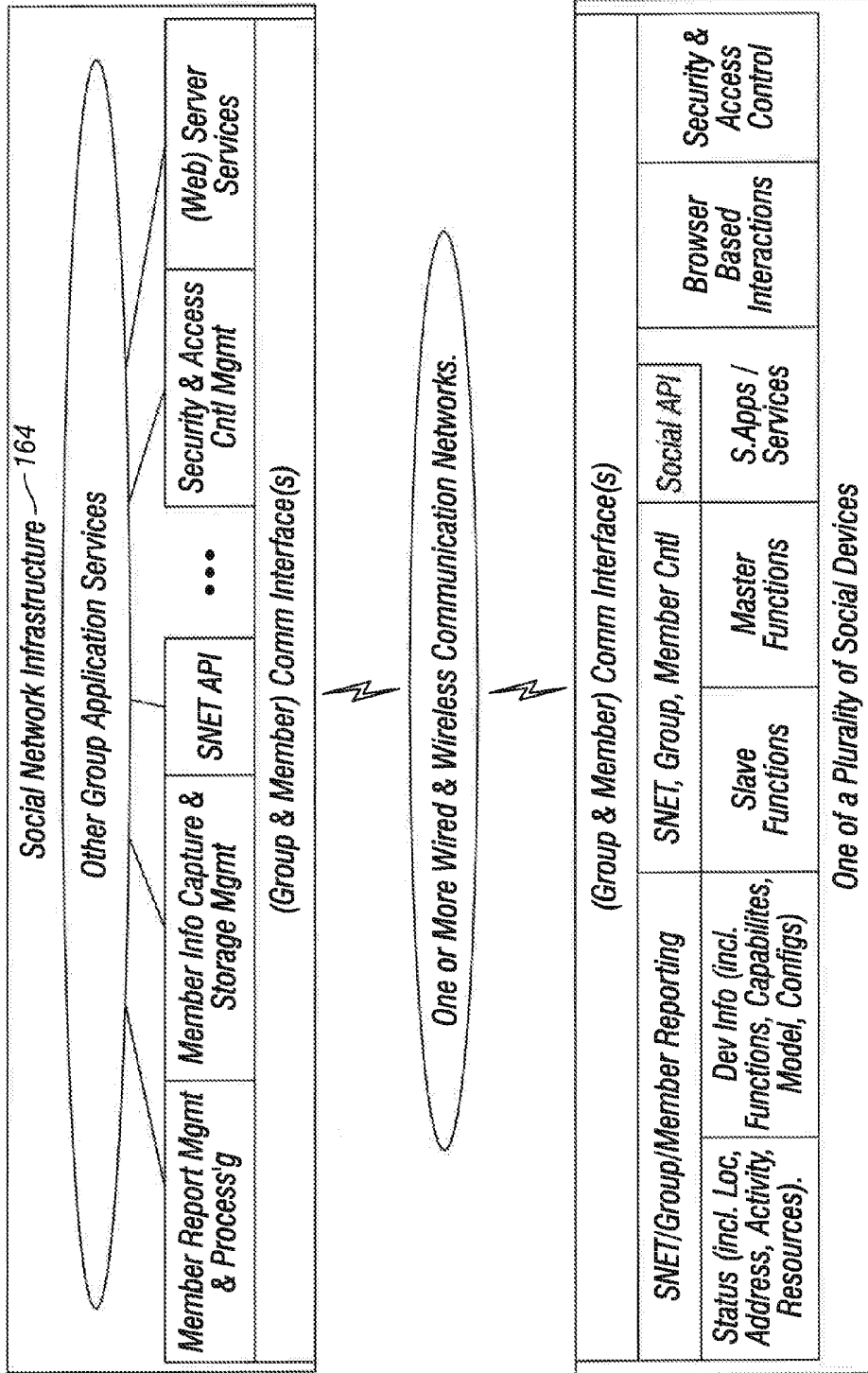


FIG. 19

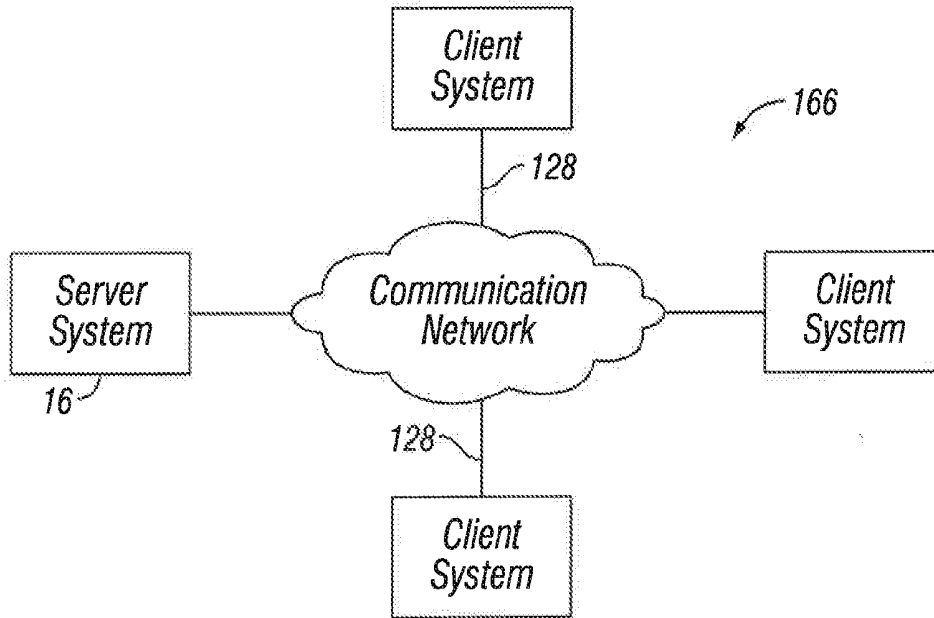


FIG. 20

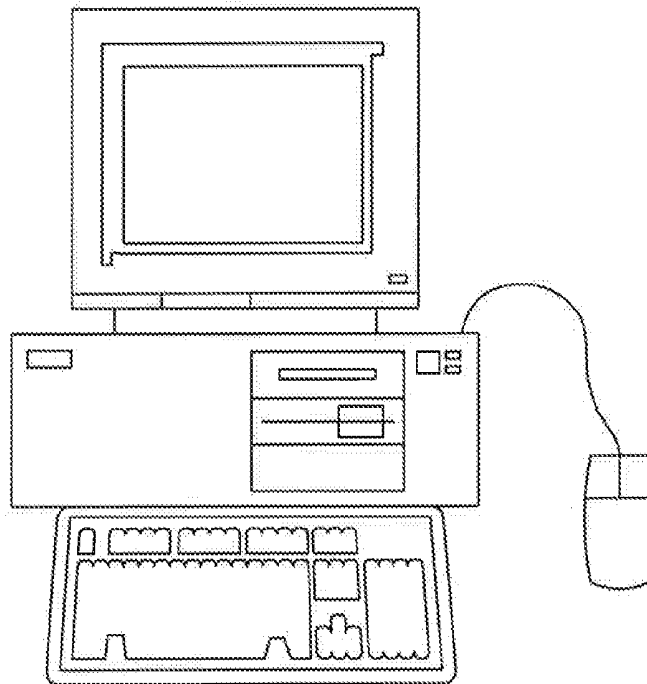


FIG. 21

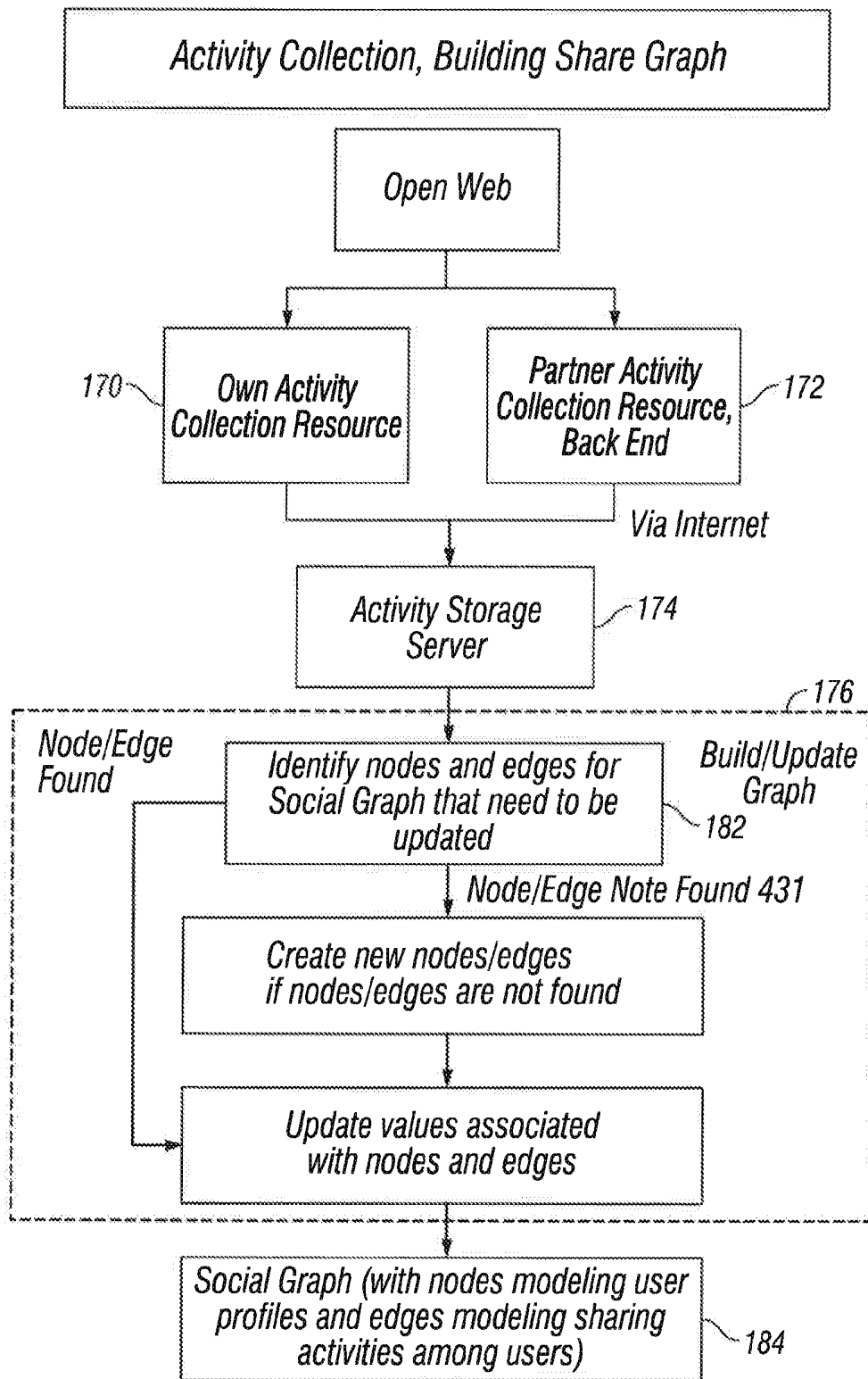


FIG. 22

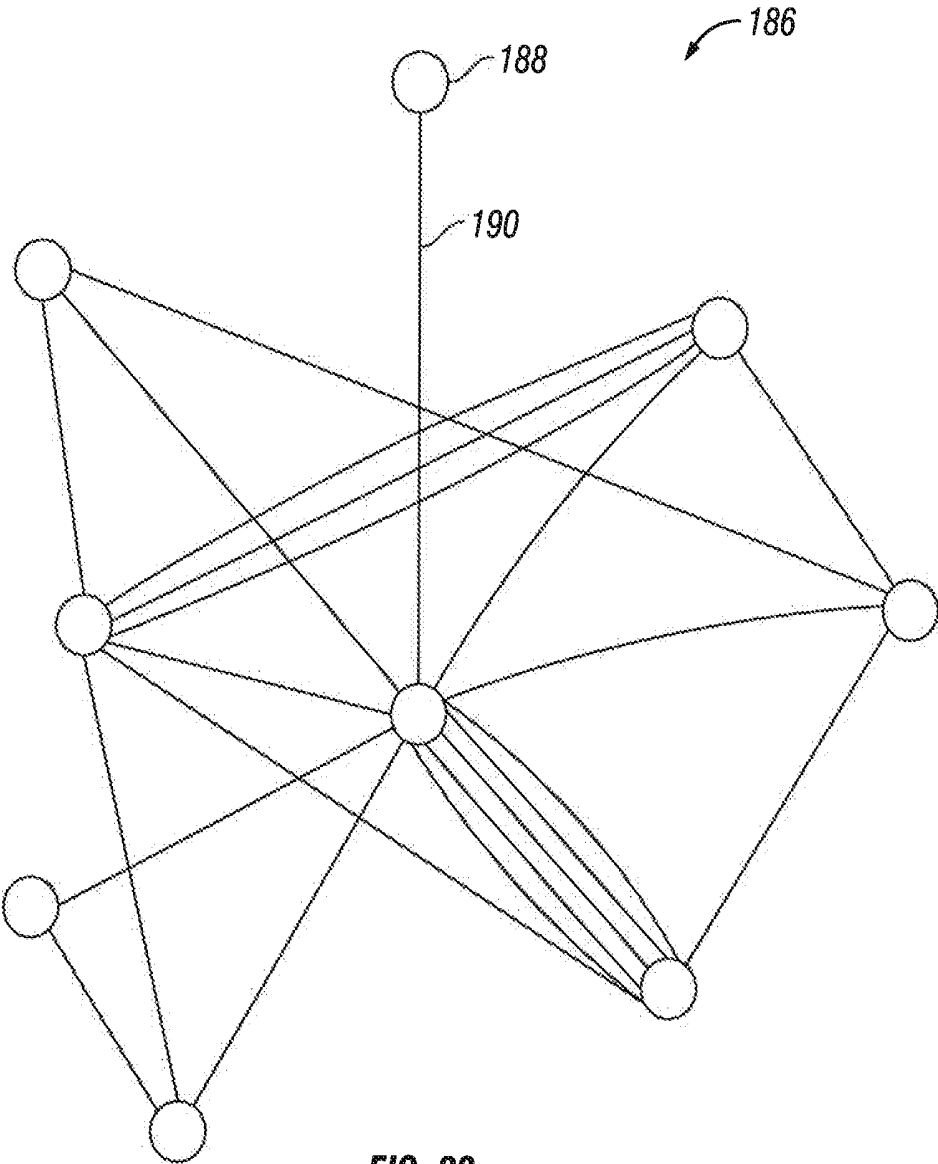


FIG. 23

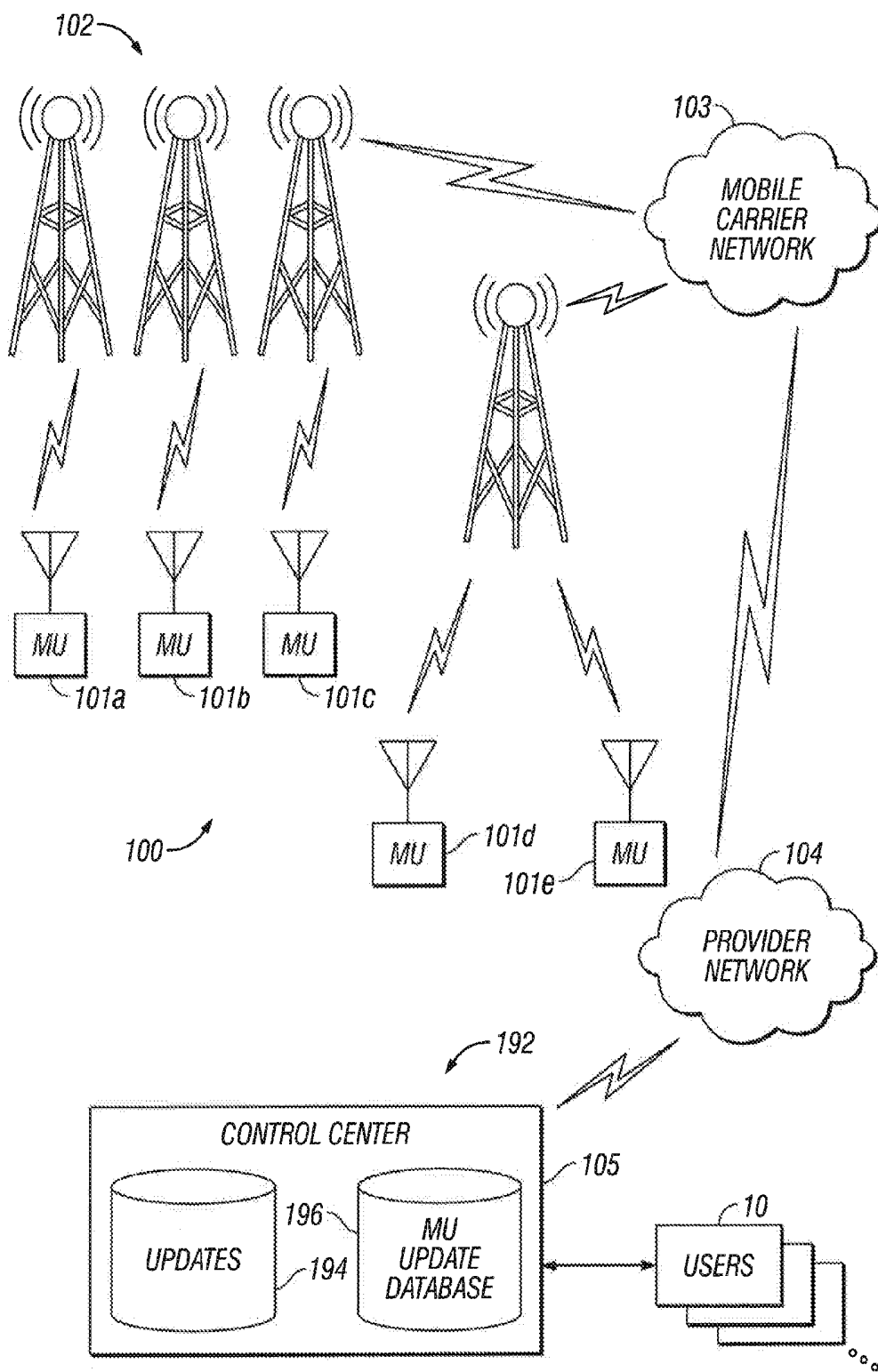


FIG. 24

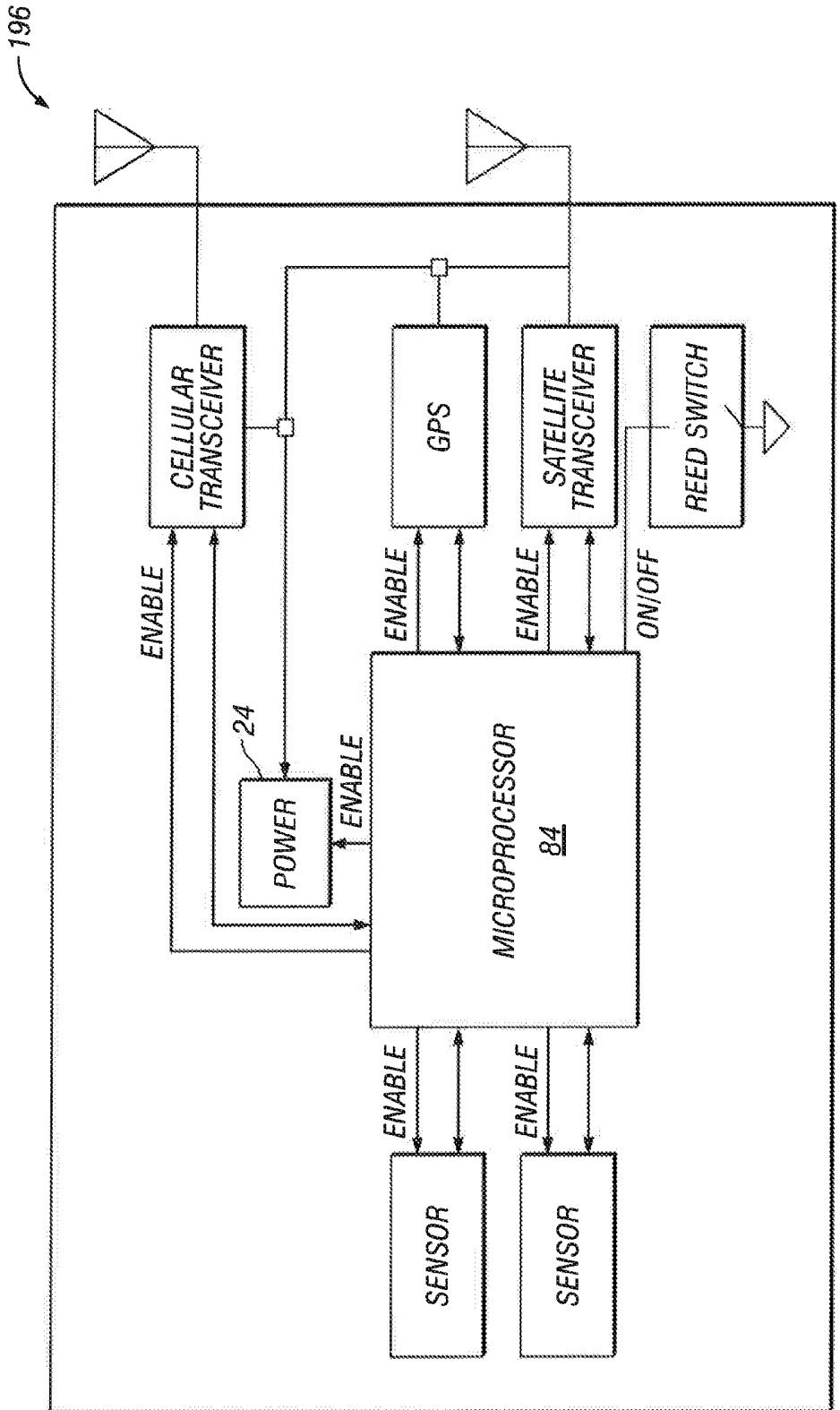


FIG. 25

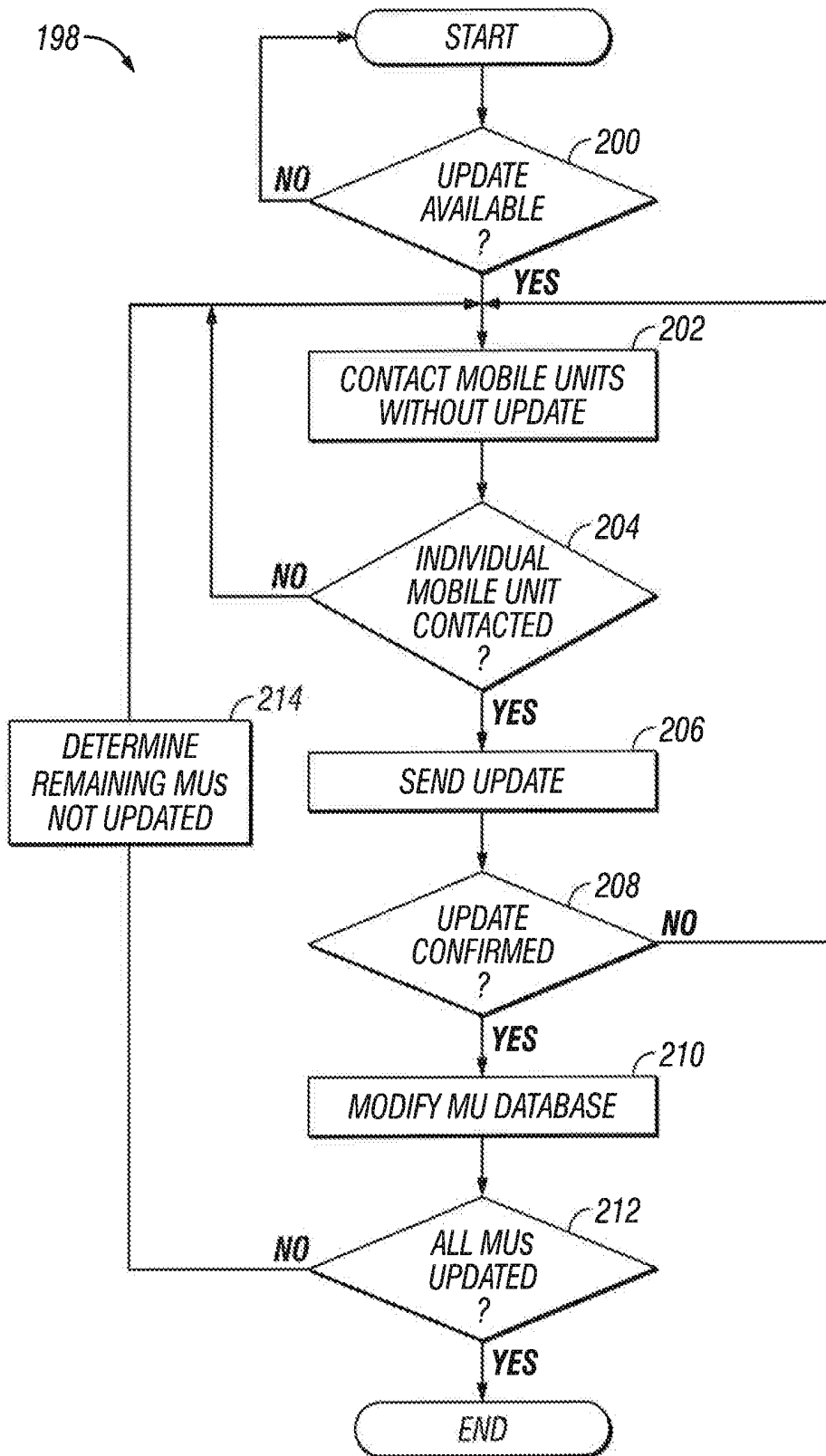


FIG. 26

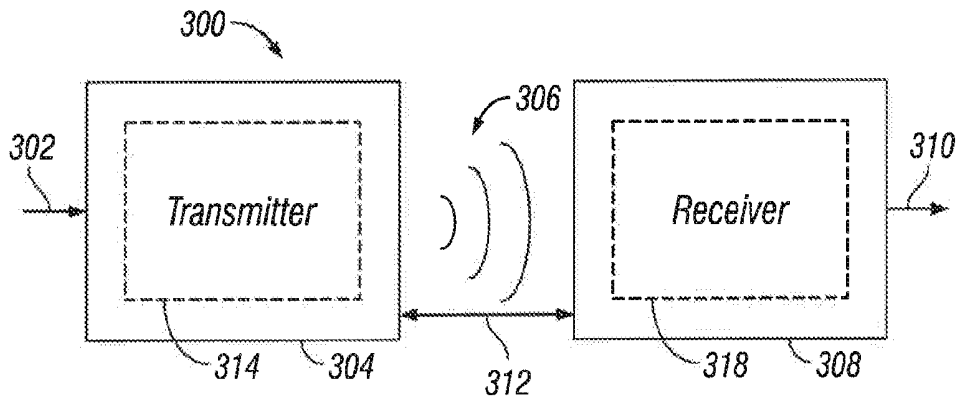


FIG. 27

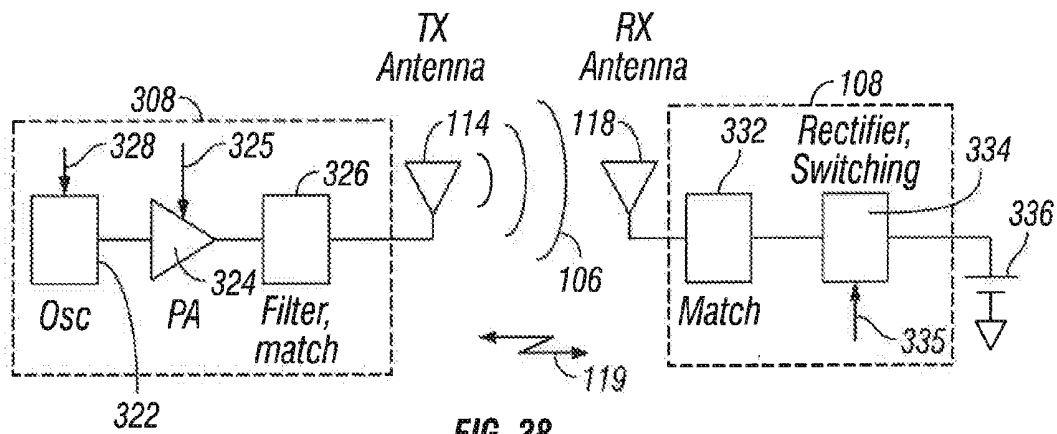


FIG. 28

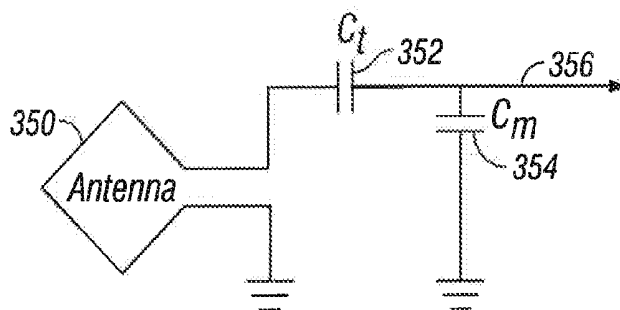


FIG. 29

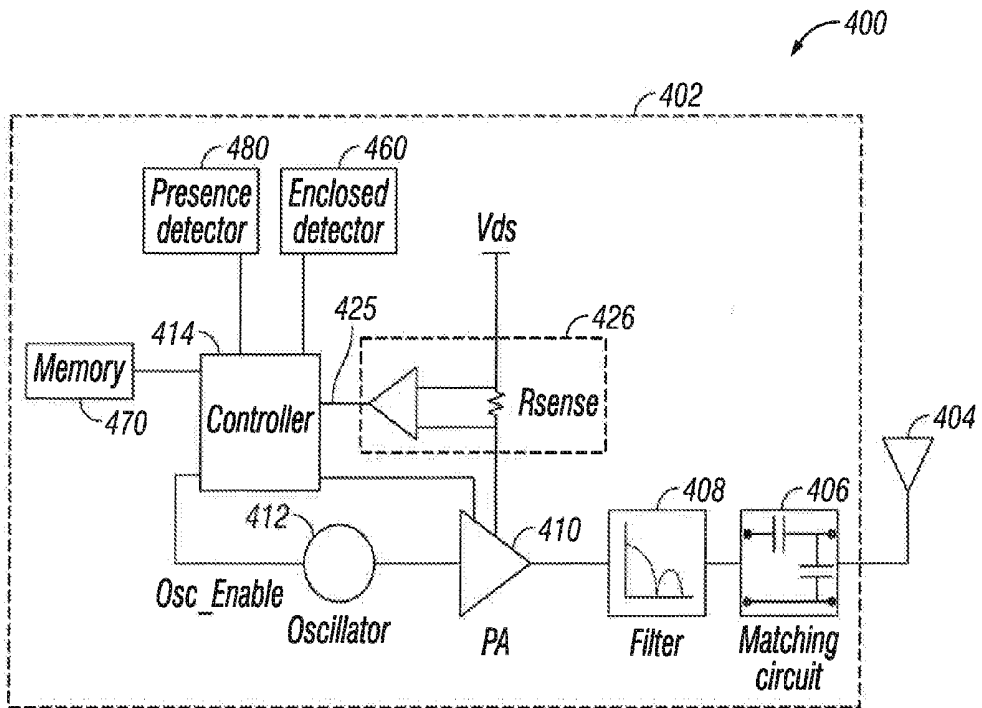


FIG. 30

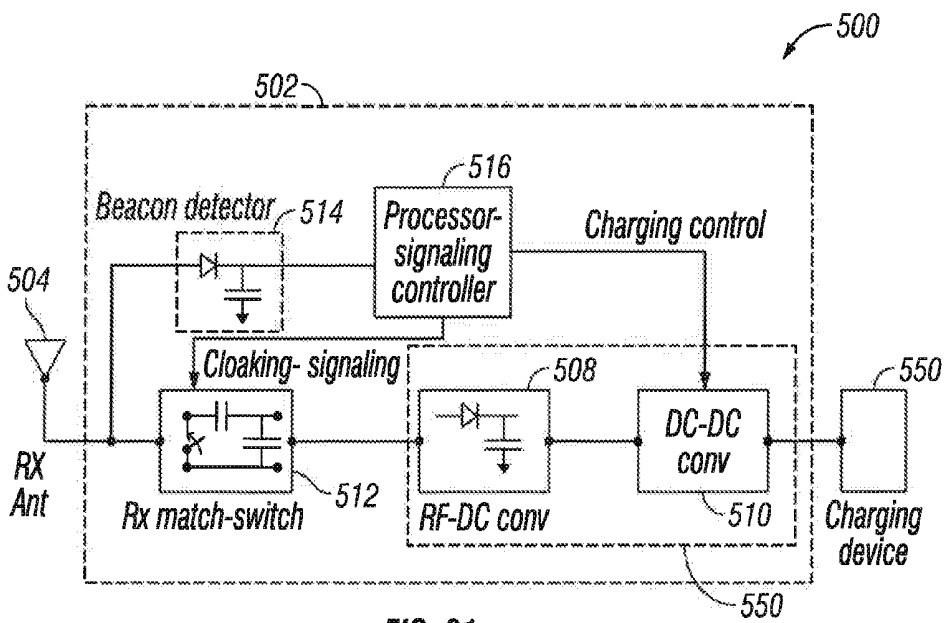


FIG. 31

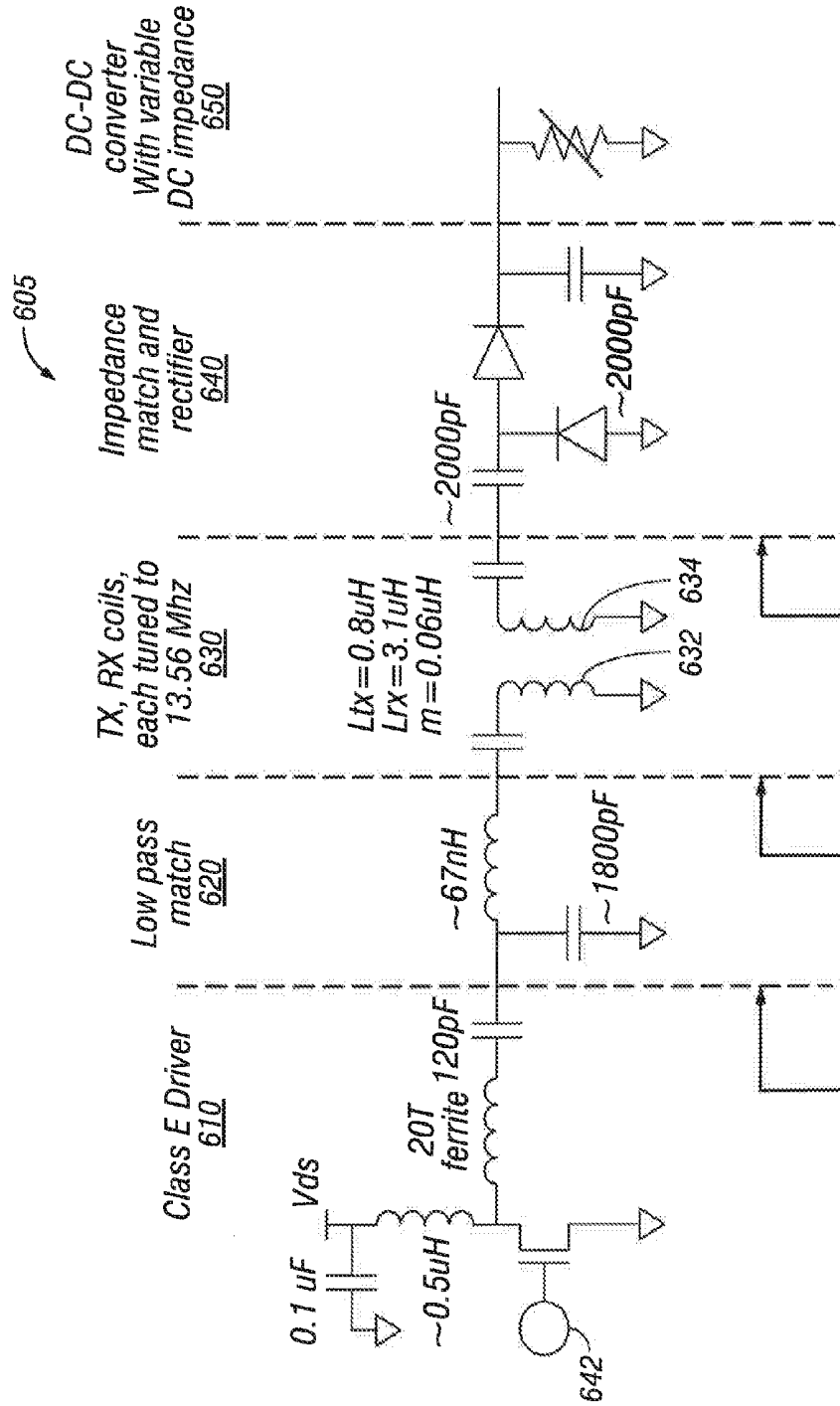


FIG. 32

Input Impedance for $R_{dc} = 10.2 \text{ Ohms}$

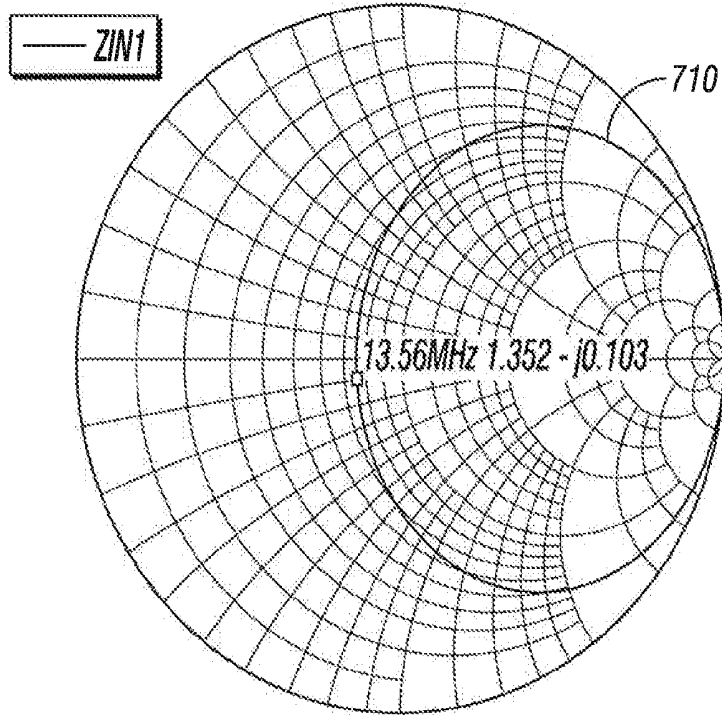


FIG. 33A

Input Impedance for $R_{dc} = 80 \text{ Ohms}$

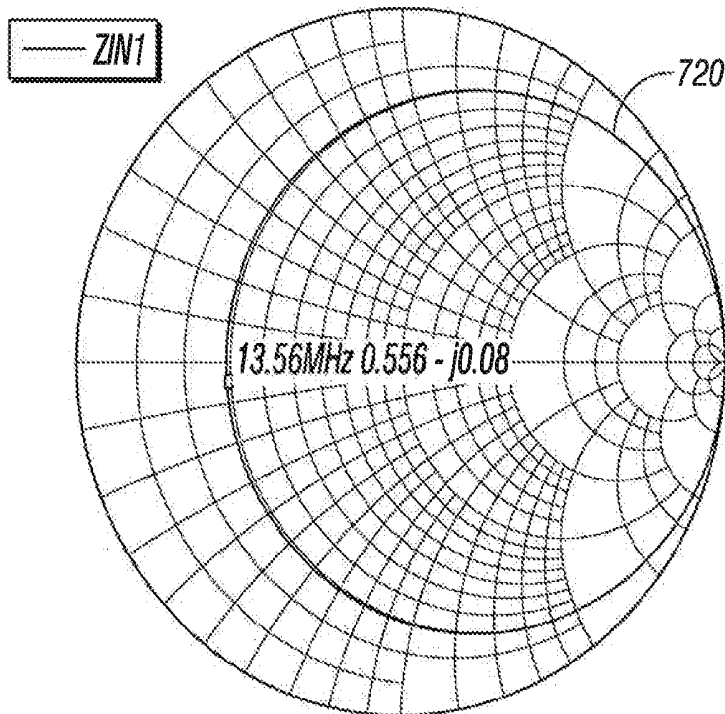


FIG. 33B

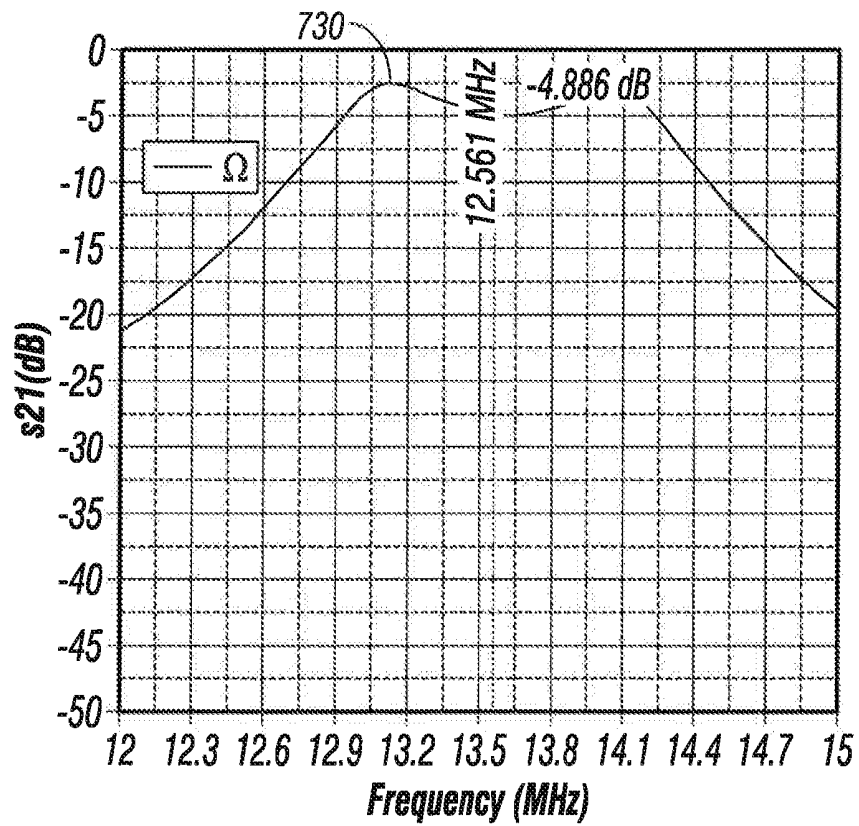


FIG. 34A

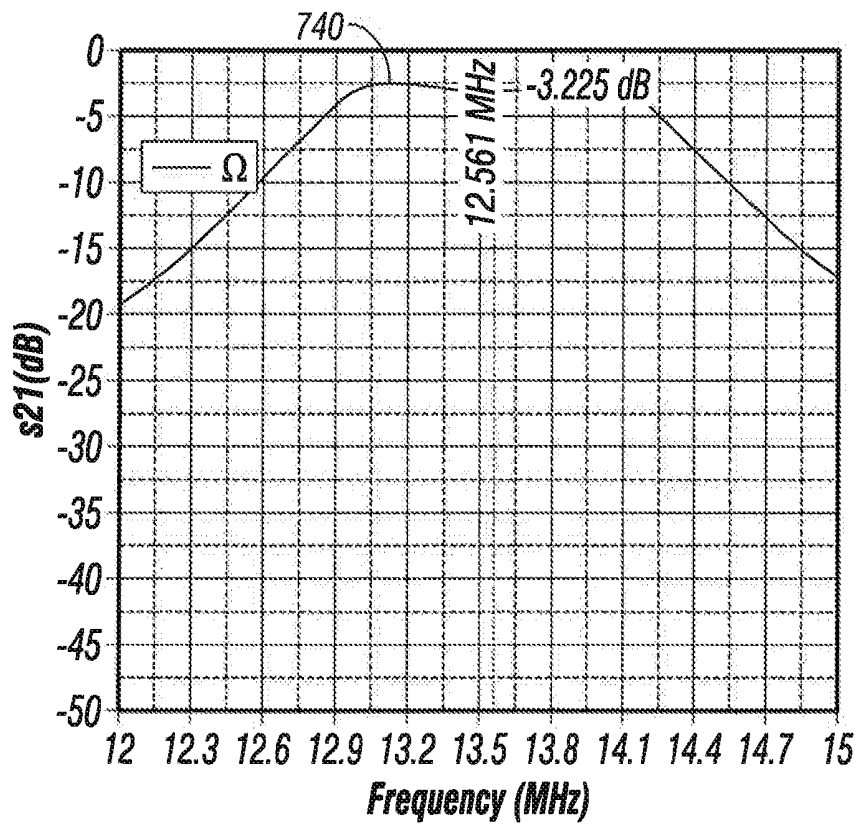


FIG. 34B

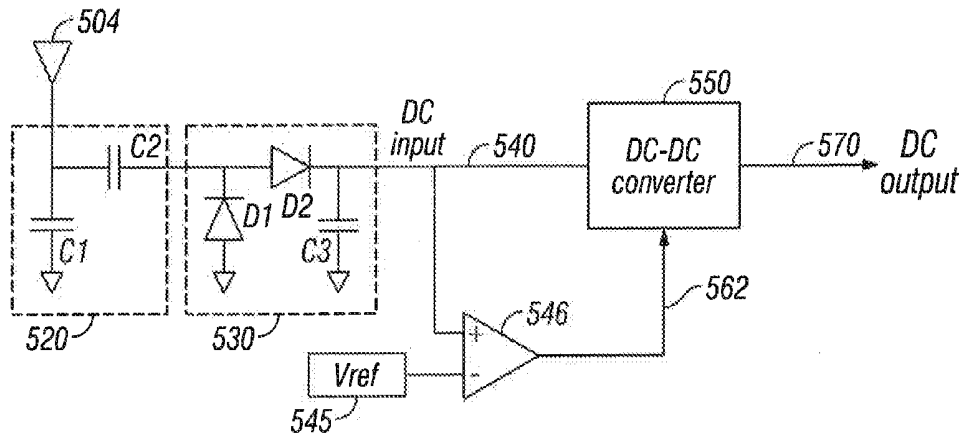


FIG. 35A

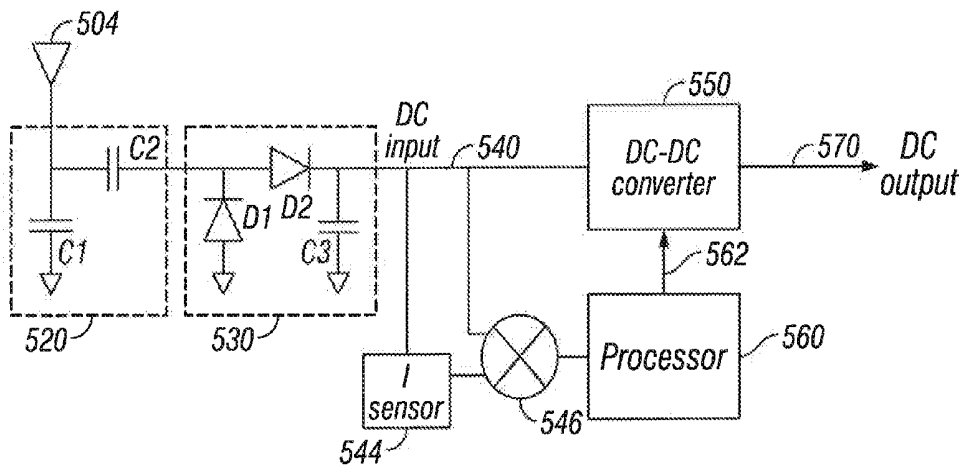


FIG. 35B

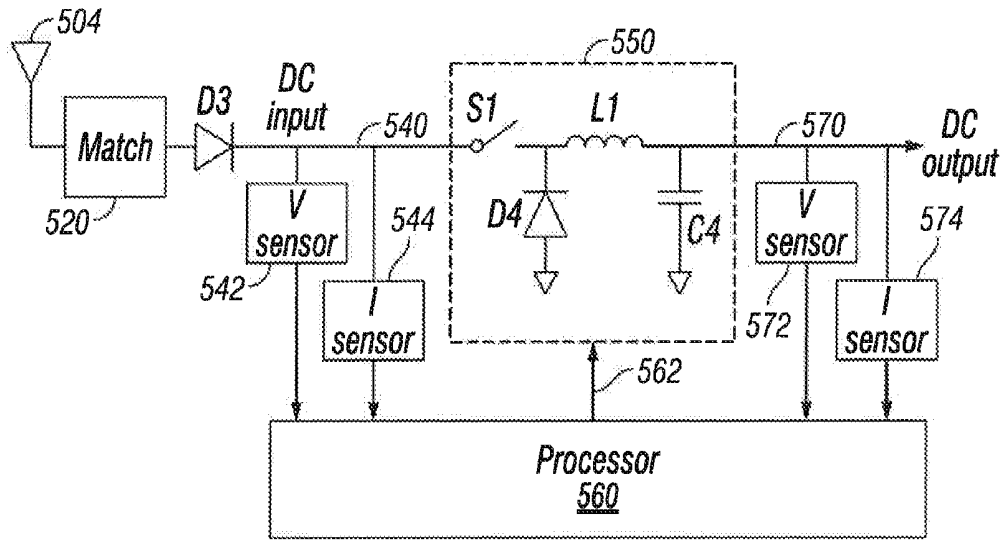


FIG. 36A

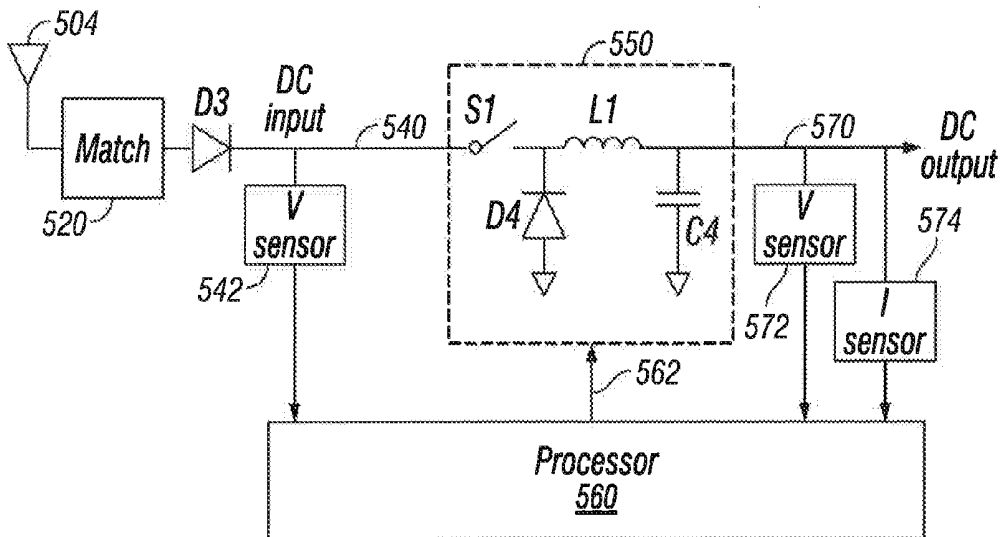


FIG. 36B

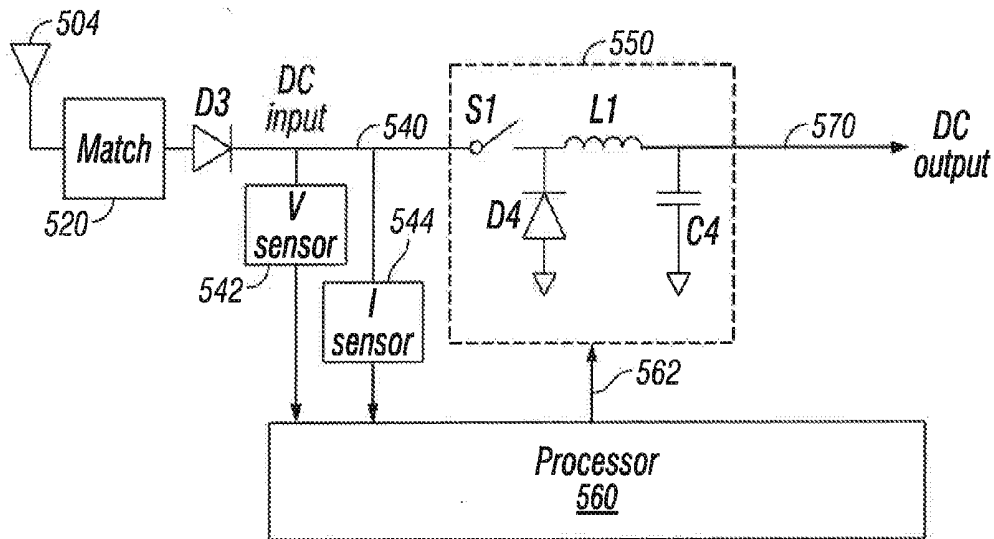


FIG. 36C

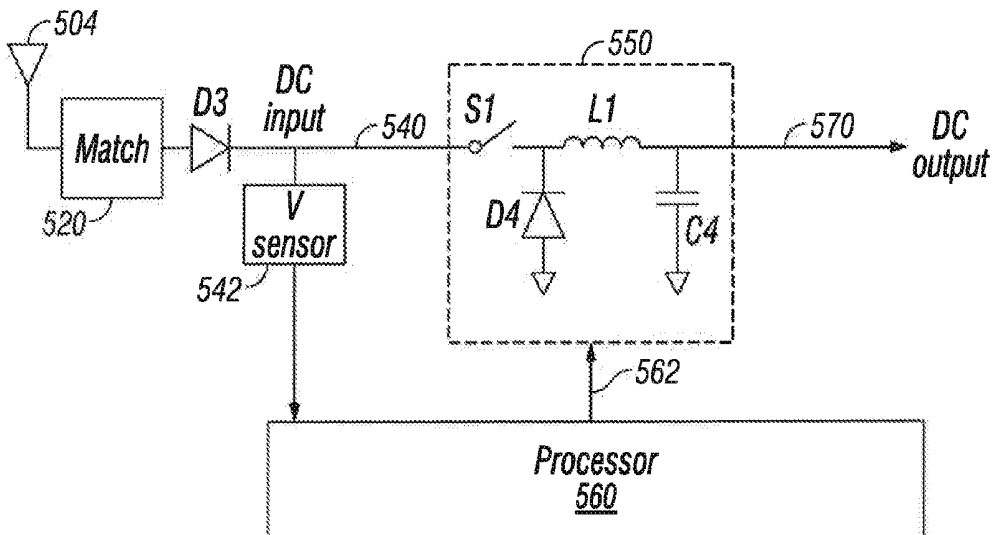


FIG. 36D

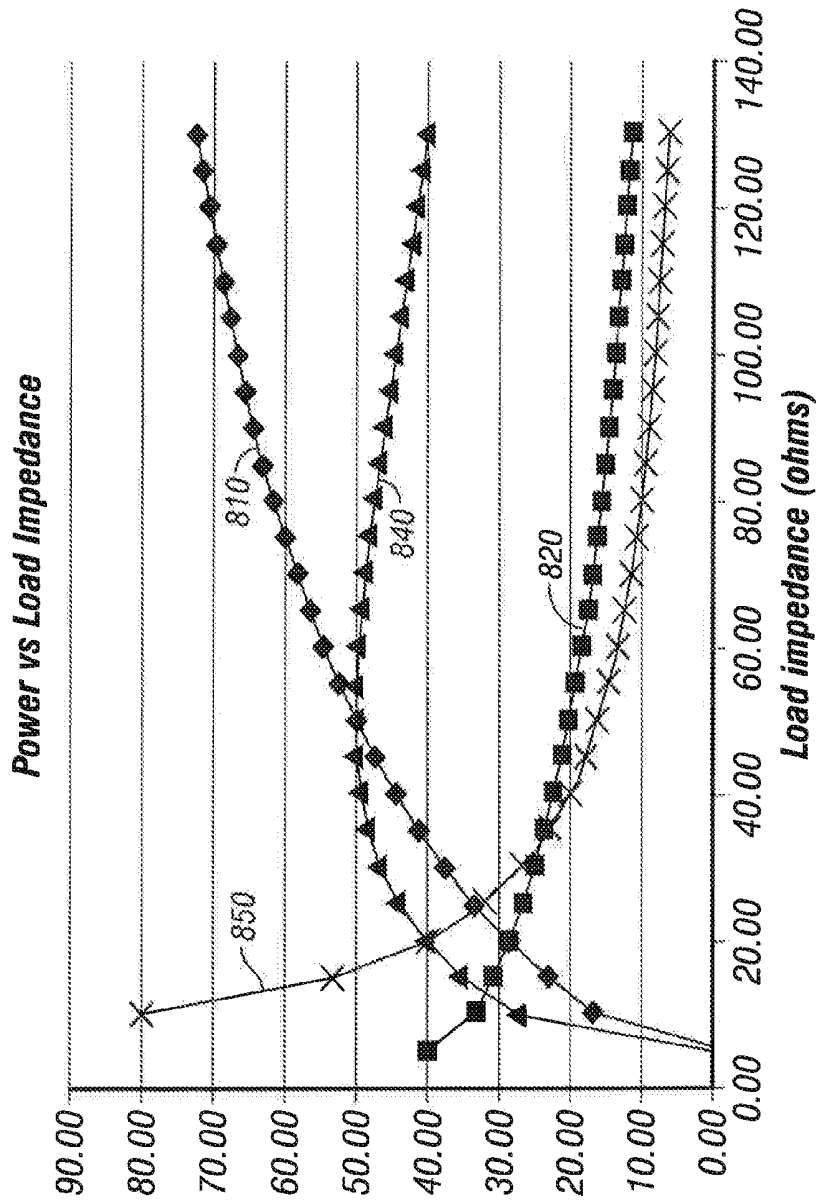


FIG. 37

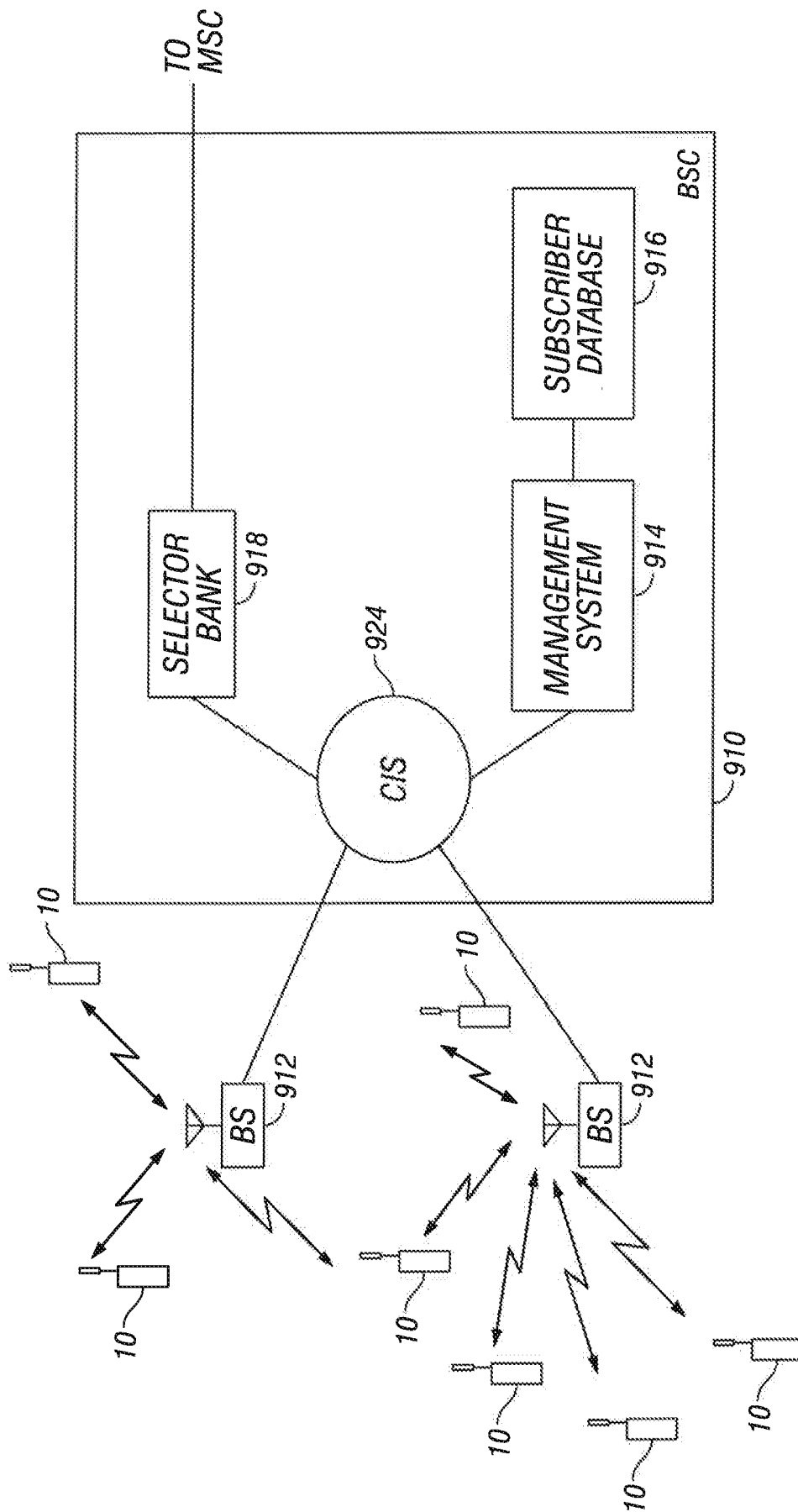


FIG. 38

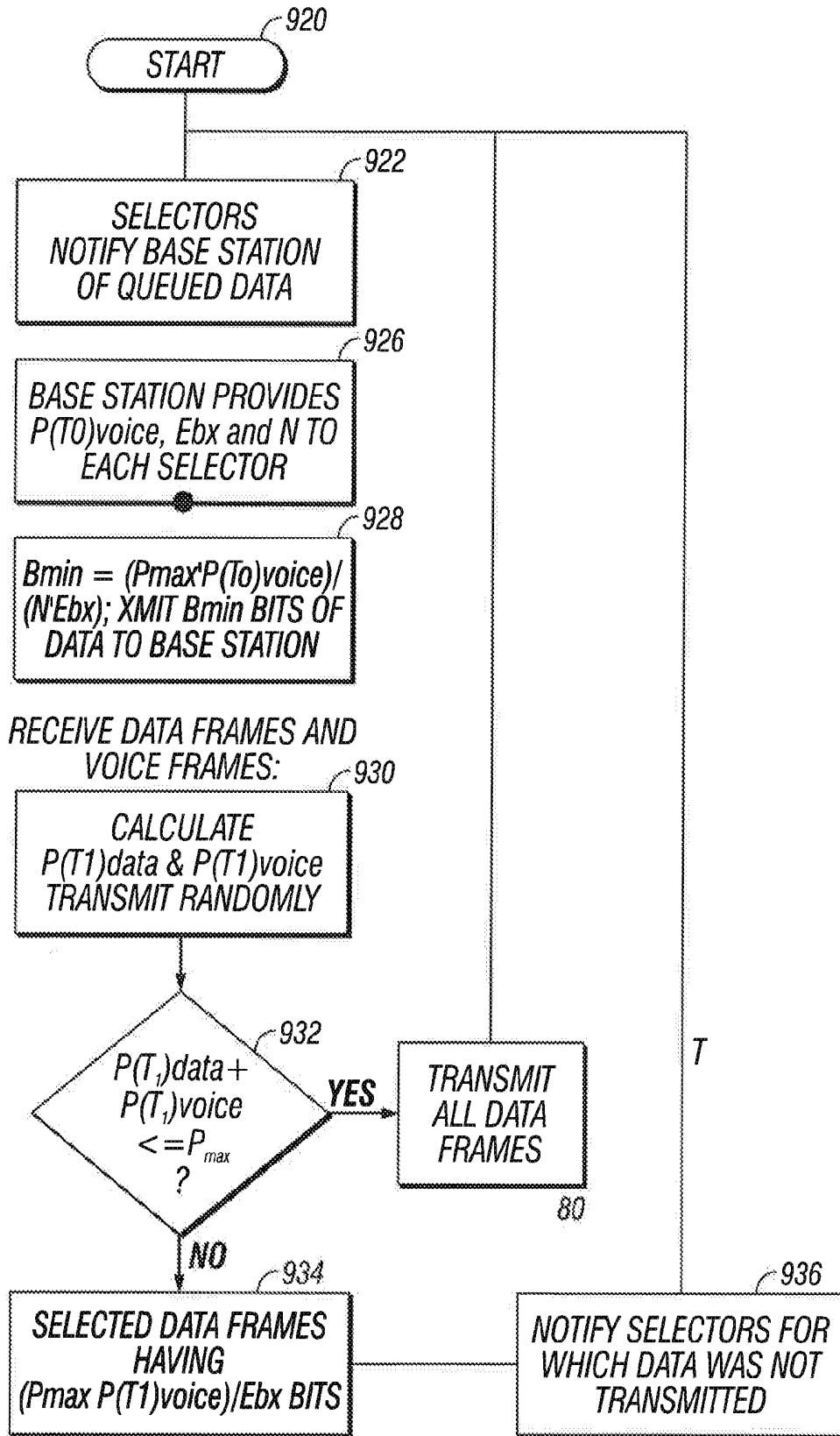


FIG. 39

MONITORING DEVICE WITH WIRELESS COMMUNICATION USING CDMA

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation in part of U.S. Ser. No. 13/923,909, U.S. Ser. No. 13/923,637, U.S. Ser. No. 13/923,614, U.S. Ser. No. 13/923,809, U.S. Ser. No. 13/923,750, U.S. Ser. No. 13/923,583, U.S. Ser. No. 13/923,560, U.S. Ser. No. 13/923,543, and U.S. Ser. No. 13/923,937, all filed Jun. 21, 2013 and all of which claim the benefit of U.S. 61/772,265, U.S. 61/812,083 and 61/823,502. All of the above-identified applications are fully incorporated herein by reference.

FIELD OF THE INVENTION

[0002] The present invention relates to wearable monitoring devices in communication with telemetry systems, and more particularly to monitoring devices suitable for use in transmitting data in a code division multiple access (CDMA) wireless telecommunications system.

DESCRIPTION OF THE RELATED ART

[0003] Telemetry systems can be implemented to acquire and transmit data from a remote source. Some telemetry systems provide information about a user's activities.

[0004] It is becoming commonplace to use wireless packet data service networks for effectuating data sessions with. In some implementations, unique identifications (ID) need to be assigned to the devices in order to facilitate certain aspects of service provisioning, e.g., security, validation and authentication, et cetera. In such scenarios, it becomes imperative that no two devices have the same indicium (i.e., collision). Further, provisioning of such indicia should be flexible so as to maintain the entire pool of indicia to a manageable level while allowing for their widespread use in multiple service environments.

[0005] The telemetry system may incorporate a wireless technology such as wireless fidelity (WiFi); infrared (IR); or ultrasound in order to facilitate finding an object and/or data transmission. As an exemplary implementation, a medical telemetry system can be implemented to remotely monitor the cardiac electrical activity of a plurality of ambulatory patients while they remain within a predefined coverage area. The medical telemetry system may also be implemented to locate and track patients within the coverage area.

[0006] One measure of the usefulness of a wireless communication system is the efficiency with which it uses the available RF bandwidth. In some instances, efficiency is defined as the sustainable data transmission rate of a system over a given amount of RF bandwidth. In other instances, efficiency is characterized as the total number of communications that can be simultaneously conducted using a given amount of bandwidth. Whatever the measure, increasing efficiency generally increases the usefulness of a wireless communication system.

[0007] There is a need for improved communication systems used by remote monitoring devices.

SUMMARY OF THE INVENTION

[0008] An object of the present invention is to provide improved wireless communication systems.

[0009] Another object of the present invention is to provide systems for transmitting and relaying information from a monitoring device using wireless communication systems.

[0010] A further object of the present invention is to provide systems for transmitting data and voice from a monitoring device in a code division multiple access (CDMA) wireless telecommunications system.

[0011] These and other objects of the present invention are achieved in, a wireless communication system for a monitoring device. One or more sensors are coupled to a monitoring device that has a unique user ID, the one or more sensors acquiring user information selected from of at least one of, a user's activities, behaviors and habit information. ID circuitry is at the monitoring device. Also included is ID storage, a communication system that reads and transmits the unique ID from an ID storage, a power source and a pathway system to route signals through the circuitry. A telemetry system includes a database of user ID's. The telemetry system is in communication with the monitoring device and analyzes data from monitoring device based on at least one of, user's activities, behaviors and habit information and creating personalized information about the user. A telemetry system controller transmits a set of data frames relative to the monitoring device. A set of data frames is transmitted from the monitoring device. The monitoring device optionally transmits a set of voice frames if they exist and when there is additional capacity.

[0012] In another embodiment of the present invention, a wireless communication system for a monitoring device includes one or more sensors coupled to the monitoring device that has a unique user ID. The one or more sensors acquire user information selected from of at least one of, a user's activities, behaviors and habit information. ID circuitry is at the monitoring device along with ID storage, a communication system that reads and transmits the unique ID from an ID storage, a power source and a pathway system to route signals through the circuitry. A telemetry system includes a database of user ID's. The telemetry system is in communication with the monitoring device. The telemetry system analyzes telemetry data from the monitoring device based on at least one of, user's activities, behaviors and habit information and creating personalized information about the user. A telemetry system controller transmits a set of voice frames relative to the monitoring device and optionally transmits a set of data frames from the monitoring device if they exist and when there is additional capacity.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIGS. 1(a) and 1(b) illustrate one embodiment of a wearable device of the present invention, where one size fits all.

[0014] FIG. 2 illustrates one embodiment of electronics that can be included in the wearable device.

[0015] FIG. 3 illustrates one embodiment of a telemetry system of the present invention.

[0016] FIG. 4 is a diagram of the programming input schematic of the secure sensor/transmitter array of FIG. 7.

[0017] FIG. 5 is a block diagram of the system of programming the sensor/transmitter(s) comprising the secure sensor/transmitter array of FIG. 7.

[0018] FIG. 6 is a block diagram of the jam command and security/randomization bits of the secure sensor/transmitter array of FIG. 7.

[0019] FIG. 7 is a logic circuit diagram of the sensor/transmitter programming input schematic in one embodiment of the present invention.

[0020] FIG. 8 is a block diagram of an embodiment of a computer implemented system for determining the location of a remote sensor utilizing the methods of the present invention

[0021] FIG. 9 is a block diagram illustrating one embodiment of a SNAPSHOT GPS receiver for use according to the present invention.

[0022] FIG. 10 is a block diagram of a remote sensor shown in communication with two different external communication devices.

[0023] FIG. 11 is a diagram of the active RF and RF backscatter antennas.

[0024] FIG. 12 is a diagram of the encoding scheme for the symbols in the active RF protocol.

[0025] FIG. 13 is a diagram of the packet structure in the IRDA protocol.

[0026] FIG. 14 is a diagram of the encoding scheme in the IRDA protocol.

[0027] FIG. 15 illustrates one embodiment of a wireless network that can be used with the present invention.

[0028] FIGS. 16(a)-16(d) illustrate various embodiments of the interaction of a wearable device of the present invention with an interaction engine, a transaction engine, a decoding engine, and a payment system and a third party.

[0029] FIG. 17 illustrates an embodiment of a social network circle with social devices in accordance with one embodiment of the present invention.

[0030] FIG. 18 illustrates an embodiment of a social group with a variety of members in accordance with one embodiment of the present invention.

[0031] FIG. 19 is a functional block diagram illustrating a social network infrastructure and social devices in accordance with one embodiment of the invention.

[0032] FIG. 20 illustrates a simplified block diagram of a client-server system and network in one embodiment of the present invention.

[0033] FIG. 21 illustrates a more detailed diagram of an exemplary client or server computer that can be used in one embodiment of the present invention.

[0034] FIG. 22 illustrates a system for activity collection and building a social graph including sharing activity between users in one embodiment of the present invention.

[0035] FIG. 23 illustrates a social graph with nodes representing users and edges representing sharing activity between the users in one embodiment of the present invention.

[0036] FIG. 24 is a block diagram of an embodiment of a system for distributing firmware updates to a large number of monitoring devices.

[0037] FIG. 25 is a block diagram of an embodiment of an asset tag for a monitoring device having wireless communications capabilities.

[0038] FIG. 26 is a flow chart for an embodiment of a method of distributing firmware updates to a large number of monitoring devices.

[0039] FIG. 27 illustrates one embodiment of a wireless power transfer system that can be used with the present invention.

[0040] FIG. 28 illustrates another wireless power transfer system that can be used with the present invention.

[0041] FIG. 29 illustrates one embodiment of a loop antenna for use in one various embodiments of the present invention.

[0042] FIG. 30 illustrates one embodiment of a transmitter that can be used with the present invention.

[0043] FIG. 31 illustrates one embodiment of a receiver that can be used with the present invention.

[0044] FIG. 32 illustrates one embodiment of transmit circuitry and receive circuitry that can be used with the present invention.

[0045] FIGS. 33(a) and 33(b) show Smith charts illustrating change in input impedance of a coupled coil pair responsive to a change in DC impedance at the receiver device.

[0046] FIGS. 34(a) and 34(b) are amplitude plots showing improved coupling between a coupled coil pair responsive to a change in DC impedance at the receiver device in one embodiment of the present invention.

[0047] FIGS. 35(a) and 35(b) are schematics of receiver devices for adjusting DC impedance at the receiver device in one embodiment of the present invention.

[0048] FIGS. 36(a) through 36(d) are schematics of receiver devices illustrating embodiments for adjusting DC impedance at the receiver device using a pulse-width modulation converter of the present invention.

[0049] FIG. 37 illustrates various input and output parameters that can be used when adjusting DC impedance at the receiver device.

[0050] FIG. 38 is a block diagram of one embodiment of a communication system used with the monitoring device of the present invention.

[0051] FIG. 39 is a flow diagram illustrating the operation of one embodiment of a communication system that can be used with a monitoring device of the present invention.

DETAILED DESCRIPTION

[0052] As used herein, the term engine refers to software, firmware, hardware, or other component that can be used to effectuate a purpose. The engine will typically include software instructions that are stored in non-volatile memory (also referred to as secondary memory). When the software instructions are executed, at least a subset of the software instructions can be loaded into memory (also referred to as primary memory) by a processor. The processor then executes the software instructions in memory. The processor may be a shared processor, a dedicated processor, or a combination of shared or dedicated processors. A typical program will include calls to hardware components (such as I/O devices), which typically requires the execution of drivers. The drivers may or may not be considered part of the engine, but the distinction is not critical.

[0053] As used herein, the term database is used broadly to include any known or convenient means for storing data, whether centralized or distributed, relational or otherwise.

[0054] As used herein a mobile device includes, but is not limited to, a cell phone, such as Apple's iPhone®, other portable electronic devices, such as Apple's iPod Touches®, Apple's iPads®, and mobile devices based on Google's Android® operating system, and any other portable electronic device that includes software, firmware, hardware, or a combination thereof that is capable of at least receiving the signal, decoding if needed, exchanging information with a transaction server to verify the buyer and/or seller's account information, conducting the transaction, and generating a receipt. Typical components of mobile device may include

but are not limited to persistent memories like flash ROM, random access memory like SRAM, a camera, a battery, LCD driver, a display, a cellular antenna, a speaker, a BLUE-TOOTH® circuit, and WIFI circuitry, where the persistent memory may contain programs, applications, and/or an operating system for the mobile device.

[0055] As used herein, the terms “social network” and “SNET” comprise a grouping or social structure of devices and/or individuals, as well as connections, links and interdependencies between such devices and/or individuals. Members or actors (including devices) within or affiliated with a SNET may be referred to herein as “nodes”, “social devices”, “SNET members”, “SNET devices”, “user devices” and/or “modules”. In addition, the terms “SNET circle”, “SNET group” and “SNET sub-circle” generally denote a social network that comprises social devices and, as contextually appropriate, human SNET members and personal area networks (“PANs”).

[0056] As used herein, the term “wearable device” is anything that can be worn by an individual and that has a back side that in some embodiments contacts a user’s skin and a face side. Examples of wearable device include but are not limited to a cap, arm band, wristband, garment, and the like.

[0057] As used herein, the term “computer” is a general purpose device that can be programmed to carry out a finite set of arithmetic or logical operations. Since a sequence of operations can be readily changed, the computer can solve more than one kind of problem. A computer can include of at least one processing element, typically a central processing unit (CPU) and some form of memory. The processing element carries out arithmetic and logic operations, and a sequencing and control unit that can change the order of operations based on stored information. Peripheral devices allow information to be retrieved from an external source, and the result of operations saved and retrieved.

[0058] As used herein, the term “Internet” is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support email. The communications infrastructure of the Internet consists of its hardware components and a system of software layers that control various aspects of the architecture.

[0059] As used herein, the term “extranet” is a computer network that allows controlled access from the outside. An extranet can be an extension of an organization’s intranet that is extended to users outside the organization that can be partners, vendors, and suppliers, in isolation from all other Internet users. An extranet can be an intranet mapped onto the public Internet or some other transmission system not accessible to the general public, but managed by more than one company’s administrator(s). Examples of extranet-style networks include but are not limited to:

[0060] LANs or WANs belonging to multiple organizations and interconnected and accessed using remote dial-up

[0061] LANs or WANs belonging to multiple organizations and interconnected and accessed using dedicated lines

[0062] Virtual private network (VPN) that is comprised of LANs or WANs belonging to multiple organizations, and that extends usage to remote users using special “tunneling” software that creates a secure, usually encrypted network connection over public lines, sometimes via an ISP.

[0063] As used herein, the term “Intranet” is a network that is owned by a single organization that controls its security policies and network management. Examples of intranets include but are not limited to:

[0064] A LAN

[0065] A Wide-area network (WAN) that is comprised of a LAN that extends usage to remote employees with dial-up access

[0066] A WAN that is comprised of interconnected LANs using dedicated communication lines

[0067] A Virtual private network (VPN) that is comprised of a LAN or WAN that extends usage to remote employees or networks using special “tunneling” software that creates a secure, usually encrypted connection over public lines, sometimes via an Internet Service Provider (ISP).

[0068] As used herein, the term (patient monitoring) includes: (i) cardiac monitoring, which generally refers to continuous electrocardiography with assessment of the patient’s condition relative to their cardiac rhythm. A small monitor worn by an ambulatory patient for this purpose is known as a Holter monitor. Cardiac monitoring can also involve cardiac output monitoring via an invasive Swan-Ganz catheter (ii) Hemodynamic monitoring, which monitors the blood pressure and blood flow within the circulatory system. Blood pressure can be measured either invasively through an inserted blood pressure transducer assembly, or noninvasively with an inflatable blood pressure cuff. (iii) Respiratory monitoring, such as: pulse oximetry which involves measurement of the saturated percentage of oxygen in the blood, referred to as SpO₂, and measured by an infrared finger cuff, capnography, which involves CO₂ measurements, referred to as EtCO₂ or end-tidal carbon dioxide concentration. The respiratory rate monitored as such is called AWRR or airway respiratory rate). (iv) Respiratory rate monitoring through a thoracic transducer belt, an ECG channel or via capnography, (v) Neurological monitoring, such as of intracranial pressure. Special patient monitors can incorporate the monitoring of brain waves electroencephalography, gas anesthetic concentrations, bispectral index (BIS), and the like, (vi) Blood glucose monitoring using glucose sensors. (vii) Childbirth monitoring with sensors that monitor various aspects of childbirth. (viii) Body temperature monitoring which in one embodiment is through an adhesive pad containing a thermoelectric transducer. (ix) Stress monitoring that can utilize sensors to provide warnings when stress levels signs are rising before a human can notice it and provide alerts and suggestions. (x) Epilepsy monitoring. (xi) Toxicity monitoring, and the like.

[0069] Additionally the present invention can be used to detect differences for a variety of blood tests, including but not limited to tests for the following: sodium, potassium, chloride, urea, creatinine, calcium, albumin, fasting glucose, amylase, carcinoembryonic antigen, glycosylated hemoglobin, hemoglobin, erythrocytes hemoglobin and the like.

[0070] As used herein, the term wireless power means any form of energy associated with electric fields, magnetic fields, electromagnetic fields, or otherwise that is transmitted between from a transmitter to a receiver without the use of physical electromagnetic conductors.

[0071] For purposes of the present invention, the Internet, extranets and intranets collectively are referred to as (“Network Systems”).

[0072] As used herein, “wireless power” means any form of energy associated with electric fields, magnetic fields, electromagnetic fields, or otherwise that is transmitted between from a transmitter to a receiver without the use of physical electromagnetic conductors.

[0073] In various embodiments, the present invention provides a monitoring device 10, such as a wearable device, where in one embodiment; one size fits all, a patient monitoring device 10, and the like. As illustrated in FIGS. 1(a) and 1(b), in one embodiment of the present invention, the monitoring device 10 includes a plurality of magnets 12, with adjacent magnets having opposite polarity, with a length suitable to be worn by all people. In one embodiment, the length of the monitoring device 10 can be 10-12 inches. The magnets 12 are positioned along an interior of the monitoring device 10 to be provided for good conformation to a user’s wrist.

[0074] One or more sensors 14 are coupled to the monitoring device 10. The sensors are measuring devices. As a non-limiting example, the measuring device or sensors 14 can include RTSS devices to detect a user’s activities, motions, physical parameters, and the like, including but not limited to, a heart rate monitor, a body temperature probe, a conventional pedometer, an accelerometer and the like.

[0075] Alternatively, multifunctional sensors 14 which can perform all the aforementioned functions of RTSS may be attached or embedded in monitoring device 10. In one embodiment, each sensor can be in communication and or connect electronically and/or RF to a telemetry module 16. A variety of different sensors 14 can be utilized, including but not limited to, an accelerometer based sensor, and pressure based sensors, voltage resistance sensor, a radio frequency sensor, and the like, as recited above.

[0076] As a non-limiting example, an accelerometer, well known to those skilled in the art, detects acceleration and thus user activity. The accelerometer provides a voltage output that is proportional to the detected acceleration. Accordingly, the accelerometer senses vibration. This voltage output provides an acceleration spectrum over time; and information about loft time can be ascertained by performing calculations on that spectrum. A microprocessor subsystem, such as disclosed in U.S. Pat. No. 8,352,211, incorporated herein by reference, stores the spectrum into memory and processes the spectrum information to determine activity. Other examples of suitable accelerometer sensors are disclosed in EP 2428774 A1, incorporated herein by reference. Suitable pressure sensors are disclosed in EP 1883798 B1, incorporated herein by reference. A suitable voltage resistance sensor is disclosed in EP 1883798 B1, incorporated herein by reference. A suitable radio frequency sensor is disclosed in EP 2052352 B1, incorporated herein by reference.

[0077] Referring to FIG. 2, in various embodiments, the monitoring device 10, also known as the monitoring device, can include a power source 24, such a battery that can be rechargeable. The battery 24 can be put into a sleep state when not actively used in order to preserve power. A wake up feature allows the battery 24 and other electronics of the

monitoring device 10 to “sleep” during non-use or and is initiated into the “wake up” mode by certain predestinated events.

[0078] In one embodiment, as illustrated in FIG. 3, a telemetry system server 16 is coupled to a database 18. Each monitoring device 10 is assigned its own unique identification, ID or asset tag or more fully explained hereafter.

[0079] The data transmitted by the monitoring device 10 sensors 14 and its ID may be coded by appending a seed to digital data bits. As illustrated in FIG. 3 central processor unit 20 (CPU) validates or rejects received upon detection of the seed string appended to the digital data bits. In the alternative, the digital data bits may be coded and decoded by applying a scrambling algorithm utilizing the seed. A programming device 22 may be configured to transmit data to a sensor 14, also known as a monitoring device, utilizing a variety of alternative transmission means, including, for example, RF, IR, optical, and the like, or a magnetic loop/induction system.

[0080] In one embodiment, sensors 14 are configured to be shipped to users in a non-programmable mode with all programming already performed at the factory. A random seed may be communicated to the programming device 22 can a variety of different mechanisms, including but not limited to, via scanning a bar code, manual input, magnetic strip, random number generation, and the like.

[0081] Referring again to FIG. 2, in one embodiment, the monitoring device 10 includes a control unit 26 that puts the monitoring device 10 in a low power state. A monitoring system 28 can be included that remains active. The monitoring system 28 wakes up the electronics 30 in the monitoring device 10 from a low power state. The control unit 26 can be notified of awaking of the other components by the monitoring system 28. The control unit 26 can set a status bit on the monitoring system 28 only when the battery 24 needs to be in a full power state. The control unit 26 then forces a power cycle.

[0082] Referring to FIG. 3, one embodiment of a telemetry system 32 is illustrated. The telemetry system 32 is in the communication with the sensors 14 and or monitoring device 14 and ID of the monitoring device 10 and can include one or more receivers 34, a central server 36 with the CPU 20. The telemetry system 32 can optionally include a display 42 and an alarm 44. The telemetry system 32 receives information from sensors 14 and or the monitoring device of a user’s habits, activities, and the like, and then processes this information. Monitoring device 10 with its unique ID and sensors 14 is assigned to a specific user in order to track and/or monitor that user. For illustrative purposes assume that three users A, B AND C are being tracked and monitored by the telemetry system 32. It should, however, be appreciated that the telemetry system 32 may be implemented to track and/or monitor a much larger number of users.

[0083] In various embodiments, the telemetry system 32 can send firmware updates or repairs to the monitoring device 14 during an update mode of the monitoring system, when the monitoring device is not in use by the user. The update mode can be when the user does not know that the monitoring device is being up-dated. The update mode can occur without disrupting service to the user. The firmware update can be sent by the telemetry system 32 directly or indirectly to the monitoring device 14, with the firmware update or a copy of the firmware update then resides on the monitoring device 14.

[0084] In one embodiment of the present invention, radio frequency (RF) devices that are sensors 14 and/or chips may

serve as the identifying devices. Each source, sensor **14**, ID and the like can carry a fixed radio frequency chip encoded with identifying data which may be correlated to the individual participants, parts or objects.

[0085] Telemetry system **32** of the present invention may include a Real-Time Location System (RTLS) **46** and Real-Time Sensing System (RTSS) **48** with RF technology. The RF technology may include active and/or passive RFID sensors **14** and an RF wireless array system as a receiver **34**. The RF technology in the RTLS **46** and RTSS **48** may include UWB technology (e.g., IEEE 802.15), WLAN technology (e.g., IEEE 802.11), SAW RFID positioning system technology, GPS technology, and the like.

[0086] The sensors **14** may communicate directly with each other and/or relay telemetry data directly to base receiving RF device(s) or base receivers **34**. The base receivers **34** may forward the telemetry data to a base computer either through a direct link or through a Network System **101**. Alternatively the telemetry data may be forwarded to end user devices, including but not limited to, laptops, mobile devices and the like, either directly or through a Network System **101**. The comprehensive telemetry system **32** using RF technologies such as UWB, ZigBee, Wi-Fi, GPS data system can be utilized as described above.

[0087] The readers/antennae may be interconnected using a LAN, such as Ethernet to provide a Network System **101** communication infrastructure for the computers and servers. Active and passive RFID sensors **14** may be employed. The active sensors **14** (RFID) may have a two-way communication function, which allows the base computer system to dynamically manage the sensors **14**; vary update rates; send self-identification and telemetry data.

[0088] The active sensors **14** may employ dual-radio architecture. In one embodiment, active sensors **14** transmit radio pulses, which are used to determine precise two-dimensional or three-dimensional location and a conventional bi-directional radio, which is used as a control and telemetry channel with a sensor update rate.

[0089] The monitoring device **10** gathers telemetry data, communicates that data to a base station, BLUETOOTH® enabled device, or smart phone and the like. The monitoring device can receive firmware updates and repairs from the telemetry system, as previously stated, directly or indirectly from the base station, via a BLUETOOTH® enabled device, and the like. The monitoring device **10** can receive updates wirelessly. The base station can receive firmware updates from Network Systems **101**, take telemetry data from the monitoring device **10** and transfer it to Network Systems **101**. Telemetry data received from the base station is analyzed by servers and presented to an end user. Any third party device can receive data from the monitoring device **10** wirelessly and deliver information to the servers for processing.

[0090] In one embodiment, the monitoring device **10** uses an accelerometer, gyroscope, GPS sensor, a BLUETOOTH® chip, and a heart rate monitor.

[0091] As a non-limiting example, for heart monitoring, the accelerometer, sensor **14**, determines when to sample the sensors **14** and to improve the accuracy of the heart rate monitor. The gyroscope detects movement and orientation and the GPS sensor is used to determine location of the user. A BLUETOOTH® chip allows the device to connect wirelessly to other third party devices.

[0092] As a non-limiting example, a heart rate monitor **14** detects the user's heart rate in order to accurately determine the user's activity level, behavioral patterns and the like.

[0093] An Artificial Intelligence (AI) or Machine Learning-grade algorithms is used to identify the user's activities, behaviors, behaviors and perform analysis. Examples of AI algorithms include Classifiers, Expert systems, case based reasoning, Bayesian networks, and Behavior based AI, Neural networks, Fuzzy systems, Evolutionary computation, and hybrid intelligent systems. A brief description of these algorithms is provided in Wikipedia and stated below.

[0094] Classifiers are functions that can be tuned according to examples. A wide range of classifiers are available, each with its strengths and weaknesses. The most widely used classifiers are neural networks, support vector machines, k-nearest neighbor algorithms, Gaussian mixture models, naive Bayes classifiers, and decision trees. Expert systems apply reasoning capabilities to reach a conclusion. An expert system can process large amounts of known information and provide conclusions based on them.

[0095] A case-based reasoning system stores a set of problems and answers in an organized data structure called cases. A case based reasoning system upon being presented with a problem finds a case in its knowledge base that is most closely related to the new problem and presents its solutions as an output with suitable modifications. A behavior based AI is a modular method of building AI systems by hand. Neural networks are trainable systems with very strong pattern recognition capabilities.

[0096] Fuzzy systems provide techniques for reasoning under uncertainty and have been widely used in modern industrial and consumer product control systems. An Evolutionary Computation applies biologically inspired concepts such as populations, mutation and survival of the fittest to generate increasingly better solutions to the problem. These methods most notably divide into evolutionary algorithms (e.g., genetic algorithms) and swarm intelligence (e.g., ant algorithms). Hybrid intelligent systems are any combinations of the above. It is understood that any other algorithm, AI or otherwise, may also be used. Examples of suitable algorithms that can be used with the embodiments of the present invention are disclosed in, EP 1371004 A4, EP 1367534 A2, US 20120226639 and US 20120225719, all incorporated fully herein by reference.

[0097] In various embodiments, the monitoring device **10** has additional features. In one embodiment, the monitoring device **10** changes color, via infrared LEDs, to accurately match the wearer's skin tone. This creates a seamless and more personal integration of technology into the user's daily life. In this embodiment, there is skin contact with the monitoring device **10**.

[0098] In another embodiment, the monitoring device **10** remotely reminds and can be used to administer medications. As a non-limiting example, the monitoring device **10** can inject adrenalin. In one embodiment, the monitoring device **10** has sleep pattern recognition based on movement and heart rate.

[0099] In various embodiments, the monitoring device **10** uses algorithms to determine activity type, behavioral patterns and user habits based on collected data.

[0100] In one embodiment, the monitoring device **10** uses the accelerometer information to improve the heart rate monitor. As a non-limiting example, the monitoring device **10** detects movement and speed. Addition of this data improves

the accuracy of the heart rate monitor and corrects for any miscalculations in vibration, noise and skin color.

[0101] In one embodiment, velocity readouts and accelerometer data are used to measure when to sample heart rate. For example, if the monitoring device 10 registers zero velocity readout, the user is probably at rest or engaged in a passive activity. Thus, the monitoring device 10 knows not to sample heart rate. This results in conservation of time, energy and data storage.

[0102] User activity, performance and action can be based on the acceleration and angular velocity of the monitoring device 10. In one embodiment, the monitoring device 10 has a feature where the monitoring device 10 authorizes third party interaction based on hand gesture, on previous interactions or patterns of behavior. As a non-limiting example, if one purchases a coke every day for the last two weeks, the monitoring device 10 can “orders” the person another one based on the prior history.

[0103] In one embodiment, the monitoring device 10 features near-by monitoring device 10 recognition that provides for other monitoring device 10 devices to be recognized within a particular vicinity and are able to share and transfer data between them. The monitoring device 10’s data analysis and feedback can be based on current or previous sensor output. The monitoring device 10 can alert the user when to charge the monitoring device 10 and when it is the most convenient for the user.

[0104] In one embodiment, the monitoring device 10 provides feedback via color change. An outer shell of the monitoring device 10 can use visual feedback, including but not limited to pigment or color changes to indicate changes in user behavior or to prompt changes in user behavior. In one embodiment, the monitoring device 10 is flexible in shape. As a non-limiting example, if the user puts the monitoring device 10 over their hand it can expand or contract, morphing to change size and shape.

[0105] In one embodiment, the monitoring device 10 can have a sync feature for multiple bands at the same time.

[0106] In one embodiment, the monitoring device 10 has data transfer to an external device that can be included or not included in system 32. Monitoring device 10 could be a data leaching device. For example, the user can relay information to someone else’s device (intermediary device) to access Network Systems connected device.

[0107] In one embodiment, the monitoring device 10 can disable the recording of one or more sensors 14 based on location, acceleration (or lack thereof) and the like.

[0108] In one embodiment, the monitoring device 10 detects different types of transportation and activity based on sensor data. In one embodiment, monitoring device 10 can unlock doors or cars. The user can turn it on and off. As a non-limiting example, it can be turned off by having a capacitor switch on top and bottom and is placed in a way that one couldn’t accidentally turn it off. As a non-limiting example, turning it off can be done by rotating the monitoring device 10 once.

[0109] In one embodiment, the monitoring device 10 recognizes the wearer based on biometric information, previous data, movement pattern, and the like. In one embodiment, the monitoring device 10 detects a new user based on an inability to match to user/usage patterns.

[0110] As non-limiting examples, a variety of different sensors 14 can be used such as, an altimeter, blood oxygen recognition, heart rate from wrist via sonar, Doppler, based on

sound wave and movement, based on pressure, and the like. A pressure sensor 14 can be placed on a circulatory vessel such as a vein to detect pulse.

[0111] With the monitoring device 10 of the present invention, mechanical actions of the user can be triggered, recognized and evaluated.

[0112] As a non-limiting example, with multiple users and wearable devices 10, a separate monitoring device 10 ID is assigned to each of the users A, B AND C, and thereafter the assigned transmitter/monitor 14 generates user activity data and/or user tracking data. For purposes of this disclosure, monitoring data is defined to include data acquired during the process of monitoring or evaluating a predefined characteristic. The user activity data tracks data from the sensors 14 is transferred to the receivers 34 via the wireless connections 38 represented by a dashed line.

[0113] A Network System 101 of receivers 34 transfers the user activity and/or tracking data to system server 16 via connection 50. System server 16 includes a processor 52 configured to process the user data in a known manner. For example, the processor 52 may convert raw user data acquired by the sensors 14 into more conveniently readable data.

[0114] As a non-limiting example, the display 42 can be implemented to graphically convey user information from system server 16 in a conveniently readable manner. As a non-limiting example, the user may be a cardiac patient with user monitoring data graphically conveyed as a conventional ECG plot comprising a sequence of P-waves, a QRS complexes and a T-waves. As another example, user tracking data may be graphically conveyed as an icon superimposed onto a map to indicate the user’s relative location. Alarm 44 may be included in this embodiment.

[0115] In some embodiments, system 32 ID circuitry delivers a unique ID to the wearable device from database 18. BLUETOOTH® chips can be coupled with other wearable devices 10 in the area. This data is then stored, as more fully explained in the following paragraph. The unique ID can be utilized for a variety of different applications including but not limited to payments, social networking and the like.

[0116] The ID circuitry of system 32 can include a number of system/components: unique ID storage, communication system, which reads and transmits the unique ID from the unique ID storage, battery 24 or power system that provides power to enable communication with the monitoring device 10, a pathway system to route signals to through the circuitry, a cluster that crunches information, and a control system, to orchestrate the communication between different systems. All of these systems can be implemented in hardware, software or a combination thereof. Continuing with the telemetry system 32, sensors 14 and sensing devices are disposed on wearable devices 10 worn by users. Data, such as movement, location, speed, acceleration, and the like, can be acquired, captured and provided to system 32.

[0117] System 32 and an associated Network System 101 can include an identification reference, including user activity, performance and reference information for each individual sensor 14 and location.

[0118] The user activity, performance metrics, data and the like captured by system 32 can be recorded into standard relational databases SQL server, and/or other formats and can be exported in real-time.

[0119] In various embodiments, the monitoring device 10 and/or system 32 are fully sealed and have inductively charges. All communication is done wirelessly.

[0120] In one embodiment, there are no electrical contacts, physical contacts or connections with the monitoring device 10. The monitoring device 10 is seamless. The telemetry system 32 can include a microprocessor with CPU 20, memory, interface electronics and conditioning electronics 33 configured to receive a signal from the sensors 14. In one embodiment, all or a portion of the conditioning electronics 33 are at the monitoring device 10.

[0121] In one embodiment, the CPU 20 includes a processor 52, which can be a microprocessor, read only memory used to store instructions that the processor may fetch in executing its program, a random access memory (RAM) used by the processor 52 to store information and a master dock. The microprocessor 52 is controlled by the master clock that provides a master timing signal used to sequence the microprocessor 52 through its internal states in its execution of each processed instruction. In one embodiment, the microprocessor 52, and especially the CPU 20, is a low power device, such as CMOS, as is the necessary logic used to implement the processor design. The telemetry system 32 can store information about the user's activity in memory.

[0122] This memory may be external to the CPU 20 but can reside in the RAM. The memory may be nonvolatile such as battery backed RAM or electrically erasable programmable read only memory (EEPROM). Signals from the sensors 14 can be in communication with conditioning electronics 33 that with a filter 35, with scale and can determine the presence of certain conditions. This conditioning essentially cleans the signal up for processing by CPU 20 and in some cases pre-processes the information. These signals are then passed to interface electronics, which converts the analog voltage or currents to binary ones and zeroes understood by the CPU 20. The telemetry system 32 can also provide for intelligence in the signal processing, such as achieved by the CPU 20 in evaluating historical data.

[0123] In one embodiment, the actions of the user wearing the monitoring device 10 with the unique ID can be used for different activities and can have different classifications at system 32.

[0124] The classification can be in response to the user's location, where the user spends it time, with which the user spends its time, determination of working relationships, family relationships, social relationships, and the like. These last few determinations can be based on the time of day, the types of interactions, comparisons of the amount of time with others, the time of day, a frequency of contact with others, the type of contact with others, the location and type of place where the user is at, and the like. These results are stored in database 18.

[0125] In one embodiment, the user wearing the monitoring device 10 can access this information from any place where data is presented to the user, including but not limited to mobile devices, the WEB, applications program identifiers, and the like.

[0126] As a non-limiting example, the monitoring device 10 communicates with a base station at system 32. The monitoring device 10 can intelligently switch between data transfer and charging based on sensor readout. The monitoring device 10 can represent data based on connected devices.

[0127] In one embodiment, the monitoring device 10 has the capability of providing recommendations, popularity of locations or activities based on acquired data from the user.

[0128] In one embodiment, the monitoring device 10 has the capability of introducing the user to other people or users based on their data and the user's data.

[0129] In one embodiment, the monitoring device 10 can determine emotion of the user.

[0130] In one embodiment, the monitoring device 10 uses incremental data transfer via BLUETOOTH® and the like. The monitoring device 10 can transmit data through the inductive coupling for wireless charging. The user is also able to change the frequency of data transmission.

[0131] The monitoring device 10 can engage in intelligent switching between incremental and full syncing of data based on available communication routes. As a non-limiting example, this can be via cellular networks, WiFi, BLUETOOTH® and the like. In one embodiment, the monitoring device 10 has data storage. As a non-limiting example, storage of telemetry data on monitoring device 10 can be amounts up to about 16 mg.

[0132] In one embodiment, data transferred if it's in a selected proximity of a base station of system 32 or in proximity of an associated connected Network System 101. In one embodiment, the monitoring device 10 has a dynamic change of data capture frequency. The monitoring device 10 can be programmed to instantly change how often it samples any sensor 14 based upon the sensor data. Intelligent data sampling is based on sensor readout.

[0133] The monitoring device 10 can receive firmware updates via a base station 110 of system 32. In one embodiment, the monitoring device 10 presents analyzed data and feedback on a website. In one embodiment, the monitoring device 10's software is based on unique human movement. The monitoring device 10 is able to identify its wearer based on the unique patterns of movement, location check-ins and daily habits of the user.

[0134] In one embodiment, the app can be used on a mobile device, including but not limited to a smart phone and the like.

[0135] In one embodiment, a breakdown of recounting data that has been collecting is presented for analysis of that data. Observation or recommendations can be presented based on historical information and live information. The importance of the data can be based on past user behavior.

[0136] In one embodiment, the monitoring device 10 has artificial intelligence. A wearable device processor 54 implements logic resources that exist on monitoring device 10.

[0137] In one embodiment, monitoring device 10 engages in the routing of user information to third parties based on predefined rules, based on system 32 analyses.

[0138] In one embodiment, monitoring device 10 includes one or more processors 54 that implement intelligent algorithmic processing and transfer of information to third parties. Feedback can be provided to the end user that is based on visual, tactile, gesture information and the like.

[0139] The ID can be sent from the monitoring device 10 in a variety of different transmit modes, which may be provided as part of the firmware or software of an ID or sensor transmitter 14, and which may be utilized selectively during the operation of said sensor transmitter 14, may include "burst" transmit modes, wherein a burst of data information is transmitted, or "parcel" transmit modes, wherein timed data packets of data, which may, as desired, comprise partial data strings, are transmitted, and, if desired, repeated during time intervals. Further, the sensors 14 may have programmed therein diagnostic routines or other test modes which assist during manufacture and use, providing the operator with

operational status and verification information on said sensor/transmitter 14, as needed. Referring to FIG. 4, system 32 includes data base 18 which contains the desired transmitter, sensor, 14 personality data, as well as, the address/device ID bits for each monitoring device 10.

[0140] In one embodiment, the initial programming of the monitoring device 10 for the ID, as well as optionally other personal information of the user, is done securely, as unauthorized future alteration of same thereafter can be utilized as a means of violating system integrity.

[0141] In one embodiment, an inductive field coil is used for programming the sensors 14 and ID of monitoring device 10.

[0142] As illustrated in FIG. 4, the monitoring device 10 can include a sensor 14 with an output that be received by an amplifier 56 and decoded by an I/O decoder 58 to determine I/O logic levels, as well as, both clock and data information 60. Many such methods are commonly available including ratio encoding, Manchester encoding, Non-Return to Zero (NRZ) encoding, or the like; alternatively, a UART type approach can be used. Once so converted, clock and data signals containing the information bits are passed to a memory 62. Any of these connections provides a logical link from the system's database 18 to the sensor 14, ID of the monitoring device 10, as shown in FIG. 5.

[0143] In one embodiment, illustrated in FIG. 5, the system 32 chooses the necessary programmable sensor functions and stores them into database 18. In one embodiment, in order to insure that an unauthorized user cannot connect into and program monitoring device 10 the following procedure may be used:

[0144] Both the sensor 14 and receiver 34 contain an identical, repeatable pseudo randomization algorithm in ROM or in ASIC logic.

[0145] Referring to FIG. 6, the algorithm is applied to outgoing programming data 64 from system 32 and produces a number of security/randomization bits 66 that can be appended to the outgoing programming message or message 68 and sent to a sensor 14.

[0146] Referring to FIG. 7 the sensor 14 likewise applies this pseudo randomization algorithm as the security/randomization bits 66 to the outgoing programming data, now forming the incoming programming data 70 to sensor 14 and produces a several bit result in the shift register 71. The scrambling algorithm is devised such that a small difference in the programming bit stream causes a great difference in the pseudo randomization result. As a non-limiting example, the present invention can use a 16 bit polynomial to produce this pseudo randomization.

[0147] Optionally, in one embodiment, before a sensor 14 accepts this programming, stored in an address and personality register 73, both the pseudo random code, stored in data in a shift register 75 from system 32 and a sensor 14, in a shift register 71 must match via a comparator ID, 77, indicating unauthorized acceptance use. In addition to insuring authorized access, this process also insures that the data itself is correct. The longer the polynomial sequence used, the greater the security.

[0148] In one embodiment, spread spectrum or other RF transmission is used and can include programming to determine that the frequency or spread spectrum code is unique to the area. If a spread spectrum code, system code, or frequency channel is found to be occupied at a future time of use. Re-programming of the monitoring device 10 is then done

with a new, unused spread spectrum code or system code or frequency channel can be selected, or, in the alternative, CPU 20.

[0149] As illustrated in FIG. 5, step "E" would include, for example, the step of the sensor 14, inputting the programming message and saving a seed in memory 62; with the sensor 14 utilizing the seed to code digital data bits transmitted.

[0150] As illustrated in FIG. 8, the location of a monitoring device 10 with the ID and sensors 14 can be determined. As a non-limiting example, in one embodiment the monitoring device 10 includes a sensor 14 that can provide a position signal having positioning data (e.g., raw GPD data or pseudo ranges) and the ID is transmitted from the monitoring device 10 to system server 16. Server 16 receives the position signal and analyzes the signal to generate information representing the location of the monitoring device 10. Server 16 transmits this location information to a client computer where the location of the monitoring device 10, allowing a user to identify the location of the remote sensor 14.

[0151] In one embodiment, the position signal transmitted by the remote sensor 14 can also include an emergency code. For example, in the event of an emergency, such as a medical emergency or otherwise, a user may press a "panic button" that can be on the monitoring device 10 or by use of a user's mobile device. Pressing the panic button may cause mobile device 74 to transmit an emergency signal to a cell site 76 where the emergency signal is relayed to server 16. In response, server 16 can transmit Doppler information regarding in-view satellites, a fix command and a time trigger signal to the monitoring device 10.

[0152] When the location of the monitoring device 10 has been determined, software running on server 16 configures server 16 such that a call or other signal is sent to a local emergency operator in the vicinity of remote sensor 14. When the call or signal is received at the emergency operator station, the location of remote sensor 14 is transmitted and displayed. In some cases, where separate panic buttons are available for identifying medical, police, fire or other types of emergencies, the nature of the emergency is also displayed for the emergency operator. Based on this information, the emergency operator can initiate an emergency response by providing the location of remote sensor 14 to the required emergency service (police, fire department, ambulance service, etc.). In other embodiments, instead of or in addition to a position report for the remote sensor 14, the emergency operator may also be provided with information which identifies an emergency response vehicle in close proximity to remote sensor 14.

[0153] As illustrated in FIG. 9, a sensor 14 of the monitoring device 10 can include a SNAPSHOT GPS receiver 72. As described above, sensor 14 uses information transmitted from separately located base station 110, mobile devices, computers, and other devices, to assist in determining the position of the remote sensor 14, as more fully disclosed in U.S. Pat. No. 6,661,372, incorporated herein by reference.

[0154] As non-limiting examples, and as illustrated in FIG. 10, the sensors 14 can be a thermal transducer 78, an acoustic transducer 80, and a magnetic transducer 82. It will be appreciated that the present invention is not limited. The transducers 78, 80, and 82 in the monitoring device 10 can communicate with a microprocessor 84 also located in the monitoring device 10. The monitoring device 10 can communicate with other devices via an RF transceiver 86, an IRDA transceiver 88, and/or an RF backscatter transceiver 90. Each

of the components in the monitoring device **10** receives power as necessary from the battery **24**, which may include the rechargeable battery.

[0155] The acoustic transducer **80** may include a microphone, a low-pass filter, a gain amplifier, and a threshold comparator. The acoustic transducer **80** may include an omnidirectional microphone, although any other suitable acoustic transducer device would suffice. The microphone may be a surface mount MEMS device that has a frequency range of 100 Hz to 10 kHz. A single MCP602 operational amplifier is used on the acoustic sensor to amplify and low-pass filter the acoustic signal from the microphone. Another operational amplifier is used to generate a voltage reference used for single biasing and detection. The microphone output is biased to the midway point between the circuit supply voltage and ground to allow for both positive and negative signal swings. The biased signal is filtered with a second order low-pass Butterworth filter to remove upper frequency noise. It is then amplified with an adjustable gain that is controlled by a digital resistor potentiometer. This digital resistor operates on an I2C bus and is controlled by the microprocessor **84**. Lastly, the amplified acoustic signal is threshold detected against a static voltage to detect sufficiently large acoustic signals. The digital output of the threshold detector is connected to the microprocessor **84** for processing.

[0156] The magnetic transducer **82** can include a magnetic sensor integrated circuit, a differential instrumentation amplifier, a low-pass filter, two gain amplifiers, and a threshold detector. The magnetic transducer **82** may include an NVE AA002-02 GMR (giant magneto resistive) field sensor, although any suitable magnetic sensor would suffice. This sensor has a saturation field of 15 Oe, a linear range of 0 to 10.5 Oe, and a sensitivity of 3 mVn/Oe. Two MCP602 CMOS operational amplifiers are used on the magnetic sensor to amplify and low-pass filter the analog output signal. An INA122UA instrumentation amplifier is used as a difference amplifier for the differential output from the magnetic sensor. The magnetic sensor IC can be based on Spintronics technology. Its output includes a differential voltage pair proportional to the detected magnetic field. The differential voltage pair is amplified and converted to a single voltage by the instrumentation amplifier. The AC-coupled signal is then amplified and filtered with a low-pass filter to remove upper frequency noise and boost the low-voltage signal output. The signal is amplified a second time by an adjustable gain controlled by a digital resistor similar to the acoustic sensor. Lastly, the amplified magnetic signal is threshold detected against a static voltage, to detect sufficiently large changes in magnetic fields. The digital output of the threshold detector can be connected to the microprocessor **84** for processing.

[0157] A DS1803E-010 digitally controlled 10 kOhm variable resistor can be used in both the acoustic and magnetic sensor circuits. It is used to adjust the gain of one gain stage in each circuit. The digital resistor is controlled through an I2C interface. A LMV393IPWR comparator is also used in both the magnetic and acoustic sensor circuits for determining when a sufficiently strong sensor signal has been detected. It compares the analog sensor signal against the voltage reference and its output is tied to the microprocessor **84** for data collection.

[0158] The thermal transducer **78** may include a Burr Brown TMP 100NA/250 12-bit digital temperature sensor, although any suitable thermal sensor would suffice. The digital temperature sensor has an operating range of -55 to +120

degree C., an accuracy of 0.5 degree C. and a maximum resolution of 0.0625 degree C.

[0159] Even though it is a 12-bit sensor, suitable results are achieved with only 9-bit conversions with only the 8 most significant bits used. The sensor has an I2C interface and is normally kept in sleep mode for low power operation. When directed by the microprocessor **84**, the thermal transducer can perform a 9-bit temperature conversion in 75 milliseconds.

[0160] The RF transceiver **86** may include an RF Monolithic DR3000 transceiver, although any suitable transceiver or separate transmitter and receiver **34** would suffice. This transceiver **86** allows for both digital transmission and reception. The transceiver **86** can have an operating frequency of 916.5 MHz and is capable of baud rates between 2.4 kbps and 19.2 kbps. It can use OOK modulation and has an output power of 0.75 mW. It also can use digital inputs and outputs for direct connection with the microprocessor **84**. The transceiver **86** can use an antenna **92** (FIG. 11) that may include a 17 mil thick plain steel electric guitar G-string cut to a length of 8.18 cm. It is used in a monopole over ground configuration and can require a matching circuit of one inductor and one capacitor. Alternatively, Frequency Shift Keying (FSK), Quadrature Phase Shift Keying (QPSK), or any other suitable modulation scheme may be utilized.

[0161] The IRDA transceiver **88** may include a Sharp GP2W0110YPS infrared transceiver, although any suitable IRDA compliant infrared transceiver would suffice. This transceiver **88** can be IRDA v1.2 compliant and in one embodiment has an operating range of 0.7 meters. In one embodiment, it is capable of 115.2 kbps data speeds.

[0162] The RF backscatter transmission device **90** may include circuitry available from Alien Technology (of Morgan Hill, Calif.) for receiving and transmitting signals via RF backscatter. Battery **24** may be a 3.6 volt ½ AA lithium battery with a capacity of 1.2 amp hours. The battery **24** can be a power source **24** that can include a Texas Instruments TPS76930 DBVT voltage regulator to regulate the output signal to 3 volts and with a maximum current of 100 mA. The voltage regulator can include a LDO.

[0163] The RF backscatter transceiver **86** in the monitoring device **10** communicates with an RF backscatter reader **94** such as a class 3 reader from Alien Technology. The reader **94** transmits data to the backscatter transceiver **90** of the monitoring device **10** by broadcasting encoded RF pulses and receives data back from the transceiver **86** by continually broadcasting RF energy to the sensor **10** and monitoring the modulated RF reflections from the sensor **10**.

[0164] The RF backscatter transceiver **90** can include a printed circuit board (PCB) patch antenna for RF reception, and RF modulation, a Schotky diode detector circuit, a comparator circuit for signal decoding, and a logic circuit for wake-up. The logic circuit monitors the incoming data, and when an appropriate wake-up pattern is detected, it triggers the microprocessor **84** so that data reception can begin. In one embodiment, the reader **94** has an operating frequency between 2402 MHz and 2480 MHz, and uses frequency hopping in this band to reduce noise interference. A modulation method used by the reader **94** can be On-Off Keying (OOK). In one embodiment, the transmission power is 1 watt. The operation of the reader **94** may be controlled by an external computer (not shown) as directed by Labview software via a RS-232 serial link.

[0165] The RF transceiver **86** can communicate with an external RF transceiver **96** such as a DR3000 transceiver from

Radio Monolithics, Inc. In one embodiment, it operates at 916.5 MHz, uses OOK modulation, has a communication range of 100 meters line of sight, and a baud rate of 19.2 kbps. The active RF antenna **92** can be a quarter-wavelength monopole made from a guitar G-string and appropriate matching circuitry. Two control lines from the microprocessor **84** can be used to select the mode of operation, choosing from transmit, receive, and sleep. The active RF receiver **34** consumes the most power in receive mode compared to the other two communication links.

[0166] FIG. 6 shows the relative positioning and shape of the active RF antenna **92** and the RF backscatter antenna **98**.

[0167] The IRDA transceiver **88** of the monitoring device **10** can communicate with an external IRDA transceiver **100** that may be identical to the IRDA transceiver **88**. Alternatively, the IRDA transceiver **100** can be one such as is provided in most personal digital assistants (PDA) as well as many other consumer devices. The IRDA communication link follows the standard IRDA signal and coding protocol and is modeled after a standard UART interface. In one embodiment, the IRDA transceiver **88** is capable of data speeds less than 115.2 kbps, and may only have a range of 0.7 meters for transmission. One advantage of the IRDA communication link is that it does not require any of the RF spectrums for operation, but it typically does require line-of-sight communication.

[0168] When any one of the transceivers **86**, **88** and **90** on the monitoring device **10** detect the beginning of valid data on their respective communication link, all other transceivers are disabled, thereby preventing the corruption of incoming data with the noise or partial data packets on the other communication links. However, if the data on the active transceiver proves to be erroneous, the other transceivers will be re-enabled if appropriate to allow normal operation to continue. If the data received by the active transceiver is valid, however, the other transceivers will remain disabled for several hundred milliseconds longer in the high probability that the next data packet will be transmitted on the same communication link. If, after this extended delay, no additional packets are received, then the other transceivers will be re-enabled as appropriate.

[0169] In one embodiment, the active RF protocol has no wake-up or synchronization packets, and the packets sent to and from the sensor are identical. In one embodiment, the format of an active RF packet is shown in FIG. 2. It can include a preamble to reset and spin-up the state machine of the RF receiver **34** and to properly bias the receiver's **34** data slicer/threshold detector for optimum noise rejection and signal regeneration, two framing bits to indicate the beginning and end of the data bytes, and the data bytes themselves.

[0170] Furthermore, the encoding scheme for the three symbols is shown in FIG. 12. The entire packet is DC balanced to maintain an optimal level on the data slicer/threshold detector and the receiver **34**. Data is sent most significant bit first.

[0171] The IRDA communication link can follow the standard IRDA protocol for bit encoding and UART protocol for byte transmission. Packets transmitted on the IRDA link can contain no preamble or framing bits, but they do have a header that contains two bytes. The first byte is an ASCII "T" which denotes the beginning of a valid IRDA packet. The second byte equals the number of preceding bytes in the packet. This value is used by the receiver **34** to determine when the entire packet has been received and processing of information can

begin. The packet structure is shown in FIG. 13 and the IRDA/UART encoding scheme is shown in FIG. 14.

[0172] The data bytes contained in a packet transmitted to the sensor **10** through any of the communication links conform to a packet format. The CMD section of a packet is a single byte that identifies the type of packet being sent. The CMD byte appears above the beginning and end of the packet and the two must be identical. The reason for including the redundant byte is to further eliminate the chance of a packet's CMD identifier being corrupted at the receiver **34**, even if the CHECKSUM is correct.

[0173] The PAYLOAD contains all of the data that must be sent to, or returned from, the sensor. The PAYLOAD is broken down into individual bytes with the overall number of bytes and their content dependent on the type of packet being sent.

[0174] The CHECKSUM is a 16-bit CRC that is performed on all bytes in the data packet excluding the end CMD byte in packets generated by the external device. The CHECKSUM is sent most significant byte first.

[0175] The transceivers **86**, **88** and **90** may be required to communicate over a greater distance than do the components described herein. Upgrading these components to be suitable for longer distance transmission is considered to be within the spirit of this invention. The type of transducer is not limited to the specific transducer types described herein. In addition, the logic described herein for arbitrating between which communication device to use to communicate with the outside world and which sensor data to provide at what time is but one possible approach to arbitration logic within such a remote sensor **10**.

[0176] FIG. 15 illustrates one embodiment of an exemplary Network System **101** that can be used with the present invention. As shown in FIG. 15 a wireless packet data service Network System **102** that can be utilized with the monitoring device **10**. An enterprise Network System **104**, which may be a packet-switched network, can include one or more geographic sites and be organized as a local area network (LAN), wide area network (WAN) or metropolitan area network (MAN), and the like. One or more application servers **106-1** through **106-N** can be included and disposed as part of the enterprise network **104** are operable to provide or effectuate a host of internal and external services such as email, video mail, Network Systems **101** access, corporate data access, messaging, calendaring and scheduling, information management, and the like using the unique IDs of the wearable devices **10**. The monitoring device **10** can be in communication with a variety of personal information devices other than the monitoring device **10**, including but not limited to, computers, laptop computers, mobile devices, and the like.

[0177] Additionally, system server **16** may be interfaced with the enterprise Network System **104** to access or effectuate any of the services from a remote location using a monitoring device **10**. A secure communication link with end-to-end encryption may be established that is mediated through an external IP network, i.e., a public packet-switched network such as Network Systems **108**, as well as the wireless packet data service Network System **102** operable with a monitoring device **10** via suitable wireless Network System **101** infrastructure that includes a base station (BS) **110**. In one embodiment, a trusted relay Network System **101** **112** may be disposed between Network Systems **108** and the infrastructure of wireless packet data service Network System **102**.

[0178] In another embodiment, the infrastructure of the trusted relay network **112** may be integrated with the wireless

packet data service network **102**, and the functionality of the relay infrastructure can be consolidated as a separate layer within a “one-network” environment. Additionally, as non-limiting examples, monitoring device **10** may be capable of receiving and sending messages, web browsing, interfacing with corporate application servers, and the like, regardless of the relationship between the networks **102** and **112**. Accordingly, a “network node” may include both relay functionality and wireless network infrastructure functionality in some exemplary implementations.

[0179] In one embodiment, the wireless packet data service Network System **102** is implemented in any known or heretofore unknown communications technologies and network protocols, as long as a packet-switched data service is available therein for transmitting packetized information. For instance, the wireless packet data service Network System **102** may be comprised of a General Packet Radio Service (GPRS) network that provides a packet radio access for mobile devices using the cellular infrastructure of a Global System for Mobile Communications (GSM)-based carrier network. In other implementations, the wireless packet data service Network System **102** may comprise an Enhanced Data Rates for GSM Evolution (EDGE) network, an Integrated Digital Enhanced Network (IDEN), a Code Division Multiple Access (CDMA) network, a Universal Mobile Telecommunications System (UMTS) network, or any 3rd Generation (3G) network.

[0180] Referring now to FIGS. **16(a)** through **16(d)**, in one embodiment, the monitoring device **10** is in communication with an interaction engine **120** that can be at a mobile device **74** or system **32**. The interface engine can be a software application running on mobile device **74** associated with another party, including but not limited to a merchant, an associate, a friend, and the like. The enables the monitoring device **10** user and a merchant to interact with a transaction engine **114** to and enter into a financial transaction for the transfer of funds from a third party payment system **116** that is independent of the monitoring device **10** user’s financial account **118**, and complete a transaction. It should be noted that the payment system **116** can be affiliated with the financial account **118** or can be a separate and non-affiliated with the financial account **118**. The interaction engine **120** can take input of information related to a transfer of funds from the monitoring device **10** users’ financial accounts **118** as input to the transaction engine **114** to initiate and complete a financial transaction, including but not limited the purchase and payment of goods and services. In one embodiment, this input to the interaction engine **114** can include, an amount of a transaction, additional items related to the transaction, authorization and/or signature of the monitoring device **10** users.

[0181] In one embodiment, the mobile device **74** receives information from the monitoring device **10**, e.g., the unique ID.

[0182] The interaction engine **120** can also present products or services provided by a merchant to directly to or through system **32** to the monitoring device **10** user. In one embodiment, the monitoring device **10** users can use the mobile device **74**, the WEB, and the like, to view, text, pictures, audio, and videos, and browse through the products and services on the mobile device **74**, personal computers, other communication devices, the WEB, and anything that is BLUETOOTH®, anything associated with Network Systems **101**, and the like.

[0183] In one embodiment, the transaction engine **114**, which can be at the mobile device **74**, or external to the mobile device **74**, including but not limited to monitoring device **10** and the like, takes decoded financial transaction card information from a decoding engine **122**, internal or external to the mobile device **74**, and a transaction amount from an interaction engine **120**, also internal or external to the mobile device. The transaction engine **114** then contacts the payment service **116**, and or the monitoring device **10** users’ financial account **118**, such as an acquiring bank that handles such authorization request, directly or through the payment system **116**, which may then communicate with a financial transaction card issuing bank to either authorize or deny the transaction. The payment system **116** can include a user database, a transaction database, a product database, and the like. These databases can also be external to payment system **116**. If the third party authorizes the transaction, then the transaction engine **114** transfers funds deducted from the account of the monitoring device **10** user, or the payment system **116** can already have those funds readily available, to an account of a third party which can be another monitoring device **10** user, a merchant, and the like, and provides transaction or transfer of fund results to the interaction engine **120** for presentation to a third party.

[0184] In one embodiment, the transaction engine **114** does not have the financial account or financial card information of the monitoring device **10** user that is doing the transfer. In some embodiments, the transaction engine **114** keeps only selected information of the monitoring device **10** user’s financial accounts **118** or financial transaction cards.

[0185] In one embodiment, the wearable device communicates directly, without mobile device **74**, with the payment system **116** and/or the user’s financial account **118** or associated financial institution.

[0186] In one embodiment, the transaction engine **114** communicates and interacts with the financial account **118** or associated financial institution directly or through the payment system **116**, through a user database, product database, and transaction database, which databases can be separate from or included in the payment system **116**, over a Network System **101**. The Network System **101** can be a communication network, as recited above, and can be based on well-known communication protocols, including but not limited to, a TCP/IP protocol.

[0187] With social networking applications, the monitoring device **10**, with its unique ID, is an ID device. Information from the monitoring device **10** relating to social networking, and the like, communicates with system **32**. In this manner, the wearable devices **10**, with their own unique ID’s, can be recognized. This can occur at different locations, close by, distanced, and notifications can be sent to the different users wearing a monitoring device **10** for a variety of social networking and other communication applications. Additionally, monitoring device **10**, with its sensors **14** and ID can communicate directly to social networking sites, Network System **101** Systems, cloud services, and the like.

[0188] In one embodiment, with the current permissions given by the wearable device users, marketers, companies or individuals who wish can deliver advertisement monitoring device **10** users. More particularly, system **32** can be configured to allow marketers, and the like, to deliver advertisements to consumers to buy products or services offered by the marketer. Advertisements can also be sent to monitoring device **10** users with the appropriate permissions. In one

embodiment, system 32 maintains the anonymity of the monitoring device 10 users while allowing the marketers to have their advertisements delivered to those that fall within their defined market segment.

[0189] In one embodiment, the wearable device ID of a user provides a method of identifying and contacting users of a social networking service. The method may include the steps of signing up for a social networking service, displaying the wearable device ID, viewing another person's unique wearable device ID displayed by another user, and finding that user on a social networking service website by searching for the user using the wearable device ID viewed.

[0190] System 32 may serve a number of purposes without straying from the scope of the present invention. For example, the social networking service may allow monitoring device 10 users to engage in non-romantic relationships, keep in touch with acquaintances, friends and family, professional business relationships, and romantic relationships, may allow communication between wearable device users on a message board or Network Systems 101 forum, and may allow users to follow up on missed-connections that otherwise would not have been realized.

[0191] In one embodiment, the step of providing personal information to start an account with system 10 for different applications may be performed by a purchasing or acquiring a monitoring device 10, with a unique assigned ID, and the user can fill in an online form. This form may require users to fill in fields on the form. These fields may include: first and last name, email address, a desired password, phone number, gender, birth date, address, geographic region, education information, employment information, interests, relationship information and interests, family information, religious views, ethnicity, physical features including hair color, eye color, measurements, and the like, type of relationship being sought, living situation, answers to quiz questions, and a personal description about interesting personality traits, among other things. In addition, users may upload one or a plurality of photographs for other users to view, or for users to store the photo or photos on the server of system 32.

[0192] In another embodiment the step of providing personal information to start an account with system 32 by monitoring device 10 users may be performed automatically. In this embodiment, system 32 can access a social networking service, access, via computer, contact lists or other sources of information that may include the type of information listed above.

[0193] In a further embodiment, the step of providing personal information to system 32 can be automated by importing data containing the personal information required from other social networking services including but not limited to Facebook®, LinkedIn®, MySpace®, Match.com®, eHarmony.com®, a user's email or contact list, v-card, and the like.

[0194] The unique wearable device ID may allow the user to be searched and identified by other users and potential users. Also, a computer generated email address may be provided to a user. In one embodiment, this email address may be the user's user ID followed by "@iseenya.com." In another embodiment, the email address may be the user's user ID directed to another domain name.

[0195] In one embodiment, a computer generated personal page may be provided to a monitoring device 10 user. The personal page may utilize a computer to automatically import the information provided when signing up with system 32 or

a social networking service. In another embodiment, the information and formatting of the personal page can be customizable.

[0196] When mobile device 74 is used, it communicates with one or more sensors 14 that are at the monitoring device 10, as more fully herein. The mobile device can 74 pull from system 32 updates from the server 16, including but not limited to settings such as alarms, name of the wearable device wearer using the ID, a sensor 14 and the like. Sensors 14 at the monitoring device 10 can send streams of information, both encrypted and non-encrypted to the mobile device and then to the server at system 32. Server 16 sends encrypted, and can also send non-encrypted information, to mobile device 74. Processing of this information can be achieved at the mobile device 74, and/or server 16. Mobile device 74 can receive raw sensor information from the monitoring device 10. This information can be compressed as well as non-compressed. A compression algorithm, at the wearable device and/or mobile device 74 or system 32, can be used in order to minimize the amount of information that server 16 sends. System 32 can include additional encryption and/or decryption systems.

[0197] Referring now to FIG. 17, a social network circle/group 124 (hereinafter "SNET circle") comprising social devices 126, including monitoring device 10, is shown. Beyond traditional social networking features and services, a SNET circle 124 and associated social devices 124 according to various embodiments of the invention include numerous novel features and attributes as described more fully below with general reference to the illustration. Monitoring device 10 can utilize network 101 for communication with the SNET circle, as well as with other social networking sites, or through system 32.

[0198] Briefly, membership in the SNET circle 124 may comprise docked and undocked social devices 124 and human SNET circle members [104] 128, as well as proxies thereof. Further, SNET circle 124 nodes may include device services and software (e.g., applications) of various types participating as members. By way of example, SNET circle members might include artificial intelligence agents/social robots 130, SNET security device(s) 132, appliances, vehicles and service providers 134, common or authorized members/functionality of other SNET circles 124, and the like. Further, access to specific content and resources of a SNET circle 124 may be shared with members of additional SNET(s) 124, including remote or web-based applications. Such access can be conditioned on acceptable profiling and association data. Similarly, social devices or individuals may be granted temporary or ad hoc memberships, with or without restricted access.

[0199] In the illustrated embodiment, formation, maintenance and operation of SNET circle 124 is performed by standalone or distributed SNET processing circuitry and software 136. It is noted that the "SNET processing circuitry" may comprise hardware, software, applications, or various combinations thereof, and be configurable to support various functionalities disclosed herein. Further, the SNET processing circuitry 136 may be included in a standalone server, server farm, cloud-based resources, Network System 101, system 32 and/or the various types of devices described below, and incorporate authentication and security functionality 138. In addition, specialized middleware may also be utilized by SNETs according to the invention, including standardized middleware with an associated certification process.

Interactions and interdependencies within the SNET circle **124** may involve one or more of a social device association/control module **140**, a SNET circle member profiling module **142**, and an adaptive resource allocation and arbitration module **144** as described more fully below.

[0200] Distribution of internal and external SNET content/media **146** can be accomplished in a variety of ways in accordance with various embodiments of the invention. For example, media distribution may involve an adaptive or parallel Network System **101** routing infrastructure involving a wide variety of communication protocols and wired and/or wireless communications channels. SNET content/media **146** may comprise, for example, various user-driven (advertising) channels, pictures, videos, links, online text, etc. Access to such content, as well as communications with and remote access to social devices **124** of the SNET circle **124**, may occur over a Network Systems backbone **148**, cellular communication system, WAN, LAN, and the like.

[0201] FIG. **18** illustrates an embodiment of a social group **150** comprising a variety of members in accordance with the present invention that can communicate through their wearable devices **10** and other devices, including but not limited to mobile devices **74**. In this embodiment, membership in the social group **150** may include a variety of novel social system members [0204] **152** functioning in various capacities within the social group **150**. As will be understood, certain of the social system members **152** may support direct or indirect associations between the social group **150** and human members/non-members and users **154**.

[0202] In the illustrated embodiment, social system members (or nodes) **152** include one or more local or remote servers and server clusters that provide a support infrastructure for social group functionality and member operations (routing, data storage, services, etc.). Communications within the social group and with non-members may occur via dedicated or multi-function communication path devices.

[0203] Social system members **152** further include devices configured to operate as nodes within the social group **150**. Social functionality in such devices and other social system members **152** can be implemented through various means. For example, a device may have integral hardware/firmware/software to support social group access and member operations. Alternatively, a general purpose device **152a** may include social code that enables participation in the social group **150**. In a further embodiment, a device **152b** designed to include social functionality may participate in the social group **150** through a combination of non-social code and a social shim layer or driver wrapper. In yet another embodiment, a member device **152c** having a social design may utilize additional social code, including code specific to a social group **150**.

[0204] Participation in the social group **150** is supported through functionality that includes automated and member-triggered membership invitations and processing (membership management) **156**. More particularly, membership management **156** may function to invite prospective members to participate in the social group **150** through automatic, automated and member-triggered processes. For example, membership management **156** might be configured by a human user **154** to establish a social group **150** by automatically inviting/accepting social system members having certain characteristics (such as devices owned or controlled by the user or acquaintances of the user).

[0205] Processing of accepted invitations and unsolicited requests to join the social group **150** may be conditioned upon input or authorization from an existing social system member (s) **152** or human user(s) **154** (e.g., through a user interface). Similarly, membership management **156** may be configured to generate automated suggestions regarding which prospective members receive an invitation. Various other approaches, such as those described herein, can be used to establish membership in accordance with the invention.

[0206] Access to and visibility of resources of a social group **150**, including services and data, may be managed through general and member class-specific access configurations **158**. For example, if membership in the social group **150** includes family members and associated devices, a uniform access configuration (or separate device and human configurations) could be applied across the class in an automatic or automated manner. In other embodiments, access control and constraints are imposed on a per-member basis.

[0207] The social group **150** may offer a wide variety of member services **162**, including both internal and external services accessible by social system members **152**. By way of example, the social group **150** may offer email or other communication services between full members and/or authorized guest members and visitors. As with other resources of the social group **150**, access control and constraints on member services **162** may be applied to individual members or classes of members.

[0208] FIG. **19** is a functional block diagram illustrating a social network (SNET) infrastructure **164**, as more fully described and disclosed in EP 2582116, fully incorporated herein by reference.

[0209] In one embodiment, illustrated in FIG. **20**, wearable devices **10** are in communication with a distributed computer network **166** that can include networks **102**, **104**, **112**, coupled to Network Systems **108** and system **32** via a plurality of communication links **168**. Communication network **166** provides a mechanism for communication with system **16**, monitoring device **10**, social media networks, mobile devices **74**, payment systems, **116**, the engines **114**, **120**, **122**, components of system **16**, and with all third parties, as described above.

[0210] The communication network **166** may itself be comprised of many interconnected computer systems and communication links. Communication links **168** may be hardware links, optical links, satellite or other wireless communications links, wave propagation links, or any other mechanisms for communication of information. Various communication protocols may be used to facilitate communication between the various systems shown in FIG. **20**. These communication protocols may include TCP/IP, HTTP protocols, wireless application protocol (WAP), vendor-specific protocols, customized protocols, and others.

[0211] While in one embodiment, communication network **166** is the Network System **101**, in other embodiments, communication network **166** may be any suitable communication network **166** including a local area network (LAN), a wide area network (WAN), a wireless network, an intranet, a private network, a public network, a switched network, and combinations of these, and the like.

[0212] System **32** is responsible for receiving information requests from wearable devices **10**, third parties, and the like, performing processing required satisfying the requests, and for forwarding the results corresponding to the requests back to the requesting monitoring device **10** and other systems.

The processing required to satisfy the request may be performed by server 16 or may alternatively be delegated to other servers connected to communication network 166.

[0213] FIG. 21 shows an exemplary computer system that can be utilized with the wearable devices 10. In an embodiment, a user interfaces with system 32 using a monitoring device 10 and then through a computer workstation system, such as shown in FIG. 21, a mobile device, and the like.

[0214] The communication network 166 may be the Network System 101, among other things. The network may be a wireless, a wired network (e.g., using copper), telephone network, packet network, an optical network (e.g., using optical fiber), or a wireless network, or any combination of these. For example, data and other information may be passed between the computer and components (or steps) of a system of the invention using a wireless network using a protocol such as Wi-Fi (IEEE standards 802.11, 802.11a, 802.11b, 802.11e, 802.11g, 802.11i, 802.11n, and 802.11ac, just to name a few examples), near field communication (NFC), radio-frequency identification (RFID), mobile or cellular wireless (e.g., 2G, 3G, 4G, 3GPP LTE, WiMAX, LTE, Flash-OFDM, HIPERMAN, iBurst, EDGE Evolution, UMTS, UMTS-TDD, IxRDD, and EV-DO). For example, signals from a computer may be transferred, at least in part, wirelessly to components or other computers.

[0215] FIG. 22 shows a system for activity collection and building a social graph for network monitoring device 10 users. The system monitors users as they surf the Web, their activities, locations, status, interests, and other things. This can be achieved without regard to whether the wearable device users 10 are logged into a membership site, such as a social networking site.

[0216] Resources 170 and 172 gather activity data and pass this data to an activity storage server 174, typically via Network Systems 108. Partner resource 172 may be processed by a partner back end, and then this data is passed to activity storage server 174.

[0217] Monitoring device 10 users can use social media sharing application or sites. Applications (e.g., a mobile device app or sites allow sharing of information with others. These can be used to collect activity data. A monitoring device 10 user (sender) can share information (e.g., video, photo, link, article, or other) by posting to a site. The monitoring device 10 user can post directly on the site or use an application program, such as a mobile application on a smartphone or tablet computer. When another user (recipient) clicks or vies the link, there is connection activity between the sender and recipient. This activity data is captured by system 32.

[0218] Messenger applications such as those on mobile device 74 or sites can allow Network Systems or Web messaging with others. Network Systems messaging is different from short messaging server (SMS) or text messaging. Messenger applications can be used to collect sharing activity data.

[0219] Users use messenger application to send links and other information to other users, and also achieve this using their wearable devices 10. A user (sender) can copy a link (e.g., via a clipboard) and send to one or more users via the messenger application with mobile device 74 and with its monitoring device 10. When a recipient user clicks on the link, there is connection activity between the sender and recipient for that link.

[0220] Sharing activity data can be captured as described above. There can be different data collectors for different devices and platforms. The activity data is transmitted to and stored at activity storage server 174, typically through Network Systems. Server 174 stores the data for further processing. There can be a significant amount of real-time data that is collected for processing. Distributed computing and processing can be used to process the data.

[0221] The activity data collected is stored at server 174, usually in a database or file systems on hard drives of server 174. There may be many terabytes of data that need are to be processed. Taking the stored activity data as input is a build-update graph component (e.g., executable code running on one or more servers or other computers). Build-update graph component 178 can run on the same server that stores the activity data, or may run on a separate server that accesses storage server 174.

[0222] In one embodiment, a build-update graph 180 builds or updates a social graph using the collected activity data. The social graph can be stored in one or more databases or file systems. In one embodiment, build-update graph 180 can include three components: (1) identify nodes and edges for social graph that need to be updated, (2) create new nodes/edges if nodes/edges are not found, and (3) update values associated with nodes and edges.

[0223] For the incoming activity data collected, identify nodes 182 scan through and find the nodes and edges of the social graph that need to be updated.

[0224] When system 32 is processing a user activity data it has the ID of the monitoring device 10 user and attributes this activity to that monitoring device 10 user.

[0225] When a node or edge is found, update values update the node or an edge (e.g., associated with the node). When a node or edge is not found, a new node or edge is created in the graph. The result of build/update graph is a social graph 184 with nodes modeling user profiles and edge modeling sharing activities among users.

[0226] FIG. 23 shows a sample social graph 186 where circles 188 represent nodes and lines are edges 190 representing sharing interactions between nodes 182. There can be one or more edges 190 between two nodes 182. Several edges 190 between nodes 182 can indicate sharing activities along several categories: e.g., travel, computers, sports, and others.

[0227] Nodes 182 connected together directly have one degree of separation. Nodes 182 connected through one other node have two degrees of separation. Depending on a number of intervening nodes 182 between two nodes 182, this will be a number of degrees of separation between the two nodes 182.

[0228] In a specific implementation, edges 190 between nodes 182 indicate sharing activities along several categories such as travel, computers, sports, and the like. For each additional new sharing category, an additional edge 190 is added. In a specific implementation, for each additional new sharing interest category, an additional edge 190 is added. Further, in an implementation, the sharing interaction or edges 190 between the nodes 182 can be weighted (e.g., weighting in a range from 0 to 1), so that certain types of sharing interactions are given different significance. Weight can be used to represent a relative strength of interaction related to a particular interest category.

[0229] Some types of sharing activities that are tracked for the social graph (or share graph) include: sending messages between users; sending files between users; sending videos between users; sending an e-mail (e.g., Web e-mail) with a

link from one user to another such as sharing a link to various social media sites; and sending instant messages between users. For mobile devices **74** the sharing activities can further include: sending SMS-type messages between users. In some embodiments, messages can be sending from wearable devices **10**.

[0230] Once two users connect, such as one monitoring device **10** sending another monitoring device **10** user a message containing a link concerning a topic. When the recipient user clicks on the link from the sender user, system **32** will add an edge **190** to graph **186** to represent the activity. An edge **190** is added to the graph **186** to represent this sharing activity between the two users.

[0231] In a specific implementation, two monitoring device **10** users are connected when one user (sender) shares information with another user or group and the other user (recipient) consumes the information that was sent (e.g., clicked-back on the shared link, opened an attachment, opened a message). For example, simply placing a link on Facebook® wall so that all Facebook® “friends” can see this link or tweeting a link to Twitter® followers will not create a connection between the sender, or sharer, and people in the graph. This would create significant noise in the system. The connections are created between the sender and only those users who clicked back on (or otherwise consumed) the message.

[0232] In one embodiment, more recently sent messages are given a greater weight than older messages.

[0233] Referring now to FIG. **24**, in one embodiment, telemetry system **32** monitors and provides firmware updates to a plurality of monitoring devices **10** that are programmed to report location, data and/or status periodically, in response to an event, or in response to a request by telemetry system **32**. The monitoring devices **10** through a Network System **101** (not shown) are in communication with a control or monitoring center **192** which collects the location and/or status data for each of all or a selected portion of the monitoring devices **10**.

[0234] When programming, software, firmware, configuration or similar updates are available for the monitoring devices **10**, the control center **192** collects those firmware updates and the identity of the monitoring devices **10** requiring those updates and stores that information. Separate databases may be employed for the updates **194** and the monitoring device **10** update status **196**, or the databases may be combined. Users can access control center **192** to upload updates, check on the status of their monitoring device **10** or to retrieve location, data and reporting information related to the monitoring devices **10**. The control center **192** can then attempt to contact each mobile device requiring the update or can wait until it receives a message from each monitoring device **10**. Once the control center **192** establishes contact, it initializes the firmware update process and begins sending the update to each monitoring device **10** to which contact has been established. Once a monitoring device **10** receives the entire update and has installed it, it can send a confirmation to the control center **192** which is then noted in the MU update database **196**. If the confirmation is not received, for instance because a communication link was broken and the entire update was not received, the control center **192** tries to re-contact each non-updated monitoring device **10** and each monitoring device **10** to which the control center **192** has not yet made contact.

[0235] For each monitoring device **10** that has received and confirmed the update, the MU update database **196** is updated

to reflect that the monitoring device **10** is up to date. The control center **192** continues this process until each of the monitoring devices **10** has confirmed the installation of the updated firmware. The users of each monitoring device **10** can be sent reports reflecting the status of the software update process. While a particular number of monitoring devices **10** are represented in FIG. **24**, any number of monitoring devices **10** can be accommodated using the concepts described herein.

[0236] FIG. **25** discloses one embodiment of monitoring device **10**, with the ID or asset tag **196**. The tag **196** can include microprocessor **84** programmable to execute desired instructions and to control the operation of tag **196**. The microprocessor **84** may have internal memory capable of storing data and programming information or may use memory external to the microprocessor **84**. The tag **196** can also include a cellular transceiver and associated cellular antenna to perform cellular communications. Power for the cellular transceiver is supplied by a power system or battery **24**. The tag **196** can also include a satellite location determination device, which can be GPS or satellite service based, and a satellite transmitter, receiver or transceiver, which can use a satellite antenna.

[0237] As described, communications with the control center **192** can be done using satellite, Network System **101** or other long range communication systems. Sensors **10** can be embedded in or connected to the monitoring device **10**, as described above. A reed switch **207** is an electrical switch that is activated by a magnetic field and can be used to enable or disable the monitoring device **10**.

[0238] Referring now to FIG. **26**, a flow chart of an embodiment of a method **198** for updating the software, firmware programming, configuration, or similar updates for remote devices/monitoring devices **10** is described. The method begins in decision block **200** by detecting an available update for one or more of a plurality of monitoring devices **10**, each of the monitoring devices geographically distributed from the control center **192**. The control center **192** then attempts to contact each monitoring device **10**, as shown by block **202**, or waits to be contacted by each monitoring device **10**. Particular monitoring devices **10** may be initially unavailable to the control center by being out of range or unable to establish a good communications link.

[0239] Decision block **204** determines whether individual units have contacted the control center. If a unit has not contacted the control center the method can either wait or return to block **202** where the control center re-contacts the monitoring device **10**.

[0240] Once a particular monitoring device **10** has been contacted, the control center **192** sends the update to that monitoring device **10** to be installed by the monitoring device **10**, as shown by block **206**. Once finished, the monitoring device **10** confirms completion as shown by block **208** of the installation and returns to normal operation. If the update is not confirmed by the monitoring device **10** having been installed, the method returns to block **202** to re-attempt the update. The update may fail for a variety of reasons, including loss of communications contact with the control center, or interruption due to events at the monitoring device **10**. Once the update has been confirmed at that monitoring device **10**, the MU update database at the control center is updated to reflect the completion of the update for that monitoring device **10**, as shown by block **210**.

[0241] The control center 192 periodically checks to see if all the monitoring devices 10 required to install the update have been complete, as shown by block 212, and if not, determines the remaining monitoring devices 10 to be updated, block 214, and attempts to contact those monitoring devices 10 to complete the update process. While method 198 illustrates one embodiment of the update process, one skilled in the art would recognize that variations on the process can be implemented without departing from the scope of the present invention.

[0242] In one embodiment of the present invention a wireless transmission or charging system 300 is provided that can be part of or distinct from telemetry system, as illustrated in FIG. 27. System 300 is in communication with monitoring devices 10, and also with telemetry system 32 when it is separate from telemetry system 32. Input power 302 is provided to a transmitter 304 for generating a radiated field 306 for providing energy transfer. A receiver 308 couples to the radiated field 306 and generates an output power 310 for storing or consumption by a device (not shown) coupled to the output power 310. Both the transmitter 304 and the receiver 308 are separated by a distance 312. In one exemplary embodiment, transmitter 304 and receiver 308 are configured according to a mutual resonant relationship and when the resonant frequency of receiver 308 and the resonant frequency of transmitter 304 are very close, transmission losses between the transmitter 304 and the receiver 308 are minimal when the receiver 308 is located in the “near-field” of the radiated field 306.

[0243] Transmitter 304 can include a transmit antenna 314 for providing a means for energy transmission and receiver 308 further includes a receive antenna 318 for providing a means for energy reception. The transmit and receive antennas are sized according to applications and devices to be associated therewith. An efficient energy transfer can occur by coupling a large portion of the energy in the near-field of the transmitting antenna to a receiving antenna rather than propagating most of the energy in an electromagnetic wave to the far field. When in this near-field a coupling mode may be developed between the transmit antenna 314 and the receive antenna 318. The area around the antennas 314 and 318 where this near-field coupling may occur is referred to herein as a coupling-mode region.

[0244] Referring to FIG. 28, the transmitter 304 can include an oscillator 322, a power amplifier 324 and a filter and matching circuit 326. The oscillator is configured to generate a desired frequency, which may be adjusted in response to adjustment signal 323. The oscillator signal may be amplified by the power amplifier 324 with an amplification amount responsive to control signal 325. The filter and matching circuit 326 may be included to filter out harmonics or other unwanted frequencies and match the impedance of the transmitter 304 to the transmit antenna 314.

[0245] The receiver 308 may include a matching circuit 332 and a rectifier and switching circuit 334 to generate a DC power output to charge a battery 336 as shown in FIG. 28 or power a device coupled to the receiver (not shown). The rectifier and switching circuit 334 shown receives a control signal 335. The matching circuit 332 may be included to match the impedance of the receiver 308 to the receive antenna 318. The receiver 308 and transmitter 304 may communicate on a separate communication channel 319.

[0246] As illustrated in FIG. 29, antennas can be utilized as a “loop” antenna 350, which may also be referred to herein as

a “magnetic” antenna. Loop antennas may be configured to include an air core or a physical core such as a ferrite core. Air core loop antennas may be more tolerable to extraneous physical devices placed in the vicinity of the core. Furthermore, an air core loop antenna allows the placement of other components within the core area. In addition, an air core loop may more readily enable placement of the receive antenna 318 (FIG. 28) within a plane of the transmit antenna 314 (FIG. 28) where the coupled-mode region of the transmit antenna 314 (FIG. 28) may be more powerful.

[0247] In one embodiment, efficient transfer of energy between the transmitter 304 and receiver 308 occurs during matched or nearly matched resonance between the transmitter 304 and the receiver 308. However, even when resonance between the transmitter 304 and receiver 308 are not matched, energy may be transferred at a lower efficiency. Transfer of energy can be by coupling energy from the near-field of the transmitting antenna to the receiving antenna residing in the neighborhood where this near-field is established rather than propagating the energy from the transmitting antenna into free space.

[0248] The resonant frequency of the loop or magnetic antennas is based on the inductance and capacitance. Inductance in a loop antenna is generally simply the inductance created by the loop, whereas, capacitance is generally added to the loop antenna’s inductance to create a resonant structure at a desired resonant frequency. As a non-limiting example, capacitor 352 and capacitor 354 may be added to the antenna to create a resonant circuit that generates resonant signal 356. Accordingly, for larger diameter loop antennas, the size of capacitance needed to induce resonance decreases as the diameter or inductance of the loop increases. Furthermore, as the diameter of the loop or magnetic antenna increases, the efficient energy transfer area of the near-field increases. Of course, other resonant circuits are possible. As another non-limiting example, a capacitor may be placed in parallel between the two terminals of the loop antenna. In addition, those of ordinary skill in the art will recognize that for transmit antennas the resonant signal 356 may be an input to the loop antenna 350.

[0249] In some embodiments, power is coupled between two antennas that are in the near-fields of each other. The near-field is an area around the antenna in which electromagnetic fields exist but may not propagate or radiate away from the antenna. They can be confined to a volume that is near the physical volume of the antenna. As non-limiting examples, magnetic type antennas such as single and multi-turn loop antennas can be used for both transmit (Tx) and receive (Rx) antenna systems since magnetic near-field amplitudes tend to be higher for magnetic type antennas in comparison to the electric near-fields of an electric-type antenna (e.g., a small dipole). This can provide higher coupling between the pair. Furthermore, “electric” antennas (e.g., dipoles and monopoles) or a combination of magnetic and electric antennas is also contemplated.

[0250] The Tx antenna can be operated at a frequency that is low enough and with an antenna size that is large enough to achieve good coupling (e.g., >-4 dB) to a small receive antenna at significantly larger distances than allowed by far field and inductive approaches mentioned earlier. If the transmit antenna is sized correctly, high coupling levels (e.g., -1 to -4 dB) can be achieved when the receive antenna on a host device is placed within a coupling-mode region (i.e., in the near-field) of the driven transmit loop antenna.

[0251] FIG. 30 illustrates an embodiment of a transmitter 400 that can be utilized the transmitter 400 includes transmit circuitry 402 and a transmit antenna 404. Generally, transmit circuitry 402 provides RF power to the transmit antenna 404 by providing an oscillating signal resulting in generation of near-field energy about the transmit antenna 404. By way of example, transmitter 400 may operate at the 13.56 MHz ISM band.

[0252] In one embodiment, transmit circuitry 402 includes a fixed impedance matching circuit 406 for matching the impedance of the transmit circuitry 402 (e.g., 50 ohms) to the transmit antenna 404 and a low pass filter (LPF) 408 configured to reduce harmonic emissions to levels to prevent self-jamming of devices coupled to receivers 308 (FIG. 27). In other embodiments of the matching circuit can include inductors and transformers. In one embodiment, the low pass filter has different filter topologies, including but not limited to, notch filters that attenuate specific frequencies while passing others and may include an adaptive impedance match, that can be varied based on measurable transmit metrics, such as output power to the antenna or DC current draw by the power amplifier.

[0253] Transmit circuitry 402 can include a power amplifier 410 that drives an RF signal as determined by an oscillator 412 (also referred to herein as a signal generator). The transmit circuitry may be comprised of discrete devices or circuits, or alternately, may be comprised of an integrated assembly. An exemplary RF power output from transmit antenna 404 may be on the order of 2.5 to 8.0 Watts.

[0254] Transmit circuitry 402 can include a controller 414 for enabling the oscillator 412 during transmit phases (or duty cycles) for specific receivers, for adjusting the frequency of the oscillator, for adjusting the output power level, for implementing a communication protocol for interacting with neighboring devices through their attached receivers. The controller 414 is also for determining impedance changes at the transmit antenna 404 due to changes in the coupling-mode region due to receivers placed therein.

[0255] The transmit circuitry 402 can include a load sensing circuit 416 for detecting the presence or absence of active receivers in the vicinity of the near-field generated by transmit antenna 404. By way of example, a load sensing circuit 416 monitors the current flowing to the power amplifier 410, which is affected by the presence or absence of active receivers in the vicinity of the near-field generated by transmit antenna 404. Detection of changes to the loading on the power amplifier 410 are monitored by controller 414 for use in determining whether to enable the oscillator 412 for transmitting energy to communicate with an active receiver.

[0256] Transmit antenna 404 can be an antenna strip with a thickness, width and metal type selected to keep resistive losses low. The transmitter 400 may gather and track information about the whereabouts and status of receiver devices that may be associated with the transmitter 400. Thus, the transmitter circuitry 402 may include a presence detector 480, an enclosed detector 490, or a combination thereof, connected to the controller 414 (also referred to as a processor herein). The controller 414 may adjust an amount of power delivered by the amplifier 410 in response to presence signals from the presence detector 480 and the enclosed detector 490. The transmitter can receive power through a number of power sources, including but not limited to, an AC-DC converter to convert conventional AC power present in a building, a DC-DC converter to convert a conventional DC power source to a

voltage suitable for the transmitter 400, or directly from a conventional DC power source.

[0257] In one embodiment, the presence detector 480 can be a motion detector utilized to sense the initial presence of a device to be charged that is inserted into the coverage area of the transmitter. After detection, the transmitter may be turned on and the RF power received by the device may be used to toggle a switch on the receiver device in a pre-determined manner, which in turn results in changes to the driving point impedance of the transmitter.

[0258] In one embodiment, the presence detector 480 is a detector capable of detecting a human, for example, by infrared detection, motion detection, or other suitable means. In various embodiments, regulations can be provided that limit an amount of power that a transmit antenna can transmit at a specific frequency.

[0259] As a non-limiting example, the enclosed detector 490 (may also be referred to herein as an enclosed compartment detector or an enclosed space detector) may be a device such as a sense switch for determining when an enclosure is in a closed or open state. When a transmitter is in an enclosure that is in an enclosed state, a power level of the transmitter may be increased.

[0260] As illustrated in FIG. 31, a receiver 500 includes receive circuitry 502 and a receive antenna 504. Receiver 500 further couples to device 550 for providing received power thereto. It should be noted that receiver 500 is illustrated as being external to device 550 but may be integrated into device 550. Generally, energy is propagated wirelessly to receive antenna 504 and then coupled through receive circuitry 502 to device 550.

[0261] The receive antenna 504 is tuned to resonate at the same frequency, or near the same frequency, as transmit antenna 404 (FIG. 30). Receive antenna 504 may be similarly dimensioned with transmit antenna 404 or may be differently sized based upon the dimensions of the associated device 550. By way of example, device 550 may be a portable electronic device having diametric or length dimension smaller than the diameter of length of transmit antenna 404. In such an example, receive antenna 504 may be implemented as a multi-turn antenna in order to reduce the capacitance value of a tuning capacitor (not shown) and increase the receive antenna's impedance. By way of example, receive antenna 504 may be placed around the substantial circumference of device 550 in order to maximize the antenna diameter and reduce the number of loop turns (i.e., windings) of the receive antenna and the inter-winding capacitance.

[0262] Receive circuitry 502 provides an impedance match to the receive antenna 504. Receive circuitry 502 includes power conversion circuitry 506 for converting a received RF energy source into charging power for use by device 550. Power conversion circuitry 506 includes an RF-to-DC converter 508 and may also include a DC-to-DC converter 510. RF-to-DC converter 508 rectifies the RF energy signal received at receive antenna 504 into a non-alternating power while DC-to-DC converter 510 converts the rectified RF energy signal into an energy potential (e.g., voltage) that is compatible with device 550. Various RF-to-DC converters are contemplated, including partial and full rectifiers, regulators, bridges, doublers, as well as linear and switching converters.

[0263] Receive circuitry 502 may further include switching circuitry 512 for connecting receive antenna 504 to the power conversion circuitry 506 or alternatively for disconnecting the power conversion circuitry 506. Disconnecting receive

antenna 504 from power conversion circuitry 506 not only suspends charging of device 550, but also changes the “load” as “seen” by the transmitter 200 (FIG. 28), which can be used to “cloak” the receiver from the transmitter.

[0264] As disclosed above, transmitter 400 includes load sensing circuit 416 which detects fluctuations in the bias current provided to transmitter power amplifier 410. Accordingly, transmitter 400 has a mechanism for determining when receivers are present in the transmitter’s near-field.

[0265] In an exemplary embodiment, communication between the transmitter and the receiver refers to a device sensing and charging control mechanism, rather than conventional two-way communication. In other words, the transmitter uses on/off keying of the transmitted signal to adjust whether energy is available in the near-field. The receivers interpret these changes in energy as a message from the transmitter. From the receiver side, the receiver uses tuning and de-tuning of the receive antenna to adjust how much power is being accepted from the near-field. The transmitter can detect this difference in power used from the near-field and interpret these changes as a message from the receiver.

[0266] In one embodiment, receive circuitry 502 has signaling detector and beacon circuitry 514 used to identify received energy fluctuations that can correspond to informational signaling from the transmitter to the receiver. The signaling and beacon circuitry 514 can detect the transmission of a reduced RF signal energy (i.e., a beacon signal) and to rectify the reduced RF signal energy into a nominal power for awakening either un-powered or power-depleted circuits within receive circuitry 502 in order to configure receive circuitry 502 for wireless charging.

[0267] Receive circuitry 502 can have processor 516 for coordinating the processes of receiver 500 described herein including the control of switching circuitry 512 described herein. Cloaking of receiver 500 can also occur upon the occurrence of other events including detection of an external wired charging source (e.g., wall/USB power) providing charging power to device 550. Processor 516, in addition to controlling the cloaking of the receiver, can also monitor beacon circuitry 514 to determine a beacon state and extract messages sent from the transmitter. Processor 516 can also adjust DC-to-DC converter 510 for improved performance.

[0268] In some exemplary embodiments, the receive circuitry 520 can signal a power requirement to a transmitter in the form of, for example, desired power level, maximum power level, desired current level, maximum current level, desired voltage level, and maximum voltage level. Based on these levels, and the actual amount of power received from the transmitter, the processor 516 can adjust the operation of the DC-to-DC converter 510 to regulate its output in the form of adjusting the current level, adjusting the voltage level, or a combination thereof.

[0269] FIG. 32 shows a schematic of transmit circuitry and receive circuitry showing coupling there between and an adjustable DC load 650. As shown in FIG. 32, a charging system 605 can be characterized by a coupled coil transformer model 630 where the transmitter electronics are connected to a primary coil 632 (i.e., a transmit antenna) and the rectifier/regulator electronics on the receiver side are connected to a secondary coil 634 (i.e., a receive antenna).

[0270] A driver 610 generates an oscillating signal at a desired resonance frequency, such as, for example, about 13.56 MHz. As one example, this driver 610 can be configured as a class E driver as illustrated in FIG. 32. A low pass

matching circuit 620 filters and impedance matches the signal from the driver 610 to the transmit antenna 632 of the coupled coil transformer model 630.

[0271] Energy is transferred through near field radiation to the receive antenna 634 of the coupled coil transformer model 630. The oscillating signal coupled to the receive antenna 634 is coupled to an impedance match and rectifier circuit 640 to provide an AC impedance match for the receive antenna 634 and rectify the oscillating signal to a substantially DC signal. A DC-to-DC converter 650 converts the DC signal from the rectifier 640 to a DC output useable by circuitry on a receiver device (not shown). The DC-to-DC converter 650 is also configured to adjust the DC impedance seen by the rectifier 640, which in turn adjusts the overall AC impedance of the input to the rectifier 640. As a result, changes in the DC impedance at the input of the DC-to-DC converter 650 can create a better match to the impedance of the receive antenna 634 and better mutual coupling between the receive antenna 634 and the transmit antenna 632.

[0272] The self inductances (L_{tx} and L_{rx}), mutual inductance (m), and loss resistances of the transformer model 630 can be derived from the measured or simulated coupling characteristics of the antenna pair.

[0273] It can be shown that given the mutual inductance (m), and the resistive losses, R_1 and R_2 of the transmit and receive antennas, respectively, there is an optimum load for the receive antenna that will maximize power transfer efficiency. This optimal load can be defined as:

$$R_{eff} = R_1 * [1 + (\omega m)^2 / (R_1 * R_2)]^{0.5}$$

[0274] Typically, R_{eff} can be in a range from 1 to 20 ohms. Through the use of DC load control, the RF load seen by the receive coil 634 can be set to its most efficient value, as the mutual inductance (m) varies due to the reasons described above.

[0275] Another use for controlling the RF load is that a variation in load can be used to control the power delivered to the receiver device. This can be at the expense of some efficiency, but enables the maximum use of available power when serving a mix of wireless devices in various charge states.

[0276] In one embodiment, RF load can be used to widen the bandwidth of the transfer function, a result which depends on the matching network 620 between a very low impedance, or reactive impedance, transmit power amplifier 610, typical for wireless charging amplifiers, and the transmitting antenna 632. This bandwidth adjustment can work best over a large variation in the mutual inductance (m) and load if the input matching circuit includes a third tuned inductance (not shown), mutually coupled to the TX antenna 632. In this case, the bandwidth will increase linearly with increasing RF load resistance if the power amplifier has a very low source impedance.

[0277] This input series tuned DC-to-DC converter 650 results in a second impedance inversion, the first being between the transmit and receive antennas (632 and 634). As a result, when the load impedance increases the input impedance increases. This allows the load to “cloak” the receiver from the transmitter simply by raising the load impedance of the receiver.

[0278] Without this cloaking feature, the load from the receiver would have to present a short in order to cloak, using a mechanism such as element 312 discussed above with reference to FIG. 31. As a result, a charging pad with no receiver

device present would appear as a highly tuned short circuit rather than an open circuit. Furthermore, when multiple uncloaked loads are present the total input conductance for the transmit antenna 632 will be the sum of the individual conductance's of the receive antennas 634 and power will be distributed according to their relative value.

[0279] FIGS. 33(a) and 33(b) show Smith charts illustrating change in input impedance of a coupled coil pair (no inductive match added) responsive to a change in DC impedance at the receiver device. In FIGS. 33(a) and 33(b), the darkened circles 710 and 720, respectively, indicate constant resistance circles.

[0280] Referring to FIGS. 33(a) and 32, a DC impedance R_{dc} of about 10.2 ohms at the input to the DC-to-DC converter 650 results in a complex input impedance at the transmit antenna 632 of about 50 ohms and very little reactance. Referring to FIGS. 33(a) and 32, a DC impedance R_{dc} of about 80 ohms at the input to the DC-to-DC converter 650 results in a complex input impedance at the transmit antenna 632 of much less than 50 ohms, with very little reactance.

[0281] FIGS. 34(a) and 34(b) show amplitude plots (730 and 740, respectively) show improved coupling between a coupled coil pair responsive to a change in DC impedance at the receiver device. In FIG. 34(a) the amplitude at the center frequency of 13.56 MHz is about -4.886 dB. After adjusting the input impedance to the DC-to-DC converter 450 (FIG. 32), the amplitude at the center frequency of 13.56 MHz is improved to about -3.225 dB resulting in better coupling between the receive antenna and the transmit antenna, which results in more power transferred to the receive antenna.

[0282] FIGS. 35(a) and 35(b) show simplified schematics of receiver devices illustrating exemplary embodiments for adjusting DC impedance at the receiver device. In both FIGS. 9A and 9B, the receive antenna 504 feeds an exemplary impedance matching circuit 520 including capacitors C1 and C2. An output from the impedance matching circuit 520 feeds a simple rectifier 530 (as one example) including diodes D1 and D2 and capacitor C3 for converting the RF frequency to a DC voltage. Of course, many other impedance matching circuits 520 and rectifiers 530 are contemplated as within the scope of embodiments of the present invention. A DC-to-DC converter 550 converts the DC input signal 540 from the rectifier to a DC output signal 570 suitable for use by a receiver device (not shown).

[0283] FIG. 35(a) illustrates a simple apparatus for maintaining an optimal power point impedance in a wireless power transmission system. A comparator, 548 compares the DC input signal 540 to a voltage reference 545, which is selected such that for a given expected power, the impedance as seen by the transmitter will result in the maximum amount of power coupled to the DC output signal 570. The output 561 of the comparator 548 feeds the DC-to-DC converter 550 with a signal to indicate whether the DC-to-DC converter 550 should increase or decrease its input DC impedance. In embodiments that use a switching DC-to-DC converter 550, this output of the comparator 561 can be converted to a pulse-width-modulation (PWM) signal, which adjusts the input DC impedance, as is explained below. This input voltage feedback circuit regulates input DC impedance by increasing the PWM pulse width as the voltage increases, thus decreasing impedance and voltage.

[0284] FIG. 35(b) an apparatus that can be used for maintaining an optimal power point impedance in a wireless power transmission system. In FIG. 35(b), a current sensor 544 can

be included and a multiplexer 546 can be used to switch whether voltage or current at the DC input signal 540 is sampled by a processor 560 at any given time. In this system, voltage (V_r) and current (I_r) of the DC input signal 540 is measured, and a PWM signal 562 to the DC-to-DC converter 550 can be varied over a pre-allowed range. The processor 560 can determine which pulse width for the PWM signal 562 produces the maximum power (i.e., current times voltage), which is an indication of the best DC input impedance. This determined pulse width can be used for operation to transfer an optimal amount of power to the DC output signal 570. This sample and adjust process can be repeated as often as desired to track changing coupling ratios, transmit powers or transmit impedances.

[0285] DC impedance is defined by (voltage/current). Therefore, at any given current and desired impedance, there exists a desired voltage=(current*desired impedance). With a PWM converter, this desired voltage (and as a result desired impedance) can be achieved by providing a feedback term that compares the input voltage to the (current*desired impedance) term, and adjusts the pulse width up or down to maintain that term.

[0286] FIGS. 36(a) through 36(d) illustrate simplified schematics of receiver devices illustrating exemplary embodiments for adjusting DC impedance at the receiver device using a pulse-width modulation converter. In FIGS. 10A-10D, common elements include the receive antenna 504 feeding an impedance matching circuit 520. An output from the impedance matching circuit 520 feeds a simple rectifier, which is shown simply as diode D3. Of course, many other impedance matching circuits 520 and rectifiers are contemplated as within the scope of embodiments of the present invention. A DC-to-DC converter 550 converts the DC input signal 540 from the rectifier to a DC output signal 570 suitable for use by a receiver device (not show). A processor 560 samples parameters of the DC input signal 540, the DC output signal 270, or a combination thereof and generates a PWM signal 562 for the DC-to-DC converter 550.

[0287] The DC-to-DC converter 550 is a switch-mode converter wherein the PWM signal 562 controls a switch S1 to periodically charge a filtering circuit including diode D4, inductor L1, and capacitor C4. Those of ordinary skill in the art will recognize the DC-to-DC converter 550 as a buck converter, which converts a voltage on the DC input signal 540 to a lower voltage on the DC output signal 570. While not shown, those of ordinary skill in the art will also recognize that the switch-mode DC-to-DC converter 550 can also be implemented as a boost converter to generate a DC output signal 570 with a voltage that is higher the voltage on the DC input signal 540.

[0288] In most cases, a requirement to regulate the output voltage of the wireless power receiver will be most important. For battery charging, for example, it is often critical to not exceed a maximum output current or a maximum output voltage. This means that often the output voltage control term will dominate the control rules for the pulse width of the PWM signal 562.

[0289] In one embodiment, DC impedance control uses a feedback term in the switch-mode DC-to-DC converter 550 to effectively simulate a steady-state DC resistance in the receiver. In other words, the DC impedance is controlled by adjusting the frequency or duty cycle of the PWM signal 562 to the switch-mode DC-to-DC converter 550 to simulate a given DC impedance.

[0290] Feedback for the system is created by sampling one or more characteristics of the DC input signal 540, the DC output signal 570, or a combination thereof by a processor 560. The processor 560 then uses this sampled information, possibly along with other information such as expected power transfer and efficiency of the DC-to-DC converter 550 to adjust the PWM signal 562, which adjust the DC input signal and the DC output signal to close the feedback loop.

[0291] Individual differences of what is sampled and how the parameters of the PWM signal are generated are discussed with reference to four different exemplary embodiments illustrated as FIGS. 10A-10D.

[0292] In FIG. 36(a), the processor 560 samples a voltage of the DC input signal 540, a current of the DC input signal 540, a voltage of the DC output signal 570, and a current of the DC output signal 570.

[0293] In some embodiments, a voltage sensor 542 can be used between the DC input signal 540 and the processor 560. Similarly, a voltage sensor 572 can be used between the DC output signal 570 and the processor 560. In other embodiments the voltage sensors 542 and 572 may not be needed and the processor 460 can directly sample voltages on the DC input signal 540 and the DC output signal 570.

[0294] In some embodiments, a current sensor 544 can be used between the DC input signal 540 and the processor 560. Similarly, a current sensor 574 can be used between the DC output signal 570 and the processor 560. In other embodiments the current sensors 544 and 574 may not be needed and the processor 560 can directly sample current on the DC input signal 540 and the DC output signal 570.

[0295] With current and voltage measurements of both the DC input signal 540 and the DC output signal 570, the processor 560 can determine all the parameters needed for the power conversion system. Power-in on the DC input signal 540 can be determined as voltage-in times current-in. Power-out on the DC output signal 570 can be determined as voltage-out times current-out. Efficiency of the DC-to-DC converter 550 can be determined as a difference between power-out and power-in. The DC impedance of the DC input signal 540 can be determined as voltage-in divided by current-in.

[0296] The processor 560 can periodically sample all of the inputs (e.g., about once every second, or other suitable period) to determine power output at that time. In response, the processor 560 can change the duty cycle of the PWM signal 562, which will change the DC impedance of the DC input signal 540. For example, a narrow pulse width on the PWM signal 562 allows the input voltage to stay relatively high and the input current to stay relatively low, which leads to a higher DC impedance for the DC input signal 540. Conversely, a wider pulse width on the PWM signal 562 allows more current to be drawn from the DC input signal 540, resulting in a lower input voltage and a lower DC impedance for the DC input signal 540.

[0297] The periodic sampling and adjusting creates the feedback loop that can find an optimal DC impedance for the DC input signal 540, and as a result, an optimal power for the DC output signal 570. Details of finding these values are discussed below with reference to FIG. 37.

[0298] In FIG. 36(b), the processor 560 samples a voltage of the DC input signal 540, a voltage of the DC output signal 570, and a current of the DC output signal 570. As explained above with reference to FIG. 36(a), the voltage sensor 542, the voltage sensor 572, and the current sensor 574 can be

included between their respective signals and the processor 560 depending on the embodiment.

[0299] As with FIGS. 36(a) and 36(b), power-out on the DC output signal 570 can be determined as voltage-out times current-out. In many cases, the efficiency of the DC-to-DC converter 550 will be known and relatively constant over the desired operating range. Thus, the processor 560 can estimate power-in on the DC input signal 540 based on power-out and an estimation of efficiency at the current operation point for the DC-to-DC converter 550. With power-in estimated, and voltage-in measured, the DC impedance of the DC input signal 540 can be determined. Once again, the periodic sampling and adjusting creates the feedback loop that can find an optimal DC impedance for the DC input signal 540, and as a result, an optimal power for the DC output signal 570.

[0300] In FIG. 36(c), the processor 560 samples a voltage of the DC input signal 540 and a current of the DC input signal 540. As explained above with reference to FIG. 36(a), the voltage sensor 542 and the current sensor 544 can be included between the DC input signal 540 and the processor 560 depending on the embodiment.

[0301] In FIG. 36(c), power-in on the DC input signal 540 can be determined as voltage-in times current-in and the DC impedance of the DC input signal 540 can be determined as voltage-in divided by current-in. As with FIG. 36(b), in FIG. 36(c) the efficiency of the DC-to-DC converter 550 will be known and relatively constant over the desired operating range. Thus, the processor 560 can estimate power-out on the DC output signal 570 based on power-in and an estimation of efficiency at the current operation point for the DC-to-DC converter 550. Once again, the periodic sampling and adjusting creates the feedback loop that can find an optimal DC impedance for the DC input signal 540, and as a result, an optimal power for the DC output signal 570.

[0302] In FIG. 36(d), the processor 560 samples only voltage of the DC input signal 540. As explained above with reference to FIG. 36(a), the voltage sensor 542 can be included between the DC input signal 540 and the processor 560 depending on the embodiment.

[0303] In FIG. 36(d), a pre-determined estimate can be made as to how much power is expected to be received through the receive antenna and rectifier and delivered on the DC input signal. Using this pre-determined estimate DC impedance of the DC input signal 540 can be determined relative to the voltage-in. As with FIG. 36(b), in FIG. 36(c) the efficiency of the DC-to-DC converter 550 will be known and relatively constant over the desired operating range. Thus, the processor 560 can estimate power-out on the DC output signal 570 based on the pre-determined power-in estimate and an estimation of efficiency at the current operation point for the DC-to-DC converter 550. Once again, the periodic sampling and adjusting creates the feedback loop that can find an optimal DC impedance for the DC input signal 540, and as a result, an optimal power for the DC output signal 570.

[0304] The pre-determined power estimate can be a fixed value programmed in to the receiver device or can be communicated to the receiver device from the transmitter device, which include a mechanism for determining how much of the power transmitted will be coupled to that particular receiver device.

[0305] FIG. 37 illustrates various input and output parameters that can be used when adjusting DC impedance at the receiver device. This graph represents a system that has a specific source impedance, but where a load resistor is

allowed to vary over a wide range. This load resistor is represented as the variable resistor of the DC-to-DC converter **650** of FIG. **32**. Alternatively, the load resistor can be represented by the DC impedance of the DC input signal **540** to the DC-to-DC converter **550** shown in FIGS. **36(a)**-**36(d)**.

[**0306**] In FIG. **37**, a 50 ohm source impedance is driven by a signal with a 1:1 source-to-load coupling. Line **820** shows the current through the load resistor. Notice as the load impedance increases, the current decreases due to Ohm's Law. Line **810** shows the voltage across the load resistor. Notice that as the load impedance increases, the voltage increases as well per the resistor divider equation.

[**0307**] These two data sets for current and voltage of the load resistor give the power across the load resistor, as shown by line **840**. Note that the power peaks at a certain load impedance. In this case (1:1 load coupling) this maximum power point occurs when the load impedance equals, or is near, the source impedance. If the coupling is different, the peak power point can be shifted as well.

[**0308**] Line **850** represents a PWM setting (out of 100) that has an inverse relationship to output impedance. This is the function exhibited by most buck converters. As can be seen, there is one ideal PWM setting that maximizes power received by the load resistor. Wireless power impedance control schemes used with reference to exemplary embodiments discussed herein attempt to discover and maintain this ideal PWM setting.

[**0309**] In some embodiments, as in FIGS. **32**, and **36(a)** through **36(d)**, the DC impedance of the DC input signal **540**, and as a result the AC impedance of the receive antenna can be effectively de-tuned from optimal power transfer to limit the amount of power delivered on the DC output signal **570**. This limiting of power can be useful where the receiver device cannot accept the maximum power deliverable from the DC-to-DC converter **550**.

[**0310**] The various illustrative logical blocks, modules, and circuits described in connection with the exemplary embodiments disclosed herein can be implemented or performed with a general purpose processor, a Digital Signal Processor (DSP), an Application Specific Integrated Circuit (ASIC), a Field Programmable Gate Array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general purpose processor can be a microprocessor, but in the alternative, the processor can be any conventional processor, controller, microcontroller, or state machine. A processor can also be implemented as a combination of computing devices, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration.

[**0311**] The steps of a method or algorithm described in connection with the exemplary embodiments disclosed herein can be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module can reside in Random Access Memory (RAM), flash memory, Read Only Memory (ROM), Electrically Programmable ROM (EPROM), Electrically Erasable Programmable ROM (EEPROM), registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary storage medium is coupled to the processor such that the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium can be

integral to the processor. The processor and the storage medium can reside in an ASIC. The ASIC can reside in a user terminal. In the alternative, the processor and the storage medium can reside as discrete components in a user terminal.

[**0312**] In various embodiments, the functions described can be implemented in hardware, software, firmware, or any combination thereof. If implemented in software, the functions can be stored on or transmitted over as one or more instructions or code on a computer-readable medium. Computer-readable media includes both computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A storage media can be any available media that can be accessed by a computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium that can be used to carry or store desired program code in the form of instructions or data structures and that can be accessed by a computer. Also, any connection is properly termed a computer-readable medium. For example, if the software is transmitted from a website, server, or other remote source using a coaxial cable, fiber optic cable, twisted pair, digital subscriber line (DSL), or wireless technologies such as infrared, radio, and microwave, then the coaxial cable, fiber optic cable, twisted pair, DSL, or wireless technologies such as infrared, radio, and microwave are included in the definition of medium. Disk and disc, as used herein, includes compact disc (CD), laser disc, optical disc, digital versatile disc (DVD), floppy disk and Blu-ray disc where disks usually reproduce data magnetically, while discs reproduce data optically with lasers. Combinations of the above should also be included within the scope of computer-readable media.

[**0313**] FIG. **38** is a block diagram of a portion of a remote communication system including a base station controller (BSC) **910** or telemetry system **32**, a pair of base stations **912**, and a set of monitoring devices **10** configured in accordance with one embodiment of the invention. Monitoring devices **10** conduct wireless communications by establishing bidirectional RF links with base stations **912**. The bidirectional links are comprised of a forward link signal transmitted from each base station **912**, and a reverse link signal transmitted from each monitoring device **10**.

[**0314**] In one embodiment, the forward and reverse link signals are processed in accordance with the IS-95 over-the-air interface standard, which calls for the use of CDMA signal processing. CDMA signal processing allows multiple spread spectrum RF signals to be transmitted at the same RF frequency range via modulation and demodulation with a set of pseudorandom noise (PN) codes.

[**0315**] Each base station **912** conducts communications with multiple monitoring devices **10** by generating a set of forward link signals. (The term "forward link signal" is also used to describe a set of forward link signals transmitted from a base station **912**, however, for the purpose of describing the present invention, forward link signal refers to a forward link transmission used for a single traffic channel.) Additionally, each base station **912** receives a set of reverse link signals from a set of monitoring devices **10**. The number of forward link signals that can be transmitted simultaneously by a base station **912** is typically limited by the maximum transmit power capability (P_{max}) of the particular base station **912**, the amount of multipath generated, or a predetermined limit

set in response to a network plan. The number of reverse link signals is typically limited by the bit energy to noise ratio (Eb/NO) required by a base station 912 to properly process a particular reverse link signal.

[0316] The IS-95 standard also calls for the data transmitted over the forward and reverse link signals to be processed in 20 ms increments that correspond to frames. Within BSC 910 and base stations 912, the various subsystems shown exchange the frames, as well as control information such as signaling messages, via the use of packets. The packets contain an address that indicates the subsystem to which they are directed, so that they may be properly routed by CDMA interconnect management system 914. Management system 914 controls the configuration and operation of the other systems that make up BSC 912 via signaling messages also transmitted using packets using information stored in monitoring system database 916.

[0317] In one embodiment, a monitoring device 10 can enter soft handoff, as shown in FIG. 39, whereby two or more bidirectional RF links are simultaneously established with two or more corresponding base stations 912 or telemetry systems 32. Soft handoff allows a monitoring device 10 to move from the coverage area of one base station 912 or telemetry system 32, to the coverage area of another base station 912 or telemetry system 32 while maintaining at least one bidirectional link at all times. Soft handoff can be contrasted with hard handoff during which the first bidirectional interface is terminated before the second bidirectional interface is established.

[0318] To conduct soft handoff, a set of selectors (not shown) within selector bank 916 perform various functions including performing call distribution and call selection functions used for conducting soft handoff, as well as tracking the base station 912 or stations 912 with which a monitoring device 10 is interfacing at any given time. The selectors are preferably comprised of a set of software instructions running on one or more microprocessors.

[0319] Monitoring device 10 communication distribution involves generating copies of each frame directed to the monitoring device 10 in soft handoff and forwarding one copy of the frame to each base station 912 or telemetry system interfacing with that monitoring device 10. Thus, one copy of the frame is transmitted from each base station 912 or telemetry system.

[0320] Call selection involves receiving a set of frames from the set of base stations 912 interfacing with the monitoring device 10 during the soft handoff, and selecting one frame for further processing based on the integrity or quality of the frames. In one embodiment, the base stations 912 or telemetry systems 32 receive two types of frames during the processing data communications which can also include audio: frames containing voice information (voice frames) and frames containing data information (data frames).

[0321] Each base station 912 responds to the two types of frames by transmitting all the voice frames received at a total transmit power P_{vo_ce} and by transmitting a set of data frame at a total transmit power P_{data} that is less than or equal to $P_{max} - P_{vo_ce}$. By transmitting data frames in addition to voice frames, the average power at which the base station transmits is increased with respect to a base station transmitting only voice frames. In particular, the base station 912 transmits more closely to its maximum transmit power P_{max} at any given instant. This increases the average transmit power and therefore increases the total amount of information

that is transmitted by the base station 912. Increasing the total amount of information transmitted, in turn, increases the efficiency with which the base station 912 uses the available RF bandwidth. Furthermore, by transmitting data frames at a transmit power that is less than or equal to $P_{max} - P_{vo_ce}$ the average transmit power of a base station 912 is increased without interfering with the set of voice communications already being conducted.

[0322] FIG. 39 is a flow chart illustrating the steps performed by BSC 910 and base stations 912 during the processing data frames that can also include voice frames in accordance with one embodiment of the invention. The processing begins at step 920, and at step 922 a set of selectors within selector bank 916 notifies the base stations 912 or telemetry systems 32 when they have data queued for transmissions via the use of signaling messages transmitted to a monitoring device 10. The data frames are received from a switching center 924 and are directed to a monitoring device 10. In one embodiment of the invention, the data frames are distinguished from voice data files via the use of one or more status bit contained in each frame.

[0323] At a time T_0 , each base station 912 receives a set of the signaling messages from the selectors, and calculates a value N equal to the number of selectors having a data frame queued for transmission. Additionally, each base station 912 calculates a value E_{bx} equal to the average energy used to transmit a bit of data, as well as a value $P(T_0)_{vo_ce}$ equal to the transmit power used at time T_0 to transmit all the voice frames being processed.

[0324] At step 926, each telemetry system of base station 912 transmits the values N , E_{bx} and $P(T_0)_{vo_ce}$ to each selector having data frames queued for transmission. At step 926, each selector 918 calculates a value B_{min} as the minimum of a set of values $B(1)_{bs} \dots B(n)_{bs}$ where $B(n)_{bs} = (P_{max} - P(T_0)_{vo_ce}) / (N \gg E_{bx})$ for a telemetry system 32 or base station 912, n being used to conduct the associated communication from the monitoring device 10 communication. That is, if the monitoring device 10 involved in the communication is in a soft handoff involving two telemetry systems 32 or base stations 912, two values $B(1)_{bs}$ and $B(2)_{bs}$ are calculated, and B_{min} is set to the lower of $B(1)_{bs}$ and $B(2)_{bs}$. In an alternative embodiment of the invention, B_{min} is set to the higher of $B(1)_{bs}$ and $B(2)_{bs}$.

[0325] Once B_{min} has been calculated, the selector 918 transmits a data frame having B_{min} bits of data to each base station 912 involved in the communication.

[0326] At step 930 occurring at a time T_x which is after time T_0 , each telemetry system 32 or base station 912 receives a set of data frames, and possible a set of voice frames, from the selectors 914, and calculates a value $P(T_1)_{data}$ equal to the power necessary to transmit the data frames received, as well as a value $P(T_1)_{vo_ce}$ equal to the power necessary to transmit the voice frames received. Using $P(T_1)_{data}$ and $P(T_1)_{vo_ce}$ each base station 912 determines if $P(T_1)_{data} + P(T_1)_{vo_ce}$ is less than or equal to the maximum transmit power P_{max} of the base station 912 at step 932. That is, each telemetry system 32 or base station 912 determines if $P(T_1)_{data} + P(T_1)_{vo_ce} \leq P_{max}$. If so, all the data frames are transmitted along with the voice frames at step 80, and then the base station 912 returns to step 922. While the use of P_{max} is preferred, the use of other thresholds less than P_{max} is consistent with the use of the system of the present invention.

[0327] If a telemetry system 32 or base station 912 determines at step 932 that $P(T_1)_{data} + P(T_1)_{vo_ce}$ is greater than

the maximum transmit power P_{max} , the telemetry system **32** or base station **912** transmits a set of randomly selected data frames having $(P_{max}-P(T1)VOiCe)/E_{bx}$ bits of data at step **934**. Then, at step **936** the telemetry system **32** or base station **912** notifies the selectors **918** which did not have their data frames transmitted. These selectors can then attempt to retransmit the data contain in these data frames at a later time.

[0328] Generally, most or all of the data frames received by a telemetry system **32** or a base station **912** will be transmitted at time $T1$ because the transmit power used to transmit the voice frames at time $T0$ will differ little from the necessary voice frame transmit power at time $T1$. Thus, if any demand to transmit data exists, base station **912** will transmit, on average, more closely to the maximum power level. This allows the cellular telephone system to more efficiently use the available RF bandwidth.

[0329] When the transmit power necessary at time $T1$ to transmit all the voice frames increases relative to the transmit power necessary at $T0$, the present invention limits the transmission of data frames to that which will cause P_{max} power to be used, while allowing all voice frames to be transmitted or vice versa. This ensures that all the communications from a monitoring device **10** conducted will continue without interruption, while also allowing the maximum number of data frames to be transmitted given the maximum transmit power P_{max} of a base station **912**.

[0330] The foregoing description of various embodiments of the claimed subject matter has been provided for the purposes of illustration and description. It is not intended to be exhaustive or to limit the claimed subject matter to the precise forms disclosed. Many modifications and variations will be apparent to the practitioner skilled in the art. Particularly, while the concept "component" is used in the embodiments of the systems and methods described above, it will be evident that such concept can be interchangeably used with equivalent concepts such as, class, method, type, interface, module, object model, and other suitable concepts. Embodiments were chosen and described in order to best describe the principles of the invention and its practical application, thereby enabling others skilled in the relevant art to understand the claimed subject matter, the various embodiments and with various modifications that are suited to the particular use contemplated.

What is claimed is:

1. A wireless communication system for a monitoring device, comprising:

one or more sensors coupled to the monitoring device that has a unique user ID, the one or more sensors acquiring user information selected from of at least one of, a user's activities, behaviors and habit information;

ID circuitry at the monitoring device, the ID circuitry including ID storage, a communication system that reads and transmits the unique ID from an ID storage, a power source and a pathway system to route signals through the circuitry;

a telemetry system including a database of user ID's, the telemetry system communication with the monitoring device, the telemetry system analyzing data from monitoring device based on at least one of, user's activities, behaviors and habit information and creating personalized information about the user; and

a telemetry system controller for transmitting a set of data frames relative to the monitoring device and optionally a

set of voice frames from the monitoring device if they exist and when there is additional capacity.

2. The system of claim **1**, wherein the additional capacity exists if additional transmit power is available while voice frames are being transmitted.

3. The system of claim **1**, wherein the telemetry system in operation indicates a first time additional capacity to the controller, and the controller sets a set of voice frames to have an amount of voice equal to the first time additional capacity.

4. The system as set forth in claim **3**, wherein the telemetry system transmits a portion of the set of voice frames if a second time additional capacity is less than an amount of transmit power necessary to transmit all of the set of data frames.

5. The system of claim **4**, wherein the telemetry system notifies the controller of a portion of the set of data frames that were not transmitted.

6. The system of claim **1**, further comprising:

a control system at the monitoring device to orchestrate communication between different systems.

7. The system of claim **1**, further comprising:

a noise reduction element at the monitoring device to reduce signal noise.

8. The system of claim **1**, further comprising:

logic resources at the monitoring device to determine at least one of use, activity type, behavioral patterns and habits based on data relative to the user.

9. The system of claim **1**, wherein switching is performed between incremental and full syncing of data based on available communication routes.

10. The system of claim **1**, further comprising:

conditioning electronics that in operation communicate signals from the one or more sensors.

11. The system of claim **10**, wherein the conditioning electronics include a filter that determine a presence of certain conditions.

12. The system of claim **10**, wherein the conditioning electronics clean a signal for processing by a central processing unit (CPU) of the telemetry system.

13. The system of claim **12**, wherein the CPU evaluates historical data.

14. The system of claim **1**, wherein the telemetry system in operation creates different classifications for data received from the monitoring device.

15. The system of claim **14**, wherein the classifications are selected from at least one of, a user's location, where the user spends its time, with whom the user spends its time, a determination of working relationships, a determination of family relationships, a user's activities, and a user social relationships.

16. The system of claim **1**, wherein the telemetry system in operation provides firmware updates to the monitoring device.

17. The system of claim **1**, wherein streams of information are sent from at least one sensor at the monitoring device to the telemetry system.

18. The system of claim **13**, wherein the streams of information can include encrypted and non-encrypted information.

19. The system of claim **18**, wherein user information is sent from the monitoring device to a mobile device or computer.

20. A wireless communication system for a monitoring device, comprising:

one or more sensors coupled to the monitoring device that has a unique user ID, the one or more sensors acquiring user information selected from of at least one of, a user's activities, behaviors and habit information;

ID circuitry at the monitoring device, the ID circuitry including ID storage, a communication system that reads and transmits the unique ID from an ID storage, a power source and a pathway system to route signals through the circuitry;

a telemetry system including a database of user ID's, the telemetry system communicating with the monitoring device, the telemetry system analyzing telemetry data from monitoring device based on at least one of, user's activities, behaviors and habit information and creating personalized information about the user;

a telemetry system controller for transmitting a set of voice frames relative to the monitoring device and optionally a

set of data frames from the monitoring device if they exist and when there is additional capacity.

21. The system of claim **20**, wherein the additional capacity exists if additional transmit power is available while data frames are being transmitted.

22. The system of claim **20**, wherein the telemetry system in operation indicates a first time additional capacity to the controller, and the controller sets a set of data frames to have an amount of data equal to the first time additional capacity.

23. The system as set forth in claim **22**, wherein the telemetry system transmits a portion of the set of data frames if a second time additional capacity is less than an amount of transmit power necessary to transmit all of the set of video frames.

24. The system of claim **23**, wherein the telemetry system notifies the controller of a portion of the set of video frames that were not transmitted.

* * * * *

专利名称(译)	使用CDMA进行无线通信的监控设备		
公开(公告)号	US20140247148A1	公开(公告)日	2014-09-04
申请号	US13/967094	申请日	2013-08-14
[标]申请(专利权)人(译)	你好		
申请(专利权)人(译)	HELLO INC.		
当前申请(专利权)人(译)	HELLO INC.		
[标]发明人	PROUD JAMES		
发明人	PROUD, JAMES		
IPC分类号	A61B5/00 G08C17/02		
CPC分类号	A61B5/0024 G08C17/02 A61B5/0026 A61B5/0022 A61B5/0205 A61B5/02055 A61B5/1112 A61B5/1118 A61B5/443 A61B5/6831 A61B5/6898 A61B5/743 A61B90/90 A61B90/98 A61B2560/0214 A61B2562/0233 A61B2562/08 G06F19/00 G16H40/67 H02J7/00034 H02J7/025 H02J50/10 H02J50/80 H04L67/12 H04L67/125 H04L67/22		
优先权	61/772265 2013-03-04 US 61/823502 2013-05-15 US		
外部链接	Espacenet USPTO		

摘要(译)

一个或多个传感器耦合到具有唯一用户ID的监控设备，所述一个或多个传感器获取从用户的活动，行为和习惯信息中的至少一个中选择的用户信息。ID电路位于监控设备上。还包括ID存储器，一种从ID存储器读取和传输唯一ID的通信系统，电源和通过电路路由信号的通路系统。遥测系统包括用户ID的数据库。遥测系统与监视设备通信并基于用户的活动，行为和习惯信息中的至少一个来分析来自监视设备的数据并创建关于用户的个性化信息，并且控制器发送关于用户的数据帧的集合。监控设备。从监视设备发送一组数据帧。

