US 20140247141A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2014/0247141 A1**

Proud (43) **Pub. Date: Sep. 4, 2014**

(54) **MONITORING DEVICE WITH WIRELESS COMMUNICATION OVER NON-CONTIGUOUS CHANNELS**

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

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

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

(21) Appl. No.: **13/955,892**

(22) Filed: **Jul. 31, 2013**

Related U.S. Application Data

(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.

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

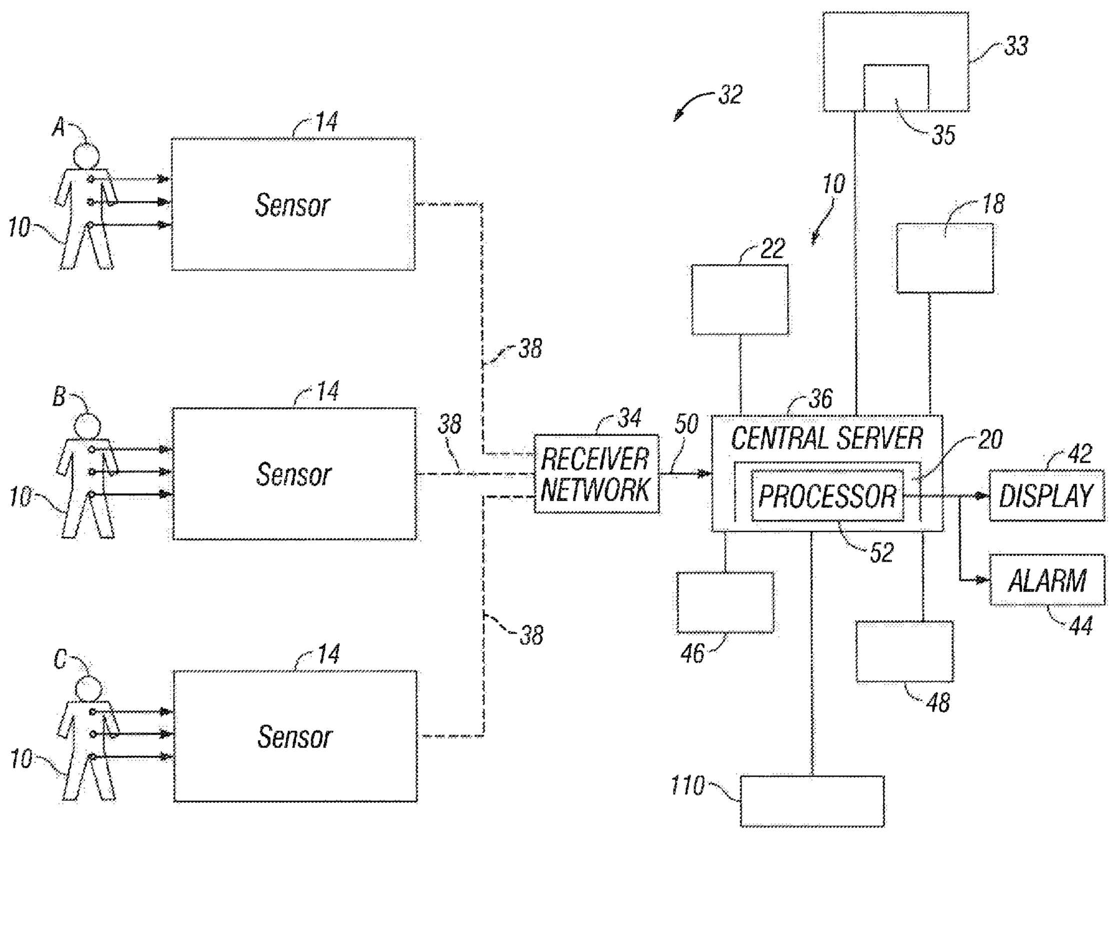
Publication Classification

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

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

(57) **ABSTRACT**

A communication system for a monitoring device. The monitoring device includes, one or more sensors, a unique user ID, ID circuitry 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. The one or more sensors acquire user information selected from of at least one of, a user's activities, behaviors and habit information. A telemetry system is in communication with the monitoring device. The monitoring device and/or the telemetry system includes a wireless communication device that in operation transmits a wireless communication packet to the other over a plurality of non-contiguous wireless communication channels.



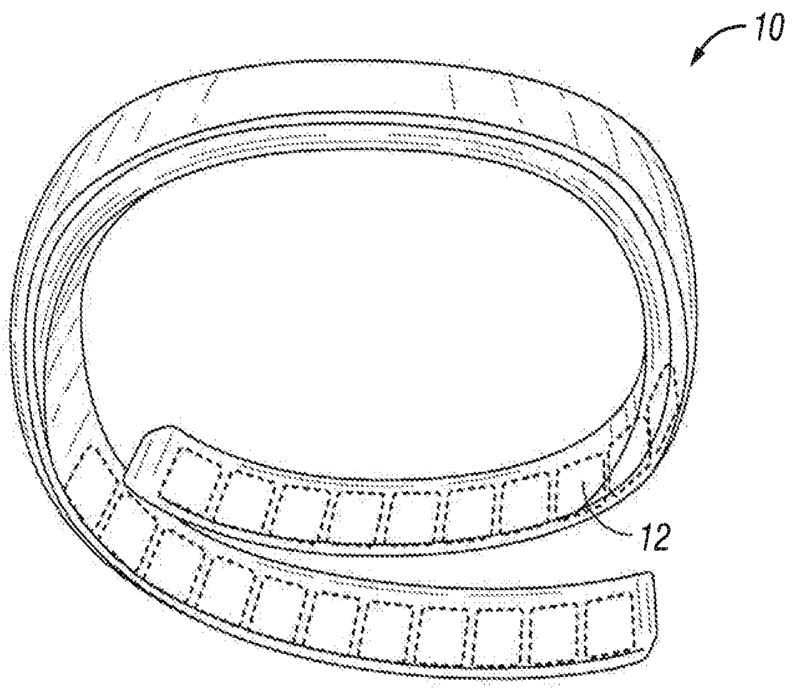


FIG. 1A

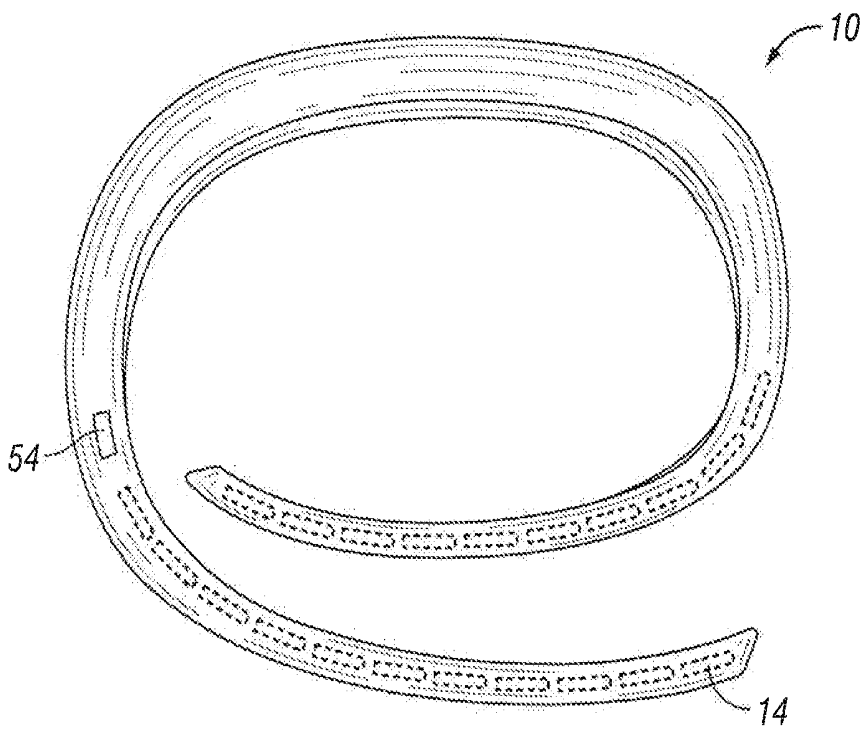


FIG. 1B

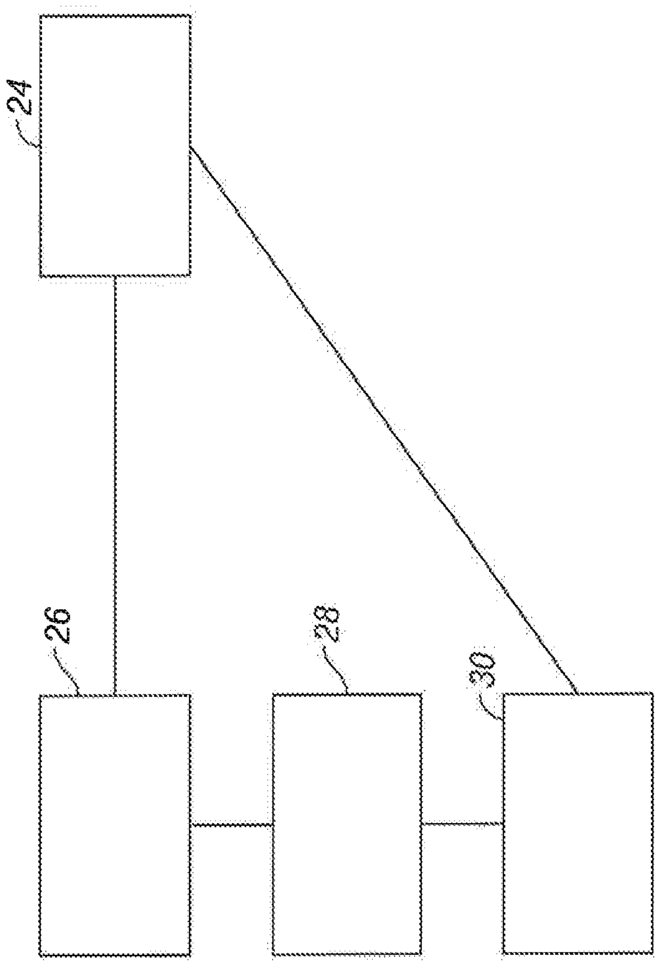


FIG. 2

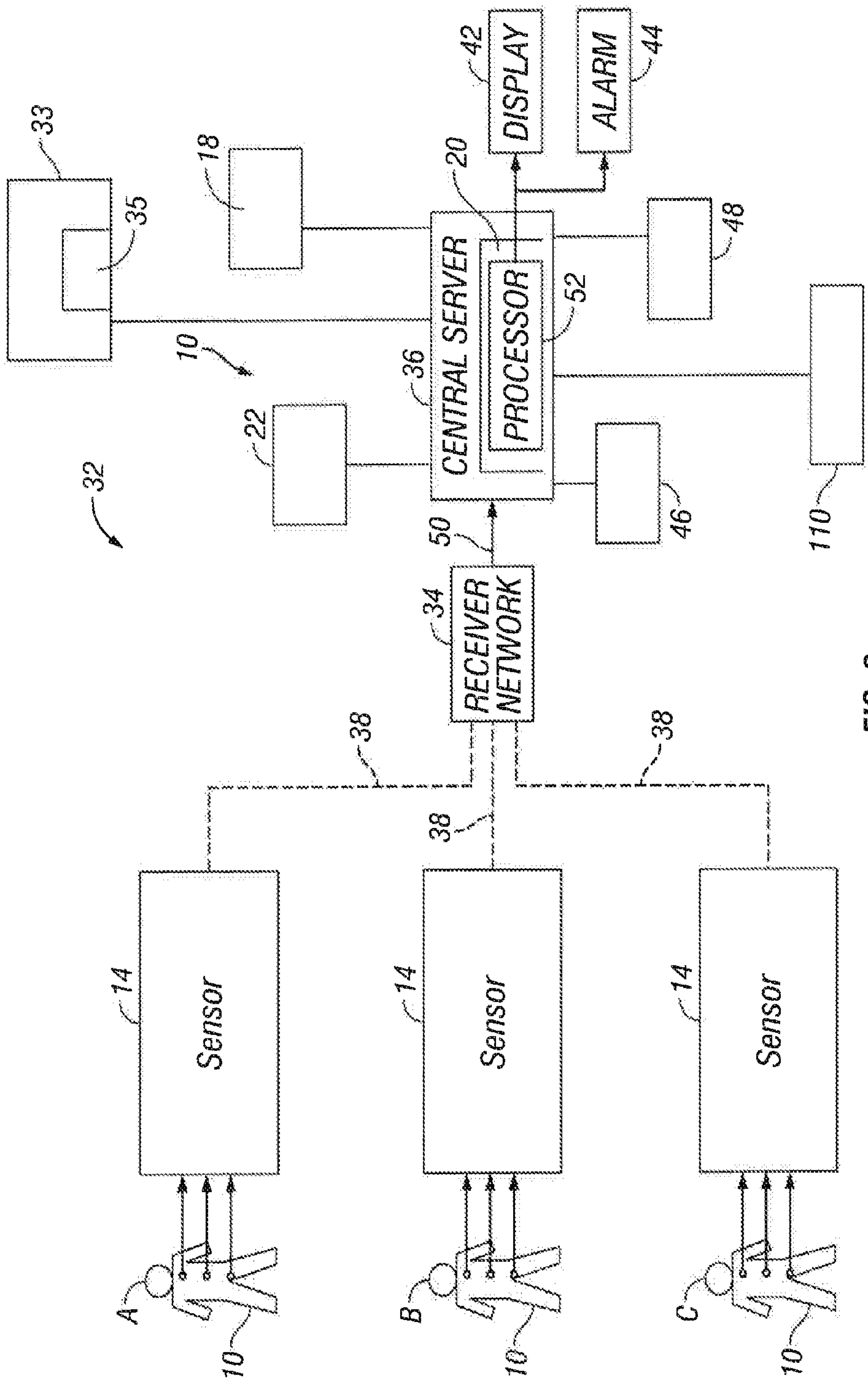

33
35
18
20
42
DISPLAY
ALARM
44
48
CENTRAL SERVER
PROCESSOR
52
36
10
22
32
46
110
50
RECEIVER NETWORK
34
38
38
38
14
Sensor
14
Sensor
14
Sensor
A
B
C
10
10
10

FIG. 3

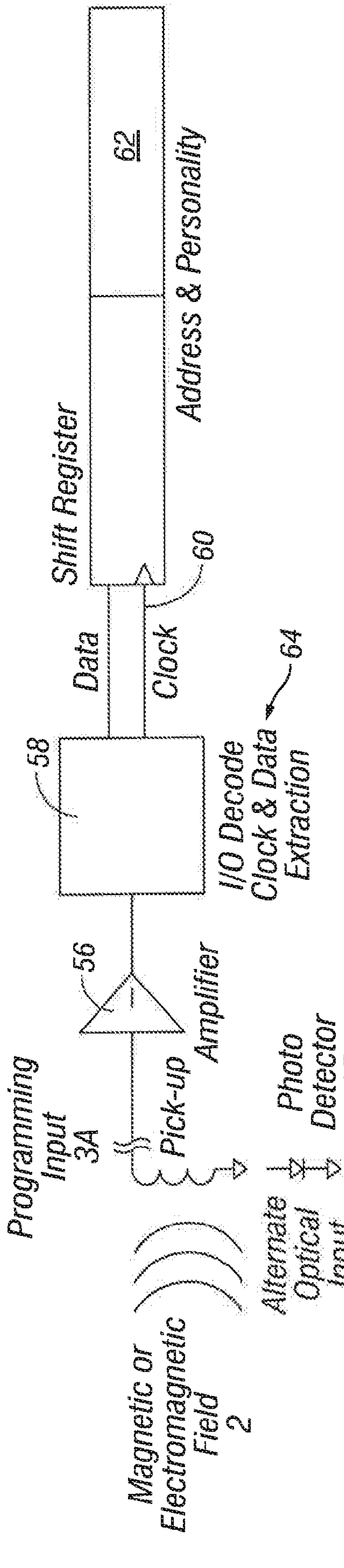

Magnetic or Electromagnetic Field 2
Alternate Optical Input 3
Programming Input 3A
Pick-up
Photo Detector 3E
56
Amplifier
58
I/O Decode Clock & Data Extraction
64
Data
Clock
60
Shift Register
62
Address & Personality

FIG. 4

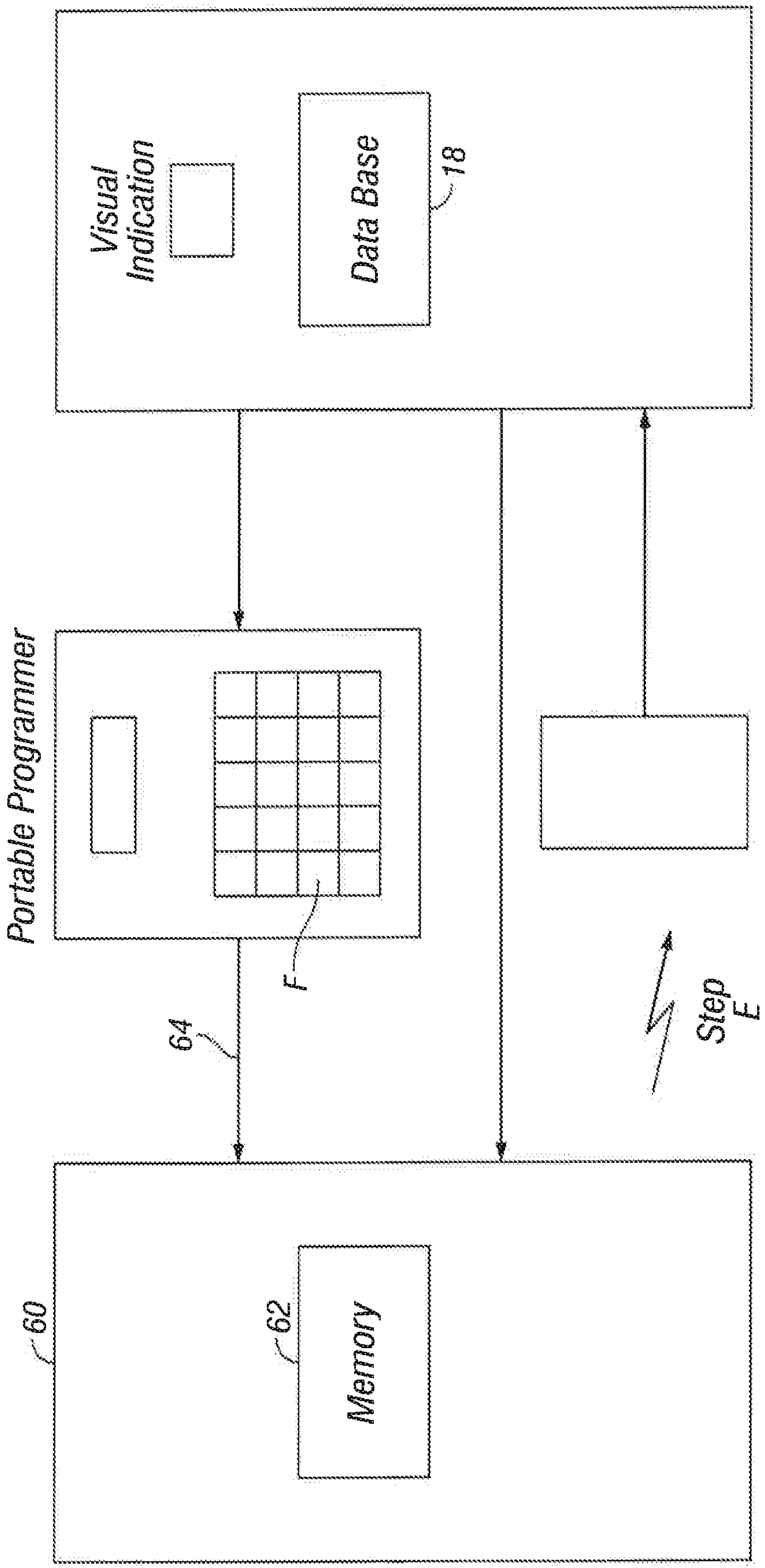

Visual Indication
Data Base
18
Portable Programmer
F
64
Step E
60
62
Memory

FIG. 5

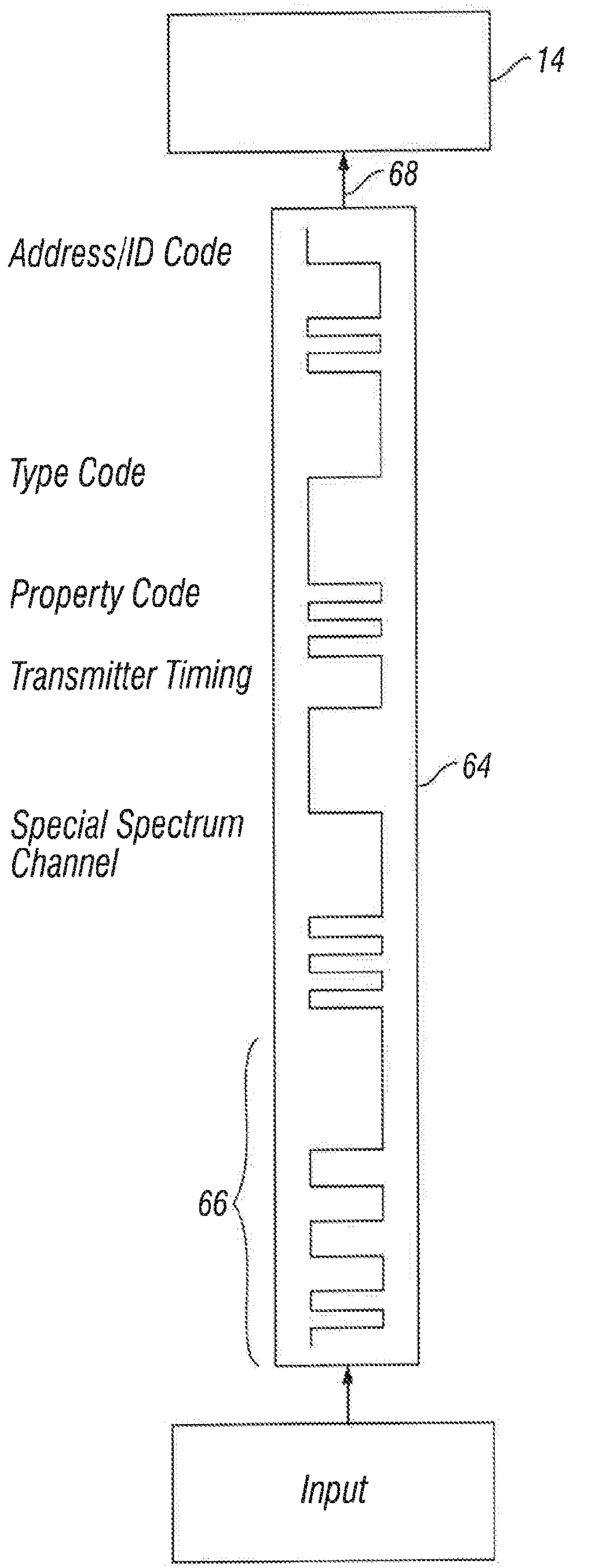

14
68
Address/ID Code
Type Code
Property Code
Transmitter Timing
64
Special Spectrum Channel
66
Input

FIG. 6

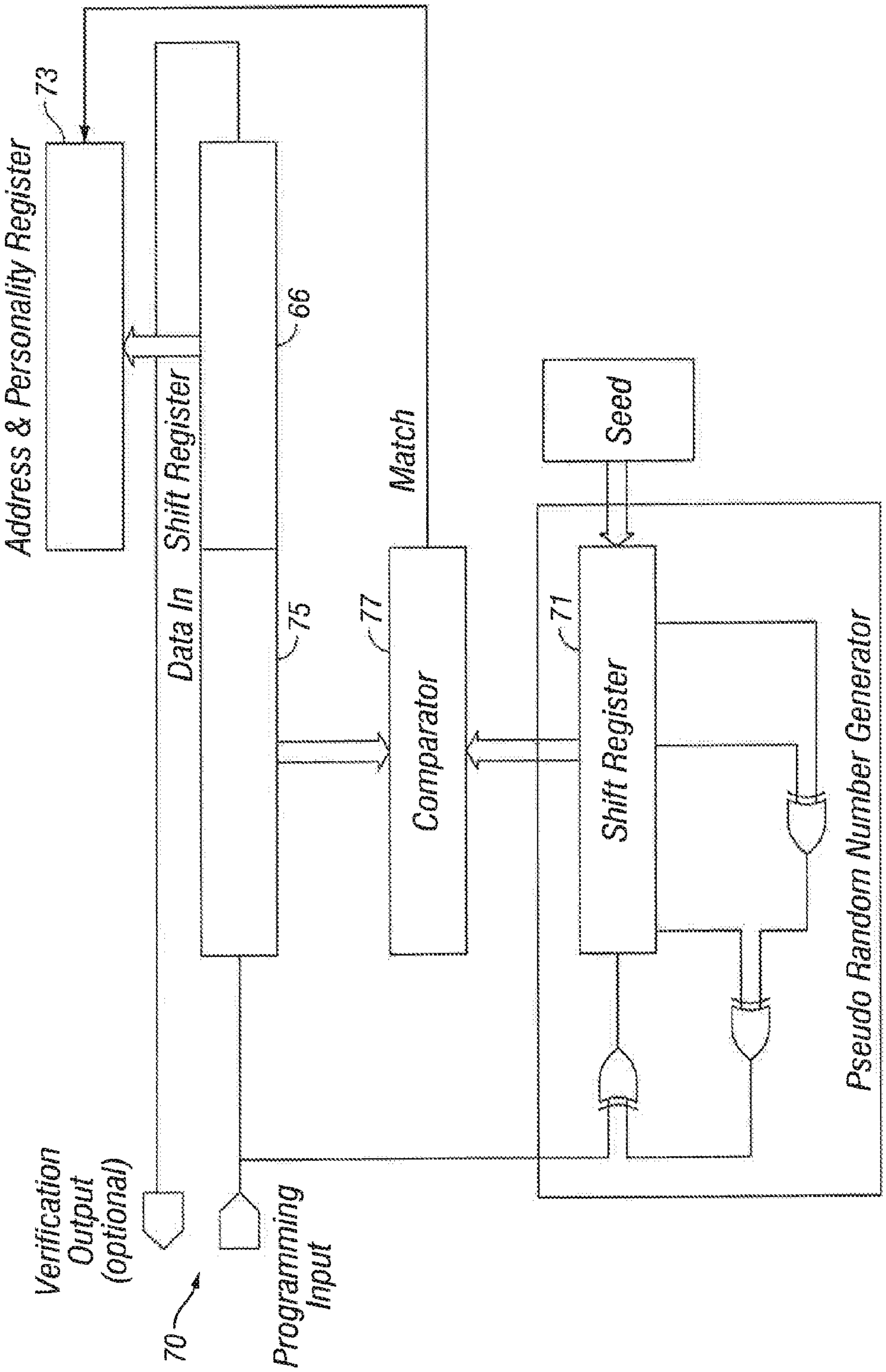

Address & Personality Register
73
Data In
Shift Register
66
75
Match
77
Comparator
Seed
71
Shift Register
Pseudo Random Number Generator
Verification Output (optional)
70
Programming Input

FIG. 7

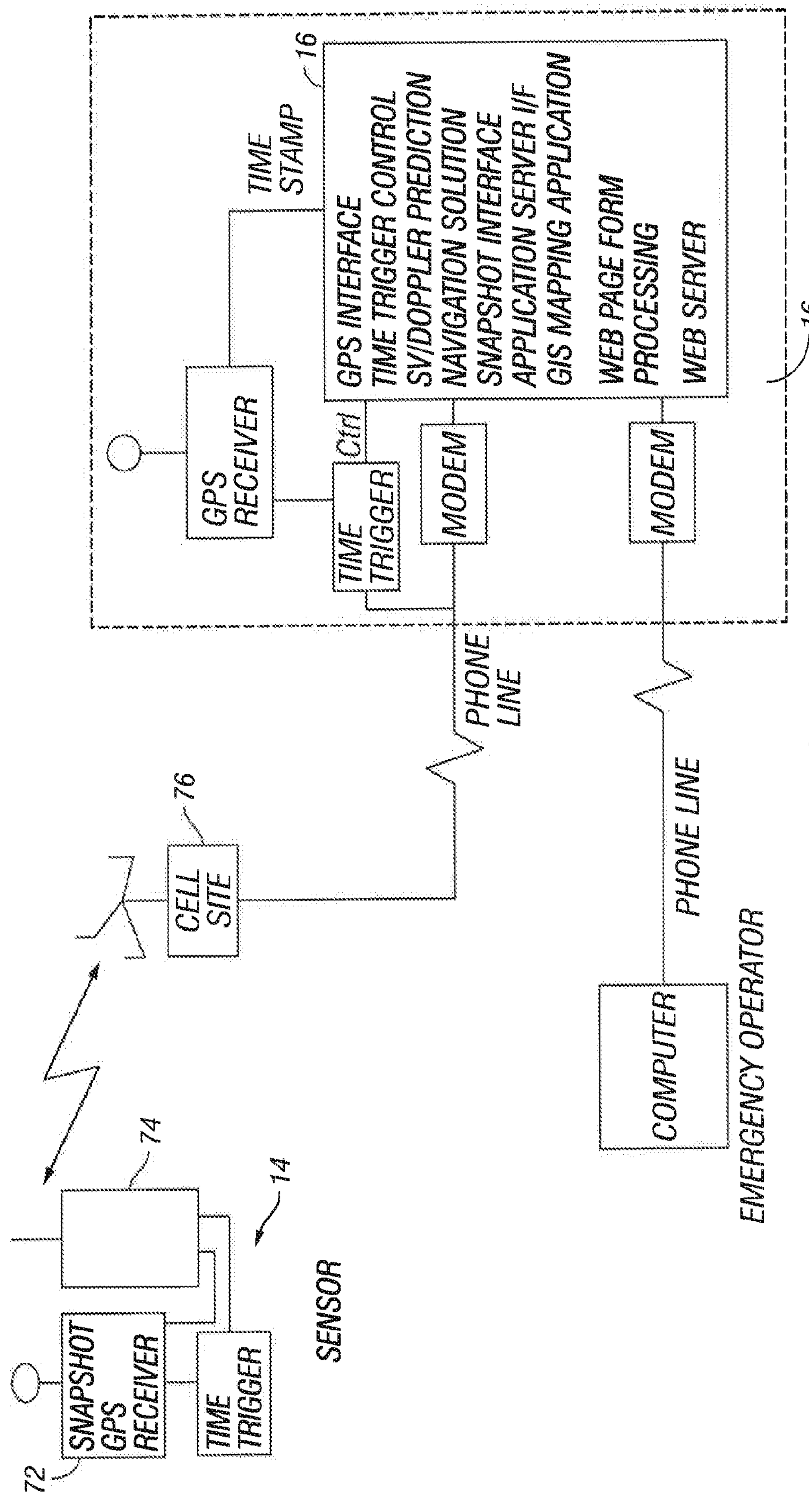

16
TIME STAMP
GPS INTERFACE
TIME TRIGGER CONTROL
SV/DOPPLER PREDICTION
NAVIGATION SOLUTION
SNAPSHOT INTERFACE
APPLICATION SERVER I/F
GIS MAPPING APPLICATION
WEB PAGE FORM PROCESSING
WEB SERVER
16
GPS RECEIVER
Ctrl
TIME TRIGGER
MODEM
MODEM
PHONE LINE
PHONE LINE
76
CELL SITE
COMPUTER
EMERGENCY OPERATOR
74
14
SENSOR
SNAPSHOT GPS RECEIVER
TIME TRIGGER
72

FIG. 8

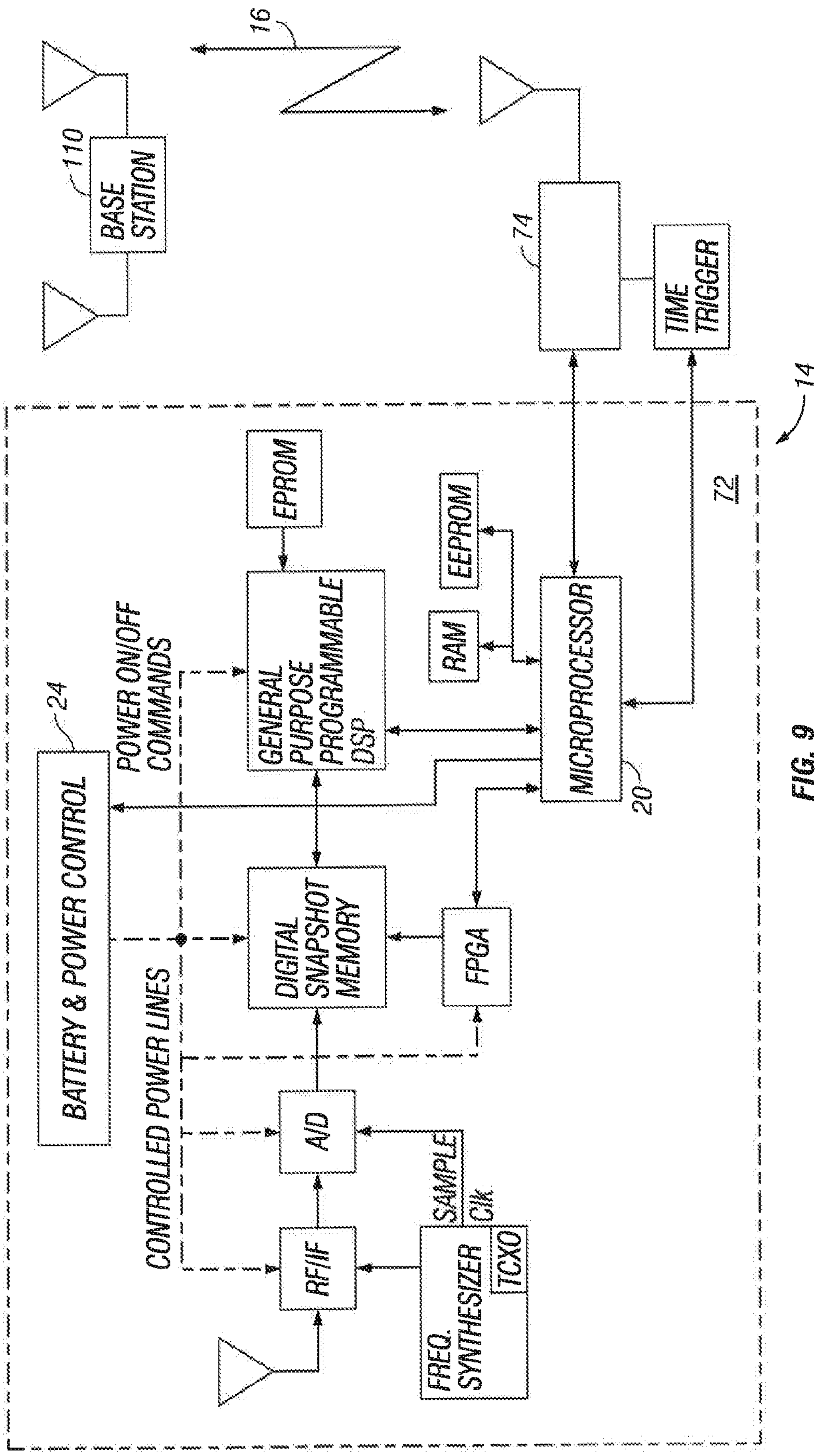

16
110
BASE STATION
74
TIME TRIGGER
14
72
EPROM
EEPROM
RAM
MICROPROCESSOR
20
GENERAL PURPOSE PROGRAMMABLE DSP
POWER ON/OFF COMMANDS
24
BATTERY & POWER CONTROL
DIGITAL SNAPSHOT MEMORY
FPGA
CONTROLLED POWER LINES
A/D
SAMPLE Clk
RF/IF
FREQ. SYNTHESIZER
TCXO

FIG. 9

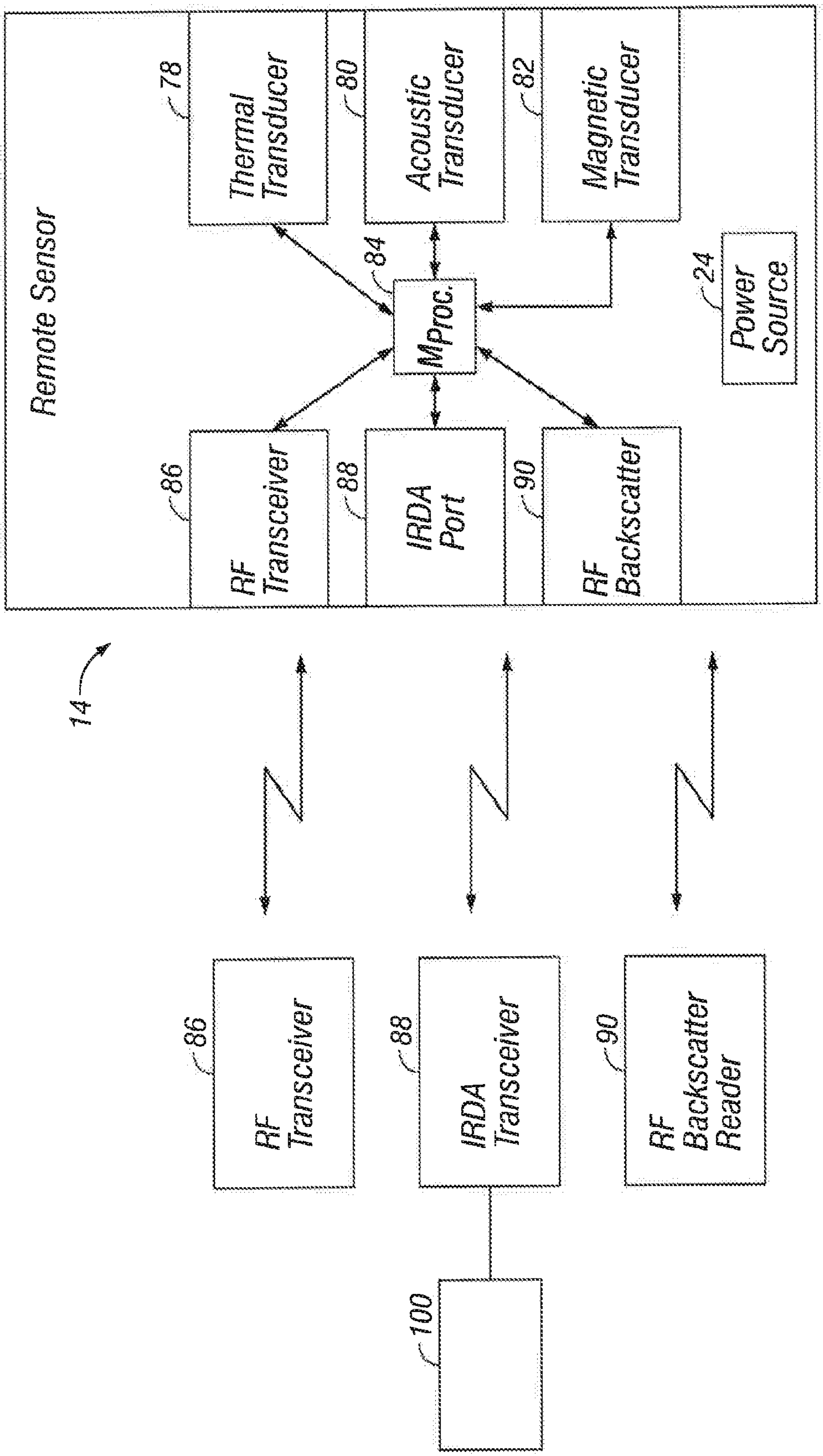

Remote Sensor
78
Thermal Transducer
80
Acoustic Transducer
82
Magnetic Transducer
84
MProc.
24
Power Source
86
RF Transceiver
88
IRDA Port
90
RF Backscatter
14
86
RF Transceiver
88
IRDA Transceiver
90
RF Backscatter Reader
100

FIG. 10

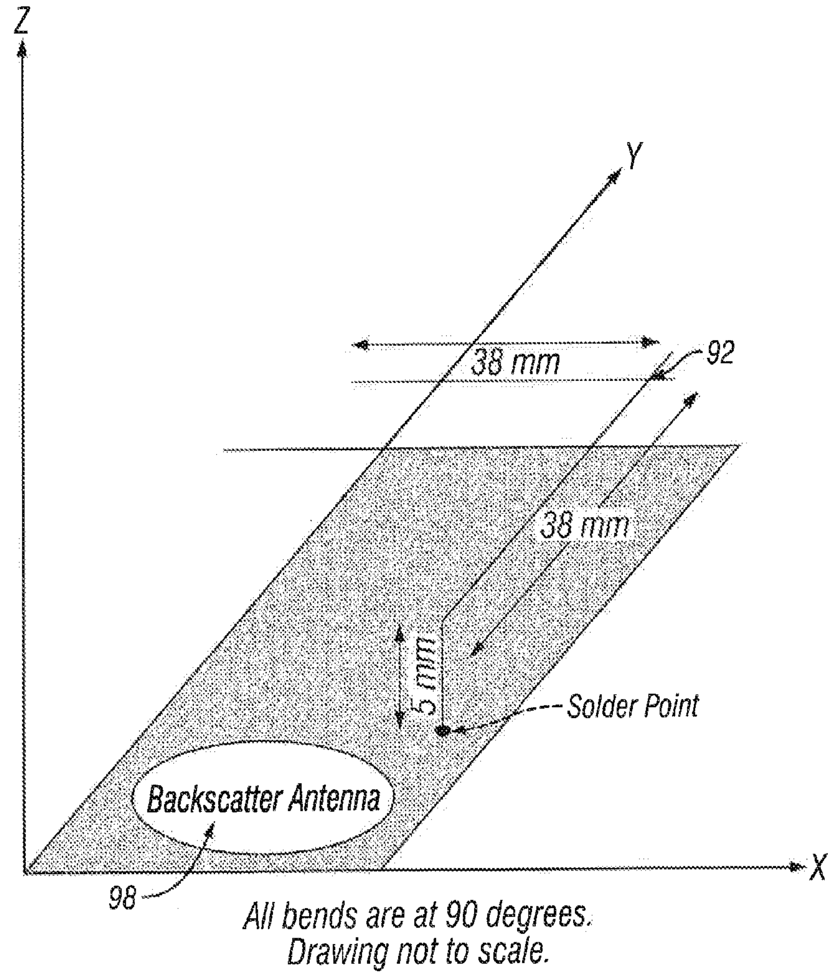
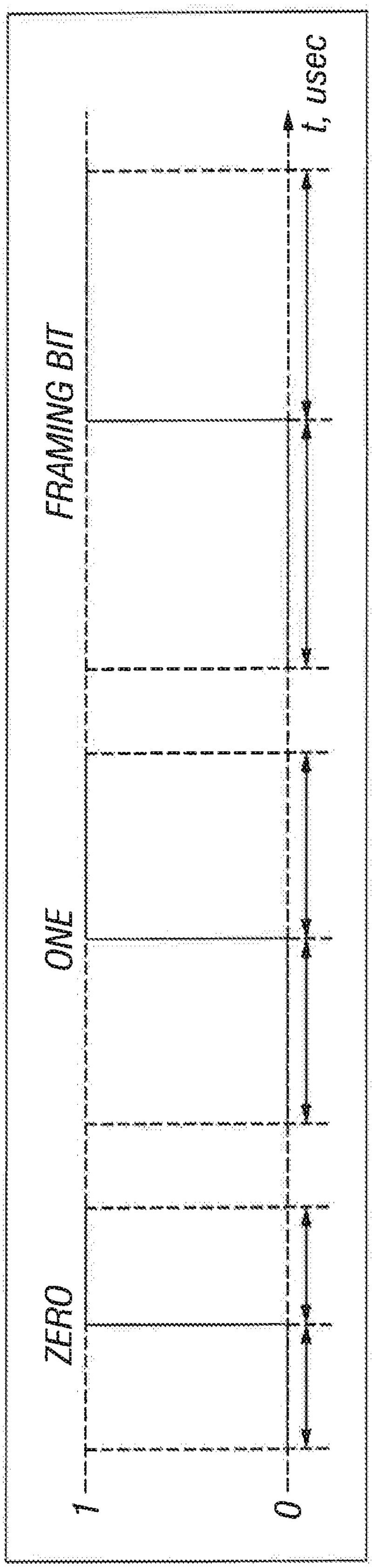
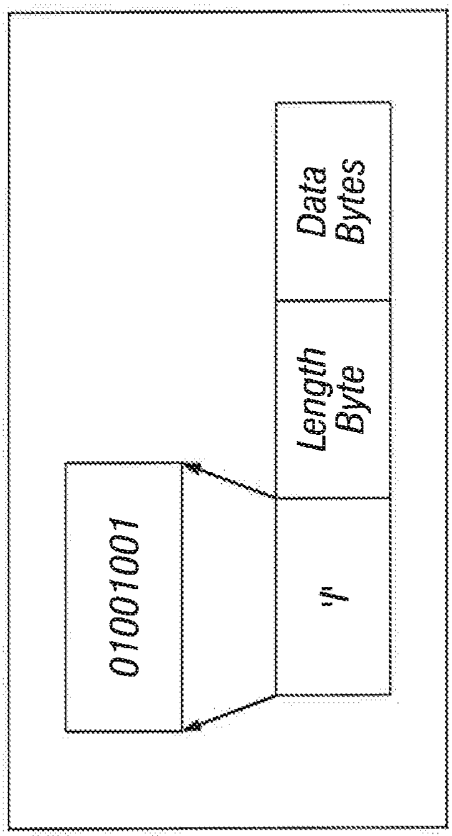

Z
Y
X
38 mm
92
38 mm
5 mm
Solder Point
Backscatter Antenna
98
All bends are at 90 degrees.
Drawing not to scale.

FIG. 11



ZERO
ONE
FRAMING BIT
t, usec
1
0

FIG. 12



01001001
'I'
Length Byte
Data Bytes

FIG. 13

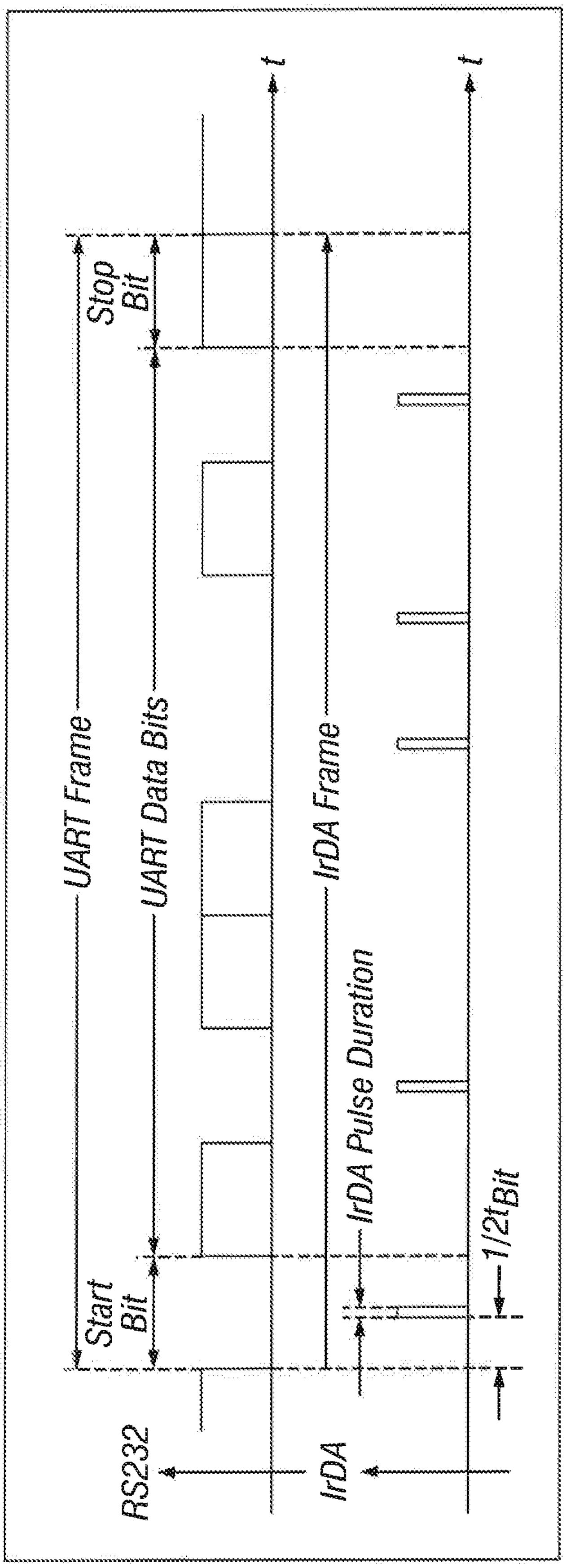

RS232
IrDA
t
t
UART Frame
UART Data Bits
IrDA Frame
Start Bit
Stop Bit
IrDA Pulse Duration
1/2tBit

FIG. 14

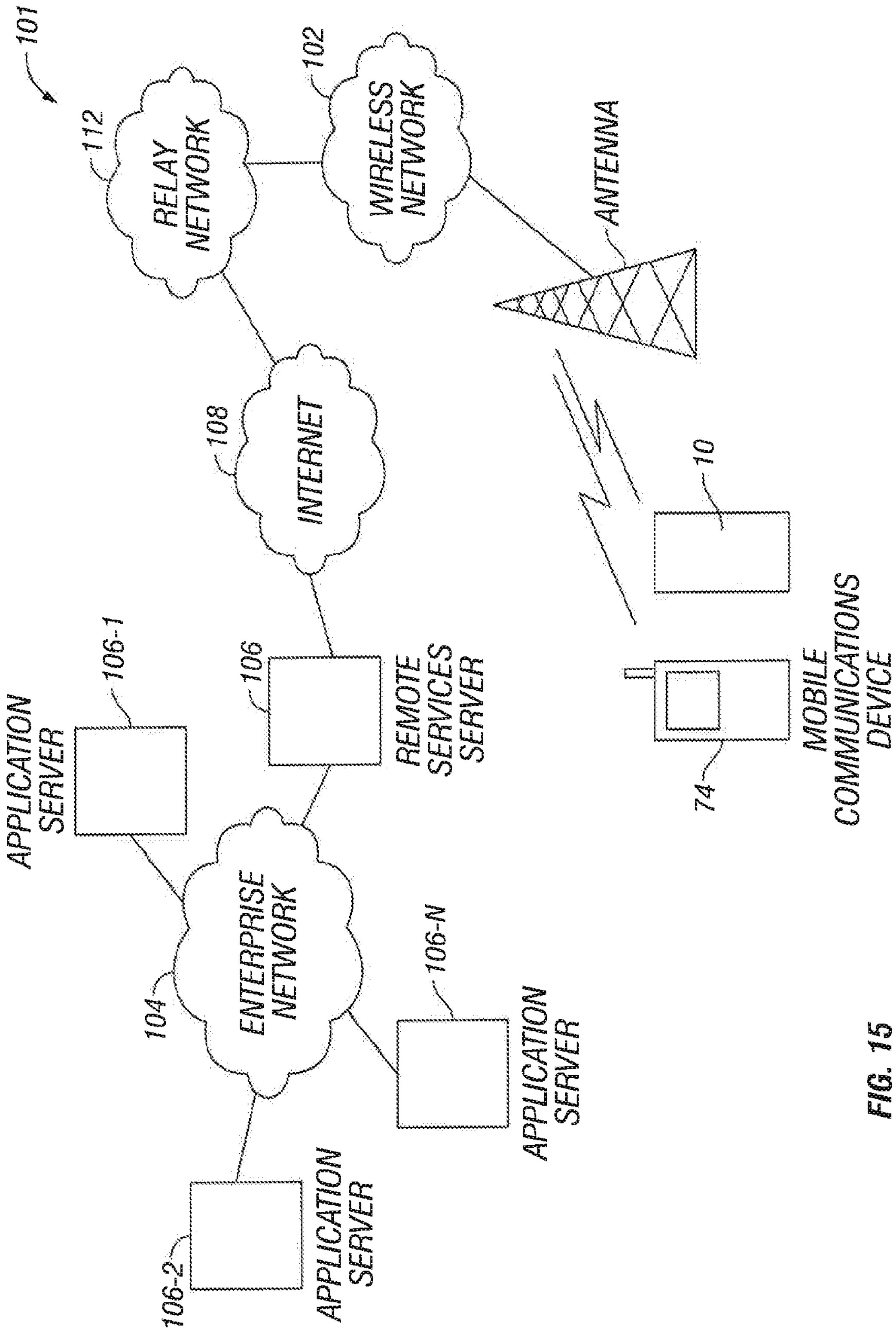

101
112
RELAY NETWORK
102
WIRELESS NETWORK
ANTENNA
108
INTERNET
10
106-1
APPLICATION SERVER
106
REMOTE SERVICES SERVER
74
MOBILE COMMUNICATIONS DEVICE
104
ENTERPRISE NETWORK
106-N
APPLICATION SERVER
106-2
APPLICATION SERVER

FIG. 15

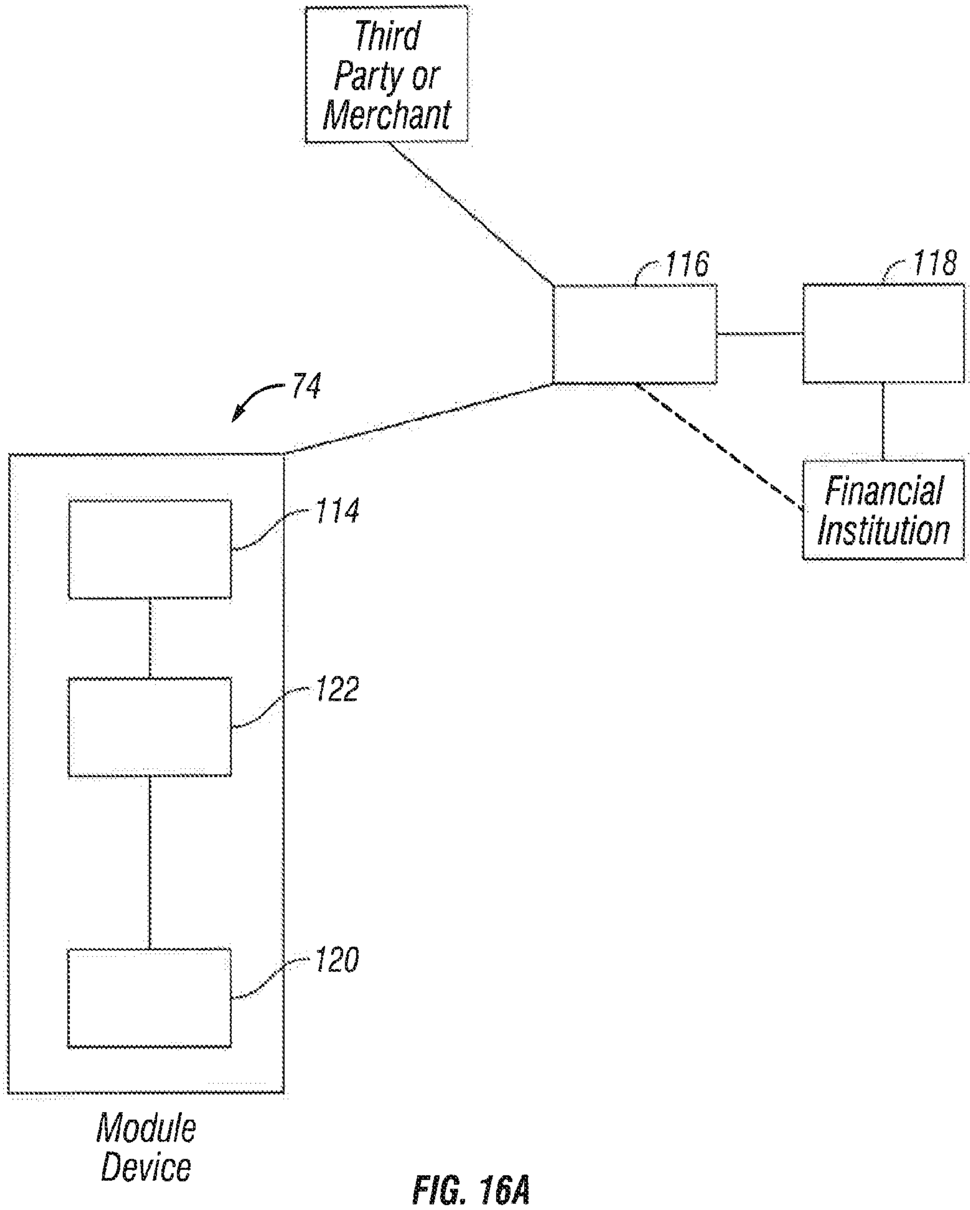

Third Party or Merchant
116
118
74
Financial Institution
114
122
120
Module Device

FIG. 16A

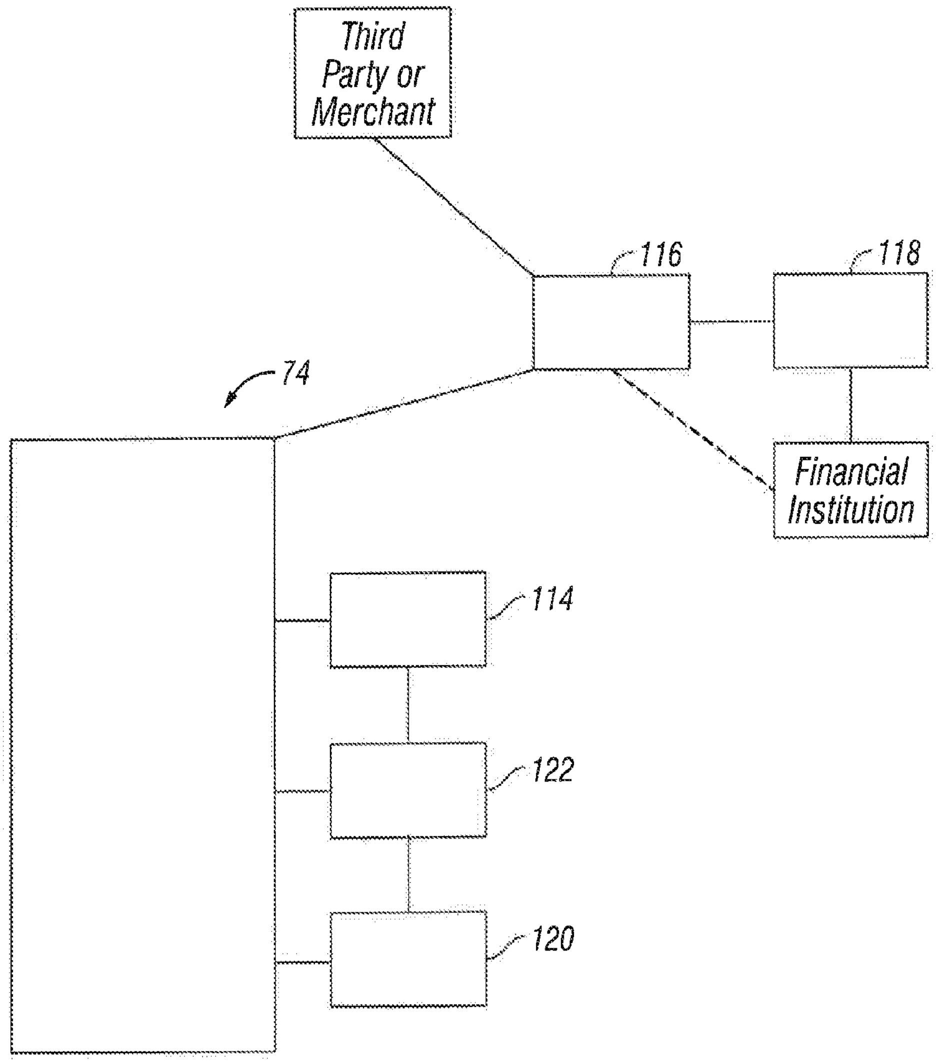

Third Party or Merchant
116
118
74
Financial Institution
114
122
120

FIG. 16B

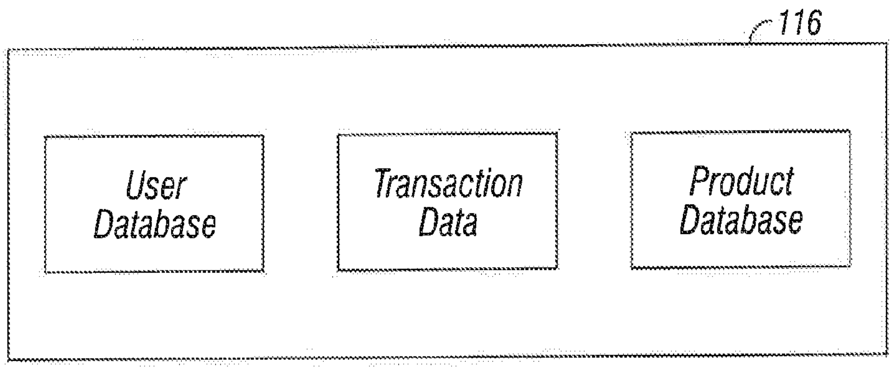


FIG. 16C

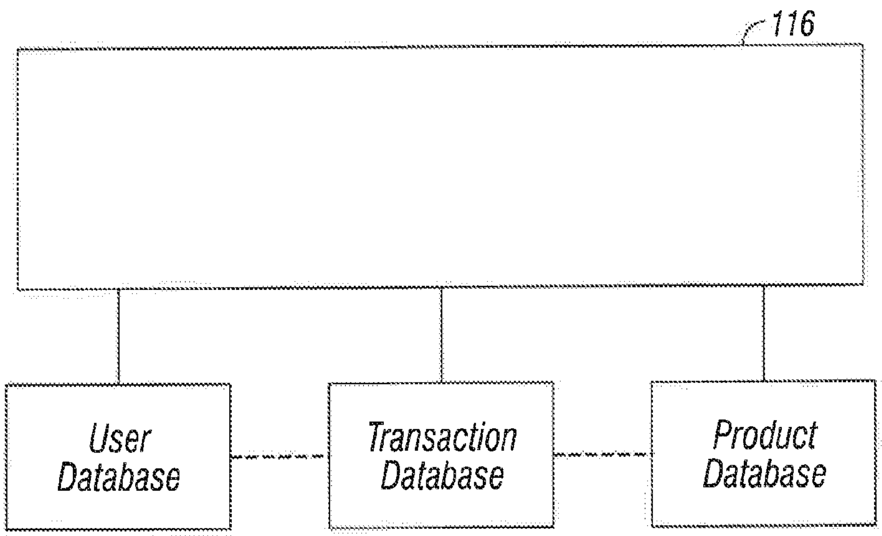


FIG. 16D

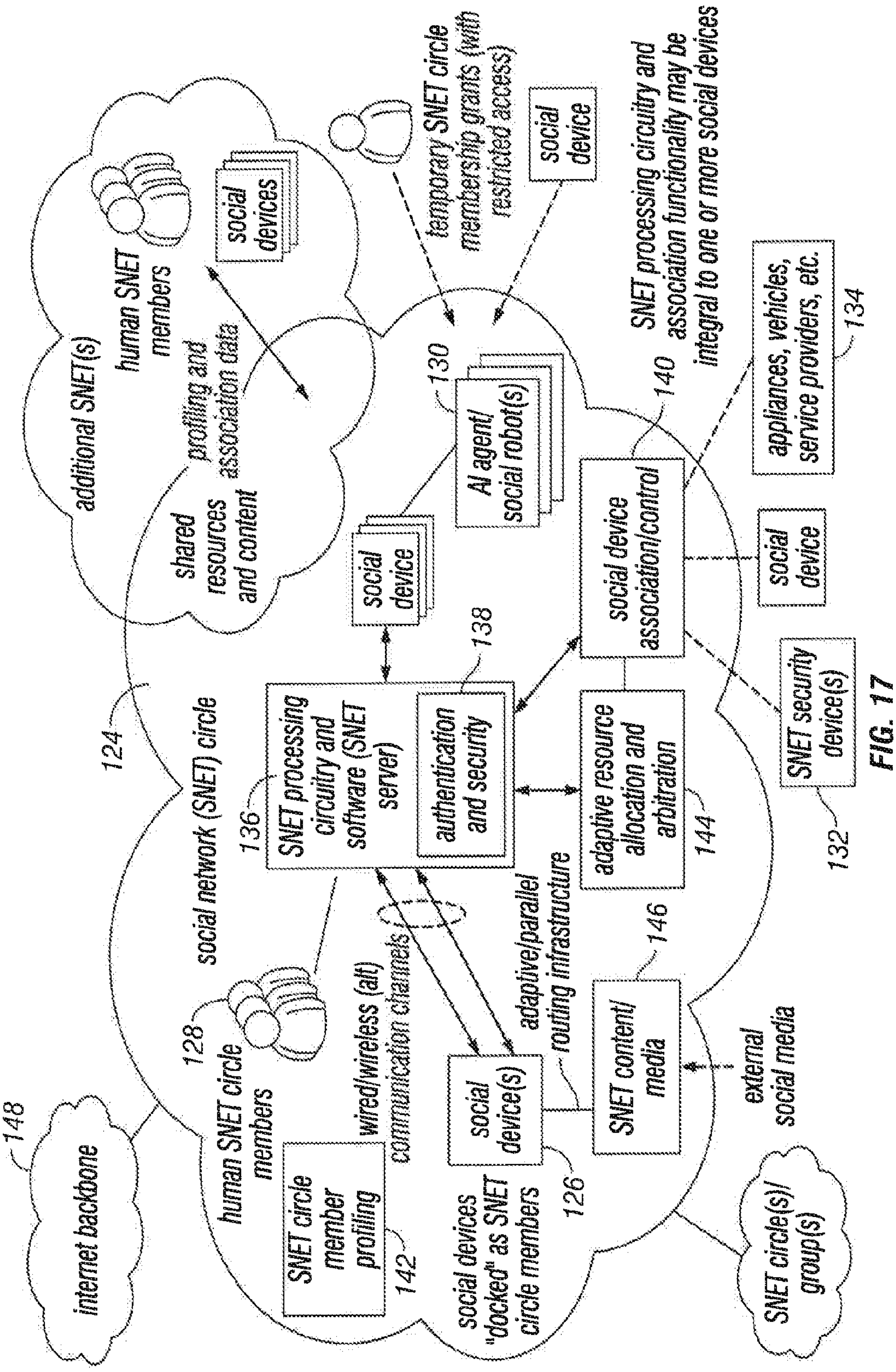

additional SNET(s)
human SNET members
social devices
profiling and association data
shared resources and content
temporary SNET circle membership grants (with restricted access)
social device
SNET processing circuitry and association functionality may be integral to one or more social devices
130
AI agent/ social robot(s)
140
appliances, vehicles, service providers, etc.
134
social device
social device association/control
social device
138
SNET processing circuitry and software (SNET server)
authentication and security
136
124
social network (SNET) circle
adaptive resource allocation and arbitration
144
SNET security device(s)
132
146
SNET content/ media
external social media
adaptive/parallel routing infrastructure
wired/wireless (alt) communication channels
128
human SNET circle members
social device(s)
126
social devices "docked" as SNET circle members
SNET circle member profiling
142
148
internet backbone
SNET circle(s)/ group(s)

FIG. 17

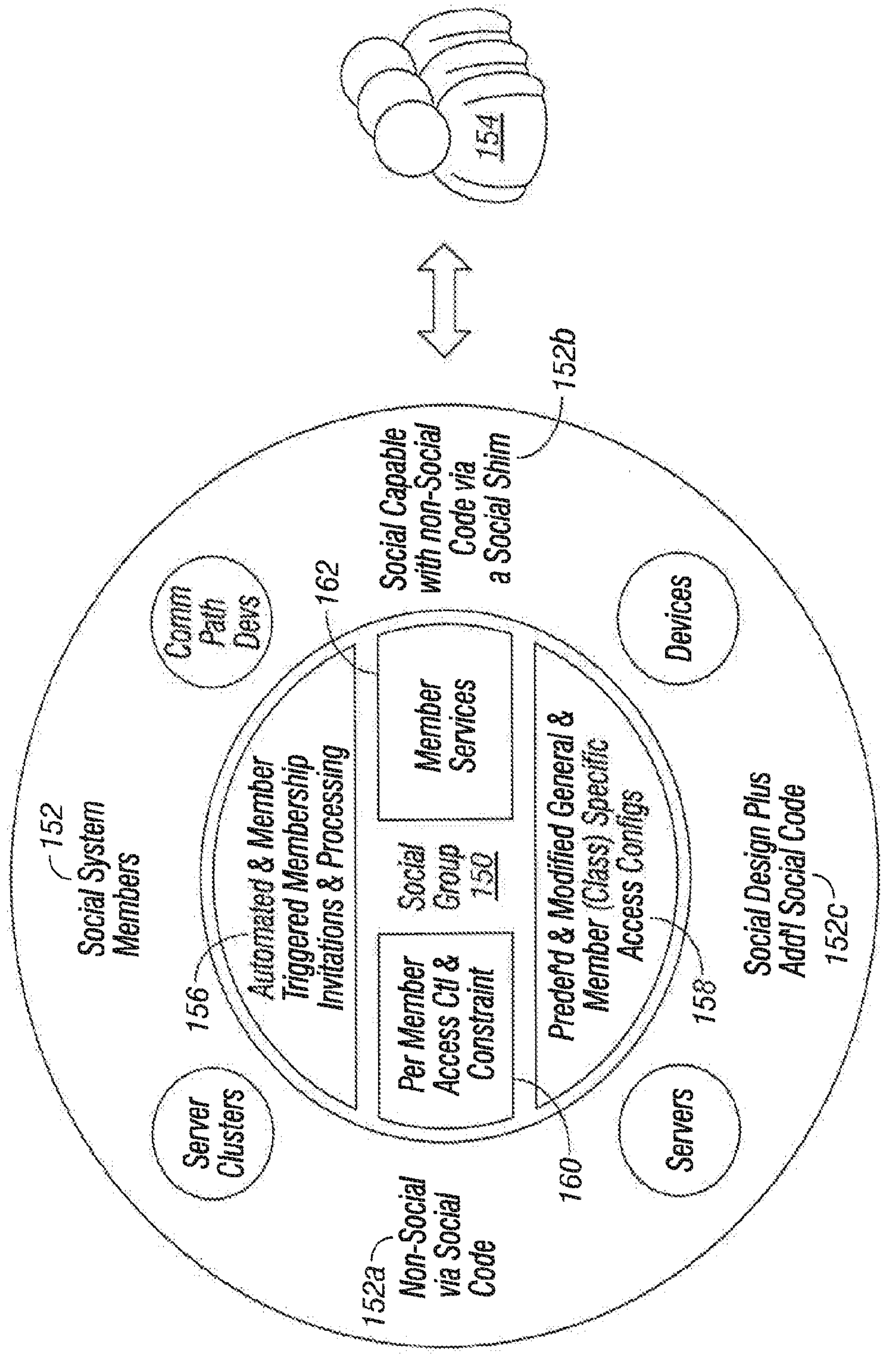

154
152 Social System Members
Server Clusters
Comm Path Devs
152a Non-Social via Social Code
Social Capable with non-Social Code via a Social Shim 152b
Servers
Devices
Social Design Plus Add'l Social Code 152c
156 Automated & Member Triggered Membership Invitations & Processing
162
Per Member Access Ctl & Constraint
Social Group 150
Member Services
160
Predef'd & Modified General & Member (Class) Specific Access Configs 158

FIG. 18

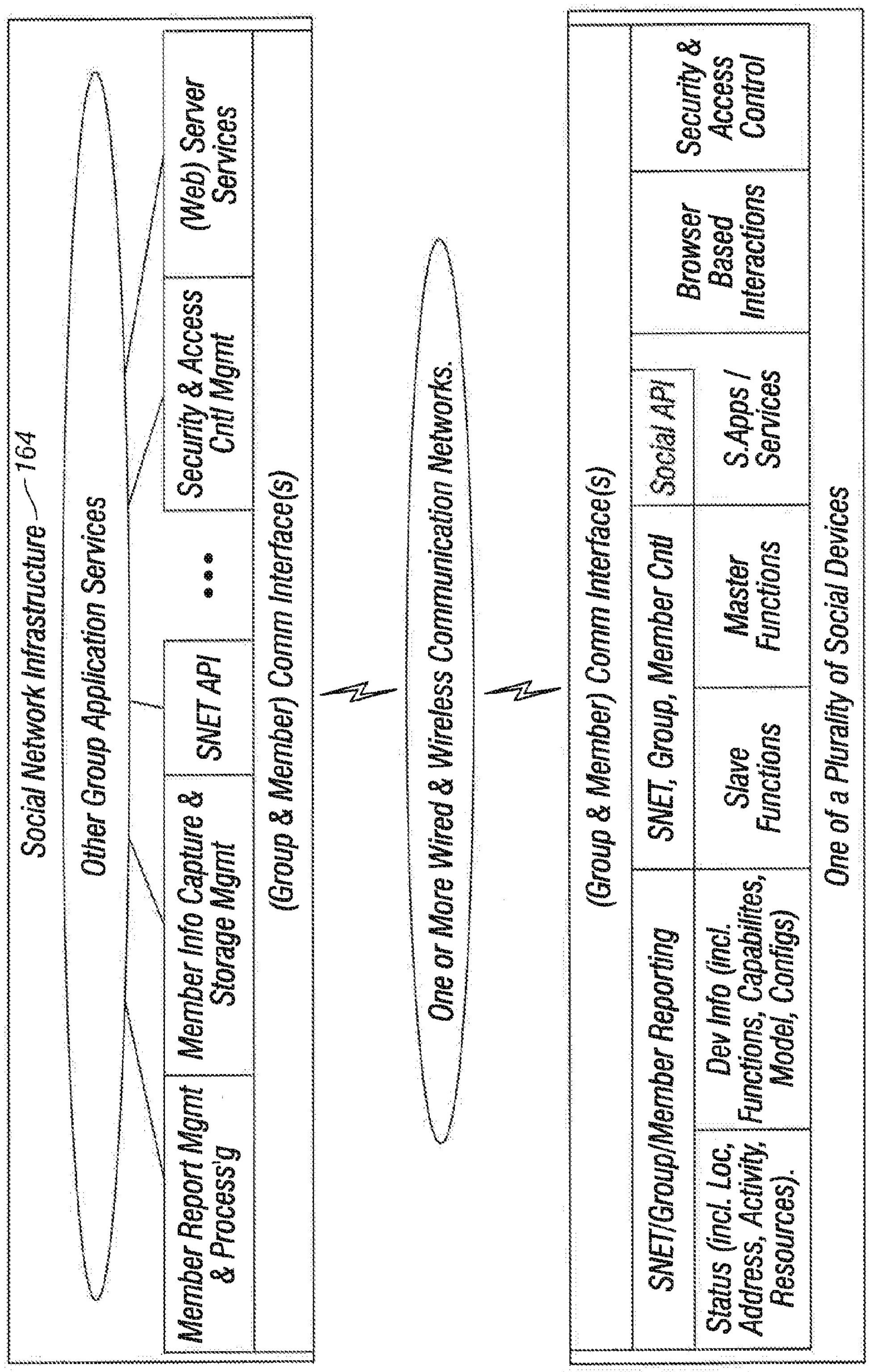

Social Network Infrastructure
164
Other Group Application Services
Member Report Mgmt & Process'g
Member Info Capture & Storage Mgmt
SNET API
• • •
Security & Access Cntl Mgmt
(Web) Server Services
(Group & Member) Comm Interface(s)
One or More Wired & Wireless Communication Networks.
(Group & Member) Comm Interface(s)
SNET/Group/Member Reporting
SNET, Group, Member Cntl
Social API
Browser Based Interactions
Security & Access Control
Status (incl. Loc, Address, Activity, Resources).
Dev Info (incl. Functions, Capabilites, Model, Configs)
Slave Functions
Master Functions
S.Apps / Services
One of a Plurality of Social Devices

FIG. 19

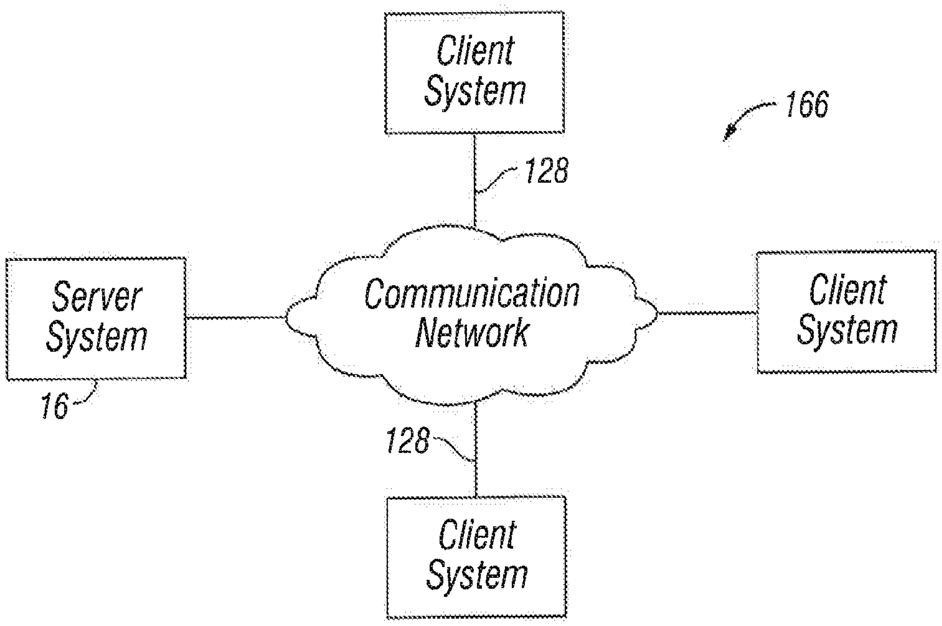

Client
System
166
128
Server
System
Communication
Network
Client
System
16
128
Client
System

FIG. 20

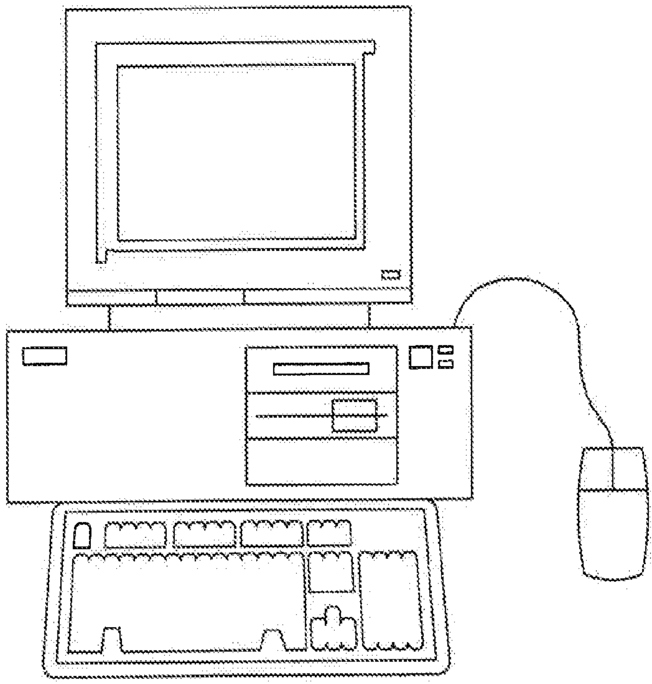
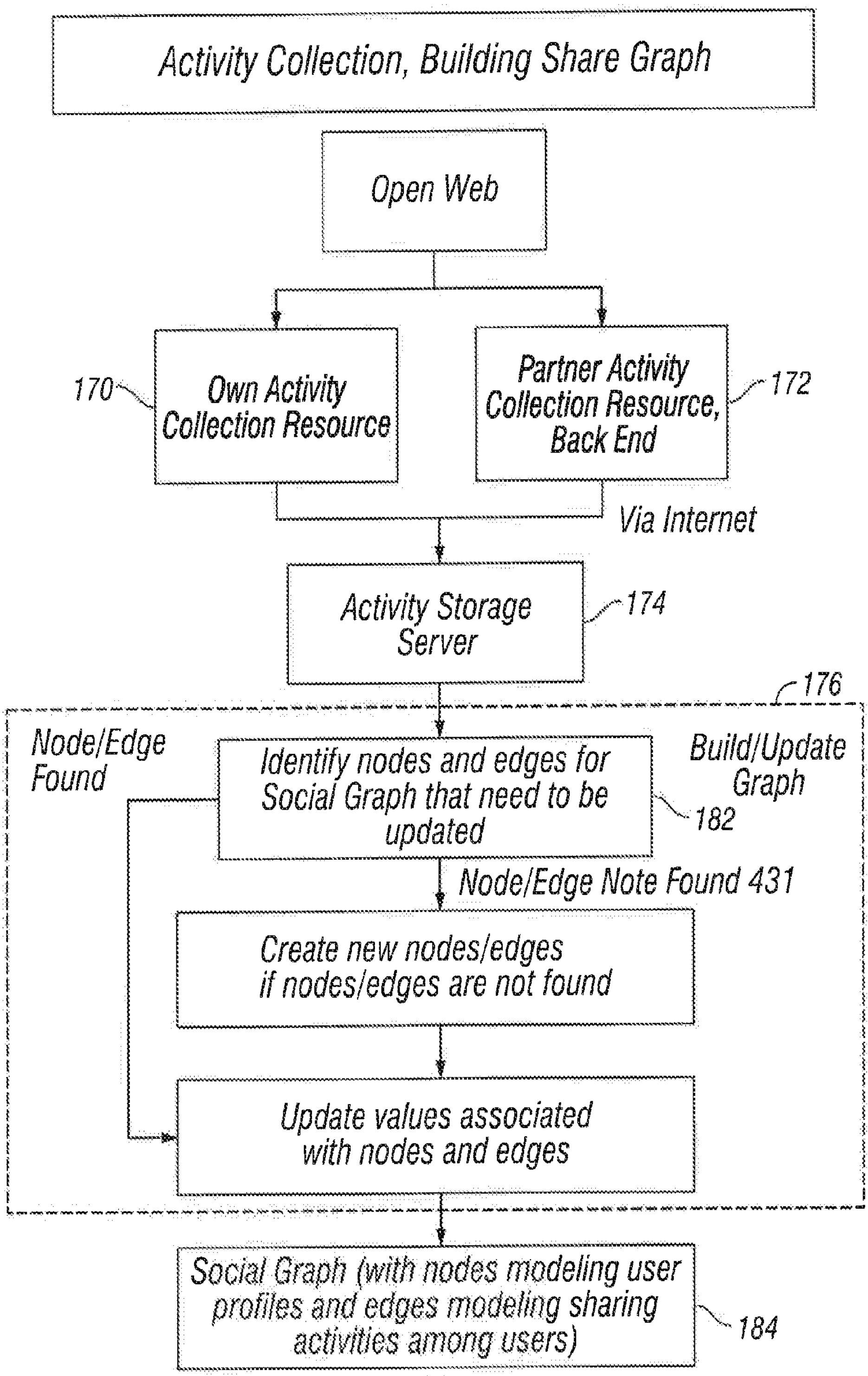


FIG. 21



Activity Collection, Building Share Graph
Open Web
170
Own Activity Collection Resource
Partner Activity Collection Resource, Back End
172
Via Internet
Activity Storage Server
174
176
Node/Edge Found
Identify nodes and edges for Social Graph that need to be updated
Build/Update Graph
182
Node/Edge Note Found 431
Create new nodes/edges if nodes/edges are not found
Update values associated with nodes and edges
Social Graph (with nodes modeling user profiles and edges modeling sharing activities among users)
184

FIG. 22

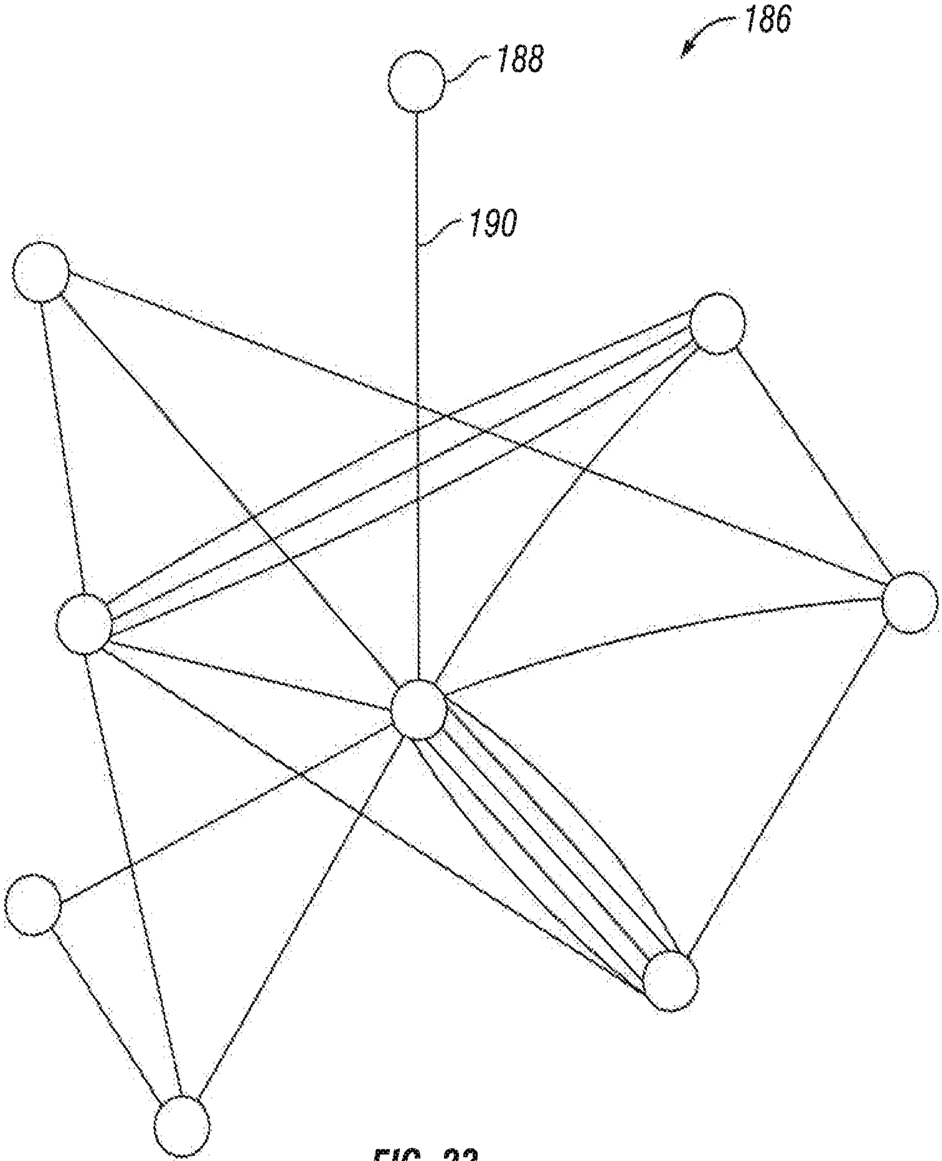


FIG. 23

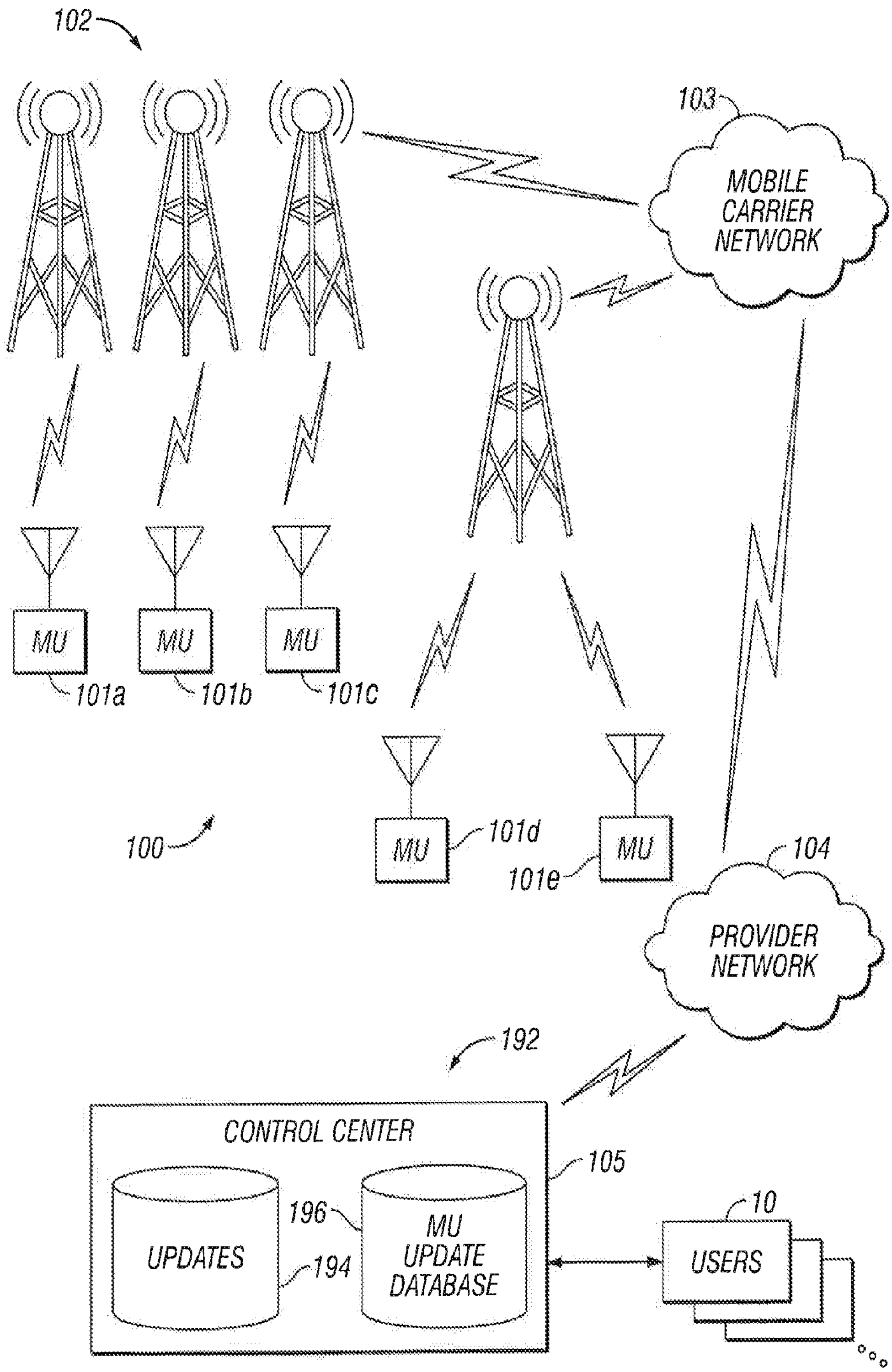

102
103
MOBILE CARRIER NETWORK
MU
MU
MU
101a
101b
101c
100
MU
101d
MU
101e
104
PROVIDER NETWORK
192
CONTROL CENTER
105
196
UPDATES
194
MU UPDATE DATABASE
10
USERS

FIG. 24

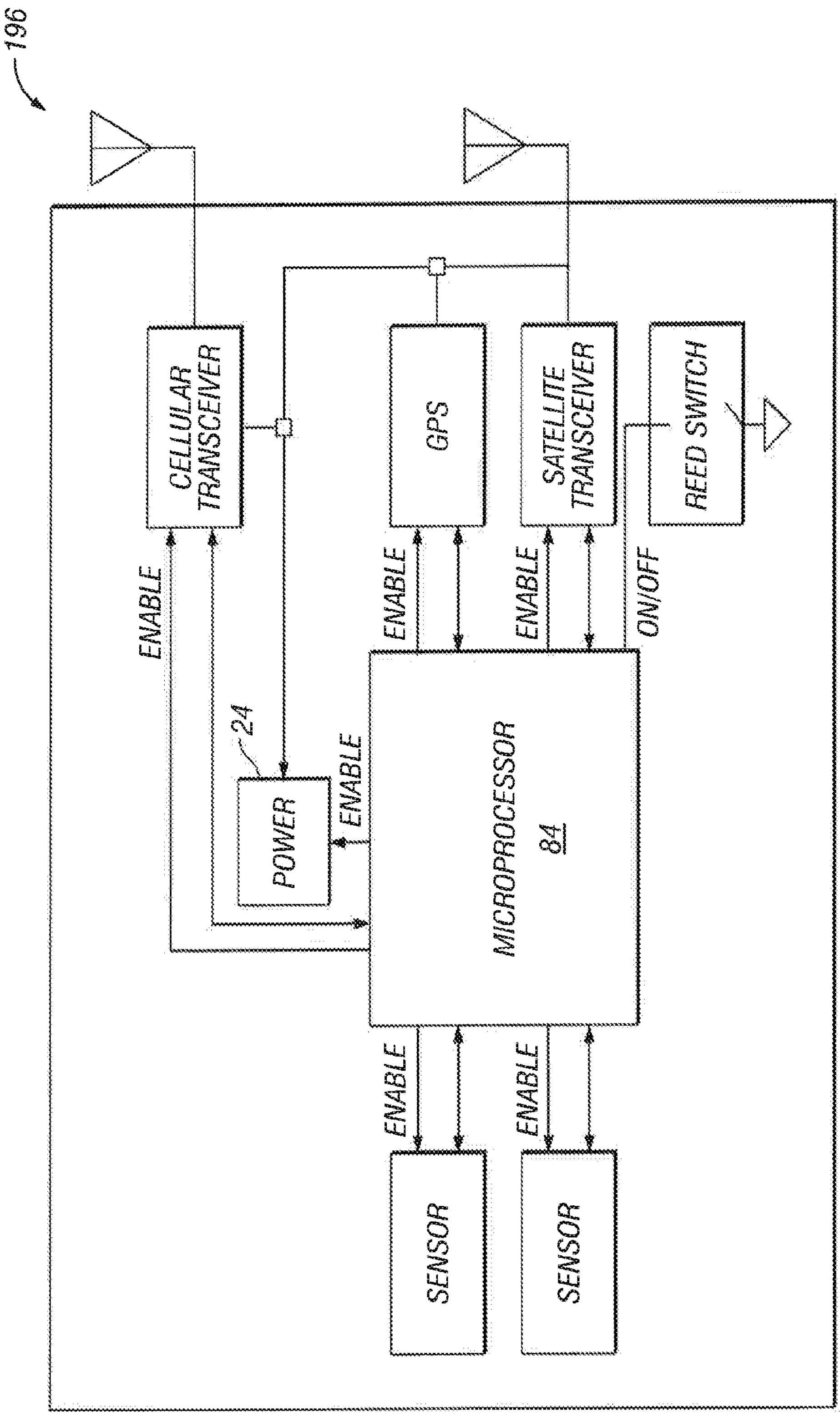

196
CELLULAR TRANSCEIVER
GPS
SATELLITE TRANSCEIVER
REED SWITCH
ENABLE
ENABLE
ENABLE
ON/OFF
24
POWER
ENABLE
MICROPROCESSOR
84
ENABLE
ENABLE
SENSOR
SENSOR

FIG. 25

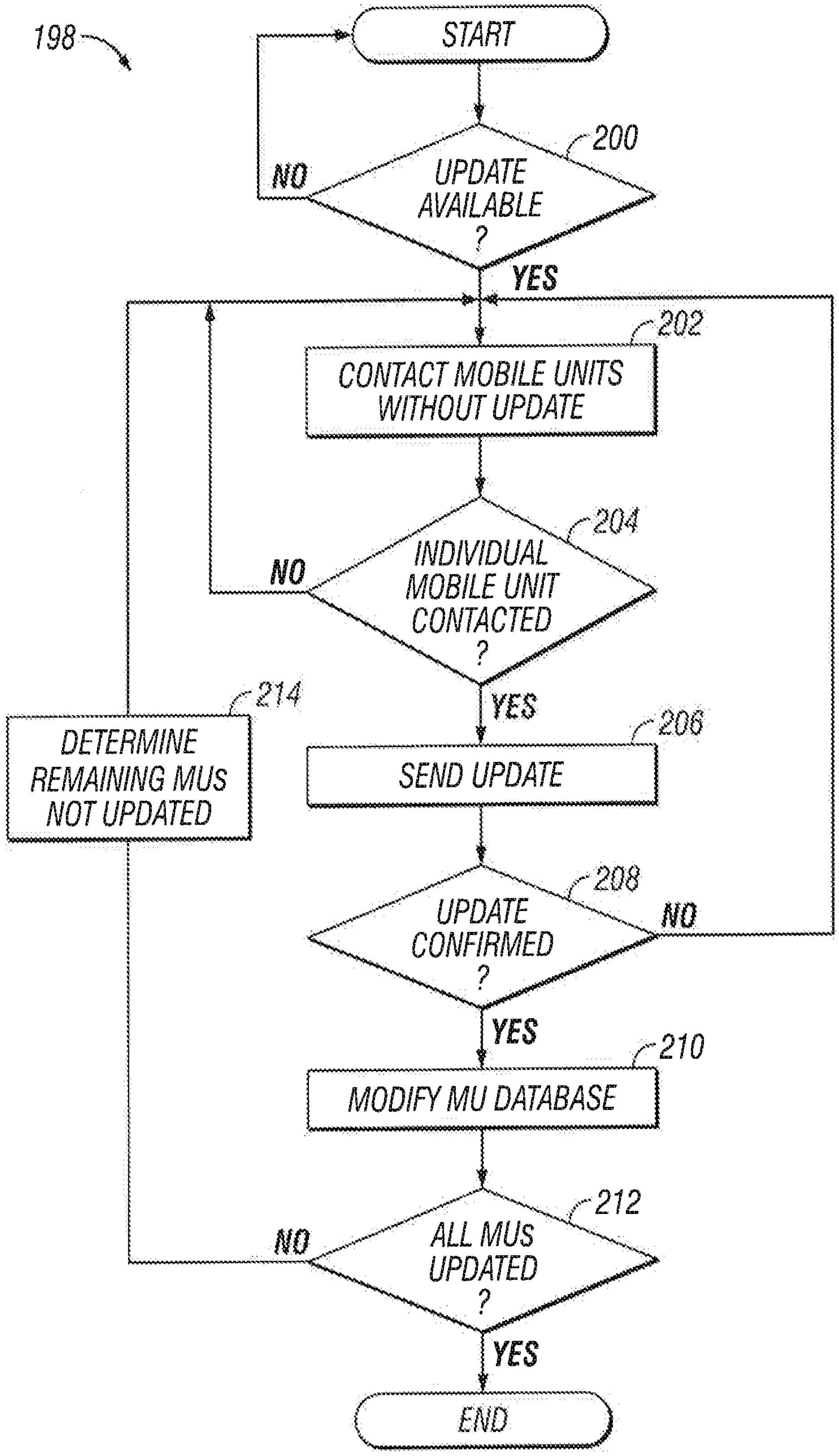

198
START
200
UPDATE AVAILABLE ?
NO
YES
202
CONTACT MOBILE UNITS WITHOUT UPDATE
204
INDIVIDUAL MOBILE UNIT CONTACTED ?
NO
YES
206
SEND UPDATE
208
UPDATE CONFIRMED ?
NO
YES
210
MODIFY MU DATABASE
214
DETERMINE REMAINING MUs NOT UPDATED
212
ALL MUs UPDATED ?
NO
YES
END

FIG. 26

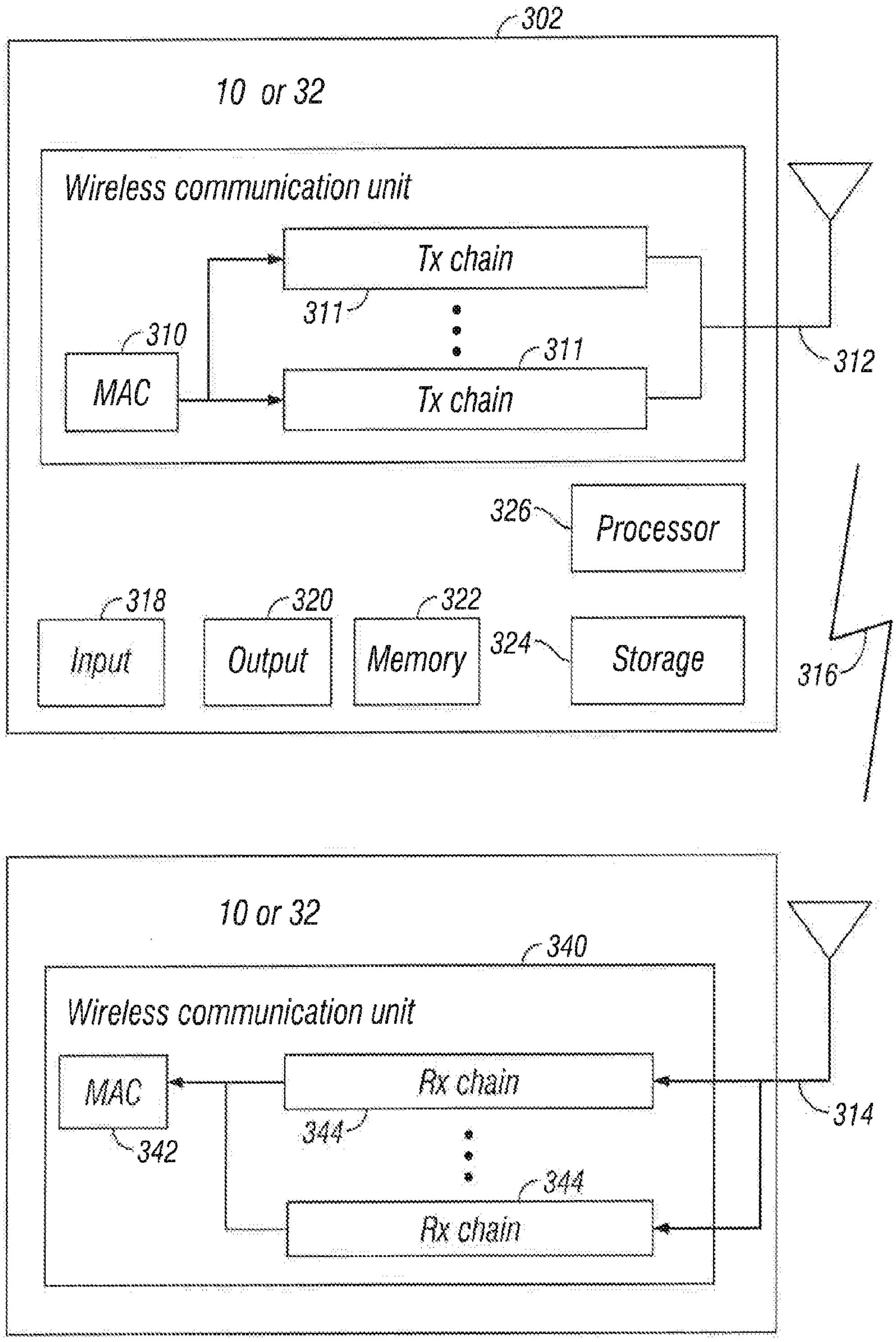
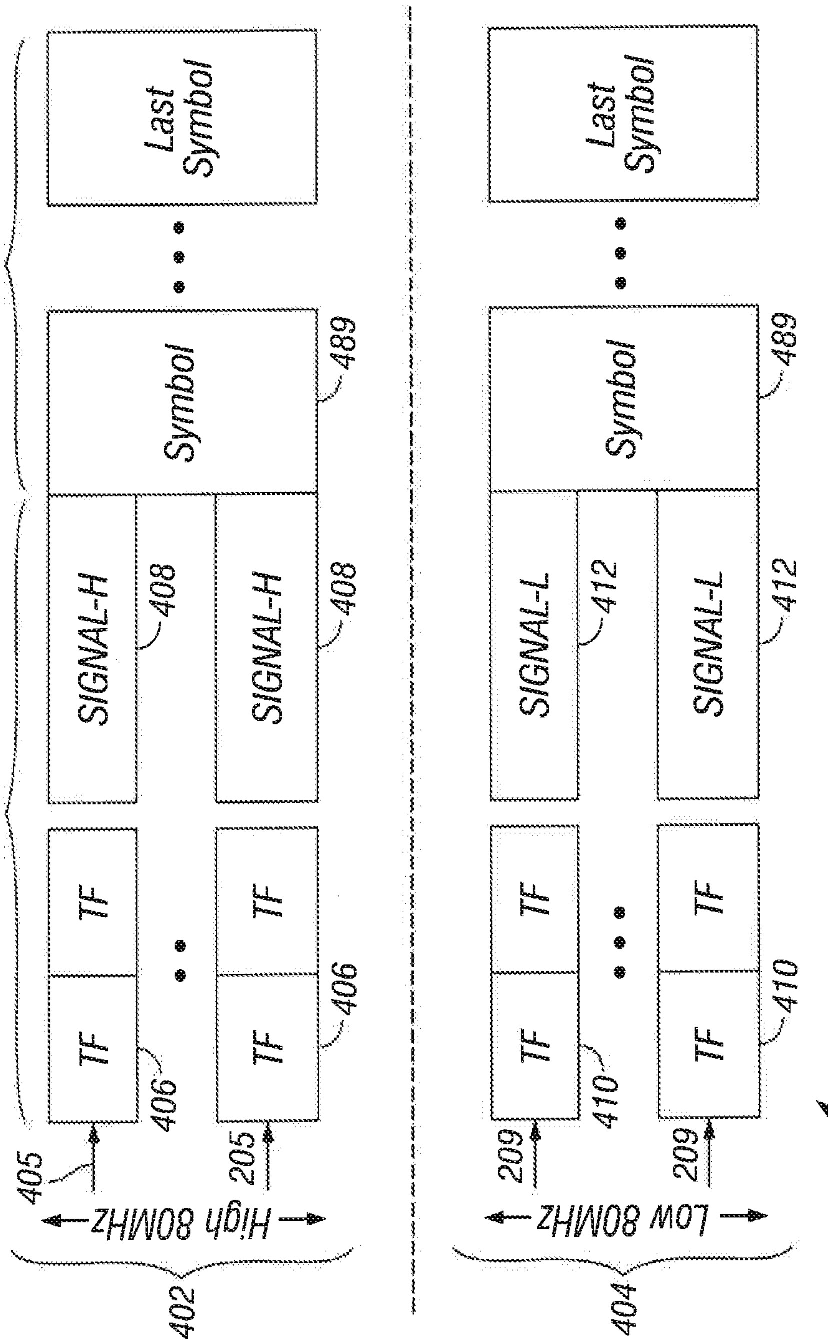

302
10 or 32
Wireless communication unit
Tx chain
311
310
MAC
311
Tx chain
312
326
Processor
318
320
322
Input
Output
Memory
324
Storage
316
10 or 32
340
Wireless communication unit
MAC
Rx chain
344
342
314
344
Rx chain

FIG. 27



High 80MHz
Low 80MHz
TF
TF
SIGNAL-H
SIGNAL-L
Symbol
Last Symbol
402
404
405
205
209
406
408
410
412
482
484
489
400

FIG. 28

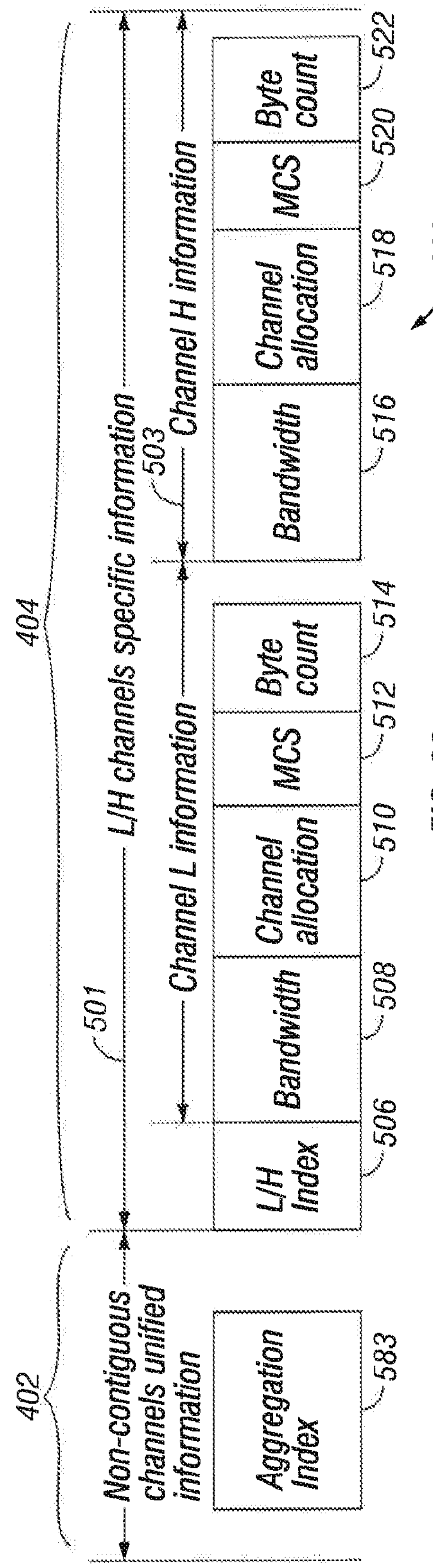

402
Non-contiguous channels unified information
Aggregation Index
583
404
L/H channels specific information
501
Channel L information
L/H Index
506
Bandwidth
508
Channel allocation
510
MCS
512
Byte count
514
503
Channel H information
Bandwidth
516
Channel allocation
518
MCS
520
Byte count
522
600

FIG. 29

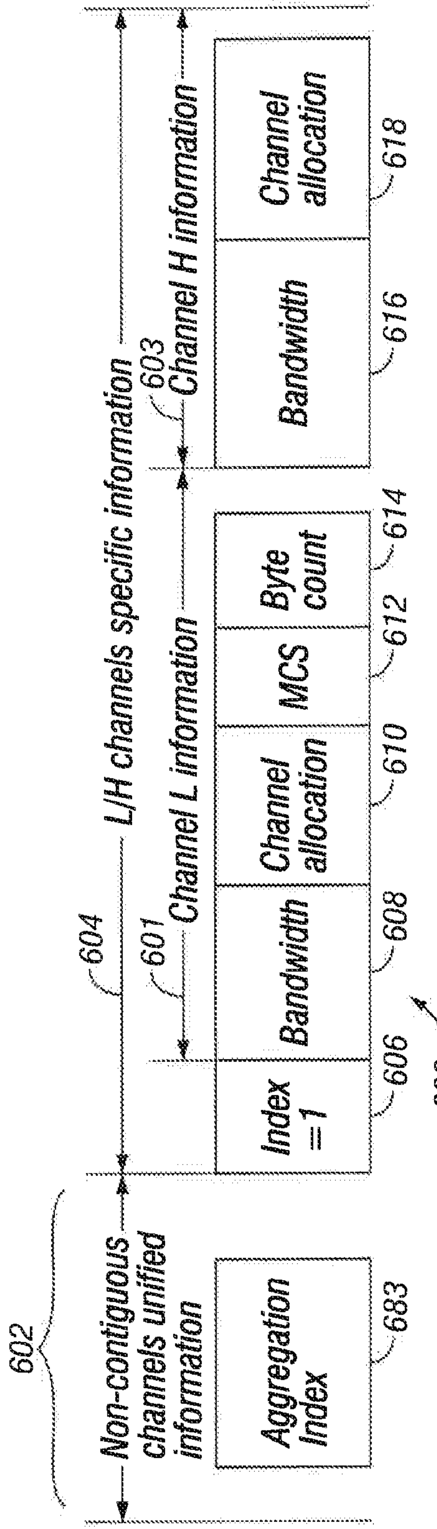

602
Non-contiguous channels unified information
Aggregation Index
683
604
L/H channels specific information
601
Channel L information
Index =1
606
Bandwidth
608
Channel allocation
610
MCS
612
Byte count
614
603
Channel H information
Bandwidth
616
Channel allocation
618
600

FIG. 30

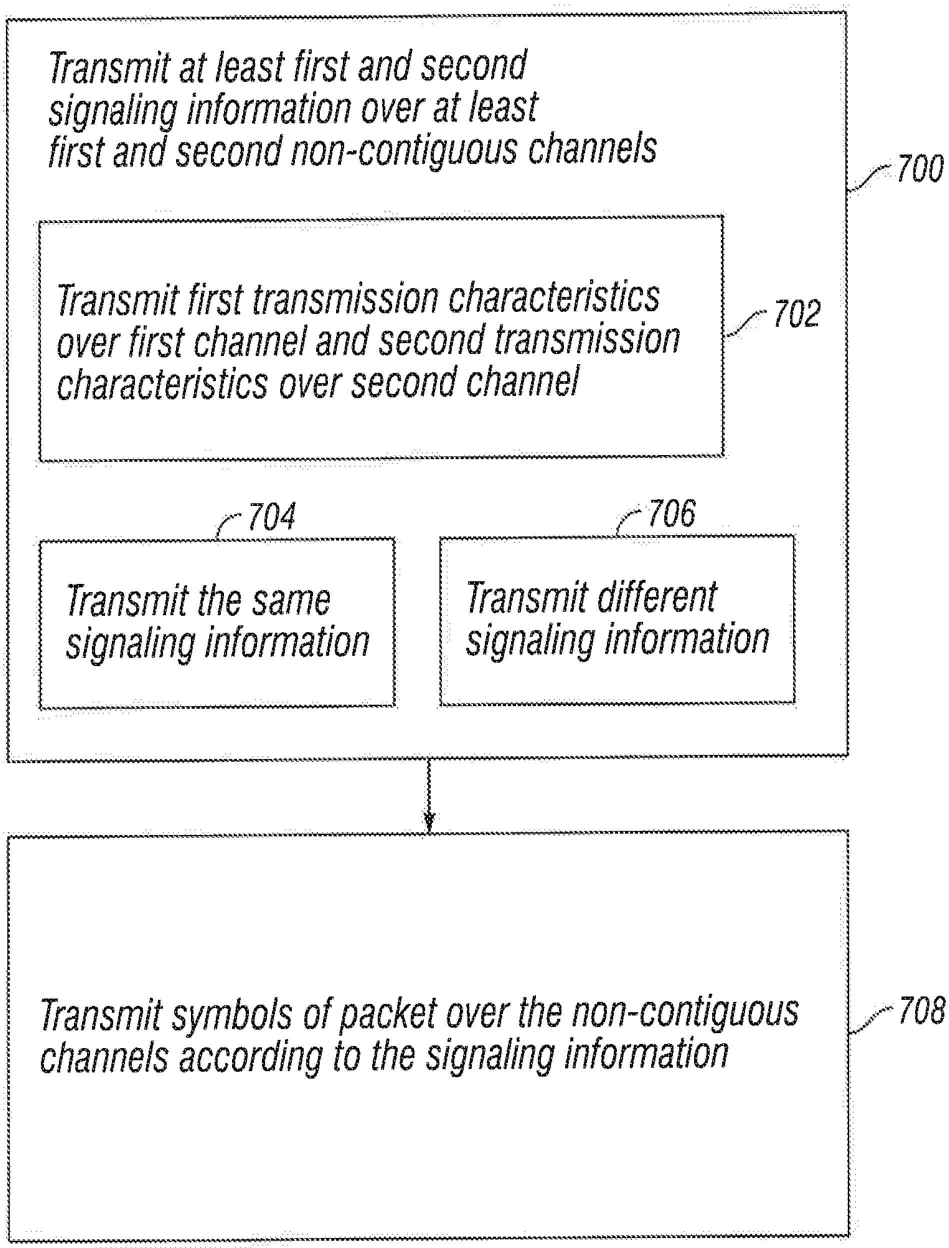

Transmit at least first and second signaling information over at least first and second non-contiguous channels
700
Transmit first transmission characteristics over first channel and second transmission characteristics over second channel
702
704
Transmit the same signaling information
706
Transmit different signaling information
Transmit symbols of packet over the non-contiguous channels according to the signaling information
708

FIG. 31

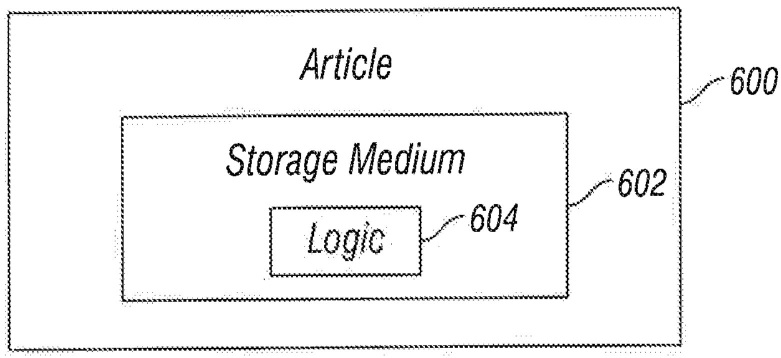

Article
600
Storage Medium
602
Logic
604

FIG. 32

MONITORING DEVICE WITH WIRELESS COMMUNICATION OVER NON-CONTIGUOUS CHANNELS

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 communicating over non-contiguous channels.

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] An increased throughput, e.g., above 1 Gigabit-per-second (Gbps) per wireless communication client, may be required in order, for example, to satisfy a demand for transferring increased amounts of data within wireless communication networks, such as, for example, wireless local area networks (WEAN) and/or wireless personal area networks (WPAN).

[0008] The increased throughput may be achieved, for example, by using a communication link having a wide bandwidth. For example, a bandwidth of more than 80 Mega-Hertz (MHz) may be required in order to provide a throughput greater than 1 Gbps, e.g., in a network operating over a frequency band of 5 Giga-Hertz (GHz) in accordance with the IEEE 802.11 standards.

[0009] A plurality of wireless communication channels may be required in order to achieve the high bandwidth. For example, more than four 20 MHz channels may be required, e.g., according to the IEEE 802.11 standards, in order to achieve a bandwidth of more than 80 MHz.

[0010] However, a likelihood of allocating a channel having a wide bandwidth may be relatively low due, for example, to interference, overlapping networks, regulatory limitations, and the like.

[0011] There is a need for improved communication systems used by remote monitoring devices.

SUMMARY OF THE INVENTION

[0012] An object of the present invention is to provide improved monitoring devices, and their methods of use.

[0013] Another object of the present invention is to provide systems, and their associated methods, for transmitting and relaying information from a monitoring device using wireless communication systems other over a plurality of non-contiguous wireless communication channels.

[0014] These and other objects of the present invention are achieved in, wireless communication system for a monitoring device. The monitoring device includes, one or more sensors, a unique user ID, ID circuitry 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. The one or more sensors acquire user information selected from of at least one of, a user's activities, behaviors and habit information. A telemetry system is in communication with the monitoring device. The monitoring device and/or the telemetry system includes a wireless communication device that in operation transmits a wireless communication packet to the other over a plurality of non-contiguous wireless communication channels.

[0015] In another embodiment of the present invention, a monitoring device is coupled to a wireless communication system. The monitoring device has one or more sensors, an antenna and 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. A telemetry system communicates with the monitoring device via a plurality of transmission chains.

[0016] In another embodiment, a method of communicating wirelessly with a monitoring device obtains from one or more sensors of the monitoring device user information selected from of at least one of, a user's activities, behaviors and habit information. A telemetry system communicates with the monitoring device. The wireless communication device transmits a wireless communication packet between the monitoring device and the monitoring device over a plurality of non-contiguous wireless communication channels.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] FIGS. **1**(*a*) and **1**(*b*) illustrate one embodiment of a wearable device of the present invention, where one size fits all.

[0018] FIG. **2** illustrates one embodiment of electronics that can be included in the wearable device.

[0019] FIG. **3** illustrates one embodiment of a telemetry system of the present invention.

[0020] FIG. **4** is a diagram of the programming input schematic of the secure sensor/transmitter array of FIG. **7**.

[0021] FIG. **5** is a block diagram of the system of programming the sensor/transmitter(s) comprising the secure sensor/transmitter array of FIG. **7**.

[0022] FIG. **6** is a block diagram of the jam command and security/randomization bits of the secure sensor/transmitter array of FIG. **7**.

[0023] FIG. **7** is a logic circuit diagram of the sensor/transmitter programming input schematic in one embodiment of the present invention.

[0024] 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.

[0025] FIG. **9** is a block diagram illustrating one embodiment of a SNAPSHOT GPS receiver for use according to the present invention.

[0026] FIG. **10** is a block diagram of a remote sensor shown in communication with two different external communication devices.

[0027] FIG. **11** is a diagram of the active RF and RF backscatter antennas.

[0028] FIG. **12** is a diagram of the encoding scheme for the symbols in the active RF protocol.

[0029] FIG. **13** is a diagram of the packet structure in the IRDA protocol.

[0030] FIG. **14** is a diagram of the encoding scheme in the IRDA protocol.

[0031] FIG. **15** illustrates one embodiment of a wireless network that can be used with the present invention.

[0032] 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.

[0033] FIG. **17** illustrates an embodiment of a social network circle with social devices in accordance with one embodiment of the present invention.

[0034] FIG. **18** illustrates an embodiment of a social group with a variety of members in accordance with one embodiment of the present invention.

[0035] FIG. **19** is a functional block diagram illustrating a social network infrastructure and social devices in accordance with one embodiment of the invention.

[0036] FIG. **20** illustrates a simplified block diagram of a client-server system and network in one embodiment of the present invention.

[0037] 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.

[0038] 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.

[0039] 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.

[0040] FIG. **24** is a block diagram of an embodiment of a system for distributing firmware updates to a large number of monitoring devices.

[0041] FIG. **25** is a block diagram of an embodiment of an asset tag for a monitoring device having wireless communications capabilities.

[0042] FIG. **26** is a flow chart for an embodiment of a method of distributing firmware updates to a large number of monitoring devices.

[0043] FIG. **27** is a schematic block diagram illustration of a system, in accordance with some demonstrative embodiments.

[0044] FIG. **28** is a schematic illustration of a transmission scheme of a wireless communication packet, in accordance with some demonstrative embodiments.

[0045] FIG. **29** is a schematic illustration of a signaling field, in accordance with one demonstrative embodiment.

[0046] FIG. **30** is a schematic illustration of a signaling field, in accordance with another demonstrative embodiment.

[0047] FIG. **31** is a schematic flow-chart illustration of a method of wireless communication over non-contiguous channels, in accordance with some demonstrative embodiments.

[0048] FIG. **32** is a schematic illustration of an article of manufacture, in accordance with some demonstrative embodiments.

DETAILED DESCRIPTION

[0049] 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.

[0050] 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.

[0051] 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 BLUETOOTH® circuit, and WIFI circuitry, where the persistent memory may contain programs, applications, and/or an operating system for the mobile device.

[0052] 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").

[0053] A 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.

[0054] 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.

[0055] 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.

[0056] 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:

- **[0057]** LANs or WANs belonging to multiple organizations and interconnected and accessed using remote dial-up
- **[0058]** LANs or WANs belonging to multiple organizations and interconnected and accessed using dedicated lines
- **[0059]** 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.

[0060] 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:

- **[0061]** A LAN
- **[0062]** A Wide-area network (WAN) that is comprised of a LAN that extends usage to remote employees with dial-up access
- **[0063]** A WAN that is comprised of interconnected LANs using dedicated communication lines
- **[0064]** 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).

[0065] For purposes of the present invention, the Internet, extranets and intranets collectively are referred to as ("Network Systems").

[0066] 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 Sp02, 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.

[0067] 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, erthrocytes hemoglobin and the like.

[0068] 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 and includes for example, a device capable of wireless communication, a communication device capable of wireless communication, a communication station capable of wireless communication, a portable or non-portable device capable of wireless communication, or the like. In some demonstrative embodiments, a wireless device may be or may include a peripheral that is integrated with a computer, or a peripheral that is attached to a computer. In some demonstrative embodiments, the term "wireless device" may optionally include a wireless service.

[0069] 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.

[0070] 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.

[0071] 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.

[0072] 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.

[0073] 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.

[0074] 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.

[0075] 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.

[0076] 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.

[0077] 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.

[0078] 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.

[0079] 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**.

[0080] 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.

[0081] 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.

[0082] 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.

[0083] 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.

[0084] 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.

[0085] 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.

[0086] In one embodiment, the monitoring device **10** uses an accelerometer, gyroscope, GPS sensor, a BLUETOOTH® chip, and a heart rate monitor.

[0087] 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.

[0088] 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.

[0089] 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.

[0090] 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.

[0091] 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.

[0092] 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.

[0093] 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**.

[0094] 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.

[0095] In various embodiments, the monitoring device **10** uses algorithms to determine activity type, behavioral patterns and user habits based on collected data.

[0096] 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.

[0097] 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 conversation of time, energy and data storage.

[0098] 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.

[0099] 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.

[0100] 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.

[0101] In one embodiment, the monitoring device **10** can have a sync feature for multiple bands at the same time.

[0102] 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.

[0103] 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.

[0104] 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.

[0105] 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.

[0106] 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.

[0107] With the monitoring device **10** of the present invention, mechanical actions of the user can be triggered, recognized and evaluated.

[0108] 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.

[0109] 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.

[0110] 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.

[0111] 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.

[0112] 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**.

[0113] 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.

[0114] 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.

[0115] In various embodiments, the monitoring device **10** and/or system **32** are fully sealed and have inductively charges. All communication is done wirelessly.

[0116] 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**.

[0117] 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.

[0118] 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 preprocesses 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.

[0119] 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**.

[0120] 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**.

[0121] 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.

[0122] 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.

[0123] 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.

[0124] 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.

[0125] In one embodiment, the monitoring device **10** can determine emotion of the user.

[0126] 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.

[0127] 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.

[0128] 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.

[0129] 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.

[0130] In one embodiment, the app can be used on a mobile device, including but not limited to a smart phone and the like.

[0131] 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.

[0132] In one embodiment, the monitoring device **10** has artificial intelligence. A wearable device processor **54** implements logic resources that exist on monitoring device **10**.

[0133] 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.

[0134] 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.

[0135] 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**.

[0136] 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.

[0137] In one embodiment, an inductive field coil is used for programming the sensors **14** and ID of monitoring device **10**.

[0138] 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**.

[0139] 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:

[0140] Both the sensor **14** and receiver **34** contain an identical, repeatable pseudo randomization algorithm in ROM or in ASIC logic.

[0141] 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**.

[0142] 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.

[0143] 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.

[0144] 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**.

[0145] 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.

[0146] 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**.

[0147] 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**

[0148] 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**.

[0149] 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.

[0150] 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.

[0151] 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.

[0152] 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.

[0153] 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.

[0154] 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.

[0155] 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.

[0156] 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.

[0157] 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.

[0158] 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.

[0159] 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**.

[0160] 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.

[0161] 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.

[0162] FIG. **6** shows the relative positioning and shape of the active RF antenna **92** and the RF backscatter antenna **98**.

[0163] 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.

[0164] 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.

[0165] 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.

[0166] 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.

[0167] 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 "I" 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**.

[0168] 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.

[0169] 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.

[0170] 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.

[0171] 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**.

[0172] 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.

[0173] 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**.

[0174] 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.

[0175] 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.

[0176] 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.

[0177] In one embodiment, the mobile device **74** receives information from the monitoring device **10**, e.g., the unique ID, 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.

[0178] 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.

[0179] 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.

[0180] 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.

[0181] 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.

[0182] 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.

[0183] 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.

[0184] 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.

[0185] 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.

[0186] 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**.

[0187] 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.

[0188] 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.

[0189] 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.

[0190] 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.

[0191] 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.

[0192] 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**.

[0193] Briefly, membership in the SNET circle **124** may comprise docked and undocked social devices **124** and human SNET circle members **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.

[0194] 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.

[0195] 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.

[0196] 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 **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**.

[0197] 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.

[0198] 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 **152***a* may include social code that enables participation in the social group **150**. In a further embodiment, a device **152***b* 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 **152***c* having a social design may utilize additional social code, including code specific to a social group **150**.

[0199] 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).

[0200] 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.

[0201] 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.

[0202] 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.

[0203] 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.

[0204] 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.

[0205] The communication network **166** may itself be comprised of many interconnected computer systems and communication links. Communication links **168** may be hardwire 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.

[0206] 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.

[0207] 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 backing 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**.

[0208] 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.

[0209] 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 802.11 ac, 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.

[0210] 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.

[0211] 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.

[0212] 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.

[0213] 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.

[0214] 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.

[0215] 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.

[0216] 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.

[0217] 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.

[0218] 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.

[0219] 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.

[0220] 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.

[0221] 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.

[0222] 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.

[0223] 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.

[0224] 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.

[0225] 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.

[0226] 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.

[0227] In one embodiment, more recently sent messages are given a greater weight than older messages.

[0228] 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**.

[0229] 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.

[0230] 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.

[0231] FIG. **25** discloses one embodiment of monitoring device **10**, with the ID or asset tag **196**. The tag **196** can includes 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.

[0232] 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**.

[0233] 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.

[0234] 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**.

[0235] 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**.

[0236] 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.

[0237] As illustrated in FIG. **27**, telemetry system **32** and monitoring device **10** are typically wireless devices capable of communicating content, data, information and/or signals over a wireless communication link **316**, e.g., as described in detail below. One or more elements of system telemetry system **32** or monitoring device may optionally be capable of communicating over any suitable wired communication links.

[0238] In some demonstrative embodiments, monitoring device **10** and/or telemetry system **32** may include a wireless communication unit **308** to transmit, via one or more antennae **312**, a wireless transmission to device **306** over wireless communication link **316**. Device **306** may include a wireless communication unit **340** to receive the wireless transmission via one or more antennae **714**. Types of antennae that may be used for antennae **312** and/or **314** may include but are not limited to internal antenna, dipole antenna, omni-directional antenna, a monopole antenna, an end fed antenna, a circularly polarized antenna, a micro-strip antenna, a diversity antenna and the like.

[0239] In some demonstrative embodiments, wireless communication link **316** may have a bandwidth of at least 160 Mega-Hertz (MHz), e.g., as described below. In other embodiments, wireless communication link **316** may have any other suitable bandwidth.

[0240] In some demonstrative embodiments, wireless communication devices monitoring device **10** and/or telemetry system **32** may also include, for example, one or more of a processor **326**, an input unit **318**, an output unit **320**, a memory unit **322**, and a storage unit **324**. Monitoring device **10** and/or telemetry system **32** may optionally include other suitable hardware components and/or software components.

[0241] Processor **326** includes, for example, a Central Processing Unit (CPU), a Digital Signal Processor (DSP), one or more processor cores, a single-core processor, a dual-core processor, a multiple-core processor, a microprocessor, a host processor, a controller, a plurality of processors or controllers, a chip, a microchip, one or more circuits, circuitry, a logic unit, an Integrated Circuit (IC), an Application-Specific IC (ASIC), or any other suitable multi-purpose or specific processor or controller. Processor **326** executes instructions, for example, of an Operating System (OS) of monitoring device **10** and/or telemetry system **32**.

[0242] Input unit **318** includes, for example, a keyboard, a keypad, a mouse, a touch-pad, a track-ball, a stylus, a microphone, or other suitable pointing device or input device. Output unit **320** includes, for example, a monitor, a screen, a flat panel display, a Cathode Ray Tube (CRT) display unit, a Liquid Crystal Display (LCD) display unit, a plasma display unit, one or more audio speakers or earphones, or other suitable output devices.

[0243] Memory unit **322** includes, for example, a Random Access Memory (RAM), a Read Only Memory (ROM), a Dynamic RAM (DRAM), a Synchronous DRAM (SD-RAM), a flash memory, a volatile memory, a non-volatile memory, a cache memory, a buffer, a short term memory unit, a long term memory unit, or other suitable memory units. Storage unit **324** includes, for example, a hard disk drive, a floppy disk drive, a Compact Disk (CD) drive, a CD-ROM drive, a DVD drive, or other suitable removable or non-removable storage units. Memory unit **322** and/or storage unit **324**, for example, may store data processed by monitoring device **10** and/or telemetry system **32**.

[0244] In some demonstrative embodiments, wireless communication link **316** may include a plurality of non-contiguous wireless communication channels.

[0245] The phrase "non-contiguous channels", as used herein, may refer to two or more wireless communication channels, which are not adjacent, neighboring, and/or bordering one another. In one example, first and second wireless communication channels may be non-contiguous if, for example, the first wireless communication channel is separated from the second wireless communication channel, e.g., by one or more other wireless communication channels, sub-channels, frequency bands, and the like.

[0246] In some demonstrative embodiments, at least one channel of the plurality of non-contiguous channels has a bandwidth at least 20 MHz, e.g., at least 80 MHz. In other embodiments, the non-contiguous wireless communication channels may have any other suitable bandwidth.

[0247] In one embodiment, wireless communication link **316** may include at least two non-contiguous channels, each having a bandwidth of 80 MHz, or any other bandwidth. In other embodiments, wireless communication link **316** may include any other suitable number of wireless communication channels, which may have any other suitable bandwidth.

[0248] Some demonstrative embodiments are described below with reference to a wireless communication link, e.g., wireless communication link **316**, including two non-contiguous wireless communication channels having equal bandwidth, e.g., two 80 MHz channels. However, in other embodiments, the wireless communication link may include two or more non-contiguous wireless communication channels of different bandwidths. In one example, the wireless communication link may include at least one channel having a bandwidth of 80 MHz and at least one channel having a bandwidth different from 80 MHz, e.g., 20 MHz, 40 MHz, 120 MHz, 160 MHz and the like. In other embodiments, wireless communication link **316** may include any other suitable combination of two or more non-contiguous channels having any suitable bandwidth.

[0249] In some embodiments, wireless communication link **316** may include one or more additional channels, which may or may not be contiguous to one or more of non-contiguous channels. For example, wireless communication link **316** may include first and second non-contiguous 80 MHz channels, and a third channel, e.g., an 80 MHz channel, which may be contiguous to one of the first and second channels.

[0250] In some demonstrative embodiments, at least one channel of the plurality of non-contiguous channels may include two or more contiguous channels or sub-channels. For example, the 80 MHz. cannel may include four contiguous 20 MHz channels, e.g., in accordance with the 802.11 standards and/or any other suitable standard and/or protocol.

[0251] In some demonstrative embodiments, wireless communication unit **308** may include a plurality of transmit (Tx) chains **311** to transmit the wireless transmission over the plurality of wireless communication channels. Wireless communication unit **340** may include a plurality of receive (Rx) chains **344** to receive the wireless transmission over the plurality of wireless communication channels. For example, wireless communication unit **308** may include two Tx chains **311** to transmit the wireless transmission over two respective non-contiguous channels of link **316** and/or wireless communication unit **340** may include two Rx chains **344** to receive the wireless transmission over the two respective non-contiguous channels of link **316**, e.g., as described in detail below.

[0252] In some demonstrative embodiments, Tx chains **311** and/or Rx chains **344** may include any suitable Physical-layer (PHY) chains and/or components; any suitable Radio-Frequency (RF) chains and/or components; and/or any other suitable elements.

[0253] In some demonstrative embodiments, wireless communication unit **308** may include a media-access-controller (MAC) **310**, e.g., a single MAC, to commonly control the transmissions via Tx chains **311**; and/or wireless communication unit **340** may include a MAC **342**, e.g., a single MAC, to commonly control the reception via Rx chains **344**, e.g., as described in detail below.

[0254] In some demonstrative embodiments, MAC **310** may control Tx chains **311** to simultaneously transmit symbols of a wireless communication packet over the plurality of non-contiguous wireless communication channels of wireless communication link **316**. MAC **342** may control Rx chains **344** to simultaneously receive the symbols of the wireless communication packet over the plurality of non-contiguous wireless communication channels of wireless communication link **316**.

[0255] In some demonstrative embodiments, wireless communication unit **308** may transmit to wireless communication unit **340** signaling information defining transmission characteristics over the plurality of non-contiguous channels of link **316**, for example, as part of a preamble of the wireless communication packet, e.g., as described in detail below.

[0256] Reference is also made to FIG. **28**, which schematically illustrates a transmission scheme of a wireless communication packet **400** over first and second non-contiguous wireless communication channels **402** and **404**, respectively, in accordance with some demonstrative embodiments.

[0257] In some demonstrative embodiments, wireless communication channel **402** ("high channel" or "H channel") may include a spectrum of wireless communication frequencies, which may greater than a spectrum of wireless communication frequencies included within wireless communication channel **404** ("low channel" or "L channel").

[0258] In some demonstrative embodiments, wireless communication channels **402** and **404** may have the same bandwidth, e.g., 80 MHz. However, wireless communication channels **402** and **404** may have different bandwidths. In one example, one of wireless communication channels **402** and **404** may have a bandwidth of 80 MHz, while another of wireless communication channels **402** and **404** may have a bandwidth different from 80 MHz, e.g., 20 MHz, 40 MHz, 120 MHz, 160, MHz, and the like.

[0259] In some demonstrative embodiments, wireless communication channel **402** may include a plurality of contiguous channels or sub-channels **405**; and/or wireless communication channel **404** may include a plurality of contiguous channels or sub-channels **409**. For example, channels **405** and/or **409** may include four 20 MHz channels, e.g., in accordance with the 802.11 standards, and/or any other suitable channels.

[0260] In some demonstrative embodiments, wireless communication packet **400** may include a preamble portion **482** followed by a data portion **484**.

[0261] In some demonstrative embodiments, preamble portion **482** may be transmitted separately and/or synchronously over each of channels **405** and **409**. Data symbols **489** of packet **400** may be transmitted over non-contiguous channels **402** and **404**, e.g., simultaneously.

[0262] In some demonstrative embodiments, preamble portion **482** may include first common preamble information transmitted over each of contiguous channels **405**; and/or second common preamble information transmitted over each of contiguous channels **405**. For example, a first plurality of training fields **406** may be transmitted over each of contiguous channels **405** and/or a second plurality of training fields **410**, which may be similar to or different from training fields **406**, may be transmitted over each of contiguous channels **406**, e.g., in accordance with the 802.11 standards and/or any other suitable standard and/or protocol.

[0263] In some demonstrative embodiments, preamble portion **482** may include a first signaling filed **408** ("signal-H"), which may be transmitted over each of channels **405**, and a second signaling filed **412** ("signal-L"), which may be transmitted over each of channels **409**.

[0264] In some demonstrative embodiments, signaling field **408** may include first signaling information defining first transmission characteristics, e.g., of data portion **484** over wireless communication channel **402**; and/or signaling field **412** may include second signaling information defining second transmission characteristics, e.g., of data portion **484**, over wireless communication channel **404**, e.g., as described below.

[0265] In some demonstrative embodiments, signaling fields **408** and **412** may include signaling information ("unified signaling information"), which may be common and/or unified for both channels **402** and **404**, For example, signaling fields **408** and **412** may include unified signaling information relating to general characteristics of the transmission of packet **400**, for example, a type of the packet, information regarding an aggregation mechanism for transmitting packet **400**, and the like, e.g., as described below with reference to FIGS. **3** and/or **4**.

[0266] In some demonstrative embodiments, signaling fields **408** and **412** may include signaling information ("channel-specific signaling information"), which may be channel-specific, e.g., different signaling information, defining different transmission characteristics for channels **402** and **404**. For example, signaling fields **408** and **412** may include channel-specific signaling information defining a different bandwidth, channel allocation, Modulation-Coding-Scheme (MCS), and/or byte-count to be used for channels **402** and **404**, e.g., as described below with reference to FIGS. **3** and/or **4**.

[0267] In some demonstrative embodiments, signaling field **408** may include information relating to channel **404**, for example, an indication that data portion **484** is to be transmitted over channel **404** and/or at least partial information relating to channel **404**; and/or field **412** may include information relating to channel **402**, for example, an indication that data portion **484** is to be transmitted over channel **402** and/or at least partial information relating to channel **402**.

[0268] In some demonstrative embodiments, signaling field **408** may also include an indication of one of channels **409**, which may be used as a general primary channel of channel **404**; and/or signaling field **412** may also include an indication of one of channels **405**, which may be used as a general primary channel of channel **402**, e.g., according to the 802.11 standards.

[0269] Reference is now made to FIG. **3**, which schematically illustrates a signaling field **500**, in accordance with one demonstrative embodiment. Signaling filed **500** may be transmitted as part of a preamble of a packet over at least first and second non-contiguous wireless communication channels. Signaling field **500** may include, for example, signaling field **408** and/or signaling field **412** (FIG. **28**).

[0270] In some demonstrative embodiments, signaling field **500** may include a unified signaling information portion **502** including unified information relating to the non-contiguous channels, e.g., to both channels **402** and **404** (FIG. **28**). For example, unified signaling information portion **502** may include an aggregation index **583** indicating whether or not the packet, which includes signaling filed **500**, e.g., packet **400** (FIG. **32**), is part of an aggregated transmission. Aggregation index **583** may have, for example, a first value, e.g., zero, to indicate that the packet includes an un-aggregated Mac-Protocol-Data-Unit (MPDU), or a second value, e.g., one, to indicate that the packet includes an Aggregated-MPDU (AMPDU), which may include a plurality of MPDUs, e.g., separated by a suitable delimiter. In some embodiments, the unified information may also include unified signaling information relating to transmission characteristics of the non-contiguous channels, e.g., a unified MCS and/or byte count.

[0271] In some demonstrative embodiments, signaling field **500** may include a channel-specific signaling information portion **504** including channel-specific signaling information relating to transmission characteristics of the non-contiguous channels, e.g., as described below.

[0272] In some demonstrative embodiments, channel-specific signaling information portion **504** may include signaling information relating to each of the non-contiguous channels. For example, channel-specific signaling information portion **504** may include information regarding each transmission characteristic for each of the non-contiguous wireless communication channels. Accordingly, substantially the same signaling information **500** may be transmitted over each of the non-contiguous wireless communication channels.

[0273] In some demonstrative embodiments, portion **504** may include an indicator **506** to indicate a wireless communication channel ("the current channel") over which signaling field **500** is being transmitted. For example, indicator **506** may include a value indicating whether signaling field **500** is being transmitted over channel **402** or channel **404** (FIG. **28**). Indicator **506** may include, for example, a first value, e.g., one, to indicate that signaling filed **500** is being transmitted over the L channel, a second value, e.g., two, to indicate that signaling filed **500** is being transmitted over the H channel, or a third value, e.g., zero, to indicate that signaling field **500** is being transmitted as part of a packet transmitted over contiguous channels.

[0274] In some demonstrative embodiments, portion **504** may also include first channel-specific signaling information **501** relating to a first channel of the non-contiguous channels, e.g., the current channel. For example, first channel-specific signaling information **501** may include signaling information relating to the H channel, e.g., if indicator **506** indicates that signaling filed **500** is being transmitted over the H channel; or signaling information relating to the L channel, e.g., if indicator **506** indicates that signaling filed **500** is being transmitted over the L channel.

[0275] In some demonstrative embodiments, portion **504** may also include at least second channel-specific signaling information **503** relating to at least a second respective channel of the non-contiguous channels, e.g., other than the current channel. For example, second channel-specific signaling information **503** may include signaling information relating to the L channel, e.g., if indicator **506** indicates that signaling filed **500** is being transmitted over the H channel; or signaling information relating to the H channel, e.g., if indicator **506** indicates that signaling filed **500** is being transmitted over the L channel.

[0276] In some demonstrative embodiments, signaling information **501** may define first transmission characteristics over the first wireless communication channel. For example, signaling information **501** may include bandwidth information **508** defining a bandwidth of the current channel; channel allocation information **510** defining an allocation of the current channel; MCS information **512** defining an MCS of the current channel, byte count information **514** defining a size relating to the packet, e.g., a total size of the packet payload or a size of the part of packet **400** (FIG. **28**) delivered over the current channel; and/or any other suitable information defining any other suitable transmission characteristics over the current channel.

[0277] In some demonstrative embodiments, signaling information **503** may define second transmission characteristics over the second wireless communication channel. For example, signaling information **503** may include bandwidth information **516** defining a bandwidth of the second channel; channel allocation information **518** defining an allocation of the second channel; MCS information **520** defining an MCS of the second channel; byte count information **522** defining a size relating to the packet, e.g., a total size of the packet payload or a size of the part of packet **400** (FIG. **28**) delivered over the second channel; and/or any other suitable information defining any other suitable transmission characteristics over the second channel.

[0278] FIG. **29** shows signaling field **500** including only first and second channel-specific signaling information elements, e.g., signaling information elements **501** and **503**, corresponding to a wireless communication link including first and second non-contiguous wireless communication channels, respectively. However, in other embodiments, signaling field **500** may include any other suitable number, e.g., greater than two, of channel-specific information elements corresponding to a respective number of wireless communication channels.

[0279] Reference is now made to FIG. **30**, which schematically illustrates a signaling field **400**, in accordance with another demonstrative embodiment. Signaling filed **400** may be transmitted as part of a preamble of a packet transmitted over at least first and second non-contiguous wireless communication channels. Signaling field **400** may include, for example, signaling field **408** and/or signaling field **412** (FIG. **30**).

[0280] In some demonstrative embodiments, signaling field **400** may include a unified signaling information portion **402** including unified signaling information relating to the non-contiguous channels, e.g., to both channels **402** and **404** (FIG. **28**). For example, unified-signaling information portion **402** may include an aggregation index **483** indicating whether or not the packet, which includes signaling filed **400**, e.g., packet **400** (FIG. **28**), is part of an aggregated transmission. Aggregation index **483** may have, for example, a first value, e.g., zero, to indicate that the packet is transmitted as part of an un-aggregated MPDU, or a second value, e.g., one, to indicate that the packet is transmitted as part of an AMPDU.

[0281] In some demonstrative embodiments, signaling field **400** may include a channel-specific signaling information portion **404** including channel-specific signaling information relating to transmission characteristics of the non-contiguous channels, e.g., as described below.

[0282] In some demonstrative embodiments, channel-specific information portion **404** may include information relating to a wireless communication channel ("the current channel") over which signaling field **400** is being transmitted, and at least partial signaling information relating to each of the other non-contiguous channels. For example, channel-specific information portion **404** may include information regarding transmission characteristics for the current channel and at least partial information relating to each of the other channels. The signaling information relating to the other channels may include, for example, information enabling a device receiving signaling field over the current channel to determine and/or identify the one or more other non-contiguous channels. Accordingly, different signaling information **400** may be transmitted over each of the non-contiguous wireless communication channels.

[0283] In some demonstrative embodiments, portion **404** may include an indicator **406** to indicate the current channel. For example, indicator **406** may include a value indicating whether signaling field **400** is being transmitted over channel **402** or channel **404** (FIG. **28**). Indicator **406** may include, for example, a first value, e.g., one, to indicate that signaling filed **400** is being transmitted over the L channel, a second value, e.g., two, to indicate that signaling filed **400** is being transmitted over the H channel, or a third value, e.g., zero, to indicate that signaling field **400** is being transmitted as part of a packet transmitted over contiguous channels.

[0284] In some demonstrative embodiments, portion **404** may also include first channel-specific signaling information **401** relating to a first channel of the non-contiguous channels, e.g., the current channel. For example, first channel-specific signaling information **401** may include information relating to the H channel, e.g., if indicator **406** indicates that signaling filed **400** is being transmitted over the H channel; or signaling information relating to the L channel, e.g., if indicator **406** indicates that signaling filed **400** is being transmitted over the L channel.

[0285] In some demonstrative embodiments, portion **404** may also include at least second channel-specific signaling information **403** relating to at least a second respective channel of the non-contiguous channels, e.g., other than the current channel. For example, second channel-specific signaling information **403** may include signaling information relating to the L channel, e.g., if indicator **506** indicates that signaling filed **400** is being transmitted over the H channel; or signaling information relating to the H channel, e.g., if indicator **406** indicates that signaling filed **400** is being transmitted over the L channel.

[0286] In some demonstrative embodiments, signaling information **401** may define first transmission characteristics over the first wireless communication channel. For example, signaling information **401** may include bandwidth information **408** defining a bandwidth of the current channel; channel allocation information **410** defining an allocation of the current channel; MCS information **412** defining an MCS of the current channel; byte count information **414** defining a size relating to the packet, e.g., a total size of the packet payload or a size of the part of packet **400** (FIG. **28**) delivered over the current channel; and/or any other suitable information defining any other suitable transmission characteristics over the current channel.

[0287] In some demonstrative embodiments, signaling information **403** may define at least some second transmission characteristics over the second wireless communication channel, for example, for example, information enabling a device receiving signaling field **400** over the current channel to determine and/or identify the second non-contiguous channel. For example, second channel-specific information **403** may include bandwidth information **416** defining a bandwidth of the second channel, channel allocation information **418** defining an allocation of the second channel and/or any other suitable information defining any other suitable transmission characteristics over the second channel.

[0288] FIG. **30** shows signaling filed **400** including only first and second channel-specific signaling information elements, e.g., signaling information elements **401** and **403**, corresponding to a wireless communication link including first and second non-contiguous wireless communication channels, respectively. However, in other embodiments, signaling field **400** may include any other suitable number, e.g., greater than two, of channel-specific signaling information elements corresponding to a respective number of wireless communication channels. For example, signaling field **400** may include signaling information element **401** corresponding to the current channel and a plurality of signaling information elements **403** corresponding to a respective plurality of non-contiguous channels.

[0289] Referring back to FIG. **27**, in some demonstrative embodiments, wireless communication unit **108** may transmit at least first signaling information over channel **402** (FIG. **28**), e.g., as part of signaling field **408** (FIG. **28**), defining first transmission characteristics over channel **402** (FIG. **28**). Wireless communication unit **308** may transmit at least second signaling information over channel **404** (FIG. **28**), e.g., as part of signaling field **410** (FIG. **28**), defining second transmission characteristics over channel **404** (FIG. **28**).

[0290] In some demonstrative embodiments, the first and second transmission characteristics may be independent of one another such that, for example, one or more of the first transmission characteristics may be selected, defined, set and/or determined independently of one or more of the second transmission characteristics, and vice versa. For example, MAC **110** may select, define, set and/or determine the bandwidth, allocation, MCS, byte count and/or any other parameter and/or mechanism of the transmission data portion **484** (FIG. **28**) over channel **402** (FIG. **28**) independently of the bandwidth, allocation, MCS, byte count and/or any other parameter and/or mechanism, respectively, of the transmission of data portion **484** (FIG. **28**) over channel **404** (FIG. **28**). For example, if channel **402** (FIG. **28**) has a first MCS, then MAC **110** may independently select, define, set and/or determine the MCS of channel **404** (FIG. **28**), e.g., to be equal to or different from the first MCS.

[0291] In some demonstrative embodiments, wireless communication unit **108** may transmit to wireless communication unit **140** at least part of the second signaling information over channel **402** (FIG. **28**), and at least part of the first signaling information over channel **404** (FIG. **28**), e.g., as described in detail below.

[0292] In some demonstrative embodiments, wireless communication unit **108** may transmit over each of channels **402** and **404** (FIG. **30**) substantially the same signaling information including both the first and second channel-specific signaling information, e.g., as described above with reference to FIG. 29.

[0293] In some demonstrative embodiments, wireless communication unit 108 may transmit different signaling information over channels 402 and 404 (FIG. 30). For example, wireless communication unit 108 may transmit only part of the second signaling information over channel 402 (FIG. 30) and/or only part of the first signaling information over channel 404 (FIG. 30). For example, wireless communication unit 108 may transmit over channel 404 (FIG. 30) at least one of a bandwidth of channel 402 (FIG. 30) and channel allocation information corresponding to channel 402 (FIG. 30); and/or transmit over channel 402 (FIG. 30) at least one of a bandwidth of channel 404 (FIG. 30) and channel allocation information corresponding to channel 404 (FIG. 30), e.g., as described above with reference to FIG. 30.

[0294] In some demonstrative embodiments, MAC 110 may implement a suitable Carrier Sense Multiple Access (CSMA) mechanism, e.g., a suitable collision-avoidance CSMA (CSMA/CA) mechanism, for communicating over wireless communication link 116. The CSMA mechanism may include a suitable back-off mechanism, e.g., in accordance with the 802.11 standards and/or any other suitable standard and/or protocol.

[0295] In some demonstrative embodiments, MAC 110 may utilize a plurality of back-off mechanisms for communicating over the plurality of non-contiguous channels of wireless communication link 116. For example, MAC 110 may communicate over a first channel of the plurality of channels, e.g., channel 402 (FIG. 30), according to a first back-off mechanism and over a second channel of the plurality of channels, e.g., channel 404 (FIG. 30), according to a second back-off mechanism. For example, MAC 110 may manage and/or countdown first and second, e.g., different, back-off periods over the first and second channels, respectively.

[0296] In some demonstrative embodiments, MAC 110 may manage the first back-off mechanism over a primary channel, e.g., a channel of channels 405 (FIG. 30), belonging to channel 402 (FIG. 30); and/or MAC 110 may manage the second back-off mechanism over a primary channel, e.g., a channel of channels 409 (FIG. 30), belonging to channel 404 (FIG. 30).

[0297] In one embodiment, the first and second back-off mechanisms may be identical, e.g., utilizing one or more identical back-off parameters, e.g., contention window parameters, and the like. In another embodiment, the first and second back-off mechanisms may be different from on another, e.g., utilizing one or more different back-off parameters, e.g., contention window parameters, and the like.

[0298] In some demonstrative embodiments, after a back-off period of the first back-off mechanism is complete, MAC 110 wait up to a predefined time period, denoted A1, for a back-off period of the second back-off mechanism to complete, prior to transmitting over the first channel. After the back-off period of the second back-off mechanism is complete, MAC 110 wait up to a predefined time period, denoted A2, for the back-off period of the first back-off mechanism to complete, prior to transmitting over the second channel. In one embodiment, the time period A1 may be equal to the time period A2. In another embodiment, the time period A1 may be different from the time period A2.

[0299] In some demonstrative embodiments, if the back-off period of the second back-off mechanism is complete within the predefined time period A1, MAC 110 may transmit over both the first and second channels.

[0300] In some demonstrative embodiments, MAC 110 may restart a back-off counter of the first back-off mechanism and a back-off counter of the second back-off mechanism after completing the transmission in both the first and second channels.

[0301] In some demonstrative embodiments, if the back-off period of the second back-off mechanism is not completed within the predefined time period A1, MAC 110 may transmit, for example, only over the first channel.

[0302] In some demonstrative embodiments, MAC 110 may restart the back-off counter of the first back-off mechanism and the back-off counter of the second back-off mechanism after completing the transmission in the first channel.

[0303] Reference is made to FIG. 31, which schematically illustrates a method of wireless communication over non-contiguous channels. In some embodiments, one or more operations of the method of FIG. 31 may be performed by one or more elements of telemetry system 32 and monitoring device 10, for example, device 402 (FIG. 30), wireless communication unit 308 (FIG. 27) and/or MAC 310 (FIG. 27).

[0304] As indicated at block 700, the method may include transmitting at least first and second signaling information over at least first and second non-contiguous channels, respectively. For example, wireless communication unit 308 (FIG. 27) may transmit signal fields 408 and 412 (FIG. 30) over non-contiguous wireless communication channels 402 and 404 (FIG. 30), respectively, e.g., as described above.

[0305] As indicated at block 702, transmitting the first and second signaling information may include transmitting first signaling information defining first transmission characteristics over the first channel, and second signaling information defining second transmission characteristics, independent of the first transmission characteristics, over the second channel. For example, wireless communication unit 108 (FIG. 27) may transmit signaling information fields 500 (FIG. 29) and/or 400 (FIG. 30) over channels 402 and/or 404 (FIG. 30), e.g., as described above.

[0306] As indicated at block 704, transmitting the first and second signaling information may include transmitting the substantially same signaling information over both the first and second non-contiguous channels. For example, wireless communication unit 108 (FIG. 27) may transmit signaling field 500 (FIG. 29) including signaling information elements 501 and 503 (FIG. 29) over each of channels 302 and 304 (FIG. 27), e.g., as described above.

[0307] As indicated at block 706, transmitting the first and second signaling information may include transmitting different signaling information over the first and second wireless communication channels. For example, wireless communication unit 308 (FIG. 27) may transmit over channel 402 (FIG. 30) signaling field 400 (FIG. 30) including signaling information element 301 (FIG. 27) relating to channel 402 (FIG. 30) and signaling information element 303 (FIG. 27) relating to channel 404 (FIG. 30); and wireless communication unit 108 (FIG. 27) may transmit over channel 404 (FIG. 30) signaling field 400 (FIG. 30) including signaling information element 301 (FIG. 27) relating to channel 404 (FIG. 30) and signaling information element 303 (FIG. 27) relating to channel 402 (FIG. 30), e.g., as described above.

[0308] As indicated at block **708**, the method may include transmitting symbols of a wireless communication packet over the first and second channels, according to the first and second transmission characteristics, respectively. For example, wireless communication unit **108** (FIG. **27**) may transmit data portion **484** (FIG. **30**) over channels **402** and **404** (FIG. **30**), e.g., as described above.

[0309] Reference is made to FIG. **32**, which schematically illustrates an article of manufacture **800**, in accordance with some demonstrative embodiments. Article **800** may include a machine-readable storage medium **802** to store logic **804**, which may be used, for example, to perform at least part of the functionality of MAC **110** (FIG. **27**) and/or to perform one or more operations of the method of FIG. **31**.

[0310] In some demonstrative embodiments, article **800** and/or machine-readable storage medium **802** may include one or more types of computer-readable storage media capable of storing data, including volatile memory, non-volatile memory, removable or non-removable memory, erasable or non-erasable memory, writeable or re-writeable memory, and the like. For example, machine-readable storage medium **802** may include, RAM, DRAM, Double-Data-Rate DRAM (DDR-DRAM), SDRAM, static RAM (SRAM), ROM, programmable ROM (PROM), erasable programmable ROM (EPROM), electrically erasable programmable ROM (EE-PROM), Compact Disk ROM (CD-ROM), Compact Disk Recordable (CD-R), Compact Disk Rewriteable (CD-RW), flash memory (e.g., NOR or NAND flash memory), content addressable memory (CAM), polymer memory, phase-change memory, ferroelectric memory, silicon-oxide-nitride-oxide-silicon (SONOS) memory, a disk, a floppy disk, a hard drive, an optical disk, a magnetic disk, a card, a magnetic card, an optical card, a tape, a cassette, and the like. The computer-readable storage media may include any suitable media involved with downloading or transferring a computer program from a remote computer to a requesting computer carried by data signals embodied in a carrier wave or other propagation medium through a communication link, e.g., a modem, radio or network connection.

[0311] In some demonstrative embodiments, logic **804** may include instructions, data, and/or code, which, if executed by a machine, may cause the machine to perform a method, process and/or operations as described herein. The machine may include, for example, any suitable processing platform, computing platform, computing device, processing device, computing system, processing system, computer, processor, or the like, and may be implemented using any suitable combination of hardware, software, firmware, and the like.

[0312] In some demonstrative embodiments, logic **804** may include, or may be implemented as, software, a software module, an application, a program, a subroutine, instructions, an instruction set, computing code, words, values, symbols, and the like. The instructions may include any suitable type of code, such as source code, compiled code, interpreted code, executable code, static code, dynamic code, and the like. The instructions may be implemented according to a predefined computer language, manner or syntax, for instructing a processor to perform a certain function. The instructions may be implemented using any suitable high-level, low-level, object-oriented, visual, compiled and/or interpreted programming language, such as C, C++, Java, BASIC, Matlab, Pascal, Visual BASIC, assembly language, machine code, and the like.

[0313] 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 in communication with the monitoring device; and

wherein at least one of the monitoring device and telemetry system includes a wireless communication device that in operation transmits a wireless communication packet to the other over a plurality of non-contiguous wireless communication channels.

2. The system of claim **1**, wherein wireless communication device transmits at least first signaling information over a first channel, and a second signaling information over a second channel.

3. The system of claim **2**, wherein the at least part of the first signaling information includes at least one of a bandwidth of the first channel and channel allocation information corresponding to the first channel.

4. The system of claim **1**, wherein the wireless communication unit in operation communicates over a first channel of the plurality of channels according to a first back-off mechanism and communicates over a second channel of the plurality of channels according to a second back-off mechanism.

5. The system of claim **4**, wherein, if a back-off period of the first back-off mechanism is complete, the wireless communication unit is has a wait up to a predefined time period for the back-off period of the second back-off mechanism to complete, prior to transmitting over the first channel.

6. The system of claim **5**, wherein, when the back-off period of the second back-off mechanism is complete within the predefined time period, the wireless communication unit transmits over the first and second channels.

7. The system of claim **1**, wherein at least one channel of the plurality of channels includes two or more contiguous channels and the wireless communication unit transmits a common preamble of the packet over the contiguous channels.

8. The system of claim 1, wherein at least one channel of the plurality of channels has a bandwidth of at least 20 megahertz (MHz).

9. The system of claim 1, wherein the plurality of channels has a total bandwidth of at least 160 megahertz (MHz).

10. The system of claim 1, wherein the monitoring device is a medical monitoring device that monitors at least one of, cardiac, hemodynamic, respiratory, respiratory rate, hemodynamic, blood pressure, pulse oximetry, capnography, respiratory, neurologic, blood glucose, childbirth, body temperature, stress, epilepsy, and toxicity.

11. The system of claim 10, further comprising:

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

12. The system of claim 10, further comprising:

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

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

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

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

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

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

18. A system comprising:

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, the monitoring device including ID circuitry at the monitoring device, the monitoring device including an antenna;

a telemetry system in communication with the monitoring device; and

a plurality of transmission chains.

19. The system of claim 18, further comprising:

a media-access-controller (MAC) to control the plurality of transmission chains to simultaneously transmit symbols of a wireless communication packet over a plurality of non-contiguous wireless communication channels.

20. The system of claim 18, wherein in operation the MAC transmits as part of a preamble of a packet, signaling information defining transmission characteristics over the plurality of non-contiguous channels.

21. The system of claim 19, wherein in operation the MAC transmits over a first channel of the plurality of non-contiguous channels first signaling information defining first transmission characteristics over the first channel, and over a second channel of the plurality of non-contiguous channels second signaling information defining second transmission characteristics.

22. The system of claim 21, wherein in operation the MAC transmits over the first channel at least part of the second signaling information, and transmits over the second channel at least part of the first signaling information.

23. The system of claim 21, wherein in operation the MAC transmits over the first channel first and second information elements including the first and second signaling information.

24. The system of claim 21, wherein in operation the MAC communicates over a first channel of the plurality of channels in response to a first back-off and communicates over a second channel of the plurality of channels in response to a second back-off.

25. A method of communicating wirelessly with a monitoring device, comprising:

a monitoring device with one or more sensors, a unique user IDID circuitry and an antenna;

obtaining via the one or more sensors user information selected from of at least one of, a user's activities, behaviors and habit information,

communicating between a telemetry system and the monitoring device; and

transmitting via a wireless communication device a wireless communication packet between the monitoring device and the monitoring device over a plurality of non-contiguous wireless communication channels.

26. The system of claim 25, further comprising:

transmitting at least first signaling information over a first channel, and a second signaling information over a second channel.

27. The system of claim 26, wherein the at least part of the first signaling information includes at least one of a bandwidth of the first channel and channel allocation information corresponding to the first channel.

28. The system of claim 25, further comprising:

communicating over a first channel of the plurality of channels according to a first back-off mechanism and communicates over a second channel of the plurality of channels according to a second back-off mechanism.

29. The system of claim 28, further comprising:

wherein, if a back-off period of the first back-off mechanism is complete, the wireless communication unit is has a wait up to a predefined time period for the back-off period of the second back-off mechanism to complete, prior to transmitting over the first channel.

30. The system of claim 29, further comprising:

wherein, when the back-off period of the second back-off mechanism is complete within the predefined time period, the wireless communication unit transmits over the first and second channels.

31. The system of claim 25, wherein

at least one channel of the plurality of channels includes two or more contiguous channels, and the wireless communication unit transmits a common preamble of the packet over the contiguous channels.

32. The system of claim 25, wherein at least one channel of the plurality of channels has a bandwidth of at least 20 megahertz (MHz).

33. The system of claim 25, wherein the plurality of channels has a total bandwidth of at least 160 megahertz (MHz).

34. The system of claim 25, wherein the monitoring device is a medical monitoring device that monitors at least one of, cardiac, hemodynamic, respiratory, respiratory rate, hemody-

namic, blood pressure, pulse oximetry, capnography, respiratory, neurologic, blood glucose, childbirth, body temperature, stress, epilepsy, and toxicity.

* * * * *

专利名称(译)	通过非连续信道进行无线通信的监控设备		
公开(公告)号	US20140247141A1	公开(公告)日	2014-09-04
申请号	US13/955892	申请日	2013-07-31
[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	G08C17/02 A61B5/0026 A61B5/0022 A61B5/0024 A61B5/02055 A61B5/1112 A61B5/1118 A61B5/443 A61B5/6831 A61B5/6898 A61B5/743 A61B2560/0214 A61B2562/0233 A61B2562/08 G06F19/00 G16H40/67 H02J7/00034 H02J7/025 H02J50/10 H02J50/80 H04L67/12 H04L67/20 H04L67/22 H04L67/306 H04W4/029 H04W4/08 H04W4/21 H04W4/80		
优先权	61/772265 2013-03-04 US 61/823502 2013-05-15 US		
外部链接	Espacenet USPTO		

摘要(译)

用于监视设备的通信系统。监视设备包括一个或多个传感器，唯一用户ID，具有ID存储器的ID电路，从ID存储器读取和发送唯一ID的通信系统，电源和通过电路路由信号的通路系统。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。遥测系统与监视设备通信。监视设备和/或遥测系统包括无线通信设备，该无线通信设备在操作中通过多个非连续无线通信信道向另一个发送无线通信分组。