

(51) International Patent Classification:
H04Q 9/00 (2006.01)(21) International Application Number:
PCT/US2014/011742(22) International Filing Date:
15 January 2014 (15.01.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/802,271 15 March 2013 (15.03.2013) US(71) Applicant: RAYTHEON COMPANY [US/US]; 870
Winter Street, Waltham, MA 02451-1449 (US).(72) Inventors: LAYTON, Jacob, Kyle; 3360 E. Hemisphere
Loop, Tuscon, AZ 85706 (US). NOTHEIS, Michael, J.;
3350 E. Hemisphere Loop, Tuscon, AZ 85706 (US).
BARRE, Paul, R.; 3350 E. Hemisphere Loop, Tuscon, AZ
85706 (US). FARRAR, Angela, M.; 3350 E. Hemisphere
Loop, Tucson, AZ 85706 (US).(74) Agent: GREEN, Robert, A.; Christie, Parker & Hale,
LLP, P.O. Box 29001, Glendale, CA 91209-9001 (US).(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM,
ZW.(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:

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

(54) Title: SCIWISE-SUPPLY CHAIN INTEGRITY THRU WIRELESS SENSING

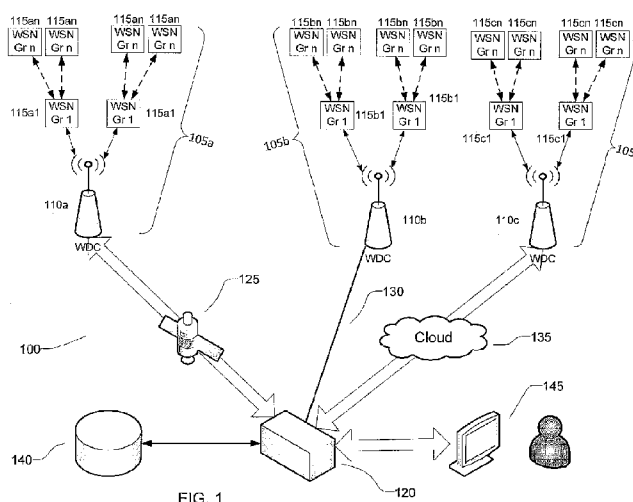


FIG. 1

(57) Abstract: A system includes an instance of a circuit that produces a substantially unique signature electrical signal at a pre-determined output point of the circuit. A sensing circuit detects the signature electrical signal from each instance of the circuit. A transmitter transmits a representation of the signature electrical signal to a wireless mesh network. Typically, the instance of a circuit, the sensing circuit, and the transceiver are together within the same device. A database includes the correspondence between signature electrical signals and individual ones of the sensing circuits. A computer receives representations of the signature electrical signals detected and transmitted from a number of devices and compares them to the database. Tampering with the circuitry in a device is suggested when the representation of the signature electrical signal is not the same as the signature electrical signal in the database for that particular sensing circuit.

SCIWISE - SUPPLY CHAIN INTEGRITY THRU WIRELESS SENSING

BACKGROUND

[0001] Mesh networking is a way to route data, voice and instructions between nodes.

Nodes in a mesh network not only transmit and receive their own data, but also relay data for other nodes in the network. A mesh network allows for continuous connections and reconfiguration around broken or blocked paths by "hopping" from node to node until the destination is reached. In other words, mesh networks are generally "self-healing" and result in very reliable networks. The most well-known example of a mesh network is the Internet.

[0002] In early mesh networks, the nodes were generally wired and not mobile. However, a mesh network can include nodes that are wireless, mobile, or both.

[0003] Many wireless mesh networks are also ad-hoc networks, such as mobile ad-hoc networks (MANet). In an ad-hoc network, a node connects, often automatically, to another node in the network when it come into range or otherwise is able to communicate with the other node. The network is self-configuring and does not have to rely on any preexisting or managed networking infrastructure, such as routers and access points. The nature of ad-hoc networks lends itself well to networks of mobile nodes, especially when the movement of the mobile nodes is not very predictable or is not controlled or known by the network.

[0004] Other wireless mesh network have a more planned configuration, with nodes classified by type, based on their function in the network, such as mesh clients, mesh routers, and gateways.

[0005] Of course, as in the Internet, what appears a node in one network may itself be an independent network. Thus, a mesh client in a wireless mesh network with a managed infrastructure may consist of a MANet without a managed network infrastructure.

[0006] The IEEE has developed a number of standards related to wireless networks. Perhaps the most well-known of these are the 802.11x series of standards that provide the framework for most commercial Wireless Local Area Network (WLAN/"WiFi") devices. Whereas IEEE 802.11x was concerned with features such as Ethernet matching speed, long range (100 m), complexity to handle seamless roaming, message forwarding, and data throughput of 2-11 Mbps; Wireless Personal Area Networks (WPANs) are focused on a space around a person or object that typically extends approximately 10 m in all directions. The foci of WPANs is low-cost, low power, short range, and very small size. The IEEE 802.15 working group initially defined three classes of WPANs that are differentiated by data

1 rate, battery drain, and quality of service (QoS). The first class, IEEE 802.15.1/Bluetooth, is
for medium data rate WPANs for handling a variety of tasks ranging from cell phones to
PDA communications and having QoS suitable for voice communications. The next class,
5 IEEE 802.15.3, is for high data rate WPANs that are suitable for multi-media applications
that require very high QoS. The last class, IEEE 802.15.4/LR-WPAN (Low Rate-WPAN), is
for low rate WPANs, intended primarily for industrial, residential, and medical applications,
especially for control and sensor signals. These applications require very low power
consumption and low cost beyond that considered by the above WPANs as well as relaxed
10 needs for data rate and QoS. The low data rate enables the LR-WPAN to consume very little
power.

[0007] The original IEEE 802.15.4 wireless protocol specifies two physical layers
operating on three frequency bands. On physical layer operates support data rates of 40 kbps
15 at 902-928 Mhz with 10 channels (Americas), and 20 kbps at 868.3 Mhz with 1 channel
(Europe). The second physical layer supports data rates of 250 kbps at 2.405-2.480 Ghz with
16 channels (world-wide). The protocol supports automatic network establishment by the
coordinator; a fully handshaked protocol for transfer reliability; and power management to
ensure low power consumption. The IEEE 802.15.4-2003 standard was approved in May of
20 2003 and was published in October of the same year.

[0008] A 2006 revision of the 802.15.4 standard specifies four physical layers operating
on the same three frequency bands, adding support for 100 and 250 kbps data rates on the
868/915 MHz frequency bands.

25 [0009] IEEE standard 802.15.4a, released in 2007, added two more physical layers: one
using Direct Sequence ultra-wideband (UWB) and the other using chirp spread spectrum
(CSS). The CSS physical layer operates on the 2450 MHz frequency band used in the
802.15.4 standard. The CSS physical layer supports data rates of 250 kbps and 1000 kbps.
30 The UWB physical layer is allocated channels across three frequency ranges: below 1 GHz,
3-5 GHz, and 6-10 GHz. The UWB physical layer requires supports for a data rate of 850
kbps as well as optional data rates of 110 kbps, 1700 kbps, 6.81 Mbps, and 27.24 Mbps. The
UWB physical layer also provides for optional feature of precision ranging.

35 [0010] IEEE standards 802.15.4-2003, 802.15.4-2006 and 802.15.4a-2007 are each
incorporated by reference as if set forth in its entirety herein.

[0011] According to the standards, "Two different device types can participate in an
IEEE 802.15.4 network; a full-function device (FFD) and a reduced-function device (RFD).

1 The FFD can operate in three modes serving as a personal area network (PAN) coordinator, a coordinator, or a device. An FFD can talk to RFDs or other FFDs, while an RFD can talk only to an FFD. An RFD is intended for applications that are extremely simple, such as a light switch or a passive infrared sensor; they do not have the need to send large amounts of data and may only associate with a single FFD at a time. Consequently, the RFD can be implemented using minimal resources and memory capacity.

5 [0012] "A system conforming to this standard consists of several components. The most basic is the device. A device may be an RFD or an FFD. Two or more devices within a POS communicating on the same physical channel constitute a WPAN. However, this WPAN shall include at least one FFD, operating as the PAN coordinator.

10 [0013] "An IEEE 802.15.4 network is part of the WPAN family of standards although the coverage of the network may extend beyond the POS, which typically defines the WPAN.

15 [0014] "A well-defined coverage area does not exist for wireless media because propagation characteristics are dynamic and uncertain. Small changes in position or direction may result in drastic differences in the signal strength or quality of the communication link. These effects occur whether a device is stationary or mobile, as moving objects may impact station-to-station propagation.

20 [0015] The 802.15.4 standard allows for two network topologies: the star topology or the peer-to-peer topology.

[0016] Nodes will be soon available for commercial use. For example, decaWave has announced

25 [0017] One example of a wireless mesh network is the network used in the Raytheon Company's Autonomic Tracking & Response System ("ATaRS"). Aspects of the ATaRS are disclosed in co-owned U.S. Patent No. 8,149,748, which is incorporated by reference as if set forth in its entirety herein. Other aspects of ATaRS are discussed in the paper and presentation, both titled *Real-time Autonomic Asset Tracking*, by R. Mueller and J. Boyd, CDCA (Charleston Defense Contractors Association) Government Industry Conference, November 2008 (available at

30 www.charlestdca.org/shared/docs/navid_2198/catid_1008/11-20-825am_bob%20mueller_draft%20cdca%20brief.ppt and

35 www.charlestdca.org/shared/docs/navid_2198/catid_1010/real-time%20autonomic%20asset%20tracking_2dannualc4isrcnf.doc, respectively), which are both also incorporated by reference as if set forth in their entirety herein.

SUMMARY

[0018] The present invention includes an instance of a circuit that produces a signature electrical signal at a predetermined output point of the circuit, the signature electrical output being substantially unique among a plurality of instances of the same circuit; a sensing circuit that detects the signature electrical signal from the instance of a circuit as an input; and a transceiver that transmits a representation of the signature electrical signal to a wireless network.

[0019] Another embodiment contains an instance of the circuit producing the signature electrical signal upon application of a voltage at a predetermined point of the circuit.

[0020] Another embodiment contains an instance of the circuit discrete from the sensing circuit.

[0021] Another embodiment contains an instance of the circuit as an integrated circuit.

[0022] Another embodiment contains an instance of the circuit and a sensing circuit in the same integrated circuit.

[0023] Another embodiment contains an instance of the circuit, a sensing circuit, and a transceiver in the same integrated circuit.

[0024] Another embodiment contains a wireless network comprising a mesh network.

[0025] Another embodiment contains a location determination circuit configured to output a representation of the location of the instance of the circuit, wherein the transceiver further transmits a representation of the output of the location determination circuit to the wireless network.

[0026] Another embodiment contains a location determination circuit comprising a GPS sensor.

[0027] Another embodiment contains a location determination circuit comprising circuitry that determines the location of the instance of the circuit relative to other nodes in the wireless network according to calculations of the length of time between the transmissions by other nodes in the wireless network and the receipt of such transmission by the transceiver.

[0028] Another embodiment contains a sensing circuit comprising an analog to digital converter and an iddt/iddt instrument and/or a degradation monitor circuit.

[0029] Another embodiment contains a sensing circuit comprising an analog to digital converter and an iddt/iddt instrument and/or a degradation monitor circuit when the instance of the circuit and the sensing circuit are in the same integrated circuit.

1 [0030] Another embodiment contains a database of signature electrical signals
corresponding to individual of the sensing circuits; a computer connected to the wireless
network that receives the representations of electrical signature received transmitted by each
of the devices and wherein a computer configured to compare the representation of the
5 signature electrical signal to signature electrical signals corresponding to the sensing circuit
of the instance of the circuit and further configured to generate a warning if the comparison
does not show substantial identity.

10 [0031] Another embodiment contains a plurality of devices each comprise an instance of
the circuit, a sensing circuit, a transceiver, and a location sensing circuit, the system further
comprising a database of individual instances of the circuit corresponding to each of the
devices comprising each instance of the circuit, a computer connected to the wireless network
that receives the representations of electrical signature received transmitted by the each of the
15 devices; wherein the computer is configured to determine the location of each of the devices
according to the representations of electrical signature received from the transceiver of each
of the devices.

20 [0032] Another embodiment contains a plurality of devices each comprising an instance
of the circuit, a sensing circuit and transceiver, the system further comprising a fault detection
circuit connected to the transceiver , wherein fault detection circuit detects that a component
of the device has malfunctioned and/or that a component of the device has experienced a
condition that precedes a malfunction, wherein after the fault detection circuit has detected a
malfunction or a condition that precedes a malfunction the transceiver transmits a notification
25 of such detection to the wireless network, a database of individual instances of the circuit
corresponding to each of the devices comprising each instance of the circuit and a computer
connected to the wireless network that receives the notifications of such detections
transmitted by the devices wherein the computer is configured to generate warnings when the
computer receives the notifications of such detections transmitted by the devices.
30

35 [0033] Another embodiment contains a fault detection circuit connected to the
transceiver, wherein fault detection circuit detects that the device has malfunctioned and/or
the device has a level of a risk of a malfunction occurring in a predetermined future period of
time, the level of risk exceeding a predetermined threshold, wherein after the fault detection
circuit has detected a malfunction or a risk exceeding a predetermined threshold the
transceiver transmits a notification of such detection to the wireless network, a database of
individual instances of the circuit corresponding to each of the devices comprising each

1 instance of the circuit and a computer connected to the wireless network that receives the notifications of such detections transmitted by the devices wherein the computer is configured to generate warnings when the computer receives he notifications of such detections transmitted by the devices.

5 **[0034]** The invention may also be a method used with instances of a circuit that produces a signature electrical signal at a predetermined output point of the circuit, the signature electrical signal being substantially unique among a plurality of instances of the same circuit, the method including detecting a signature electrical signal from an instance of a circuit,
10 transmitting a representation of the signature electrical signal to a wireless network, comparing, using a computer, the representation of the signature electrical signal to a database of signature electrical signals corresponding to individual of the sensing circuits and generating an electronic warning signal if the comparison does not show substantial identity.

15 BRIEF DESCRIPTION OF THE DRAWINGS

[0035] Fig. 1 is a block diagram of a system according an embodiment of the invention.

20 **[0036]** Fig. 2 is a block diagram of a wireless mesh network according to an embodiment of the invention.

[0037] Fig. 3 is a block diagram of a sensor associated with a WSN according to an embodiment of the invention.

25 **[0038]** Fig. 4 is a diagram showing the use of sensor equipped WSNs in wide ranging mesh networks according to an embodiment of the invention.

DETAILED DESCRIPTION

30 **[0039]** In an embodiment of the invention, as shown in FIG. 1, a system 100 includes a number of wireless mesh networks, 105a-c, which in many embodiments are 802.15.4 compliant. In such 802.15.4 compliant embodiments, each wireless mesh network includes a wireless device controller (WDC) 110a-c, which is a PAN coordinator. Each mesh network also includes a number of network nodes. The main type of network node is a wireless
35 sending node (WSN) 115a1-115c1, 115an-115cn (reference numeral 115 will be used to refer to WSNs 115a1-115c1, 115an-115cn generally and collectively).

[0040] Many or all of the WSNs 115 are associated with a sensor as is described in more detail below. Some sensors may detect environmental conditions such as temperature, humidity, and atmospheric pressure. Some sensors may detect physical conditions such as

1 shock, g-force, and vibration. Some sensors may detect location in one or more of various
known manners such as using GPS sensors, cellular or other radio triangulation, and the
proximity to other WSNs and/or the WDC whose location may be known. Some sensors may
detect biological conditions, chemical conditions, switch statuses (such as door open), and the
5 like.

[0041] The sensor information from all of the WSNs in the same mesh network is
gathered by and stored, at least temporarily, in the WDC 110. The WDC connects to a server
120 and sends the sensor information gathered from the WSNs in its mesh network to the
10 server. In various embodiments, a WDC may connect to the server by one or more of any
known manner, including by satellite 125, such as through an Iridium modem, by cellular
connection (not shown), by wired connection 130, including a private network or dedicated
telecommunications line, and by public network 135, such as the Internet. The connection
15 between a WDC and the server may be periodic, continuous, or a combination of periodic
and continuous.

[0042] In many embodiments, the system includes a database 140. In many embodiments,
the database stores the unique identifier information for a large number of chips. When the
server receives sensor information from a WDC that includes information that can be used to
20 identify a particular device associated with a WSN, as described in more detail below, the
server checks that information against the records in the database to determine if the sensor
information matches any of the records. From the results of this comparison, the server can
determine if a device associated with a WSN, such as an integrated circuit has been tampered
25 with, has been replaced by another chip, or is not in the database.

[0043] In many embodiments, the database also includes location information, both last
known and historic, for at least some of the devices in the database. In many of these
embodiments, the last known information is updated whenever sensor information that is
associated with a device in the database. Using this information, in addition to tracking the
30 location of individual devices, the system may determine when devices that should be in the
same location (e.g., the have been built into the same product) are not together.

[0044] In many embodiments, the information from the database is accessible through a
user accessible application or web site 145. In many embodiments, the server monitors the
35 information in the database and when anomalous information is detected (e.g., information
indicating IC tampering, IC counterfeiting, location anomalies), the server generates alerts
that may trigger the generation of text messages, email messages, voice phone calls, or

1 popups in user applications or web sites or any other way of alerting a person, computer, or other device of such a detection.

5 [0045] In an embodiment of the invention, as shown in FIG. 2, an 802.15.4 compliant mesh network 200 includes a single network controller, referred to as a wireless device controller (WDC) 210, which is a PAN coordinator. The mesh network also includes a plurality of network nodes. The main type of network node in the network is referred to as a Wireless Sending Node (WSN) 220.

10 [0046] A WSN always has only a single parent. A WSN may act as parent to several other WSNs. Each of those WSNs may act as parent to other WSNs. The WSNs may be arranged in groups (GR), hierarchically, from a first group (GR1) 230, closest (conceptually) to the WDC, to a last group (GRn) 260, farthest (conceptually) from the WDC, and intermediate groups (e.g., GR2 240, GR3 250) located conceptually (and often also physically) in between. A parent WSN will be in one Group (GRx) and its children will be in the next outer group (GRx+1). For example, each of the GR1 WSNs can communicate with and act as a parent to a number of GR2 child WSNs. In turn, each of the G2 WSNs may act as a parent to a number of G3 child WSNs. The WDC is often designated as group zero (GR0). The WDC itself is parent to the GR1 WSNs. In some embodiments, there are a maximum of 30 groups. In these embodiments, none of the WSNs in Group 30 would be parents to any other WSNs, since they are in the “outermost” group. Generally, each group represents a “hop” in a communication link.

25 [0047] As WSNs hook up, and establish the network, the Group 1 devices tend to be those which are physically closest to the WDC, and the Group 30 devices tend to be those which are farthest away from the WDC, but the WSNs may establish a plurality of groups even if all of the WSNs are within radio range of the WDC. Regardless, though, all Group 1 WSNs must be within radio range of the WDC and WSNs of higher number groups may or may not be within radio range of the WDC. If there network only includes a few WSNs, all within close proximity to the WDC, there could only be one group. In many embodiments, the limitations of the 802.15.4 radio link is approximately 50 meters. If a WSN is farther than 50 meters from the WDC, and there are WSNs between them, it is inevitable that there will be more than one group.

35 [0048] The number of groups into which a number of WSNs are split is largely a tradeoff. The number of groups equals the number of hops between the WDC and the WSNs of the highest number group. Further, each hop represents a limit to the physical separation (such as

1 the 50 meter range discussed above) between WSNs of difference groups. In practice, there may further limitations to the distance, due to signal obstructions, etc.

5 [0049] More groups can provide more physical coverage, but, as explained below, more groups means dividing a sync period up into smaller pieces. Smaller pieces of the sync period may impose a limit on the number of WSNs that can be in the same group, because all the devices in the same group utilize the same sub-period of the sync period. Alternatively, the sync period may need to be lengthened to avoid having to limit the number of WSNs that can be in the same group.

10 [0050] Many mesh networks are what is referred to as "beaconing networks." In some beaconing networks one or more members of the network periodically transmit beacon frames that announce the presence of the network and the basic information about the network needed by new devices to connect to the network. When a device begins operating or begins operating in a new environment, it listens for any beacon frames being transmitted by
15 other devices. If it receives a beacon frame in a format it understands, for a network using a protocol that the device supports, the device can begin negotiating with the network (i.e., a network coordinator device in the network, such as an access point in a typical 802.11 network) to join the network. In other beaconing networks, when a device begins operating or
20 begins operating in a new environment, it begins sending out beacon frames, in hopes that a network device within range receives the beacon frame and transmits information back to the device that allows the device to connect to the network.

25 [0051] In many embodiments, the system uses an ATaRS network as its wireless mesh network. In an ATaRS network, a WDC sends out a single signal in a "wave" to the WSNs. A sync signal originates at the WDC and goes (propagates) from WSN to WSN, in a wave-like downstream manner. As the signal reaches each WSN, that WSN modifies some of the data (such as what group it is in, and who its parent is) and sends it along on a very stringently
30 timed basis. The sync signal thus makes its way through the groups of WSNs, modified each time (each WSN acts like a "router"), until the last group is reached. At this point, the wave reverses and the sync signal is passed back up through the groups of WSNs, again modified each time, until it reaches the WDC.

35 [0052] A sync period is the time during which a sync signal is transmit by the WDC, propagates to the highest number group and then back to the WDC. The sync period is divided into sub-periods. Each sub-period is the time during which all of the WSNs of one group communicate with the WSNs of the next group. Thus, there are approximately twice as

1 many sub-periods as there are groups, which allow for sync and data messages to be propagated downstream, from the WDC to the WSNs in the farthest group (GR_n), and upstream from WSNs in the farthest group (GR_n) back up to the WDC, with a few "buffer" sync periods at the beginning and end of the downstream and upstream portions.

5 [0053] An important part of the sync signal is the time of the next sync signal and the length of the sub-periods. This allows the WSNs to stop activity, going into a mode of radio silence ("sleep mode"), until the time for the next sync signal plus the length of the sub-periods during which the sync signal is being passed from lower numbered groups.

10 Maximizing the time a WSN spends in sleep mode is important because transmitting and receiving RF signals often uses much, if not most, of the power consumed by a WSN.

15 [0054] In an embodiment for example purposes, three WSNs are connected in the ATaRS network. Each device is in a Group, starting from a group closest to the WDC to a group farthest from the WDC. Each WSN knows when to wake up, because the WSNs have already been synched up, and that information is contained on the last (previous) message that came from the WDC.

20 [0055] At the time designated in the last sync sequence, the WDC sends out a sync signal. Slightly before the designated time, the first device (WSN1) will wake up and power on its receiver in time for the receiver to receive a sync signal from the WDC at the designate time plus the predetermined number of buffer sync periods. The first device (WSN1) knows that it is in Group 1 (GR1), and it knows that it has to send the sync signal out again (to its children WSNs) according to a randomizing scheme. The first device (WSN1) changes the message slightly (such as Group number and parent ID), and moves it along (transmits it).
25 The next device (WSN2) knows from the previous sync message to wake up at the correct time to pick up the message from the first device (WSN1), edit it, and pass it along to the next (third) device, and so on, until the last device (WSN_n; in this example WSN3) has been reached. Then, halfway through the overall synch period, things turn around, messages are now sent upstream back to the WDC, in the same manner, from the farthest device (WSN_n), eventually to the closest device to the WDC (WSN1), and then to the WDC.

30 [0056] If the WDC needs to communicate any information to one or more of the WSNs, this information is included in the sync signal or, in some cases, one or more of the buffer periods. Likewise, if one of the WSNs needs to make a request to the WDC, it can similarly
35 insert the request in the upstream sync signal going back to the WDC.

1 **[0057]** In addition to the normal mode of network operation described above, in which
only limited amounts of data need to be transmitted through the network, it is sometimes for a
given device to send a large quantity of data to the WDC, or vice-versa. In a pipeline mode,
because of the way that the network functions, with the downstream syncs and the upstream
5 syncs, a pipe (logical/physical connection) can be established between the WDC and a WSN,
through a specific path of other WSNs, and then it is basically a throughput straight to that
given WSN, through the network. Meanwhile, all other WSNs are set to not send messages
(they go to sleep) or, if they are in the pipe, to simply pass the pipeline message along. At the
10 end of the pipeline message, the network resyncs itself and resumes normal operation. This
pipeline mode of operation allows for more information to go through the mesh than can
normally be done in the standard sync cycles.

15 **[0058]** In many embodiments, RF quiet is the default state for WSNs. All operations of
transmitting are under the control of the WDC (master device). Thus, no downstream device
will transmit without first successfully receiving a sync message. Sync messages may be sent,
for example, every 3 seconds in "fast" and "discover" mode and every 5-9 seconds in "slow"
sync mode. The mode is controlled by the WDC.

20 **[0059]** If a device does not hear a sync message downstream for a set number (e.g., 3)
sync periods, it may assume that it is out of the network and will go into the "lost" mode. It
will open up its radio and find another parent which may be the WDC, or another entirely
different device (new parent) than to which it was previously connected.

25 **[0060]** The lost device will wait a predetermined number (such as 2) sync periods (a sync
period may be, for example, 5 seconds), will pick up a new parent, and send out its sync
message so that its children can be connected up. When the device hooks up to the network
again, it will send a message upward, via the new parent, which goes all the way back to the
WDC, which resets the network addressing scheme.

30 **[0061]** Each device will recognize the network poll frequency and send its network mask
answer to its parent within that period. Any children of the device that send a network mask
message will have their message also propagated to the parent. Each child will keep track of
its parent for upstream messages.

35 **[0062]** Each data message downstream will be acknowledged by the destination child
device back to the WDC. Each message upstream will be acknowledged by the parent back to
the child during the next data sending period.

1 [0063] A given device knows when it is supposed to see a sync message from a parent. Most of the time, the device is simply monitoring messages and, if it is parent to another device(s), passing messages downstream to its children.

5 [0064] Thus, if a mesh network is not communicating data, and is in slow sync mode, each device may, for example, be in communication mode for 2 periods of upstream sync listen, 1 period of downstream sync send, and 2 periods of downstream sync listen. This works out to 5 periods of communication time and 576 periods of "timer" time which works out to a duty cycle of 0.86%, which is the only time in which the radio is consuming power. 10 Of course, the duty cycle will vary depending on the number of periods of send and listen used and the time between syncs, which, in turn, affect the effective data rate of the network and the response time.

15 [0065] It is within the scope of the invention that a mesh, such as described above, can be implemented on top of another mesh, on multiple levels to extend depth and breadth of the mesh, such as across an entire city, including many thousands of nodes. Applications may include radiation sensors, smoke detectors, traffic signals, controlling traffic signals, rerouting traffic.

20 [0066] By additionally meshing up the controlling devices of a mesh, each layer will control a subset of the mesh, allowing the mesh to grow exponentially.

25 [0067] The layering can be accomplished via frequency or time multiplexing. The different network layers can be separated in frequency or time. These can be used in separately or in conjunction to further increase the total number of meshed nodes. The current mesh network has empty periods where the mesh does no communications or work. These empty periods can be used to mesh up the controlling devices using different radios or frequencies to send information between controlling devices.

30 [0068] For example: Two WDC devices (wireless data controllers) are separated by 1 mile and are communicating with higher power radios. These devices are powered from the grid. Each WDC controls 300 mesh devices in a warehouse. Devices can move between each warehouse and will pick up the local mesh.

35 [0069] A block diagram of a sensor associated with a WSN according to an embodiment of the invention is shown in FIG. 3. A WSN 300 that communicates with a wireless mesh network 310, as described above, is included in a device 320. The device 320 includes one or more integrity signature components 330. The output(s) of the integrity signature components are connected to an integrity processor 340. The integrity processor 340 executes an integrity

1 signature process on the output(s) of the integrity signature components and the results of this process are sent to the WSN 300 for transmission to the WDC through the wireless mesh network 310.

5 **[0070]** In some embodiments, the WSN includes a processor to do internal processing, a memory, and an I/O device or connector that connects with one or more external devices, such as additional sensors. In many embodiments, the memory is non-volatile. Information from the any external sensors, as well as information such as inventory information, is stored in the memory. In some embodiments, the WSN polls the sensors periodically for their
10 readings and stores the information, with the time of the reading, in memory. In some embodiments, the WSN continuously stores readings of one or more of the sensors, again with time indications stored for the readings. In some embodiments, the data collected between mesh network sync signals is included as part of the upstream sync message transmitted by the WSN. In some embodiments, a calculation is performed on the collected
15 data that reduces the size of the data before transmission.

[0071] In many embodiments, the WSN and sensors are powered by batteries, capacitors or RF energy from a WDC or another WSN. In this way, in combination with the low power consumption of the wireless mesh network, Embedded WSNs and sensors may operate for
20 many years without any servicing or access.

[0072] In some embodiments, the WSN itself includes internal sensors. In some embodiments, the WSN is contained within the same device that contains one or more sensors that are electrically or optically connected to the WSN. In some embodiments, the
25 WSN is on the same circuit board as one or more sensors. In some embodiments, the WSN is part of the same integrated circuit as one or more sensors. It will be appreciated that any of these embodiments may be combined with each other. Thus, for example, a WSN may be on the same IC as one sensor and be connected to another, external sensor, through an I/O device or connector.

30 **[0073]** In some embodiments the sensors detect information about other electronic, electrical, or electro-mechanical devices (monitored devices). Some examples of such sensors are disclosed in U.S. Published Patent Application No. 2011/0060569 by Lynn et al., which is incorporated by reference as if set forth in its entirety herein and which is assigned to
35 Ridgetop Group, Inc. In one of these examples, a sensor monitors the following error output by an electro-mechanical actuator. If the electro-mechanical actuator is operating correctly, the following error output will include certain characteristics (nominal operation

1 characteristics). Accordingly, abnormalities in the operation of an electro-mechanical
actuator can be detected when the following error output includes different characteristics.
Often, a particular way in which the following error output differs from the nominal
operation characteristics will identify a particular type of fault, such as the failure of a
5 particular component of the electro-mechanical actuator. A particular way in which the
following error output differs from the nominal operation characteristics may also indicate a
variety of different conditions, such as a condition that precedes a particular type of
malfunction, a condition that precedes a malfunction by an expected length of time, or a
10 percentage of the nominal operation at which the device is currently operating.

[0074] In some embodiments, the sensors detect information about the electrical
characteristics of electronic components or circuits. In some embodiments, such sensors are
included within a set of integrity signature components 330 in an electronic device, circuit
15 board or IC 320. In some embodiments, the integrity signature components include an analog
to digital converter (ADC) 390 that receives analog voltages from various other circuits or
sensors in the device, circuit board, or IC 320.

[0075] For example, various sensors may detect voltage or current across or through
electronic components or circuits during operation. Various sensors may also measure
20 resistance, capacitance, and inductance of a component or portion of a circuit, typically when
the component/circuit is not operating. In the case of semiconductor components, various
sensors may detect the voltage or current threshold for the component. In the case of
integrated circuits (ICs), various sensors may apply voltages of varying amounts to various of
25 the pins of the IC and monitor the output on other pins of the IC.

[0076] In some embodiments, the sensor 360 is included on the die of the IC that is being
monitored and thus is embedded in the IC itself. An example of this type of sensor is
disclosed in U.S. Patent No. 7,239,163 to Ralston-Good et al., which is incorporated by
reference as if set forth in its entirety herein and which is assigned to Ridgetop Group, Inc.
30 An example of this type of sensor is also commercialized by Ridgetop Group, Inc. under their
trademark, PDKChek.

[0077] In some embodiments, IC-integrated sensors of this type include a bandgap
reference, analog to digital converter (ADC), or a standardized I/O interface, such as a JTAG
35 interface. An e

[0078] Often, calculations or an integrity signature process 340 may be performed on one
or more outputs of a monitored device that produce a signature that can be used to identify a

1 condition, such as those discussed above, of the monitored device. In such cases, a database
is created that contains the various possible conditions for a device and the signatures that
correspond with these conditions. The sensor, or electronics connected to the sensor, perform
the calculations on the outputs of the monitored device and sends the resulting signatures
5 through the mesh network rather than sending the raw outputs from the monitored device. A
signature may include a string of data and may be expressed in any number of coordinates
and/or dimensions. The signatures are compared to the database to determine if the signature
corresponds with any of the known conditions for the monitored device.

10 **[0079]** In a similar manner, in some embodiments, sensors take voltage readings on one
or more pins of an integrated circuit and calculate a signature for the voltage readings. In
some embodiments the voltage readings are taken at various times. In some embodiments the
voltage readings are taken while the circuit containing the integrated circuit is operating. In
15 some embodiments the voltage readings are taken when the circuit is not operating but there
are still external voltages being applied to the integrated circuit by the circuit that contains it.
In some embodiments the sensor causes one or more particular voltages to be applied to one
or more specific pins of the integrated circuit. In some embodiments any of the various
combinations of these conditions for reading voltages are present. An example of such a
20 sensor is degradation monitor chip 370. In some embodiments, degradation monitor chip 370
is not a separate chip but a portion of a larger IC. A calculation is performed on the various
voltage readings to produce a signature.

[0080] In some embodiments, a signature may indicate that the monitored device has
25 been tampering with. In some embodiments each different instance of a particular monitored
device, such as an integrated circuit, produces a combination of voltages under a particular
set of circumstances that produce a unique or semi-unique signature. In these embodiments
such a signature can be used as a unique identifier for each monitored device. Thus, if a
30 particular integrated circuit is removed from a first device and installed in a second device,
the signature for that integrated circuit will no longer match the signature that is expected for
that chip in the second device.

[0081] In some embodiments, the integrity signature components include Iddg/Iddt
instruments 380. These instruments measure integrity using static and dynamic current
35 measurements.

[0082] In many embodiments, integrated circuit sensors are included in the integrated
circuit itself. In many of these embodiments, the integrated circuit sensors are able to be

1 polled by circuitry outside the integrated circuit. Thus, a separate integrated circuit or other
circuitry can poll all integrated circuits with integrated circuit sensors for their parameter data
and either store it or forward it to a WSN.

5 [0083] Fig. 4 is a diagram showing the use of sensor equipped WSNs in wide ranging
mesh networks according to an embodiment of the invention. As discussed above, WSN may
be embedded as part of an integrated circuit 410, as part of a circuit board 420, or as part of a
larger device or machine, such as military weapon 430. In each case the WSN is connected to
a central server and database through the WDCs 400 of the mesh network.

10 [0084] Because a network of mesh networks can span the globe, the system can monitor,
in real time, the output of sensors embedded, for example, in an IC of a military weapon, can
be monitored throughout the process of manufacture 440, shipping 450, warehousing 460,
and deployment 470. In this way, such things as inventory control, performance degradation,
15 tampering, and imminent failure warnings can be continuously monitored from a central
location, or any location.

20

25

30

35

WHAT IS CLAIMED IS:

1. The system comprising:

an instance of a circuit that produces a signature electrical signal at a predetermined output point of the circuit, the signature electrical output being substantially unique among a plurality of instances of the same circuit;

a sensing circuit that detects the signature electrical signal from the instance of a circuit as an input; and

a transceiver that transmits a representation of the signature electrical signal to a wireless network.

2. The system of claim 1 wherein:

the instance of the circuit produces the signature electrical signal upon application of a voltage at a predetermined point of the circuit.

3. The system of claim 1 wherein:

the instance of the circuit is discrete from the sensing circuit.

4. The system of claim 1 wherein:

the instance of the circuit is an integrated circuit.

5. The system of claim 1 wherein:

the instance of the circuit and the sensing circuit are in the same integrated circuit.

6. The system of claim 1 wherein:

the instance of the circuit, the sensing circuit, and the transceiver are in the same integrated circuit.

7. The system of claim 1 wherein:

the wireless network comprises a mesh network.

8. The system of claim 1 further comprising:

a location determination circuit configured to output a representation of the location of the instance of the circuit;

1 wherein the transceiver further transmits a representation of the output of the location
determination circuit to the wireless network.

9. The system of claim 1 wherein:
5 the location determination circuit comprises a GPS sensor.

10. The system of claim 1 wherein:
 the location determination circuit comprising circuitry that determines the location of
10 the instance of the circuit relative to other nodes in the wireless network according to
calculations of the length of time between the transmissions by other nodes in the wireless
network and the receipt of such transmission by the transceiver.

11. The system of claim 1 wherein the sensing circuit comprises:
15 an analog to digital converter; and
 an iddt/iddt instrument and/or a degradation monitor circuit.

12. The system of claim 5 wherein the sensing circuit comprises:
20 an analog to digital converter; and
 an iddt/iddt instrument and/or a degradation monitor circuit.

13. The system of claim 1 further comprising:
25 a database of signature electrical signals corresponding to individual of the sensing
circuits;
 a computer connected to the wireless network that receives the representations of
electrical signature received transmitted by each of the devices; and
 wherein the computer configured to compare the representation of the signature
30 electrical signal to signature electrical signals corresponding to the sensing circuit of the
instance of the circuit and further configured to generate a warning if the comparison does
not show substantial identity.

1 14. The system of claim 8 wherein a plurality of devices each comprise an instance of the circuit, a sensing circuit, a transceiver, and a location sensing circuit, the system further comprising:

5 a database of individual instances of the circuit corresponding to each of the devices comprising each instance of the circuit;

a computer connected to the wireless network that receives the representations of electrical signature received transmitted by the each of the devices;

10 wherein the computer is configured to determine the location of each of the devices according to the representations of electrical signature received from the transceiver of each of the devices.

15 15. The system of claim 1 wherein a plurality of devices each comprise an instance of the circuit, a sensing circuit and transceiver, the system further comprising:

a fault detection circuit connected to the transceiver , wherein fault detection circuit detects that a component of the device has malfunctioned and/or that a component of the device has experienced a condition that precedes a malfunction;

20 wherein after the fault detection circuit has detected a malfunction or a condition that precedes a malfunction the transceiver transmits a notification of such detection to the wireless network;

a database of individual instances of the circuit corresponding to each of the devices comprising each instance of the circuit; and

25 a computer connected to the wireless network that receives the notifications of such detections transmitted by the devices;

wherein the computer is configured to generate warnings when the computer receives he notifications of such detections transmitted by the devices.

30 16. The system of claim 13 further comprising:

a fault detection circuit connected to the transceiver , wherein fault detection circuit detects that the device has malfunctioned and/or the device has a level of a risk of a malfunction occurring in a predetermined future period of time, the level of risk exceeding a predetermined threshold;

35 wherein after the fault detection circuit has detected a malfunction or a risk exceeding a predetermined threshold the transceiver transmits a notification of such detection to the wireless network;

1 a database of individual instances of the circuit corresponding to each of the devices
comprising each instance of the circuit; and

 a computer connected to the wireless network that receives the notifications of such
detections transmitted by the devices;

5 wherein the computer is configured to generate warnings when the computer
receives he notifications of such detections transmitted by the devices.

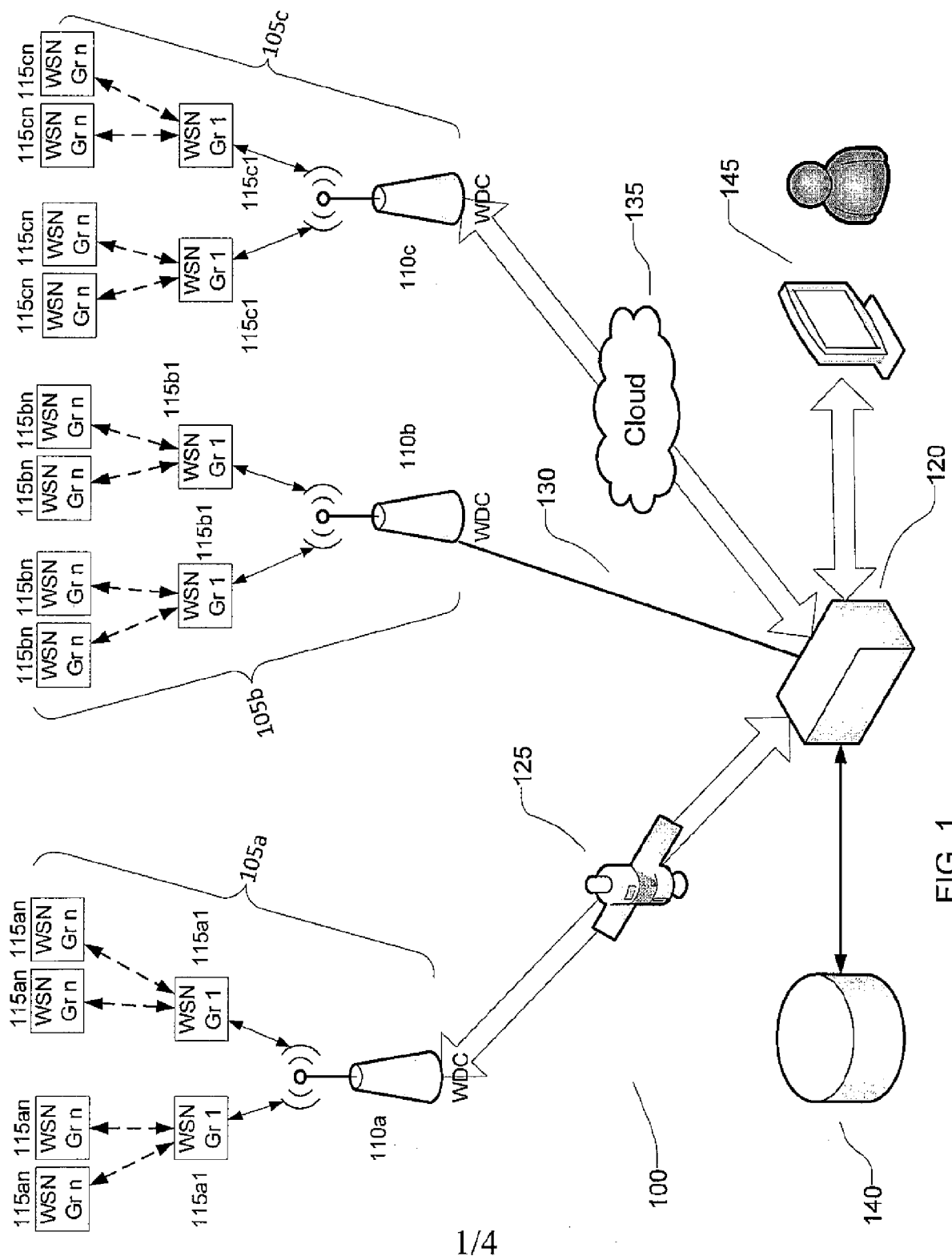
17. The method used with instances of a circuit that produces a signature electrical signal
10 at a predetermined output point of the circuit, the signature electrical signal being
substantially unique among a plurality of instances of the same circuit, the method
comprising:

 detecting a signature electrical signal from an instance of a circuit;

 transmitting a representation of the signature electrical signal to a wireless network;

15 comparing, using a computer, the representation of the signature electrical signal to a
database of signature electrical signals corresponding to individual of the sensing circuits;
and

 generating an electronic warning signal if the comparison does not show substantial
20 identity.



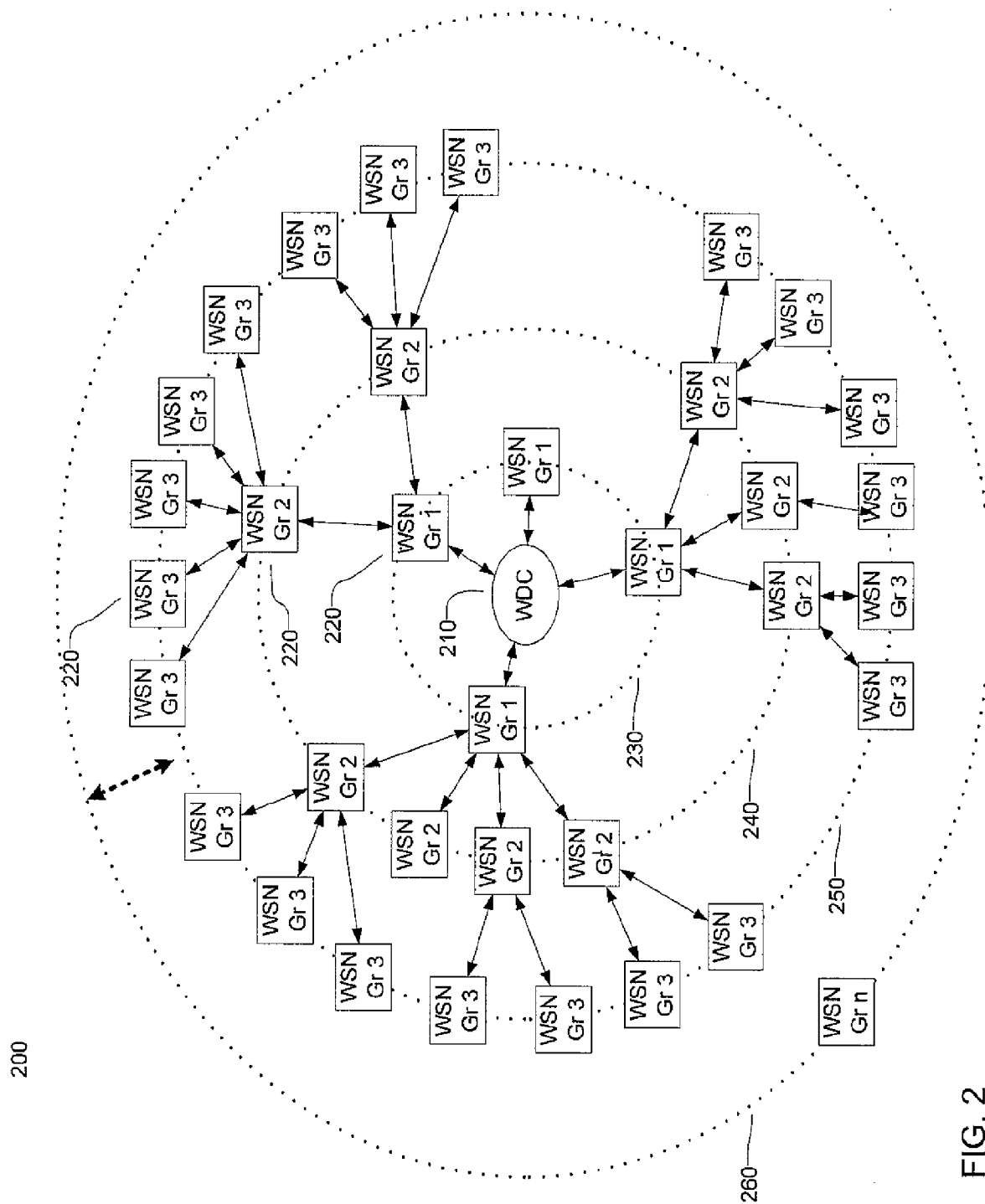


FIG. 2

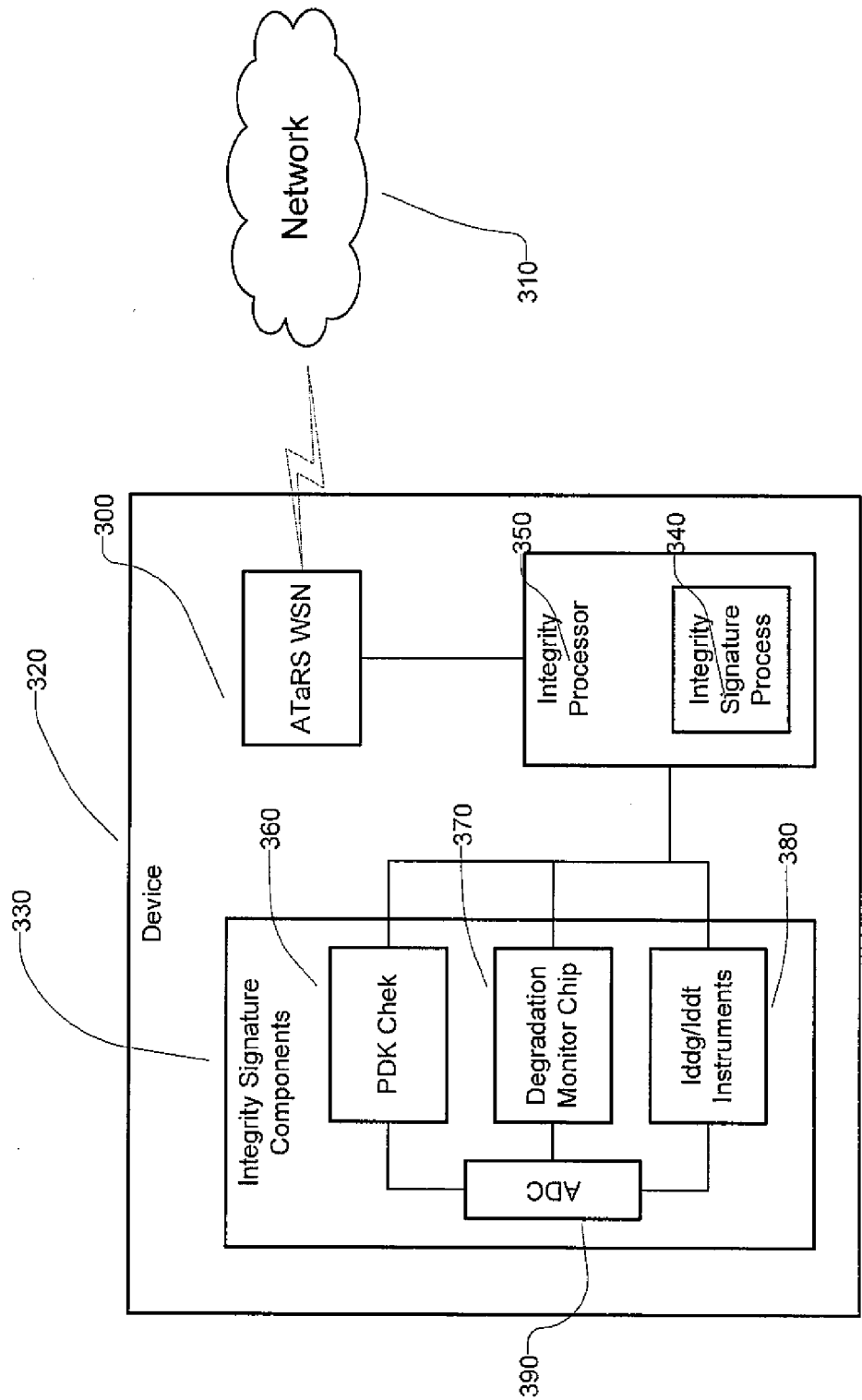


FIG. 3

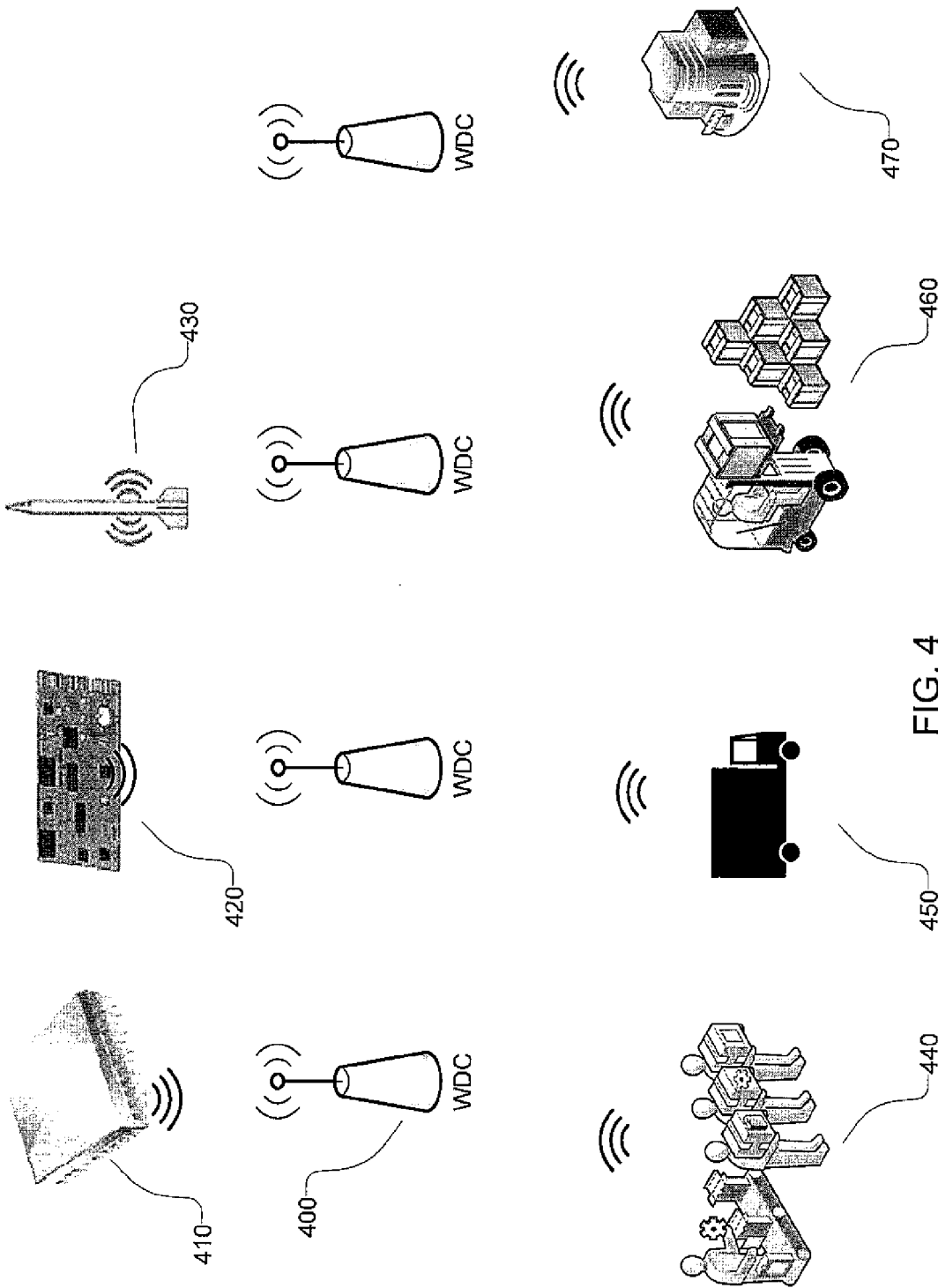


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/011742

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04Q9/00
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04Q

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

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

EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2007/025265 A1 (PORRAS PHILLIP A [US] ET AL PORRAS PHILLIP ANDREW [US] ET AL) 1 February 2007 (2007-02-01) paragraph [0002] paragraph [0007] paragraph [0018] - paragraph [0023] paragraph [0029] - paragraph [0030] paragraph [0036] claims 1-3	1-17
A	US 2007/178914 A1 (MONTENEGRO GABRIEL E [US]) 2 August 2007 (2007-08-02) paragraph [0012] - paragraph [0015] ----- -/-	1,17



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

14 May 2014

Date of mailing of the international search report

22/05/2014

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Barbelanne, Alain

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2014/011742

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2009/081407 A2 (GREENLET TECHNOLOGIES LTD [IL]; COHEN AVNER [IL]) 2 July 2009 (2009-07-02) paragraph [0015] - paragraph [0016] paragraph [0027] - paragraph [0030] paragraph [0033] claim 1 -----	1,17

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2014/011742

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007025265	A1	01-02-2007	NONE

US 2007178914	A1	02-08-2007	CN 101375626 A 25-02-2009
		EP 1980128 A1 15-10-2008	
		JP 4966319 B2 04-07-2012	
		JP 2009525680 A 09-07-2009	
		KR 20080091159 A 09-10-2008	
		US 2007178914 A1 02-08-2007	
		WO 2007089521 A1 09-08-2007	

WO 2009081407	A2	02-07-2009	CA 2748172 A1 02-07-2009
		EP 2227700 A2 15-09-2010	
		US 2010305773 A1 02-12-2010	
		WO 2009081407 A2 02-07-2009	
