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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 October 2014 (02.10.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/155221 A1

(51) International Patent Classification:
H04W 12/06 (2009.01) *H04W 84/04* (2009.01)
H04W 12/12 (2009.01) *H04W 64/00* (2009.01)
H04W 88/08 (2009.01) *H04L 29/06* (2006.01)
H04W 92/10 (2009.01)

(21) International Application Number:
PCT/IB2014/059603

(22) International Filing Date:
10 March 2014 (10.03.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/852,204 28 March 2013 (28.03.2013) US
13/971,885 21 August 2013 (21.08.2013) US

(71) Applicant: **TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)** [SE/SE]; Stockholm, SE-164 83 Stockholm (SE).

(72) Inventors: **GRIFFIOEN, Robert**; 7 Barrhaven Crescent, Ottawa, Ontario K2J 1E7 (CA). **IUN, Edwin Vai Hou**; 27 Cambior Crescent, Ottawa, Ontario K2T 1J5 (CA).

(74) Agent: **BEVINS, R. Chad**; 100 Regency Forest Drive, Suite 160, Cary, North Carolina 27518 (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: TECHNIQUE FOR CONTROLLING LOSS AND THEFT OF REMOTE RADIO EQUIPMENT IN A CELLULAR AD HOC NETWORK

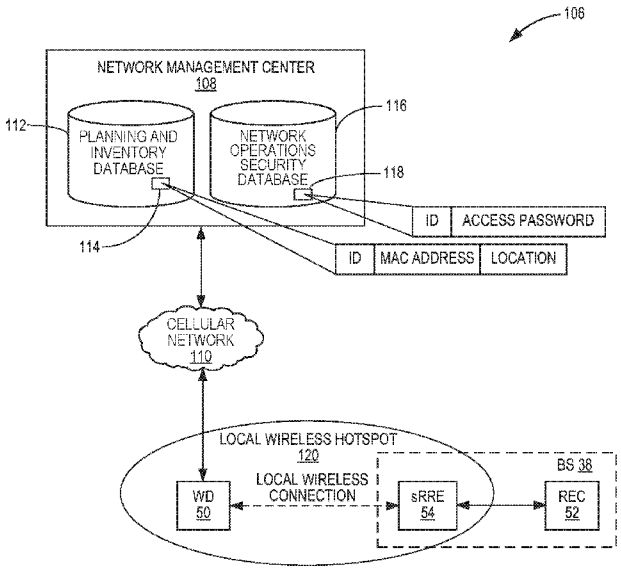

FIG. 14

(57) Abstract: The present disclosure relates to systems and methods for controlling loss and theft of a radio equipment of a base station in a cellular communications network. In one embodiment, a radio equipment (54) of a base station (38) of a cellular communications network (110) includes a radio subsystem (60) configured to wirelessly transmit and receive radio signals for the cellular communications network (110), a local wireless interface (68), memory (76), and a controller (66). During commissioning of the radio equipment (54), the controller (66) is configured to receive a physical location (78) of the radio equipment (54) and an access password (122) for the radio equipment (54) from a wireless device (50) via a local wireless connection between the radio equipment (54) and the wireless device (50) established via the local wireless interface (68). The controller (66) is configured to store the physical location (78) of the radio equipment (54) and the access password (122) for the radio equipment (54) in the memory (76) of the radio equipment (54).

WO 2014/155221 A1

TECHNIQUE FOR CONTROLLING LOSS AND THEFT OF REMOTE RADIO EQUIPMENT IN A CELLULAR AD HOC NETWORK

Related Applications

[0001] This application claims the benefit of US patent application serial number 13/971,885, filed August 21, 2013, which is a Continuation-in-Part of U.S. Application Serial No. 13/852,204 entitled LOCAL WIRELESS CONNECTIVITY FOR RADIO EQUIPMENT OF A BASE STATION IN A CELLULAR COMMUNICATIONS NETWORK, filed March 28, 2013, the disclosures of which are hereby incorporated herein by reference in their entireties.

Field of the Disclosure

[0002] The present disclosure relates to radio equipment of a base station in a cellular communications network and more particularly relates to local wireless connectivity for a radio equipment of a base station in a cellular communications network.

Background

[0003] Cellular communications networks include tens to hundreds of base stations installed at various locations. Two conventional installations are illustrated in Figures 1 and 2. Specifically, Figure 1 illustrates a conventional tower-top mounted installation 10 of a base station. As illustrated, the base station includes a Remote Radio Equipment (RRE) 12 connected to a Radio Equipment Controller (REC) 14. The RRE 12 is mounted at a top of a tower 16 and located between 0 to 20 kilometers (km) from the REC 14. The RRE 12 transmits downlink radio signals and receives uplink radio signals from wireless devices, such as a wireless device (WD) 18, located within a coverage area of the RRE 12. The coverage area of the RRE 12 may be a cell served by the base station or a sector of a cell served by the base station. In this example, the base station is a macro or high power base station where the coverage area of the RRE 12 extends from 0 to 10 km from the tower 16. Figure 2 illustrates a

conventional roof-top mounted installation 20 of the base station. In this example, the base station includes two RREs 12 connected to the REC 14. However, in the roof-top mounted installation 20, the RREs 12 are mounted at the top of a building 22, and the REC 14 is located in the basement or cellar of the building 22.

[0004] One issue with conventional base station installations such as those of Figures 1 and 2 is that the RRE(s) 12 is(are) difficult to reach when maintenance is needed. More specifically, in tower-top mounted installations, the RRE(s) 12 is(are) located at the top of the tower 16 at a height that is typically in the range of 20 to 100 meters (m). As such, when maintenance or field support personnel need to connect to the RRE(s) 12 to perform maintenance operations, the personnel may need to arrange access to the property on which the tower 16 is located and must then climb the tower 16. This is of course time consuming and expensive and creates a significant amount of risk of physical injury to the personnel and potential liability of the cellular communications network operator. Similarly, in roof-top mounted installations, the RRE(s) 12 is(are) located at the top of the building 22. As such, when maintenance or field personnel need to connect to the RRE(s) 12 to perform maintenance operations, the personnel must typically arrange access to the roof-top of the building 22 and potentially climb a mast mounted to the roof-top of the building 22. Again, this is of course time consuming and expensive and creates a significant amount of risk of physical injury to the personnel and potential liability of the cellular communications network operator. As such, there is a need for systems and methods that provide easy and efficient access to RREs for maintenance and field support personnel.

[0005] Another issue that arises with respect to installation of base stations relates to subsequent location and identification of RREs. More specifically, mobile data traffic is exploding at a 60% rate of increase every year. In order to meet this demand, small, or low power, base stations (e.g., micro and pico base stations) can be used, particularly in areas with very dense usage. It is desirable to scatter large numbers of small base stations in order to provide high data rates

to a large number of users. As an example, Figure 3 illustrates a number of small base stations, where each small base station includes three RREs (sRREs) 24 each serving a different sector 26 of a cell 28 served by the small base station. When these small base stations are scattered and used in large numbers, it is difficult to manage the locations and identities of the sRREs 24 of the small base stations. For instance, in an extreme case, the sRREs 24 for the small base stations are deployed in a temporary ad-hoc network to provide increased capacity for, as an example, a sporting event or a conference. As illustrated in Figure 4, in a typical installation, each sRRE 24 includes a remote radio unit 30 and an antenna 32 mounted on a pole 34, or mast.

[0006] During network planning and inventory, it is necessary to associate particular sRREs 24 with corresponding planned physical locations for the sRREs 24. However, when installing the sRREs 24, particularly for a temporary ad-hoc network, the physical locations at which the sRREs 24 are actually installed, or deployed, may not match the planned physical locations for the sRREs 24. Similarly, the actual sRRE 24 deployed at a physical location may not match the sRRE 24 planned for that physical location. This may occur due to, for example, human error and/or on-site adjustments made by field support personnel. Thereafter, when problems arise, the maintenance or field support personnel may not be able to locate and identify a particular sRRE 24 to perform corrective action in a timely manner. Further, even when the physical location of an sRRE 24 is found, multiple sRREs 24 are oftentimes installed at the same physical location in order to cover different sectors of the same cell 28, in which case the maintenance or field support personnel cannot easily identify the particular sRRE 24 of interest. As such, there is also a need for systems and methods that enable easy and accurate location and identification of deployed sRREs.

[0007] Additional issues that are particularly problematic with respect to sRREs 24 are theft and, even worse, industrial espionage in the form of data breaches or acquisition of intellectual property. The sRREs 24 are often installed in remote and possibly isolated locations out of the public eye. This leaves the

sRREs 24 vulnerable to theft and subsequent industrial espionage. Without accurate equipment location and identification information, it becomes a major logistics issue for a network operator to control loss or theft of sRREs 24. As such, there is a further need to deter theft of sRREs 24 and prevent industrial espionage on stolen sRREs 24.

Summary

[0008] The present disclosure relates to systems and methods for controlling loss and theft of a radio equipment of a base station in a cellular communications network. In one embodiment, a radio equipment of a base station of a cellular communications network includes a radio subsystem configured to wirelessly transmit and receive radio signals for the cellular communications network, a local wireless interface, memory, and a controller. During commissioning of the radio equipment, the controller is configured to receive a physical location of the radio equipment and an access password for the radio equipment from a wireless device via a local wireless connection between the radio equipment and the wireless device established via the local wireless interface. The controller is configured to store the physical location of the radio equipment and the access password for the radio equipment in the memory of the radio equipment. In one embodiment, after commissioning, access to the radio equipment requires the access password.

[0009] In one embodiment, the physical location and the access password, together with a device identifier of the radio equipment and a local wireless Media Access Control (MAC) address of the radio equipment, authenticate ownership of the radio equipment.

[0010] In one embodiment, the access password is provided to the radio equipment in such a manner that the access password is unknown to a user, or operator, of the wireless device.

[0011] In one embodiment, after commissioning, the controller of the radio equipment is further configured to detect an unauthorized access attempt based on the access password and, in response, disable the radio equipment. In one

embodiment, the controller is configured to detect the unauthorized access attempt in response to a predefined number of successive invalid access attempts in which one or more incorrect access passwords are utilized to attempt to gain access to the radio equipment. In one embodiment, the controller is configured to disable the radio equipment by erasing valuable information. In one particular embodiment, the valuable information includes one or more applications, one or more logs, and/or user data.

[0012] In one embodiment, the radio equipment is a small, or low power, radio equipment of a small, or low power, base station.

[0013] In one embodiment, a wireless device includes a local wireless interface and a controller configured to obtain an access password for a radio equipment of a base station of a cellular communications network from a network management center of the cellular communications network and transmit the access password to the radio equipment via a local wireless connection established between the wireless device and the radio equipment via the local wireless interface. The controller is further configured to obtain the access password and transmit the access password to the radio equipment in such a manner that the access password is unknown to a user, or operator, of the wireless device.

[0014] Those skilled in the art will appreciate the scope of the present disclosure and realize additional aspects thereof after reading the following detailed description of the preferred embodiments in association with the accompanying drawing figures.

Brief Description of the Drawing Figures

[0015] The accompanying drawing figures incorporated in and forming a part of this specification illustrate several aspects of the disclosure, and together with the description serve to explain the principles of the disclosure.

[0016] Figure 1 illustrates one conventional installation of a base station including a Radio Equipment Controller (REC) and a Remote Radio Equipment (RRE);

[0017] Figure 2 illustrates another conventional installation of a base station including an REC and an RRE;

[0018] Figure 3 illustrates a number of small, or low power, RREs that serve a coverage area within a cellular communications network;

[0019] Figure 4 illustrates one conventional installation of a small, or low power, RRE;

[0020] Figure 5 illustrates a cellular communications network in which a local wireless connection is utilized to enable a wireless device to remotely access a maintenance subsystem of an RRE of a base station according to one embodiment of the present disclosure;

[0021] Figure 6 is a block diagram of one of the base stations of Figure 5 where the base station includes an RRE having a local wireless interface that provides remote access to the maintenance subsystem of the RRE according to one embodiment of the present disclosure;

[0022] Figure 7 is a block diagram of the wireless device of Figure 5 that includes an RRE Maintenance Tool (RRE-MT) and a local wireless interface that enables the RRE-MT to remotely access the maintenance subsystem of the RRE of one of the base stations of Figure 5 according to one embodiment of the present disclosure;

[0023] Figure 8 illustrates a hotspot hosted by the wireless device of Figure 5 to enable local wireless access to the maintenance subsystem of the RRE of one of the base stations of Figure 5 according to one embodiment of the present disclosure;

[0024] Figure 9 illustrates the operation of the wireless device and the RRE of one of the base stations of Figure 5 to provide remote access to the maintenance subsystem of the base station according to one embodiment of the present disclosure;

[0025] Figure 10 illustrates a number of small, or low power, RREs serving a coverage area within a cellular communications network wherein the small RREs are equipped with local wireless interfaces that enable remote access to the

small RREs via local wireless communication according to one embodiment of the present disclosure;

[0026] Figure 11 illustrates the operation of a wireless device and one of the small RREs of Figure 10 to determine and store a physical location of the small RRE according to one embodiment of the present disclosure;

[0027] Figure 12 illustrates the operation of the wireless device to locate a desired one of the small RREs of Figure 10 using a previously determined and stored physical location of the desired small RRE according to one embodiment of the present disclosure;

[0028] Figure 13 is one example of a graphical user interface of the wireless device of Figure 10 according to one embodiment of the present disclosure;

[0029] Figure 14 illustrates a system in which an access password for authentication of ownership of a small RRE is provided to and stored by the small RRE according to one embodiment of the present disclosure;

[0030] Figure 15 is a block diagram of the small RRE of Figure 14 according to one embodiment of the present disclosure;

[0031] Figure 16 illustrates the operation of the system of Figure 14 according to one embodiment of the present disclosure; and

[0032] Figure 17 illustrates a process performed by the small RRE of Figure 14 to detect and handle an unauthorized access attempt according to one embodiment of the present disclosure.

Detailed Description

[0033] The embodiments set forth below represent the necessary information to enable those skilled in the art to practice the embodiments and illustrate the best mode of practicing the embodiments. Upon reading the following description in light of the accompanying drawing figures, those skilled in the art will understand the concepts of the disclosure and will recognize applications of these concepts not particularly addressed herein. It should be understood that these concepts and applications fall within the scope of the disclosure and the accompanying claims.

[0034] The present disclosure relates to local wireless connectivity for a radio equipment of a base station in a cellular communications network. In this regard, Figure 5 illustrates a cellular communications network 36 according to one embodiment of the present disclosure. In this particular embodiment, the cellular communications network 36 is a 3rd Generation Partnership Project (3GPP) Long Term Evolution (LTE) cellular communications network and, as such, some of the terminology used herein may be specific to 3GPP LTE cellular communications networks. However, the present disclosure is not limited to 3GPP LTE cellular communications networks. Rather, the systems and methods disclosed herein may be utilized in any type of cellular communications network.

[0035] As illustrated in Figure 5, the cellular communications network 36 includes a Radio Access Network (RAN), which includes base stations (BSs) 38-1 and 38-2 (more generally referred to herein collectively as base stations 38 and individually as base station 38) that serve corresponding cells 40-1 and 40-2 (more generally referred to herein collectively as cells 40 and individually as cell 40) of the cellular communications network 36. In one embodiment, the base stations 38-1 and 38-2 are macro base stations (e.g., eNodeBs in a 3GPP LTE cellular communications network). In another embodiment, one or more of the base stations 38-1 and 38-2 are small, or low power, base stations (e.g., micro or pico base stations in a 3GPP heterogeneous cellular communications network). A small base station transmits at lower power levels than a large base station. For example, in one embodiment, small base stations transmit at power levels of less than 5 Watts (W).

[0036] The base station 38-1 serves mobile terminals, such as a mobile terminal (MT) 42-1, as well as other types of cellular network enabled devices (e.g., a computer equipped with a cellular network interface) located in the cell 40-1. As such, the base station 38-1 is referred to herein as a serving base station 38-1 of the mobile terminal 42-1. In a similar manner, the base station 38-2 serves mobile terminals, such as a mobile terminal 42-2, as well as other types of cellular network enabled devices located in the cell 40-2. As such, the base station 38-2 is referred to herein as a serving base station 38-2 of the

mobile terminal 42-2. The mobile terminals 42-1 and 42-2 are generally referred to herein as mobile terminals 42. While only two base stations 38-1 and 38-2 and two mobile terminals 42-1 and 42-2 are illustrated in Figure 5 for clarity and ease of discussion, it will be readily appreciated that the cellular communications network 36 includes numerous base stations 38 and numerous mobile terminals 42.

[0037] The cellular communications network 36 also includes a core network 44 that includes one or more Serving Gateways (S-GWs) 46 and one or more Mobility Management Entities (MMEs) 48. In LTE, the base stations 38-1 and 38-2 are connected to the same or different S-GWs 46 via corresponding S1-u connections and connected to the same or different MMEs 48 via corresponding S1-c connections. Similarly, in this embodiment, the base stations 38-1 and 38-2 may be connected to one another via an X2 connection. The S-GWs 46 are user plane nodes connecting the core network 44 to the RAN. Among other things, the S-GWs 46 serve as mobility anchors when mobile terminals, such as the mobile terminals 42-1 and 42-2, move between cells as well as mobility anchors for other 3GPP technologies (e.g., Global System for Mobile Communications (GSM)/General Packet Radio Service (GPRS) and High Speed Packet Access (HSPA)). The MMEs 48 are control plane nodes of the core network 44. The responsibilities of the MMEs 48 include connection/release of bearers to mobile terminals, handling of idle to active transitions, and handling of security keys.

[0038] As discussed below in detail, some or all of the base stations 38 are equipped with local wireless interfaces that enable local wireless connectivity to nearby wireless devices in order to enable remote access to maintenance subsystems of the base stations 38. As used here, a “local wireless interface” is a wireless interface that enables communication via a local wireless connection. Further, a “local wireless connection” is direct point-to-point wireless connection between two devices. Some examples of a local wireless interface are IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, and 802.11n wireless interfaces. In this illustrated example, a wireless device (WD) 50 is enabled to remotely access a maintenance subsystem of a radio equipment of the base station 38-1 via a local

wireless connection between the radio equipment of the base station 38-1 and the wireless device 50. In this manner, an operator, or user, of the wireless device 50 (e.g., a maintenance or field support person) is enabled to access the maintenance subsystem of the base station 38-1 without the need to climb a tower and/or access rental property. In addition or alternatively, the local wireless connection enables maintenance or field support personnel to quickly and easily locate and identify base stations 38 of interest, as discussed below in detail. The wireless device 50 may be any type of device having a local wireless interface such as, for example, a notebook computer, a tablet computer, a smart phone, or the like.

[0039] Figure 6 is a block diagram that illustrates one of the base stations 38 of Figure 5 in more detail according to one embodiment of the present disclosure. In this embodiment, the base station 38 includes a Radio Equipment Controller (REC) 52 and a Remote Radio Equipment (RRE) 54. Notably, as used herein, a Radio Equipment (RE) is a general term that encompasses both RREs and REs that are co-located with their corresponding RECs, whereas an RRE is a RE that is physically separated from the corresponding REC (i.e., a separate device that is separated from the REC by some distance). The RRE 54 may be installed on a tower, on a roof-top of a building, or the like, and the REC 52 is physically separated from the RRE 54 by some distance. The distance between the REC 52 and the RRE 54 may be, for example, a distance up to about 20 kilometers (km). In this example, the REC 52 and the RRE 54 are connected by a fiber optic cable and communicate over the fiber optic cable according to the Common Public Radio Interface (CPRI) specification. While not essential for understanding the concepts disclosed and claimed herein, for more information regarding the CPRI specification, the interested reader is directed to the CPRI Specification v5.0 published on September 21, 2011.

[0040] As illustrated, the REC 52 includes a processing subsystem 56 and a CPRI interface 58. The processing subsystem 56 generally operates to perform baseband processing for the base station 38. In particular embodiments, the processing subsystem 56 may comprise, for example, one or several general-

purpose or special-purpose microprocessors or other microcontrollers programmed with suitable software and/or firmware to carry out some or all of the functionality of the REC 52. In addition or alternatively, the processing subsystem 56 may comprise various digital hardware blocks (e.g., one or more Application Specific Integrated Circuits (ASICs), one or more off-the-shelf digital and analog hardware components, or a combination thereof) configured to carry out some or all of the functionality of the REC 52. Additionally, in particular embodiments, the functionality of the REC 52 may be implemented, in whole or in part, by the processing subsystem 56 executing software or other instructions stored on a non-transitory computer-readable medium, such as Random Access Memory (RAM), Read Only Memory (ROM), a magnetic storage device, an optical storage device, or any other suitable type of data storage components. The CPRI interface 58 enables communication between the REC 52 and the RRE 54 via a CPRI link. Notably, the REC 52 typically includes additional components that are not illustrated in Figure 6 such as, for example, one or more interfaces that enable connection of the base station 38 to other base stations 38 and/or one or more interfaces that enable connection of the base station 38 to the core network 44 (Figure 5).

[0041] The RRE 54 includes a radio subsystem 60 and a CPRI interface 62. As discussed above, the REC 52 provides the digital baseband functionality of the base station 38. The radio subsystem 60 generally provides the analog functionality of the base station 38 (e.g., upconversion, filtering, and amplification). In operation, for the downlink direction, the RRE 54 receives digital baseband signals from the REC 52 via the CPRI interface 62. The radio subsystem 60 then processes the digital baseband signals to generate corresponding radio signals that are transmitted by the RRE 54. Conversely, for the uplink direction, the radio subsystem 60 receives radio signals and generates corresponding baseband signals. The baseband signals are provided to the REC 52 via the CPRI interface 62. The baseband signals are then processed by the REC 52.

[0042] In addition to the radio subsystem 60 and the CPRI interface 62, the RRE 54 includes a local wireless enabled RRE-Maintenance Tool (RRE-MT) subsystem 64 (hereinafter simply referred to as the "RRE-MT subsystem 64"). In this embodiment, the RRE-MT subsystem 64 includes a controller 66, a local wireless interface 68, a CPRI monitor control subsystem 70, a Light Emitting Diode (LED) status and control component 72, an alarm list 74, and memory 76. The controller 66 may be implemented as any type of controller such as, for example, a processor, an ASIC, a Field Programmable Gate Array (FPGA), or the like. In particular embodiments, the controller 66 may comprise, for example, one or several general-purpose or special-purpose microprocessors or other microcontrollers programmed with suitable software and/or firmware to carry out some or all of the functionality of the controller 66 described herein. In addition or alternatively, the controller 66 may comprise various digital hardware blocks (e.g., one or more ASICs, one or more off-the-shelf digital and analog hardware components, or a combination thereof) configured to carry out some or all of the functionality of the controller 66 described herein. Additionally, in particular embodiments, the functionality of the controller 66 described herein may be implemented, in whole or in part, by the controller 66 executing software or other instructions stored on a non-transitory computer-readable medium, such as RAM, ROM, a magnetic storage device, an optical storage device, or any other suitable type of data storage components.

[0043] The local wireless interface 68 is generally any type of local wireless interface that enables a direct point-to-point local wireless connection between the RRE 54 and the wireless device 50. In one embodiment, the local wireless interface 68 is an IEEE 802.11b, IEEE 802.11g, or IEEE 802.11n wireless interface. Notably, IEEE 802.11b and IEEE 802.11g provide ranges of about 95 meters (m) (i.e., 300 feet (ft)), whereas IEEE 802.11n provides a range of about 250 m. Further, the range of the local wireless interface 68 can be extended up to several kilometers by using high gain directional antenna(s).

[0044] The CPRI monitor control subsystem 70 enables monitoring of the CPRI link between the RRE 54 and the REC 52. In particular, the CPRI monitor

control subsystem 70 either activates or deactivates a CPRI monitoring subsystem (not shown) under the control of the controller 66. The CPRI monitoring subsystem can be implemented at any suitable location within the RRE 54 (e.g., within the CPRI interface 62) and generally operates to provide data that replicates traffic flow between the RRE 54 and the REC 52 over the CPRI link or some desired portion thereof (e.g., only the operations and management traffic). Thus, when the CPRI monitoring subsystem is activated, the CPRI monitoring subsystem provides a stream of data to the CPRI monitor control subsystem 70 that corresponds to the traffic flow, or the desired portion(s) of the traffic flow, between the RRE 54 and the REC 52 over the CPRI link. The CPRI monitor control subsystem 70 then provides the stream of data to the controller 66, which in turn can transmit the stream of data (i.e., the monitored traffic flow) to the wireless device 50 via the local wireless interface 68.

[0045] The LED status and control component 72 includes status information, or states (e.g., on, off, or blinking) of one or more LEDs of the RRE 54 as well as circuitry (e.g., a driver circuit) that enables the controller 66 to control the states of the LED(s) of the RRE 54. The alarm list 74 includes a list of alarms or alarm codes generated by the RRE 54 under predefined conditions. In general, the alarms are generated and stored in the alarm list 74 when some undesired event has occurred at the RRE 54. Lastly, the memory 76 is preferably implemented in or as FLASH memory or other non-volatile digital storage device that, in some embodiments, is used to store a physical location 78 of the RRE 54. The physical location 78 is data that defines the physical location of the RRE 54 in two-dimensional or three-dimensional space. In one preferred embodiment, the physical location 78 is a latitude and longitude coordinate pair.

[0046] As discussed below in detail, the RRE-MT subsystem 64 can perform numerous maintenance operations and enables the wireless device 50 to remotely access these maintenance operations via a local wireless connection between the RRE 54 and the wireless device 50. The maintenance operations that can be performed by the RRE-MT subsystem 64 and remotely accessed by the wireless device 50 include, in this example, monitoring traffic flow on the

CPRI link between the REC 52 and the RRE 54 via the CPRI monitor control subsystem 70, reading alarm states of the RRE 54 from the alarm list 74, and reading and/or controlling the state of the LED(s) of the RRE 54 via the LED status and control component 72. In addition, in some embodiments, the RRE-MT subsystem 64 enables the wireless device 50 to provide the physical location of the wireless device 50 to the RRE 54. The RRE-MT subsystem 64 then stores the physical location of the wireless device 50 in the memory 76 as the physical location 78 of the RRE 54. This storing of the physical location 78 is also referred to herein as a maintenance operation. Note, however, that the maintenance operations listed above are only examples. The RRE-MT subsystem 64 may perform additional or alternative maintenance operations as desired.

[0047] Figure 7 is a block diagram of the wireless device 50 of Figure 5 according to one embodiment of the present disclosure. As illustrated, the wireless device 50 includes a controller 80, a local wireless interface 82, a Global Positioning System (GPS) receiver 83, and in this embodiment a cellular network interface 84. In particular embodiments, the controller 80 may comprise, for example, one or several general-purpose or special-purpose microprocessors or other microcontrollers programmed with suitable software and/or firmware to carry out some or all of the functionality of the controller 80 described herein. In addition or alternatively, the controller 80 may comprise various digital hardware blocks (e.g., one or more ASICs, one or more off-the-shelf digital and analog hardware components, or a combination thereof) configured to carry out some or all of the functionality of the controller 80 described herein. Additionally, in particular embodiments, the functionality of the controller 80 described herein may be implemented, in whole or in part, by the controller 80 executing software or other instructions stored on a non-transitory computer-readable medium, such as RAM, ROM, a magnetic storage device, an optical storage device, or any other suitable type of data storage components. In particular, in this embodiment, a RRE-MT 86 is implemented in software and executed by the controller 80.

[0048] The RRE-MT 86 enables the wireless device 50 to access the RRE-MT subsystem 64 of the RRE 54 via the local wireless interface 82. The local wireless interface 82 is generally any type of local wireless interface that enables a direct point-to-point local wireless connection between the wireless device 50 and the RRE 54. In one embodiment, the local wireless interface 82 is an IEEE 802.11b, IEEE 802.11g, or IEEE 802.11n wireless interface. The GPS receiver 83 operates to determine a physical location of the wireless device 50. Note, however, that other location determination mechanisms can be used and, as such, the determination of the physical location of the wireless device 50 is not limited to the use of the GPS receiver 83. The cellular communications interface 84 is optional and may, in some embodiments, be used by the wireless device 50 to send and receive information (i.e., voice and/or data) via the cellular communications network 36 (Figure 5).

[0049] In one embodiment, the wireless device 50 creates, or hosts, a local wireless hotspot 88 (hereinafter simply "hotspot 88") via the local wireless interface 82 of the wireless device 50, as illustrated in Figure 8. In one preferred embodiment, the hotspot 88 is a WiFi hotspot. When the RRE 54 is located within the hotspot 88, the local wireless interface 68 of the RRE 54 connects to the hotspot 88 to thereby establish a local wireless connection with the wireless device 50. Preferably, the local wireless connection is a secure connection. For example, in one preferred embodiment, WPA2 is used to encrypt all traffic in the hotspot 88. WPA2 is a full interoperable implementation of IEEE 802.11i, which makes use of the Advanced Encryption Standard (AES) block cipher. AES is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. While not essential for understanding the concepts disclosed and claimed herein, security may be further enhanced by an absence timer as disclosed in U.S. Patent Application Serial No. 13/674,309, which was filed March 2, 2012 and is hereby incorporated herein by reference with respect to its teachings related to security enhancement using an absence timer. It should be noted that while the wireless device 50 hosts the hotspot 88 in the embodiment of Figure 8 as well as many of the

embodiments discussed below, the hotspot 88 may alternatively be hosted by the RRE 54. For security purposes, it may be beneficial for the wireless device 50 to host the hotspot 88 where the RRE 54 listens for the hotspot 88. However, with enhanced security measures such as pre-installed certificates, the hotspot 88 may alternatively be hosted by the RRE 54 while still maintaining a desirable level of security.

[0050] Figure 9 illustrates the operation of the wireless device 50 and the RRE 54 of the base station 38-1 to provide remote access to the RRE-MT subsystem 64 of the RRE 54 according to one embodiment of the present disclosure. As illustrated, the wireless device 50 creates and hosts the hotspot 88 as illustrated with respect to Figure 8 (step 1000). More specifically, the RRE-MT 86 of the wireless device 50 controls the local wireless interface 82 of the wireless device 50 to create and host the hotspot 88. Next, the local wireless interface 68 of the RRE 54 detects the hotspot 88 (step 1002). Upon detecting the hotspot 88, the controller 66 of the RRE-MT subsystem 64 of the RRE 54 controls the local wireless interface 68 to connect to the hotspot 88, thereby establishing a local wireless connection between the RRE 54 and the wireless device 50 (step 1004). Connecting to the hotspot 88 preferably requires some security mechanism such as, for example, a passphrase, a digital certificate, or the like. If a passphrase is used, the passphrase can be, but is not limited to, a predetermined passphrase for the hotspot 88. Again, in an alternative embodiment, the hotspot 88 is created and hosted by the RRE 54. In this alternative embodiment, the wireless device 50 detects the hotspot 88 and, in response, connects to the hotspot 88 to thereby establish a local wireless connection between the wireless device 50 and the RRE 54.

[0051] Once the local wireless connection is established, a maintenance session is conducted via the local wireless connection (step 1006). More specifically, in one embodiment, preferably under control of an operator of the wireless device 50, the RRE-MT 86 of the wireless device 50 sends one or more maintenance requests to the RRE-MT subsystem 64 of the RRE 54 via the local wireless connection in order to cause the RRE-MT subsystem 64 of the RRE 54

to perform corresponding maintenance operations. The one or more maintenance requests may include a request to monitor traffic flow between the RRE 54 and the REC 52 over the CPRI link, a request to monitor the operation of the RRE 54, a request for alarms in the alarm list 74 of the RRE 54, a request for the state(s) of the LED(s) of the RRE 54, a request to change the state(s) of the LED(s) of the RRE 54, or the like. In one particular embodiment discussed below in detail, the maintenance request is a request to store a provided physical location in the memory 76 of the RRE 54 as the physical location 78 of the RRE 54. Again, the types of maintenance requests given above are only examples. The present disclosure is not limited thereto. For instance, some other types of maintenance requests that may be made by the RRE-MT 86 include a request for a unique identifier of the RRE 54 (e.g., a serial number of the RRE 54), a request to reset the RRE 54, a request for the RRE 54 to provide transmit blocking, a request to control transmit output power (e.g., a request to fine tune and calibrate a transmit power level of the radio subsystem 60), a request to adjust a CPRI block configuration for the CPRI link, or any type of request to configure any subsystem of the RRE 54.

[0052] In response to the maintenance request, the RRE-MT subsystem 64 performs one or more actions indicated by the maintenance request. For instance, if the maintenance request is a request to monitor traffic flow over the CPRI link between the RRE 54 and the REC 52, the controller 66 causes the CPRI monitor control subsystem 70 to activate the CPRI monitoring subsystem. As a result of CPRI monitoring, the traffic flow between the RRE 54 and the REC 52 over the CPRI link, or some desired portion thereof (e.g., control and/or management data), is returned to the controller 66. The controller 66 then provides the monitored traffic flow to the wireless device 50 via the local wireless connection. At the wireless device 50, the RRE-MT 86 stores and/or presents the monitored traffic flow for analysis.

[0053] As another example, if the maintenance request is a request for alarms in the alarm list 74 of the RRE 54, the controller 66 reads the alarms from the alarm list 74 and returns the alarms to the wireless device 50 via the local

wireless connection. The RRE-MT 86 of the wireless device 50 then stores the alarms and/or presents the alarms for analysis. As another example, if the maintenance request is a request for the state(s) of the LED(s) of the RRE 54, the controller 66 reads the state(s) of the LED(s) from the LED status and control component 72 and returns the state(s) of the LED(s) to the wireless device 50 via the local wireless connection. The RRE-MT 86 then stores the state(s) and/or presents the state(s) for analysis. As another example, if the maintenance request is a request to change the state(s) of the LED(s) of the RRE 54 (e.g., a request to blink the LED(s)), the controller 66 causes the LED status and control component 72 to change the state(s) of the LED(s) accordingly.

[0054] Using the process of Figure 9, the operator of the wireless device 50 is enabled to remotely perform various maintenance tasks without the need to physically access the RRE 54 by climbing a tower and/or accessing rental property. As a result, the operator of the wireless device 50 can perform maintenance operations in a much more cost and time efficient manner. Further, risk to the operator and thus liability to the network operator is substantially reduced by avoiding the need to physically access the RRE 54 unless there is a need to uninstall the RRE 54 for maintenance or repair. This is a vast improvement over RREs that require a wired connection to perform maintenance operations. Also, avoiding the need for a physical connection port for maintenance operations reduces material costs, decreases failure points, and eliminates the need to occupy space on a faceplate of the RRE 54 for the physical connection port.

[0055] Thus far, the discussion has focused on remote access to the RRE-MT subsystem 64 of the RRE 54 via a local wireless connection. Figures 10 through 13 illustrate embodiments in which the local wireless connection is utilized to perform a particular maintenance operation, namely, storing a precise and accurate location of the RRE 54 as well as subsequently locating and identifying the RRE 54 when needed. This maintenance operation is particularly beneficial for embodiments where the base stations 38 are small, or low power, base stations 38 and, as such, the RREs 54 are small, or low power, RREs 54. Thus,

for the discussion of Figures 10 through 13, the RREs 54 are referred to as sRREs 54. However, it should be noted that while the discussion of Figures 10 through 13 focuses on sRREs 54, the concepts described with respect to Figures 10 through 13 may additionally or alternatively be used for the RREs 54 of high power base stations 38.

[0056] Figure 10 illustrates another embodiment of the cellular communications network 36 that includes a number of base stations 38-1 through 38-7 each including three sRREs 54 providing coverage for different sectors 90, or coverage areas, within the corresponding cells 40-1 through 40-7 served by the base stations 38-1 through 38-7 according to one embodiment of the present disclosure. In this embodiment, the base stations 38 are, for example, micro or pico base stations in a heterogeneous LTE network. The sRREs 54 for the cell 40-1 provide coverage for corresponding sectors 90-1A, 90-1B, and 90-1C within the cell 40-1, the sRREs 54 for the cell 40-2 provide coverage for corresponding sectors 90-2A, 90-2B, and 90-2C, etc. The sectors 90-1A through 90-7C illustrated in Figure 10 are more generally referred to herein as sectors 90. While not illustrated, the sRREs 54 for the cell 40-1 are connected to a corresponding REC 52 of the base station 38-1, the sRREs 54 for the cell 40-2 are connected to a corresponding REC 52 of the base station 38-2, and so on. Thus, in this embodiment, the baseband processing for the three sRREs 54 in a cell 40 is centralized at a single REC 52. However, in one alternative embodiment, each of the sRREs 54 may have its own REC 52.

[0057] Figure 11 illustrates the operation of the wireless device 50 and one of the sRREs 54 of Figure 10 to provide precise and accurate positioning of the sRRE 54 according to one embodiment of the present disclosure. This process may be performed, for instance, during commissioning or installation of the sRREs 54. As illustrated, the wireless device 50 creates and hosts the hotspot 88 in the manner discussed above (step 2000). More specifically, the RRE-MT 86 of the wireless device 50 controls the local wireless interface 82 of the wireless device 50 to create and host the hotspot 88. Next, the local wireless interface 68 of the sRRE 54 detects the hotspot 88 (step 2002). Upon detecting

the hotspot 88, the controller 66 of the RRE-MT subsystem 64 of the sRRE 54 controls the local wireless interface 68 to connect to the hotspot 88, thereby establishing a local wireless connection between the sRRE 54 and the wireless device 50 (step 2004). Connecting to the hotspot 88 preferably requires some security mechanism such as, for example, a passphrase, a digital certificate, or the like. If a passphrase is used, the passphrase can be, but is not limited to, a predetermined passphrase for the hotspot 88. Again, in an alternative embodiment, the hotspot 88 is created and hosted by the sRRE 54. In this alternative embodiment, the wireless device 50 detects the hotspot 88 and, in response, connects to the hotspot 88 to thereby establish a local wireless connection between the wireless device 50 and the sRRE 54.

[0058] In this embodiment, the wireless device 50 obtains a MAC address of the local wireless interface 68 of the sRRE 54 (step 2006). More specifically, the RRE-MT 86 instructs the controller 80 of the wireless device 50 to obtain the MAC address of the local wireless interface 68 of the sRRE 54 from the local wireless interface 82 of the wireless device 50. While illustrated as a separate step for clarity and ease of discussion, the local wireless interface 82 of the wireless device 50 may obtain the MAC address of the local wireless interface 68 of the sRRE 54 when exchanging messages with the local wireless interface 82 during setup of the local wireless connection. As discussed below, the MAC address of the local wireless interface 68 of the sRRE 54 is utilized as a unique identifier for the sRRE 54. However, the MAC address of the local wireless interface 68 is only one example of a unique identifier for the sRRE 54. Any unique identifier of the sRRE 54 may be used. For example, a serial number of the sRRE 54 may alternatively be used. In this case, the wireless device 50 can send a request for the unique identifier of the sRRE 54 (e.g., the serial number of the sRRE 54) to the sRRE 54 and receive the unique identifier of the sRRE 54 via the local wireless connection.

[0059] In addition, the RRE-MT 86 instructs the controller 80 of the wireless device 50 to obtain the physical location of the wireless device 50 (step 2008). In this embodiment, the physical location of the wireless device 50 is obtained from

the GPS receiver 83 of the wireless device 50. However, again, the GPS receiver 83 is only an example. Other location determination mechanisms may be used. Next, in this embodiment, the RRE-MT 86 instructs the controller 80 to send the physical location of the wireless device 50 to the sRRE 54 as the physical location 78 of the sRRE 54 (step 2010). More specifically, in one embodiment, the RRE-MT 86 sends a maintenance request to the RRE-MT subsystem 64 of the sRRE 54 to store a provided physical location, which is the physical location of the wireless device 50 obtained in step 2008), as the physical location 78 of the sRRE 54. In response, the RRE-MT subsystem 64 of the sRRE 54 stores the physical location provided by the wireless device 50 in the memory 76 as the physical location 78 of the sRRE 54 (step 2012). The physical location 78 of the sRRE 54 may then be utilized by the RRE 54 and/or the cellular communications network 36 in any desired manner. For example, a main operation office of the cellular communications network 36 may request the physical location 78 of the sRRE 54 via the CPRI link with the REC 52. It should be noted that steps 2010 and 2012 are not necessary. Thus, in some embodiments, the physical location of the wireless device 50 is not provided to and stored by the sRRE 54 as the physical location 78 of the sRRE 54.

[0060] At the wireless device 50, the RRE-MT 86 further instructs the controller 80 to update a remote database with the MAC address of the local wireless interface 68 of the sRRE 54 (or other unique identifier of the sRRE 54) and the physical location 78 of the sRRE 54 (step 2014). Again, the physical location 78 of the sRRE 54 is the physical location of the wireless device 50 obtained in step 2008. The MAC address serves to resolve ambiguity if multiple sRREs 54 are at the same physical location. The manner in which the remote database is updated may vary depending on the particular implementation. In one embodiment, the RRE-MT 86 instructs the controller 80 to communicate the MAC address and the physical location of the sRRE 54 to the remote database via the cellular network interface 84 of the wireless device 50. In another embodiment, the RRE-MT 86 instructs the controller 80 to store the MAC

address and the physical location of the sRRE 54 for subsequent transfer to the remote database.

[0061] In one embodiment, the remote database is a planning and inventory database maintained by an operator of the cellular communications network 36. As such, using the process of Figure 11, the planning and inventory database provides an up-to-date view of the cellular communications network 36. Using the planning and inventory database, any unintentional error such as the installation of an sRRE 54 at a physical location other than the planned physical location can be immediately detected at the time of installation.

[0062] Using the process of Figure 11, precise and accurate locations of the sRREs 54 are maintained in the remote database. Thus, even if the sRREs 54 are deployed or installed at physical locations other than those originally planned, the process of Figure 11 can be used by maintenance or field support personnel during installation to quickly and easily record the physical locations of the sRREs 54 at the time of installation. The physical locations of the sRREs 54 maintained in the remote database can subsequently be used to locate and identify sRREs 54 of interest. In this regard, Figure 12 illustrates a process for locating and identifying an sRRE 54 of interest using the physical location and MAC address of the sRRE 54 previously obtained via the process of Figure 11 according to one embodiment of the present disclosure.

[0063] During service, when it is desired to locate and identify one of the sRREs 54, a maintenance or field support person obtains the physical address and the MAC address of the sRRE 54 from the remote database. For example, a ticket may be provided to the maintenance or field support person, where the ticket includes the physical location and the MAC address of an sRRE 54 to be serviced. The operator of the wireless device 50 (e.g., the maintenance or field support person) then goes to the physical location of the sRRE 54 to be serviced.

[0064] Once at the physical location of the sRRE 54 to be serviced, the wireless device 50 creates the wireless hotspot 88 (step 3000). More specifically, the RRE-MT 86 of the wireless device 50 controls the local wireless interface 82 of the wireless device 50 to create and host the hotspot 88. Next,

the local wireless interface 68 of the sRRE 54 detects the hotspot 88 (step 3002). Upon detecting the hotspot 88, the controller 66 of the RRE-MT subsystem 64 of the sRRE 54 controls the local wireless interface 68 to connect to the hotspot 88, thereby establishing a local wireless connection between the sRRE 54 and the wireless device 50 (step 3004). Connecting to the hotspot 88 preferably requires some security mechanism such as, for example, a passphrase, a digital certificate, or the like. If a passphrase is used, the passphrase can be, but is not limited to, a predetermined passphrase for the hotspot 88. Again, in an alternative embodiment, the hotspot 88 is created and hosted by the sRRE 54. In this alternative embodiment, the wireless device 50 detects the hotspot 88 and, in response, connects to the hotspot 88 to thereby establish a local wireless connection between the wireless device 50 and the sRRE 54.

[0065] The wireless device 50 also obtains a MAC address of the local wireless interface 68 of the sRRE 54 (step 3006). More specifically, the RRE-MT 86 instructs the controller 80 of the wireless device 50 to obtain the MAC address of the local wireless interface 68 of the sRRE 54 from the local wireless interface 82 of the wireless device 50. While illustrated as a separate step for clarity and ease of discussion, the local wireless interface 82 of the wireless device 50 may obtain the MAC address of the local wireless interface 68 of the sRRE 54 when exchanging messages with the local wireless interface 82 during setup of the local wireless connection. Again, it should be noted that the MAC address of the local wireless interface 68 is only one example of a unique identifier for the sRRE 54. Any unique identifier of the sRRE 54 may be used. For example, a serial number of the sRRE 54 may alternatively be used. In this case, the wireless device 50 can send a request for the unique identifier of the sRRE 54 (e.g., the serial number of the sRRE 54) to the sRRE 54 and receive the unique identifier of the sRRE 54 via the local wireless connection.

[0066] If the MAC address (or other unique identifier) of the sRRE 54 does not match the MAC address of the sRRE 54 to be serviced, then this particular sRRE 54 is not the sRRE 54 to be serviced. This may occur in installations where, for example, multiple sRREs 54 are installed at the same physical location (e.g.,

mounted on the same pole or mast) or where multiple sRREs 54 are within local wireless range of the wireless device 50. However, in this example, the MAC address of the sRRE 54 matches the MAC address of the sRRE 54 to be serviced.

[0067] Next, in this embodiment, in order for the operator of the wireless device 50 to visually identify the sRRE 54 of interest, the RRE-MT 86 instructs the controller 80 of the wireless device 50 to send a blink request to the sRRE 54 (step 3008). In this embodiment, the blink request is provided in the form of a maintenance request to the RRE-MT subsystem 64 of the sRRE 54. In response, the controller 66 of the RRE-MT subsystem 64 of the sRRE 54 controls one or more of the LED(s) of the sRRE 54 to blink such that the operator of the sRRE 54 can visually identify the sRRE 54 of interest (step 3010). Again, this may be beneficial when, for example, multiple sRREs 54 are installed on the same pole or mast or are otherwise deployed at or near the same physical location. At this point, if desired, a maintenance session may be conducted in the manner described above (step 3012).

[0068] Figure 13 illustrates one example of a Graphical User Interface (GUI) 92 of the RRE-MT 86 according to one embodiment of the present disclosure. As illustrated, when an Identity tab 94 is selected, the GUI 92 presents the physical location of the wireless device 50 obtained from the GPS receiver 83, the MAC address of the sRRE 54 to which the wireless device 50 is connected, and various information obtained from a lookup for the MAC address of the sRRE 54 (e.g., hardware ID, software ID, etc.). If the operator of the wireless device 50 desires to send the physical location of the wireless device 50 to the sRRE 54 to be stored as the physical location 78 of the sRRE 54, the operator selects a Save GPS button 96. Upon selecting the Save GPS button 96, the physical location (i.e., the GPS location) of the wireless device 50 is sent to the sRRE 54 via the local wireless connection where the physical location is stored as the physical location 78 of the sRRE 54. Further, if the operator of the wireless device 50 desires to update the remote database with the MAC address and the physical location of the sRRE 54, the operator selects an Update dB button 98. In

response, in this embodiment, the RRE-MT 86 instructs the controller 80 to update the remote database with the MAC address and the physical location of the sRRE 54. Still further, if the operator desires to blink one or more LED(s) of the sRRE 54 for visual identification of the sRRE 54, the operator selects a Blink button 100. In response, the RRE-MT 86 instructs the controller 80 to send a maintenance request to blink the LED(s) of the sRRE 54 via the local wireless connection.

[0069] Lastly, the GUI 92 includes an LED tab 102 and an ALM tab 104. The operator of the wireless device 50 can select the LED tab 102 to view status information for the LED(s) of the sRRE 54 which, as discussed above, can be obtained from the sRRE 54 via the local wireless connection using a corresponding maintenance request. Similarly, the operator of the wireless device 50 can select the ALM tab 104 to view any alarms obtained from the sRRE 54 via the local wireless connection using a corresponding maintenance request.

[0070] While not limited by any particular advantages, the embodiments of Figures 10 through 13 provide numerous advantages over conventional techniques for locating and identifying sRREs 54 of interest. For instance, the embodiments of Figures 10 through 13 simplify management of sRRE 54 locations particularly in an ad-hoc network and give the ability to track lost or misplaced sRREs 54. In addition, by further using the remote maintenance operations discussed with respect to Figures 5 through 9, maintenance or field support personnel are enabled to quickly and easily assess the sRREs 54 before having to arrange for equipment (e.g., scaffolding or a hydraulic lift) to reach the sRREs 54.

[0071] Using the embodiments discussed above, a network operator is able to accurately track the locations of the sRREs 54 as well as quickly locate and identify the sRREs 54 when they are in the need of service. However, sRREs 54 are often installed in isolated or remote locations that are out of the public eye. As such, theft is a significant issue. Further, industrial espionage may be used to obtain valuable information from stolen sRREs 54. Figure 14 illustrates a system

106 that enables a network operator to authenticate ownership of an sRRE 54 and prevent access to the sRRE 54 by unauthorized persons according to one embodiment of the present disclosure. As illustrated, the system 106 includes the wireless device 50 as well as the REC 52 and the sRRE 54, which form the small base station 38 of a cellular communications network. In addition, the wireless device 50 is communicatively coupled to a network management center 108 of the cellular communications network via a cellular communications network 110. The cellular communications network 110 is preferably the same cellular communications network as that managed by the network management center 108. Note that the wireless device 50 may also be able to connect to the network management center 108 via other type(s) of networks such as, for example, a local wireless network (i.e., a wireless Local Area Network (LAN)).

[0072] The network management center 108 includes a planning and inventory database 112 that preferably stores an entry 114 for each sRRE 54 in the cellular communications network. Each entry 114 includes a device identifier (ID) (e.g., a serial number), a local wireless MAC address, and the physical location of the corresponding sRRE 54. Like in the embodiments above, the MAC address and the physical location of the sRRE 54 are obtained by the wireless device 50. The wireless device 50 reports the MAC address and the physical location of the sRRE 54 to the network management center 108, where they are stored in the corresponding entry 114 for the sRRE 54 in the planning and inventory database 112. The network management center 108 also includes a network operations security database 116 that includes, for each sRRE 54, an entry 118 that includes the device ID of the sRRE 54 and an access password for the sRRE 54. The access password is predefined, or pre-allocated, for the sRRE 54 by the network operator and stored in the corresponding entry 118 in the network operations security database 116.

[0073] In operation, during commissioning of the sRRE 54, a wireless connection is established between the wireless device 50 and the sRRE 54 via a local wireless hotspot 120. In one embodiment, the local wireless hotspot 120 is hosted by the wireless device 50. In another embodiment, the local wireless

hotspot 120 is hosted by the sRRE 54. The wireless device 50 obtains a physical location of the wireless device 50 via a location determination function (e.g., a GPS receiver) of the wireless device 50 and provides the physical location of the wireless device 50 to the sRRE 54, where the physical location is stored as the physical location of the sRRE 54. In addition, the wireless device 50 obtains the MAC address of the sRRE 54. The wireless device 50 sends the physical location and the MAC address to the network management center 108 for storage in the corresponding entry 114 in the planning and inventory database 112. In addition, the wireless device 50 performs a machine-to-machine transfer of the access password for the sRRE 54 from the network operations security database 116 to the sRRE 54 in such a manner that the access password is unknown to the user, or operator, of the wireless device 50. The access password is stored by the sRRE 54. Thereafter, the sRRE 54 requires the access password before access to the sRRE 54 is granted. Further, the combination of the device ID, physical location, MAC address, and access password provide proof of ownership of the sRRE 54 by the network operator.

[0074] Figure 15 illustrates the base station 38 including the REC 52 and the sRRE 54 of Figure 14 according to one embodiment of the present disclosure. This embodiment is substantially the same as that of Figure 6 but where the access password, referenced as access password 122, of the sRRE 54 is also stored in the memory 76.

[0075] Figure 16 illustrates the operation of the system 106 of Figure 14 according to one embodiment of the present disclosure. As with the other processes described herein, while the steps of Figure 16 are illustrated in a particular order, the steps may be performed in any order unless explicitly stated or otherwise required. During commissioning of the sRRE 54, the wireless device 50 creates the local wireless hotspot 120 (e.g., WiFi hotspot) (step 4000). The sRRE 54 detects the local wireless hotspot 120 (step 4002) and, in response, connects to the local wireless hotspot 120 via the local wireless interface 68 of the sRRE 54 (step 4004). At this point, a local wireless

connection has been established between the wireless device 50 and the sRRE 54.

[0076] The wireless device 50 obtains the MAC address of the sRRE 54 for the local wireless connection (i.e., the local wireless MAC address of the sRRE 54) (step 4006). The wireless device 50 also obtains the physical location of the wireless device 50 via the GPS receiver 83, or other location determination function, of the wireless device 50 (step 4008). In addition, the wireless device 50 obtains the access password for the sRRE 54 by first sending a request to the network management center 108 for the access password of the sRRE 54 (e.g., based on the device ID of the sRRE 54) (step 4010). In response to the request, the wireless device 50 receives the access password for the sRRE 54 from the network management center 108 (step 4012). The wireless device 50 sends the physical location and the access password to the sRRE 54 (step 4014).

[0077] Importantly, the access password is obtained from the network management center 108 and transferred to the sRRE 54 without being revealed to the operator of the wireless device 50. As such, the access password is unknown to the operator of the wireless device 50. This transfer of the access password is referred to herein as a machine-to-machine transfer of the access password. Note that, in the same manner, the access password may be obtained from the network management center 108 and provided to the sRRE 54 in order to subsequently access the sRRE 54 via the same wireless device 50 or some other wireless device. Still further, the wireless device 50 is also preferably access protected (e.g., password protected) such that the wireless device 50 is protected against unauthorized access. A field crew personnel would need to have the proper credentials (e.g., password) to access the wireless device 50. Thus, if the wireless device 50 is lost or stolen, an unauthorized person would be prevented from accessing the wireless device 50. The wireless device 50 may be disabled either autonomously (e.g., the wireless device 50 may disable itself after a predefined number of successive invalid access attempts) or by the network operator (e.g., the network operator may be enabled to remotely disable

the wireless device 50 upon determining or being notified that the wireless device 50 has been lost or stolen).

[0078] The sRRE 54 stores the physical location and the access password in the memory 76 as the physical location 78 and the access password 122 of the sRRE 54, respectively (step 4016). The wireless device 50 also sends the MAC address and the physical location of the sRRE 54 to the network management center 108, which stores the MAC address and the physical location of the sRRE 54 in the planning and inventory database 112 (steps 4018-4020). By storing the device ID, MAC address, physical location, and access password at the network management center 108, the network operator is enabled to uniquely identify the sRRE 54 and authenticate ownership of the sRRE 54. This may be particularly important in deployment scenarios where different network operators have equipment deployed side-by-side or in the same geographic area. Further, if the sRRE 54 is stolen, it would not be possible to configure the sRRE 54 in another network without the access password. In other words, the sRRE 54 requires entry of the access password before the sRRE 54 will allow access to the sRRE 54 for configuration. Likewise, before valuable information can be obtained from the sRRE 54 (e.g., application(s) and/or log(s)), the sRRE 54 requires entry of the access password. In this manner, industrial espionage is prevented. Thus, without the access password, the sRRE 54 cannot be managed or re-configured and is of no operational value.

[0079] Further, in one embodiment, the sRRE 54 disables itself upon detecting an unauthorized access attempt. In this regard, Figure 17 illustrates a process by which the sRRE 54 disables itself in response to detecting an unauthorized access attempt according to one embodiment of the present disclosure. First, the sRRE 54 detects an unauthorized access attempt (step 5000). In one particular embodiment, the sRRE 54 detects an unauthorized access attempt in response to a predefined number of successive invalid access attempts (access attempts with an incorrect access password). In response to detecting an unauthorized access attempt, the sRRE 54 raises an alarm and disables itself (step 5002). In one embodiment, the sRRE 54 disables itself by

erasing valuable information such as, for example, application(s), log(s), and/or user data (e.g., network configuration information). This prevents industrial espionage. Further, in one embodiment, a bootloader of the sRRE 54 may remain intact such that the owner or authorized operator can restore the sRRE 54. For instance, if application(s) are removed when disabling the sRRE 54, the owner or authorized operator can restore the sRRE 54 by re-downloading the application(s) removed when disabling the sRRE 54. In another embodiment, the sRRE 54 may be restored by returning the sRRE 54 to the manufacturer.

[0080] The embodiments of Figures 14-17 provide numerous advantages. While not being limited to any particular advantage, the embodiments of Figures 14-17 simplify management of sRREs 54 particularly in an ad hoc network; enable the network operator to authenticate ownership of the sRREs 54 using the device IDs, MAC addresses (local wireless MAC addresses), physical locations, and access passwords; allow the network operator the ability to track lost or misplaced sRREs 54; permit quick location and validation of ownership of the sRREs 54 before having to actually reach the sRREs 54 (e.g., via hydraulic lift or scaffolding equipment); avoid the need to give the access passwords of the sRREs 54 to field crew; and protect the sRREs 54 from theft.

[0081] Further, lost or stolen sRREs 54 can be immediately detected upon installation. For instance, the location of a lost or stolen sRRE 54 and the local wireless MAC address of the sRRE 54 will be reported to the network management center 108 immediately upon installation/commissioning. During this same process, the access password (allocated by the network management center 108) is pushed to the sRRE 54. If the network operator knows that the sRRE 54 (which has a particular device ID) is lost or stolen, the network operator can then locate the lost or stolen sRRE 54 and authenticate ownership of the sRRE 54 via the combination of the device ID, MAC address, physical location, and access password.

[0082] As a final note, while embodiments described above focus on the RREs 54 and the sRREs 54, the concepts described herein are not limited to RREs. More specifically, the concepts described herein are equally applicable to

REs and small REs that are co-located with their corresponding RECs. Further, while Figures 14-17 are described with respect to an sRRE, the concepts are equally applicable to RREs of macro, or high power, base stations.

[0083] The following acronyms are used throughout this disclosure.

- 3GPP 3rd Generation Partnership Project
- AES Advanced Encryption Standard
- ASIC Application Specific Integrated Circuit
- BS Base Station
- CPRI Common Public Radio Interface
- FPGA Field Programmable Gate Array
- ft Foot
- GPRS General Packet Radio Service
- GPS Global Positioning System
- GSM Global System for Mobile Communications
- GUI Graphical User Interface
- HSPA High Speed Packet Access
- ID Identifier
- km Kilometer
- LAN Local Area Network
- LED Light Emitting Diode
- LTE Long Term Evolution
- m Meter
- MAC Media Access Control
- MME Mobility Management Entity
- MT Mobile Terminal
- NIST National Institute of Standards and Technology
- RAM Random Access Memory
- RAN Radio Access Network
- REC Radio Equipment Controller
- ROM Read Only Memory

- RE Radio Equipment
- RRE Remote Radio Equipment
- RRE-MT Remote Radio Equipment Maintenance Tool
- S-GW Serving Gateway
- W Watt
- WD Wireless Device

[0084] Those skilled in the art will recognize improvements and modifications to the preferred embodiments of the present disclosure. All such improvements and modifications are considered within the scope of the concepts disclosed herein and the claims that follow.

Claims

What is claimed is:

1. A radio equipment (54) of a base station (38) for a cellular communications network (110), comprising:

a radio subsystem (60) configured to wirelessly transmit and receive radio signals for the cellular communications network (110);

a local wireless interface (68);

memory (76); and

a controller (66) associated with the local wireless interface (68) and the memory (76) that is configured to, during commissioning of the radio equipment (54):

receive a physical location (78) of the radio equipment (54) and an access password (122) for the radio equipment (54) from a wireless device (50) via a local wireless connection between the radio equipment (54) and the wireless device (50) established via the local wireless interface (68); and

store the physical location (78) of the radio equipment (54) and the access password (122) for the radio equipment (54) in the memory (76).

2. The radio equipment (54) of claim 1 wherein the physical location (78) and the access password (122), together with a device identifier of the radio equipment (54) and a Media Access Control, MAC, address of the radio equipment (54) for the local wireless interface (68), authenticate ownership of the radio equipment (54).

3. The radio equipment (54) of claim 1 wherein the wireless device (50) is a mobile terminal (42) operated by a user, and the access password (122) is received from the mobile terminal (42) in such a manner that the access password (122) is unknown to the user of the mobile terminal (42).

4. The radio equipment (54) of claim 1 wherein the controller (66) is further configured to, subsequently to receiving and storing the physical location (78) and the access password (122):

detect an unauthorized access attempt based on the access password (122); and

disable the radio equipment (54) in response to detecting the unauthorized access attempt.

5. The radio equipment (54) of claim 4 wherein the controller (66) is further configured to detect the unauthorized access attempt by detecting a predetermined number of failed access attempts in which one or more passwords that do not match the access password (122) for the radio equipment (54) were used to attempt to access the radio equipment (54).

6. The radio equipment (54) of claim 4 wherein, in order to disable the radio equipment (54), the controller (66) is further configured to erase valuable information from the radio equipment (54).

7. The radio equipment (54) of claim 6 wherein the valuable information comprises at least one of a group consisting of: one or more applications executed by the radio equipment (54), one or more logs maintained by the radio equipment (54), and user data.

8. The radio equipment (54) of claim 1 wherein the radio equipment (54) is a low power radio equipment, and the base station (38) is a low power base station.

9. The radio equipment (54) of claim 1 wherein the controller (66) is further configured to control the local wireless interface (68) to connect to a hotspot (120) hosted by the wireless device (50) to thereby establish the local wireless connection between the radio equipment (54) and the wireless device (50).

10. The radio equipment (54) of claim 1 wherein the controller (66) is further configured to control the local wireless interface (68) to create a hotspot (120), wherein the wireless device (50) connects to the hotspot (120) to thereby establish the local wireless connection between the radio equipment (54) and the wireless device (50).

11. A method of operation of a radio equipment (54) of a base station (38) for a cellular communications network (110), comprising:

receiving, during commissioning of the radio equipment (54), a physical location (78) of the radio equipment (54) and an access password (122) for the radio equipment (54) from a wireless device (50) via a local wireless connection between the radio equipment (54) and the wireless device (50) established via a local wireless interface (68) of the radio equipment (54); and

storing the physical location (78) of the radio equipment (54) and the access password (122) for the radio equipment (54) in memory (76).

12. The method of claim 11 wherein the physical location (78) and the access password (122), together with a device identifier of the radio equipment (54) and a Media Access Control, MAC, address of the radio equipment (54) for the local wireless interface (68), authenticate ownership of the radio equipment (54).

13. The method of claim 11 wherein the wireless device (50) is a mobile terminal operated by a user, and receiving the physical location (78) and the access password (122) comprises receiving the access password (122) from the mobile terminal in such a manner that the access password (122) is unknown to the user of the mobile terminal.

14. The method of claim 11 wherein subsequent to receiving and storing the physical location (78) and the access password (122):

detecting an unauthorized access attempt based on the access password (122); and

disabling the radio equipment (54) in response to detecting the unauthorized access attempt.

15. The method of claim 14 wherein detecting the unauthorized access attempt comprises detecting a predetermined number of failed access attempts in which one or more passwords that do not match the access password (122) of the radio equipment (54) were used to attempt to access the radio equipment (54).

16. The method of claim 14 wherein disabling the radio equipment (54) comprises erasing valuable information from the radio equipment (54).

17. The method of claim 16 wherein the valuable information comprises at least one of a group consisting of: one or more applications executed by the radio equipment (54), one or more logs maintained by the radio equipment (54), and user data.

18. The method of claim 11 wherein the radio equipment (54) is a low power radio equipment, and the base station (38) is a low power base station.

19. The method of claim 11 further comprising connecting to a local wireless hotspot (120) hosted by the wireless device (50) to thereby establish the local wireless connection between the radio equipment (54) and the wireless device (50).

20. The method of claim 11 further comprising creating a hotspot (120) via the local wireless interface (68) of the radio equipment (54), wherein the wireless device (50) connects to the hotspot (120) to thereby establish the local wireless connection between the radio equipment (54) and the wireless device (50).

21. A wireless device (50) comprising:

a local wireless interface (82); and

a controller (80) associated with the local wireless interface (82) configured to:

obtain an access password (122) for a radio equipment (54) of a base station (38) of a cellular communications network (110) from a network management center (108) of the cellular communications network (110); and

transmit, to the radio equipment (54), the access password (122) for the radio equipment (54) via a local wireless connection established between the wireless device (50) and the radio equipment (54) via the local wireless interface (82);

wherein the controller (80) is configured to obtain the access password (122) and transmit the access password (122) in such a manner that the access password (122) is unknown to a user of the wireless device (50).

22. The wireless device (50) of claim 21 further comprising a location determination function configured to obtain a physical location of the wireless device (50), and wherein the controller (80) is further configured to:

obtain the physical location of the wireless device (50) from the location determination function;

transmit, to the radio equipment (54), the physical location of the wireless device (50) as a physical location (78) of the radio equipment (54) via the local wireless connection established between the wireless device (50) and the radio equipment (54) via the local wireless interface (82);

obtain a local wireless Media Access Control, MAC, address of the radio equipment (54); and

provide the physical location (78) of the radio equipment (54) and the local wireless MAC address of the radio equipment (54) to the network management

center (108) for storage in association with the access password (122) and a device identifier of the radio equipment (54).

23. The wireless device (50) of claim 22 wherein the physical location (78) and the access password (122), together with the device identifier of the radio equipment (54) and the local wireless MAC address, authenticate ownership of the radio equipment (54).

24. The wireless device (50) of claim 21 further comprising a cellular network interface (84) configured to communicatively couple the wireless device (50) to the cellular communications network (110), and the controller (80) is further configured to communicate with the network management center (108) via the cellular network interface (84) to obtain the access password (122).

25. The wireless device (50) of claim 21 wherein, in order to establish the local wireless connection, the controller (80) is further configured to:

create a hotspot (120) via the local wireless interface (82), where the local wireless connection is a connection to the hotspot (120).

26. The wireless device (50) of claim 21 wherein, in order to establish the local wireless connection, the controller (80) is further configured to:

connect to a hotspot (120) hosted by the radio equipment (54) via the local wireless interface (82) to thereby establish the local wireless connection between the wireless device (50) and the radio equipment (54).

27. A method of operation of a wireless device (50) comprising:

obtaining an access password (122) for a radio equipment (54) of a base station (38) of a cellular communications network (110) from a network management center (108) of the cellular communications network (110); and

transmitting, to the radio equipment (54), the access password (122) for the radio equipment (54) via a local wireless connection established between the

wireless device (50) and the radio equipment (54) via a local wireless interface (82) of the wireless device (50);

wherein obtaining the access password (122) and transmitting the access password (122) are performed in such a manner that the access password (122) is unknown to a user of the wireless device (50).

28. The method of claim 27 further comprising:

obtaining a physical location of the wireless device (50);

transmitting, to the radio equipment (54), the physical location of the wireless device (50) as a physical location (78) of the radio equipment (54) via the local wireless connection established between the wireless device (50) and the radio equipment (54) via the local wireless interface (82) of the wireless device (50);

obtaining a local wireless Media Access Control, MAC, address of the radio equipment (54); and

providing the physical location (78) of the radio equipment (54) and the local wireless MAC address of the radio equipment (54) to the network management center (108) for storage in association with the access password (122) and a device identifier of the radio equipment (54).

29. The method of claim 28 wherein the physical location (78) and the access password (122), together with the device identifier of the radio equipment (54) and the local wireless MAC address, authenticate ownership of the radio equipment (54).

30. The method of claim 27 further comprising obtaining the access password (122) from the network management center (108) via a cellular communications network interface (84) of the wireless device (50).

31. The method of claim 27 further comprising creating a hotspot (12) via the local wireless interface (82) of the wireless device (50), where the radio

equipment (54) establishes the local wireless connection by connecting to the hotspot (120).

32. The method of claim 27 further comprising connecting to a hotspot (120) hosted by the radio equipment (54) via the local wireless interface (82) of the wireless device (50) to thereby establish the local wireless connection between the wireless device (50) and the radio equipment (54).

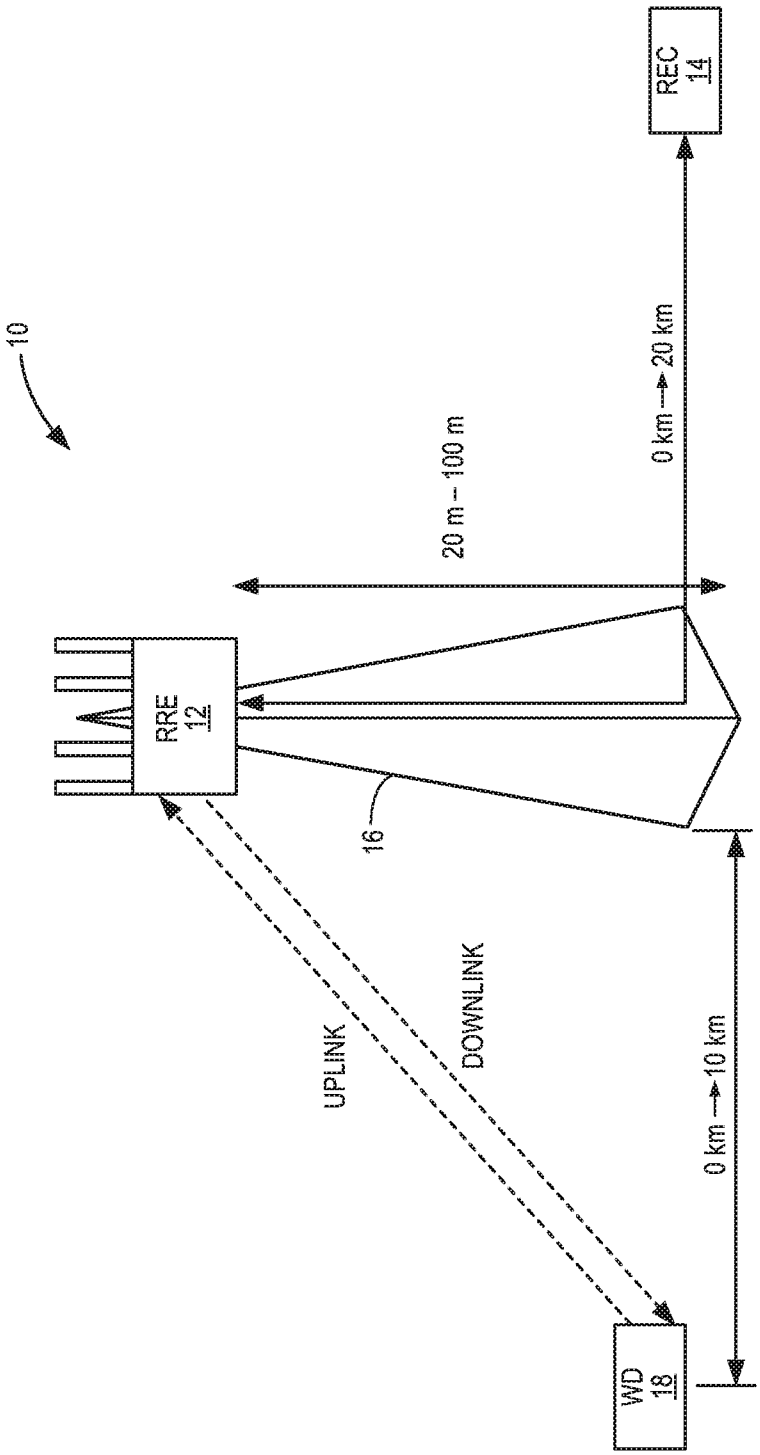

FIG. 1
(PRIOR ART)

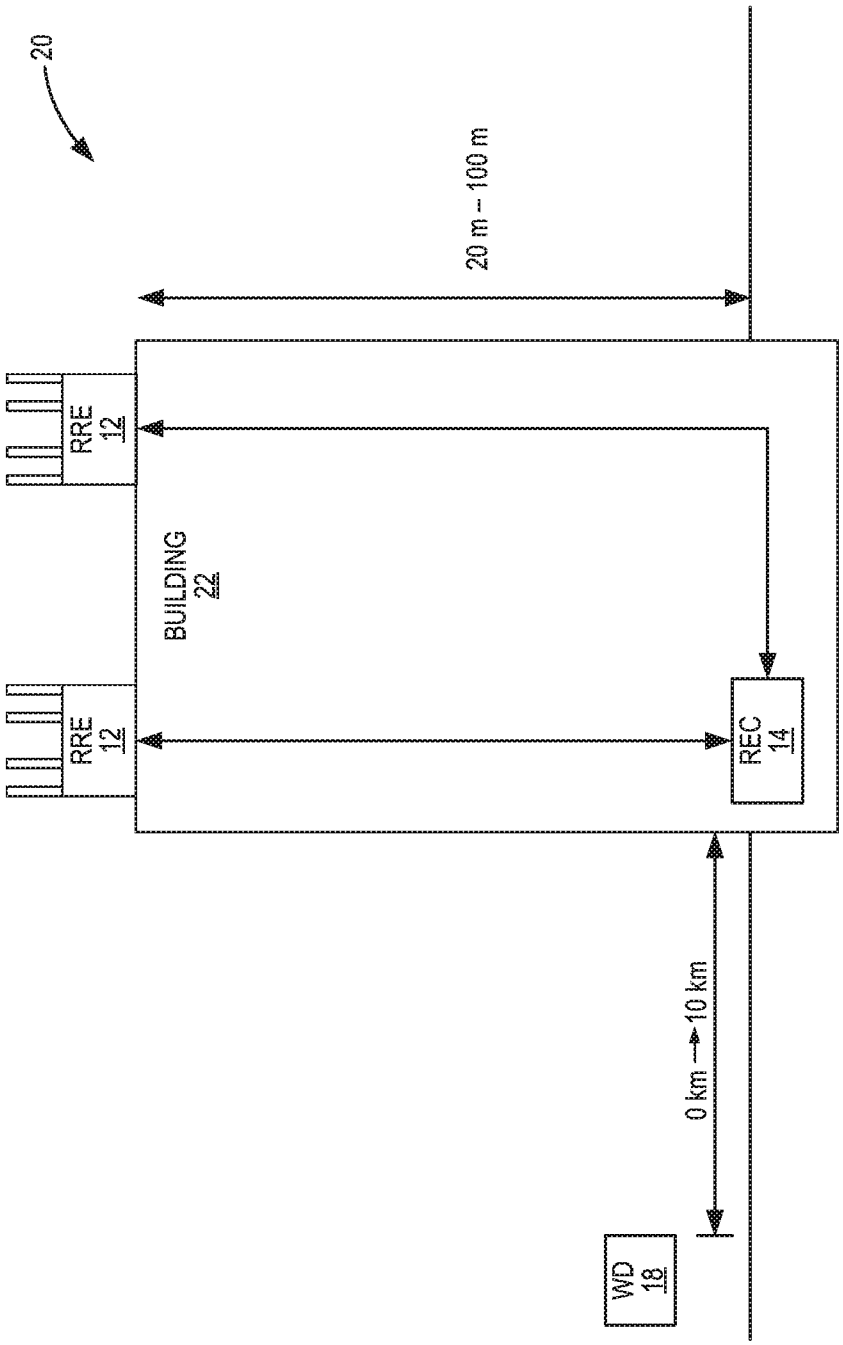

FIG. 2
(PRIOR ART)

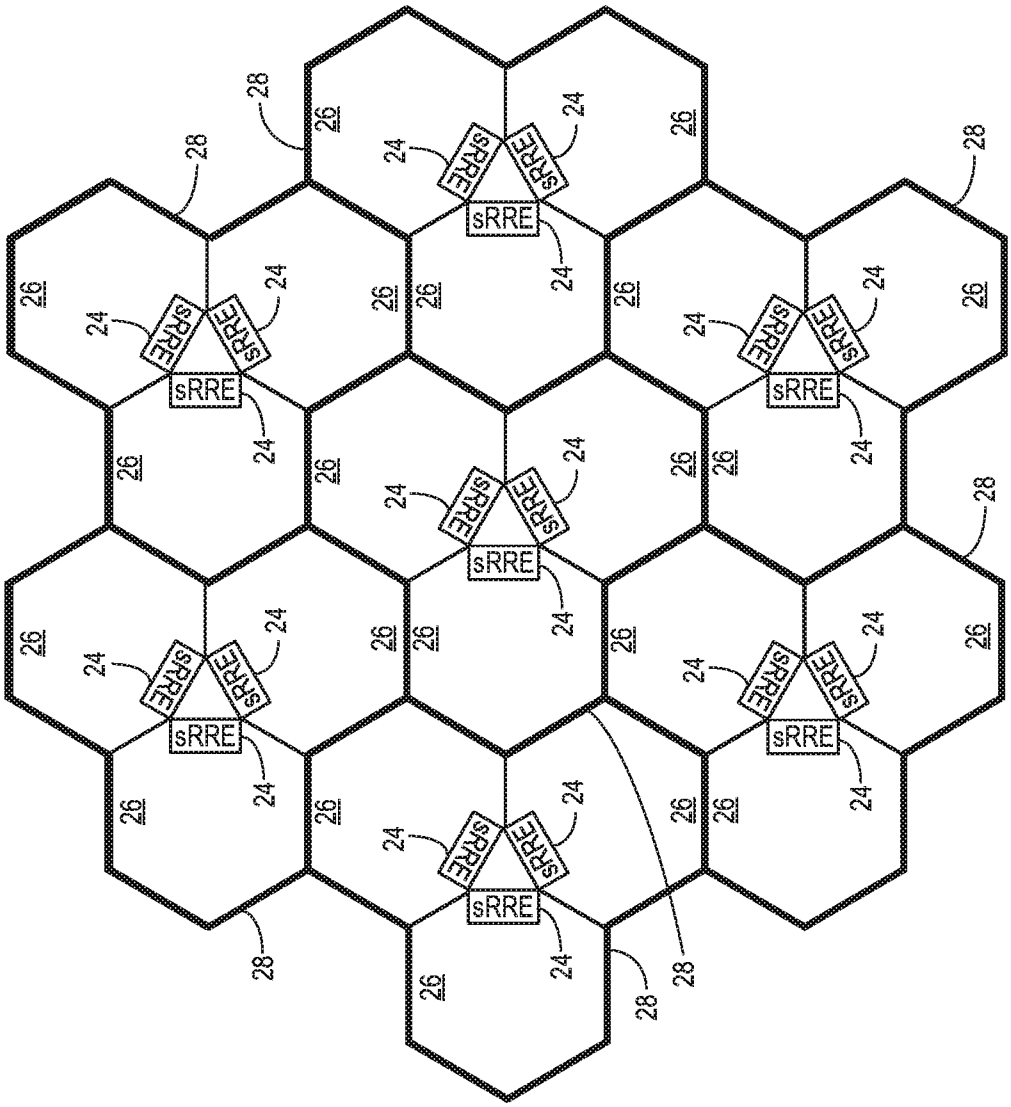

FIG. 3
(PRIOR ART)

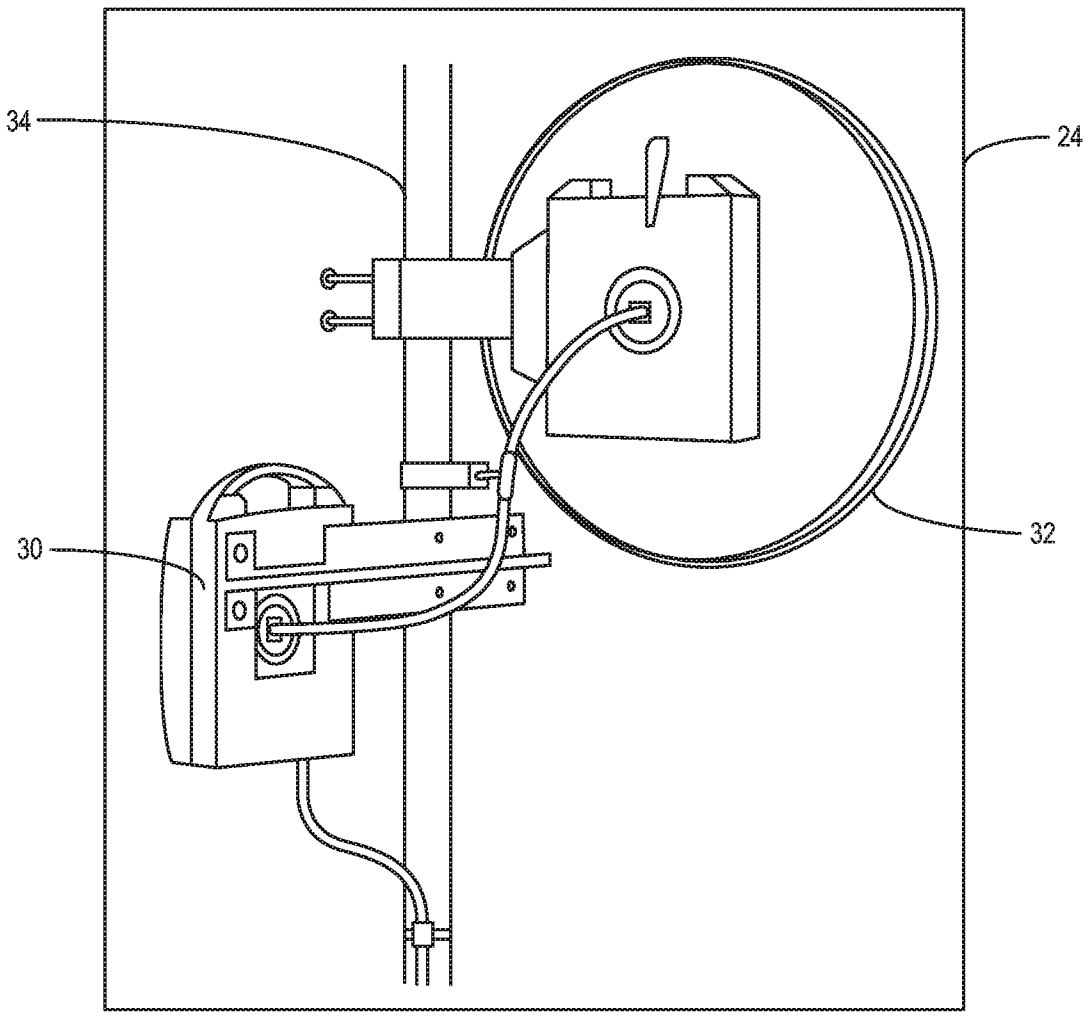

FIG. 4
(PRIOR ART)

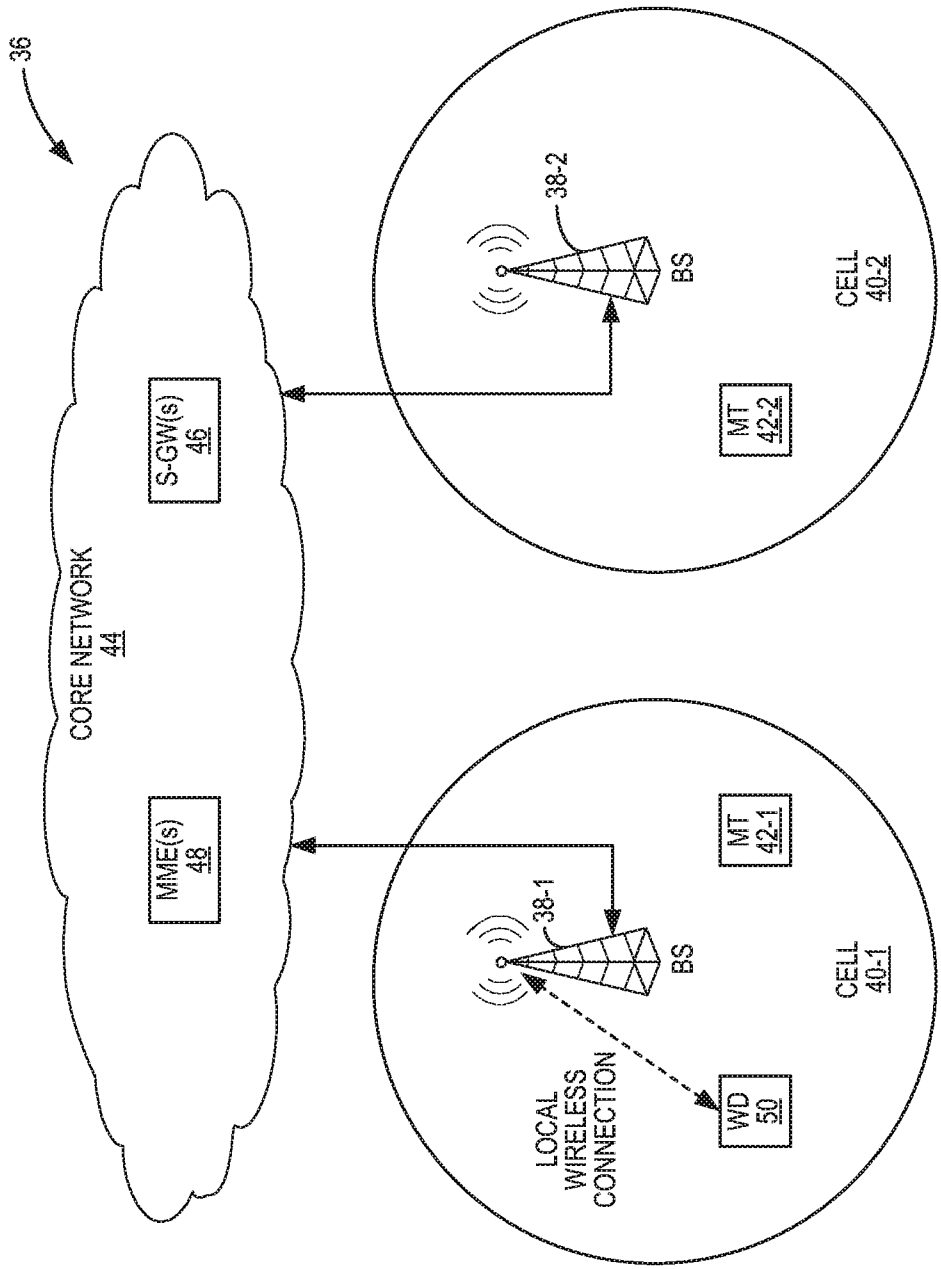
36
CORE NETWORK
44
MME(s)
48
S-GW(s)
46
38-2
BS
CELL
40-2
MT
42-2
38-1
BS
CELL
40-1
MT
42-1
LOCAL
WIRELESS
CONNECTION
WD
50

FIG. 5

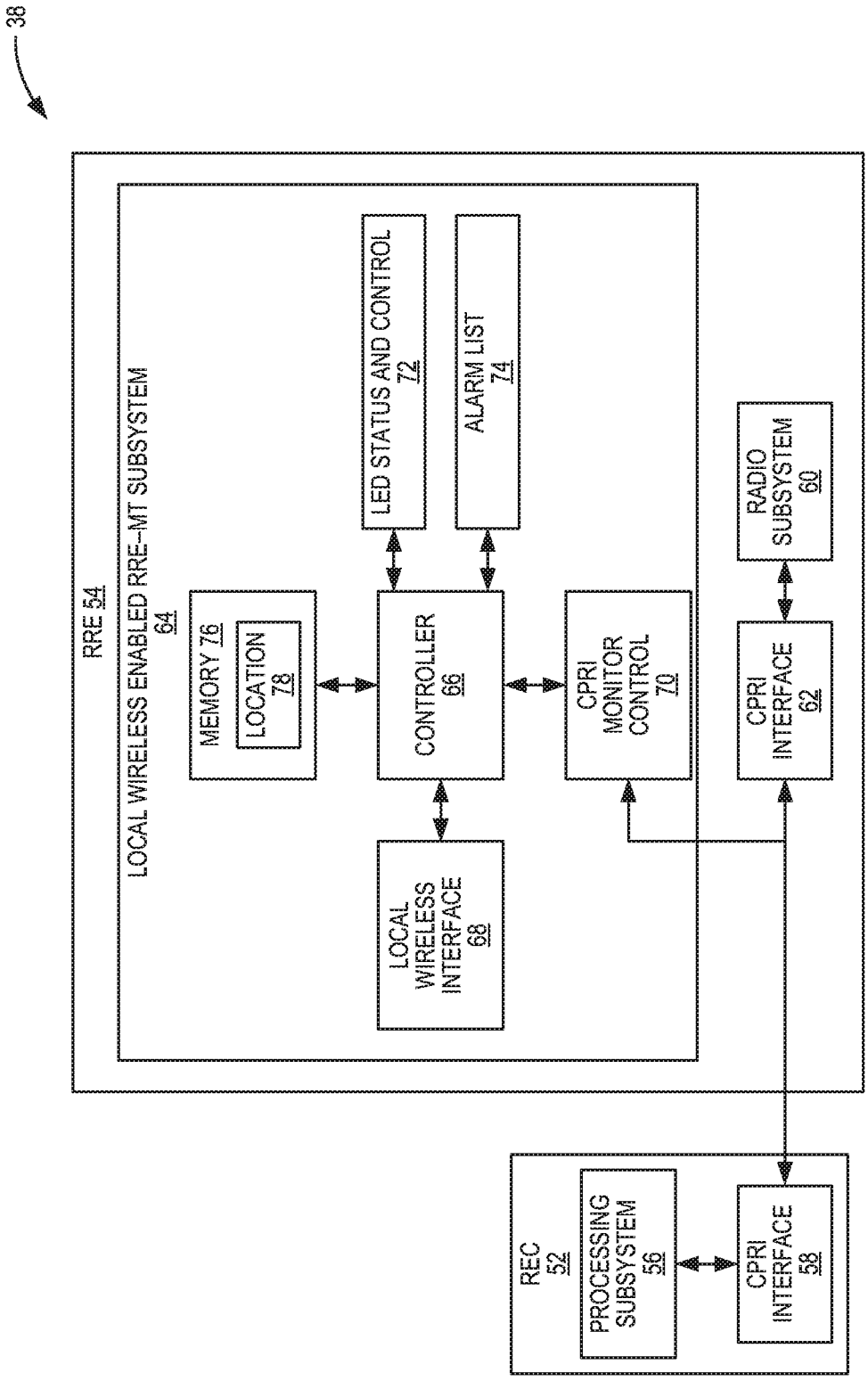
38
RRE 54
LOCAL WIRELESS ENABLED RRE–MT SUBSYSTEM 64
MEMORY 76
LOCATION 78
CONTROLLER 66
LED STATUS AND CONTROL 72
ALARM LIST 74
CPRI MONITOR CONTROL 70
LOCAL WIRELESS INTERFACE 68
RADIO SUBSYSTEM 60
CPRI INTERFACE 62
REC 52
PROCESSING SUBSYSTEM 56
CPRI INTERFACE 58

FIG. 6

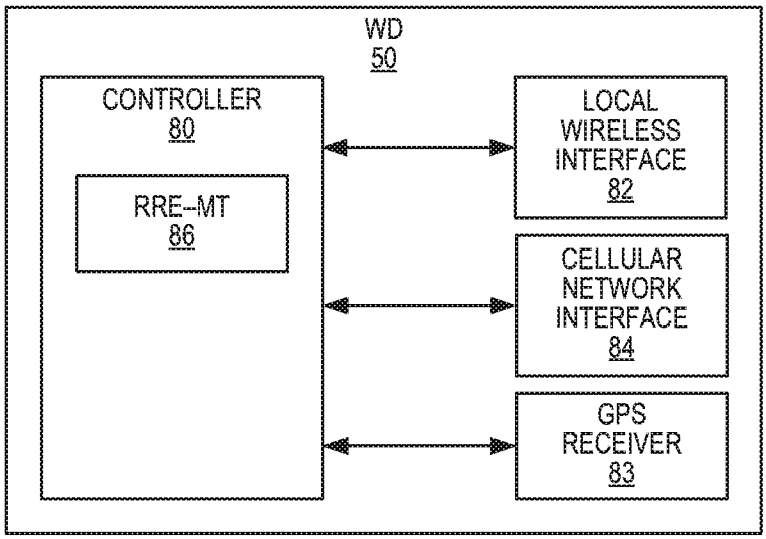
WD
50
CONTROLLER
80
RRE–MT
86
LOCAL
WIRELESS
INTERFACE
82
CELLULAR
NETWORK
INTERFACE
84
GPS
RECEIVER
83

FIG. 7

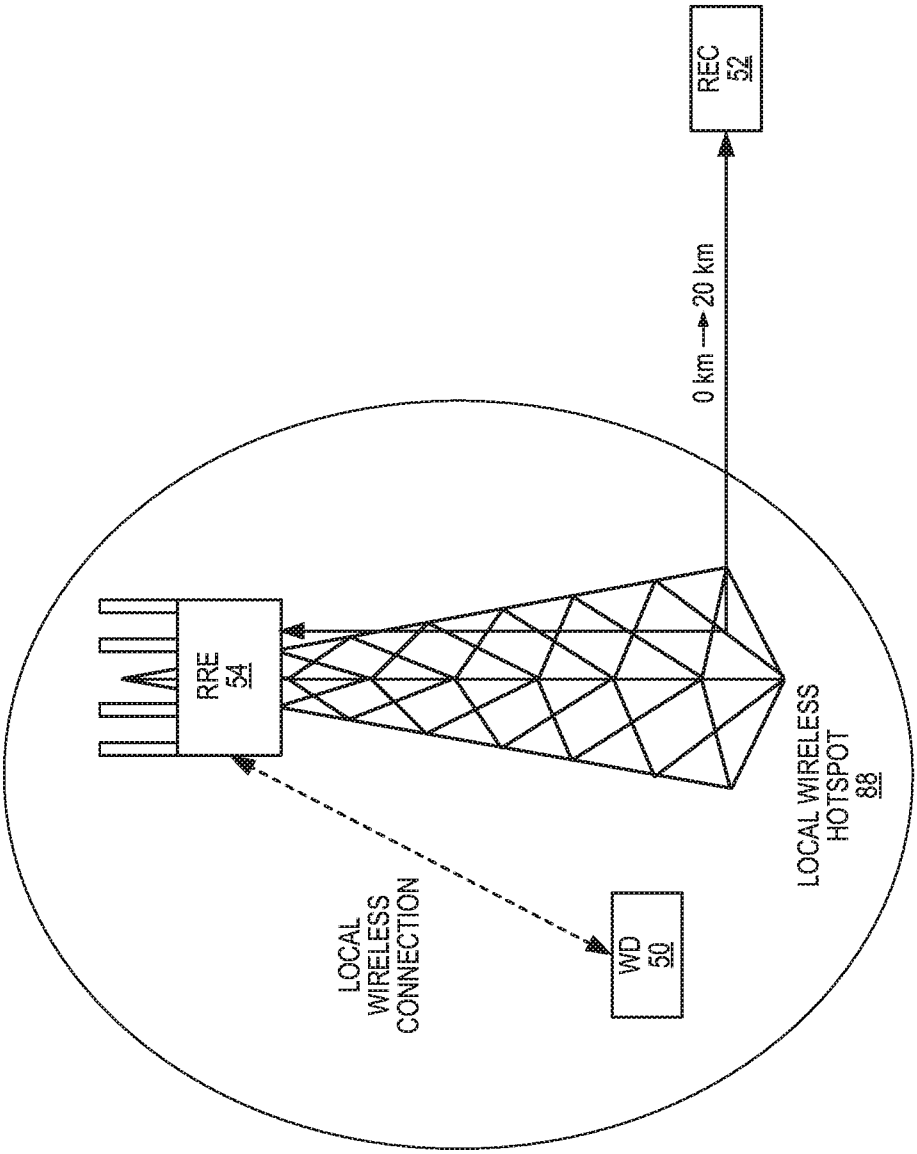
REC
52
0 km → 20 km
RRE
54
LOCAL WIRELESS
HOTSPOT
88
LOCAL
WIRELESS
CONNECTION
WD
50

FIG. 8

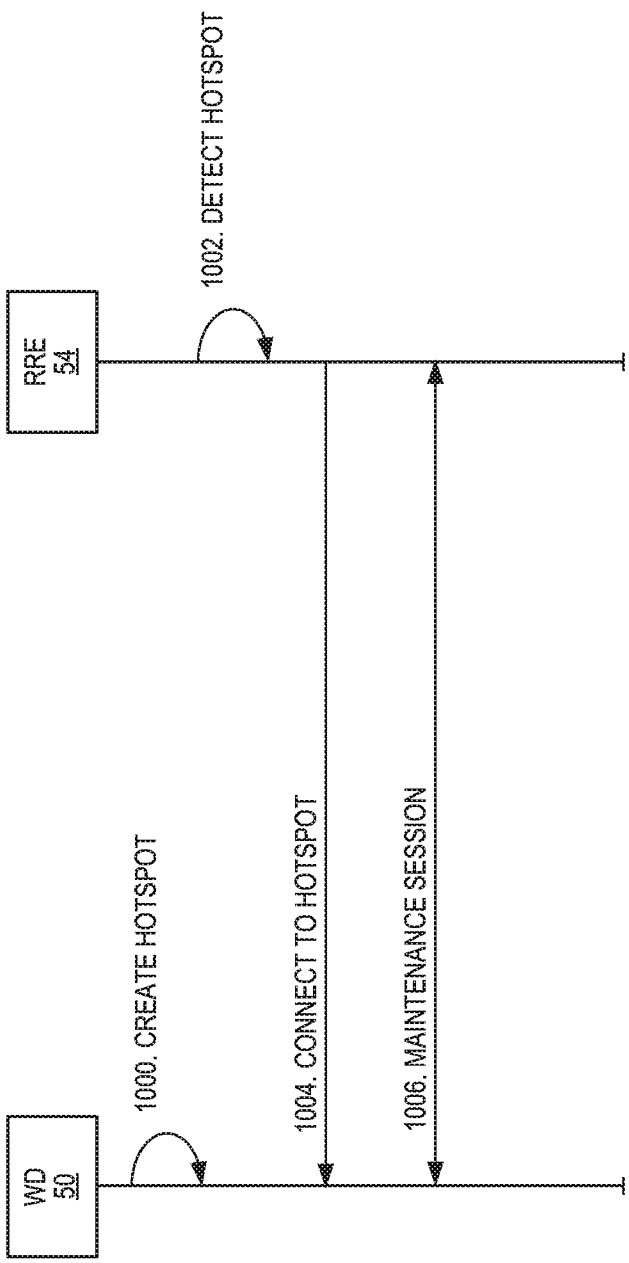
WD
50
RRE
54
1000. CREATE HOTSPOT
1002. DETECT HOTSPOT
1004. CONNECT TO HOTSPOT
1006. MAINTENANCE SESSION

FIG. 9

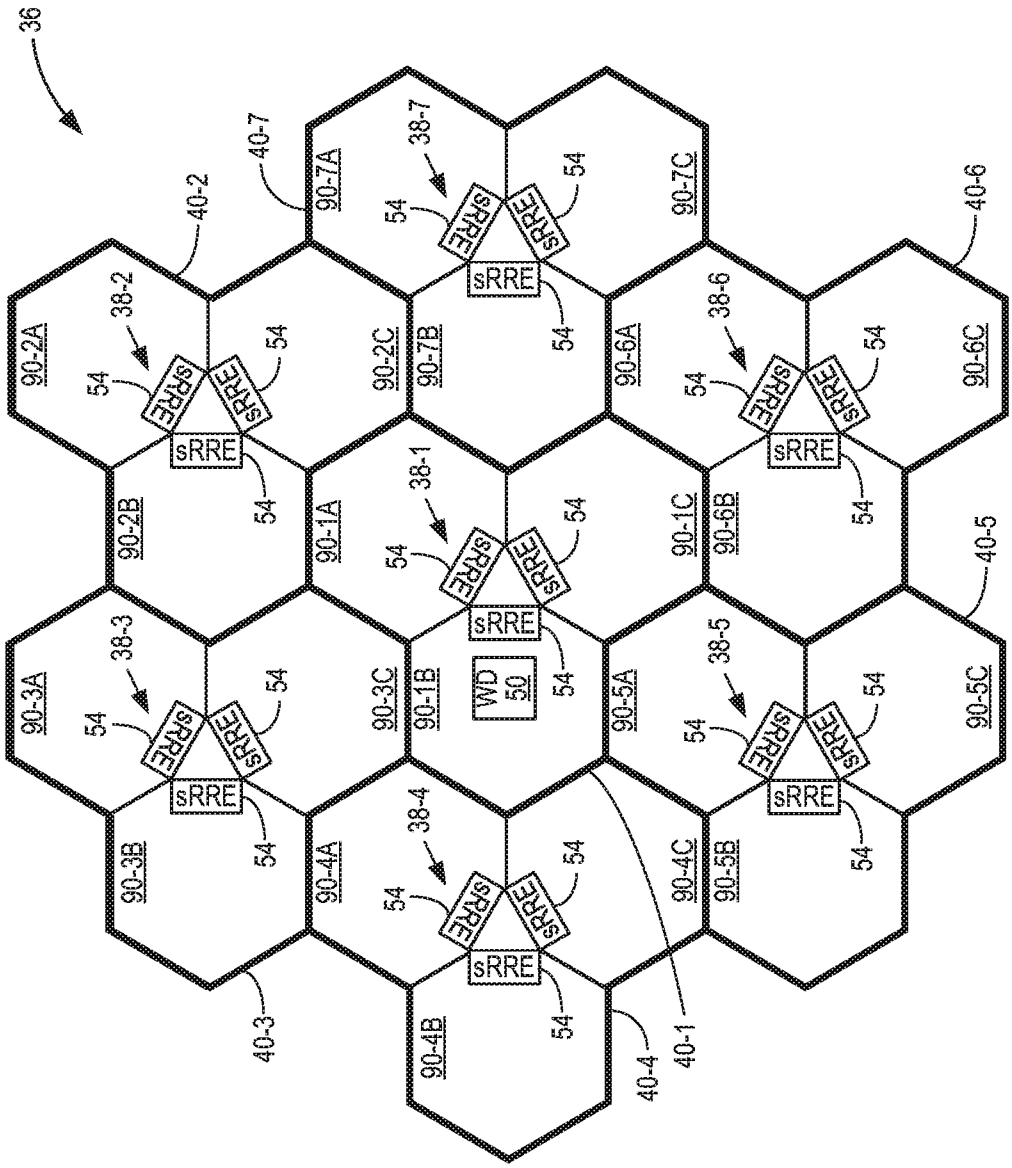
36
40-1
40-2
40-3
40-4
40-5
40-6
40-7
38-1
38-2
38-3
38-4
38-5
38-6
38-7
90-1A
90-1B
90-1C
90-2A
90-2B
90-2C
90-3A
90-3B
90-3C
90-4A
90-4B
90-4C
90-5A
90-5B
90-5C
90-6A
90-6B
90-6C
90-7A
90-7B
90-7C
WD 50
sRRE
54

FIG. 10

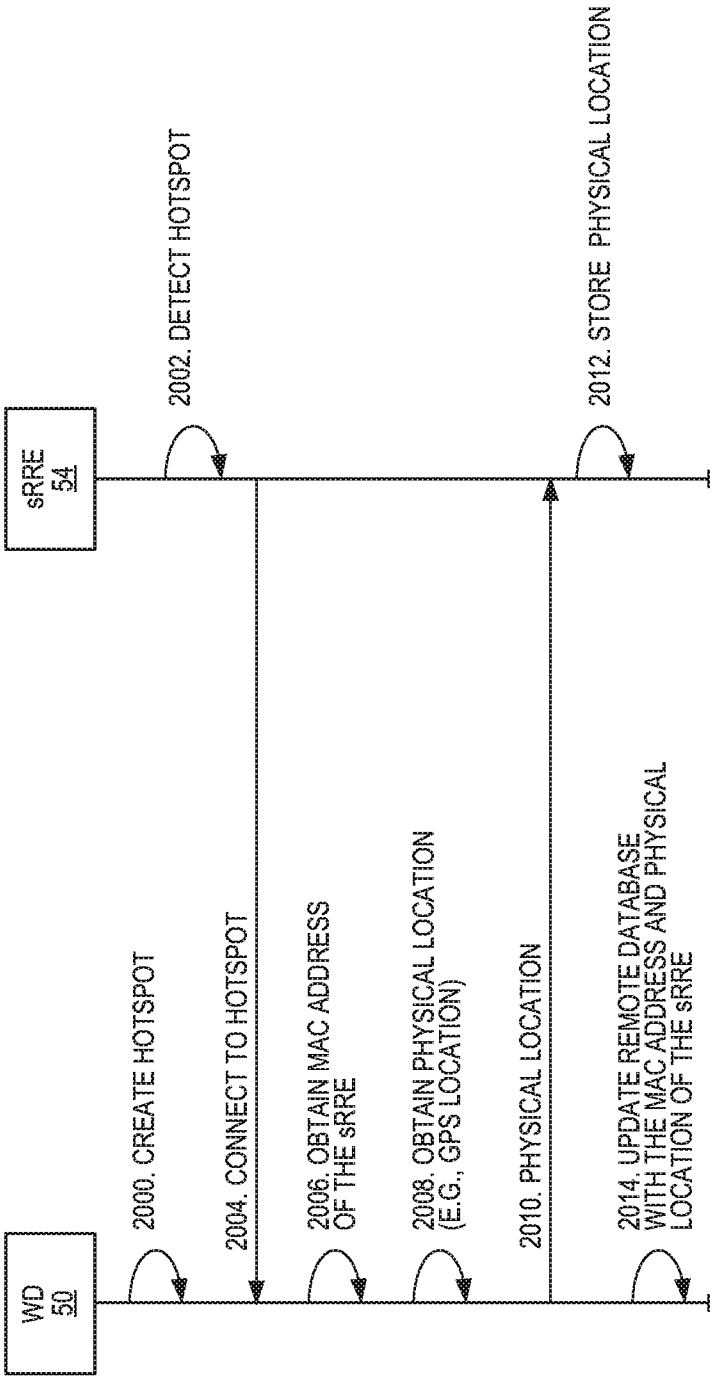
WD
50
sRRE
54
2000. CREATE HOTSPOT
2002. DETECT HOTSPOT
2004. CONNECT TO HOTSPOT
2006. OBTAIN MAC ADDRESS OF THE sRRE
2008. OBTAIN PHYSICAL LOCATION (E.G., GPS LOCATION)
2010. PHYSICAL LOCATION
2012. STORE PHYSICAL LOCATION
2014. UPDATE REMOTE DATABASE WITH THE MAC ADDRESS AND PHYSICAL LOCATION OF THE sRRE

FIG. 11

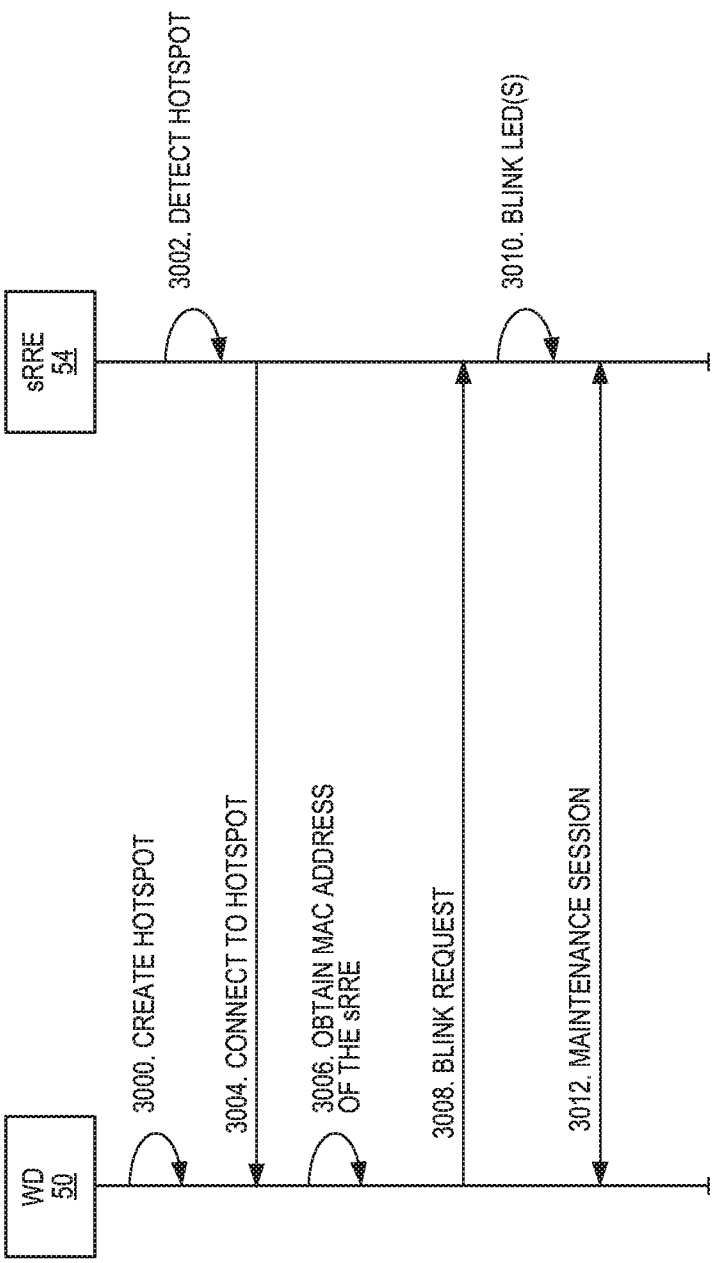
WD
50
sRRE
54
3000. CREATE HOTSPOT
3002. DETECT HOTSPOT
3004. CONNECT TO HOTSPOT
3006. OBTAIN MAC ADDRESS OF THE sRRE
3008. BLINK REQUEST
3010. BLINK LED(S)
3012. MAINTENANCE SESSION

FIG. 12

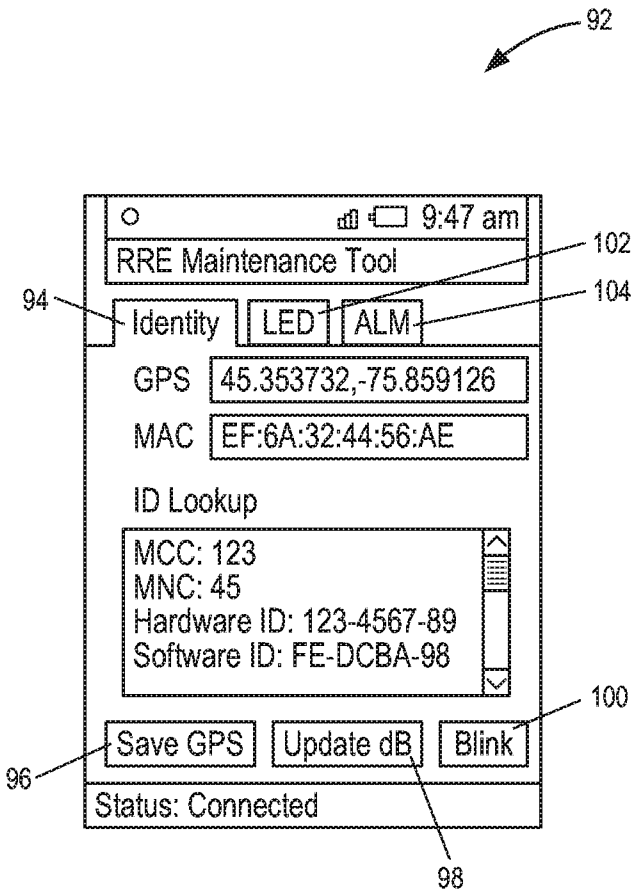
92
9:47 am
RRE Maintenance Tool
94
Identity
LED
ALM
102
104
GPS
45.353732,-75.859126
MAC
EF:6A:32:44:56:AE
ID Lookup
MCC: 123
MNC: 45
Hardware ID: 123-4567-89
Software ID: FE-DCBA-98
100
Save GPS
Update dB
Blink
96
Status: Connected
98

FIG. 13

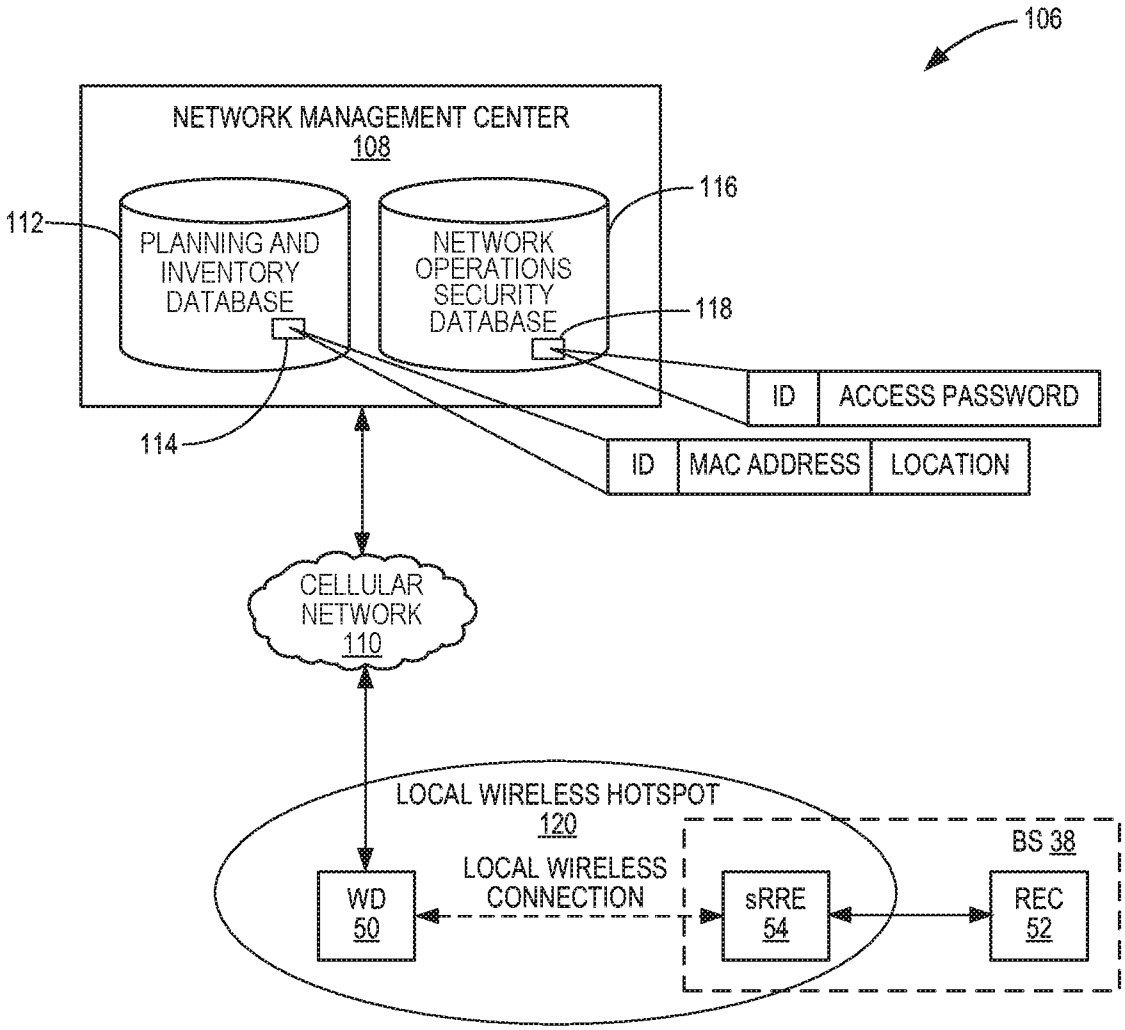
106
NETWORK MANAGEMENT CENTER
108
112
PLANNING AND INVENTORY DATABASE
116
NETWORK OPERATIONS SECURITY DATABASE
118
114
ID
ACCESS PASSWORD
ID
MAC ADDRESS
LOCATION
CELLULAR NETWORK
110
LOCAL WIRELESS HOTSPOT
120
BS 38
WD
50
LOCAL WIRELESS CONNECTION
sRRE
54
REC
52

FIG. 14

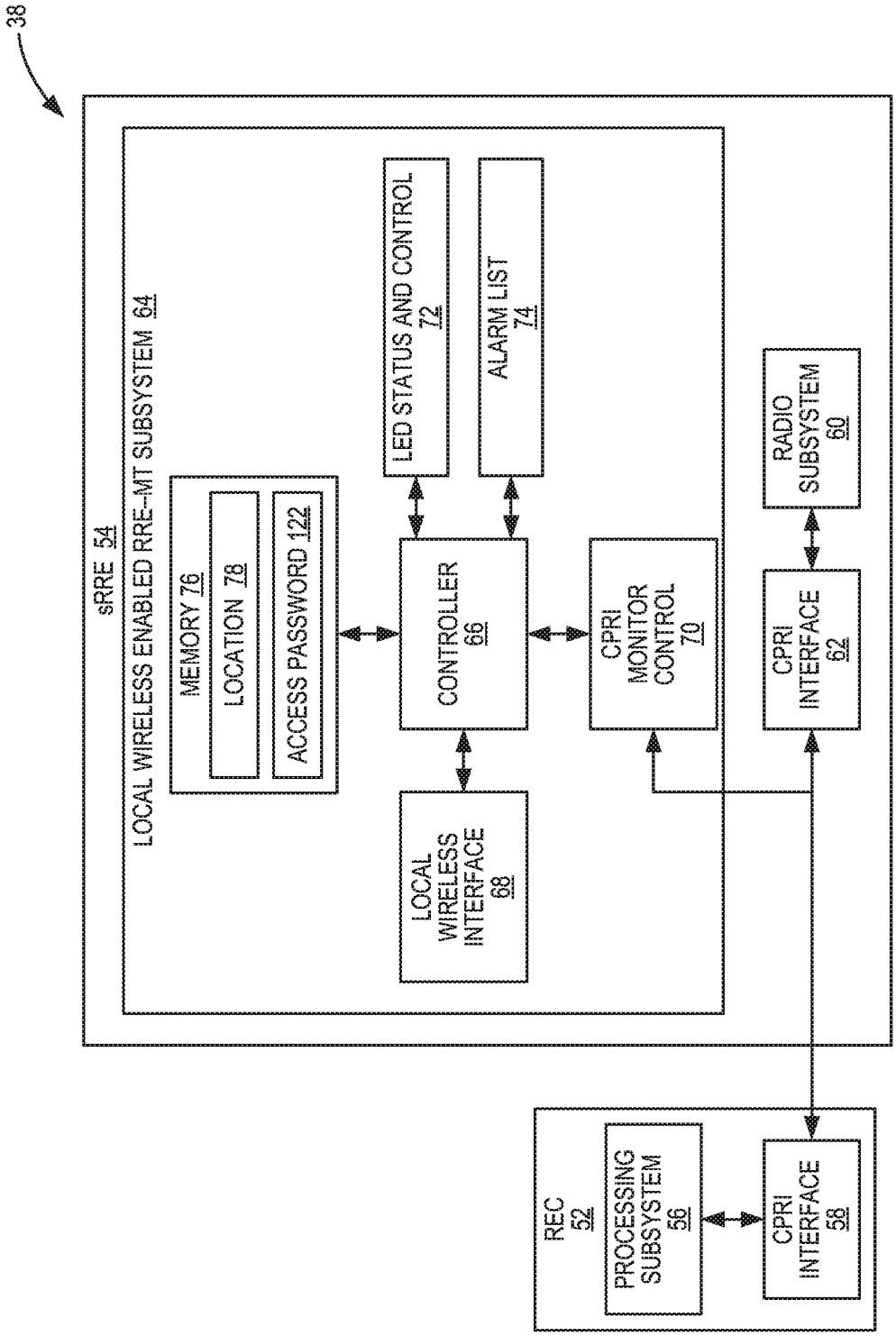
38
sRRE 54
LOCAL WIRELESS ENABLED RRE–MT SUBSYSTEM 64
MEMORY 76
LOCATION 78
ACCESS PASSWORD 122
LED STATUS AND CONTROL 72
ALARM LIST 74
CONTROLLER 66
CPRI MONITOR CONTROL 70
LOCAL WIRELESS INTERFACE 68
RADIO SUBSYSTEM 60
CPRI INTERFACE 62
REC 52
PROCESSING SUBSYSTEM 56
CPRI INTERFACE 58

FIG. 15

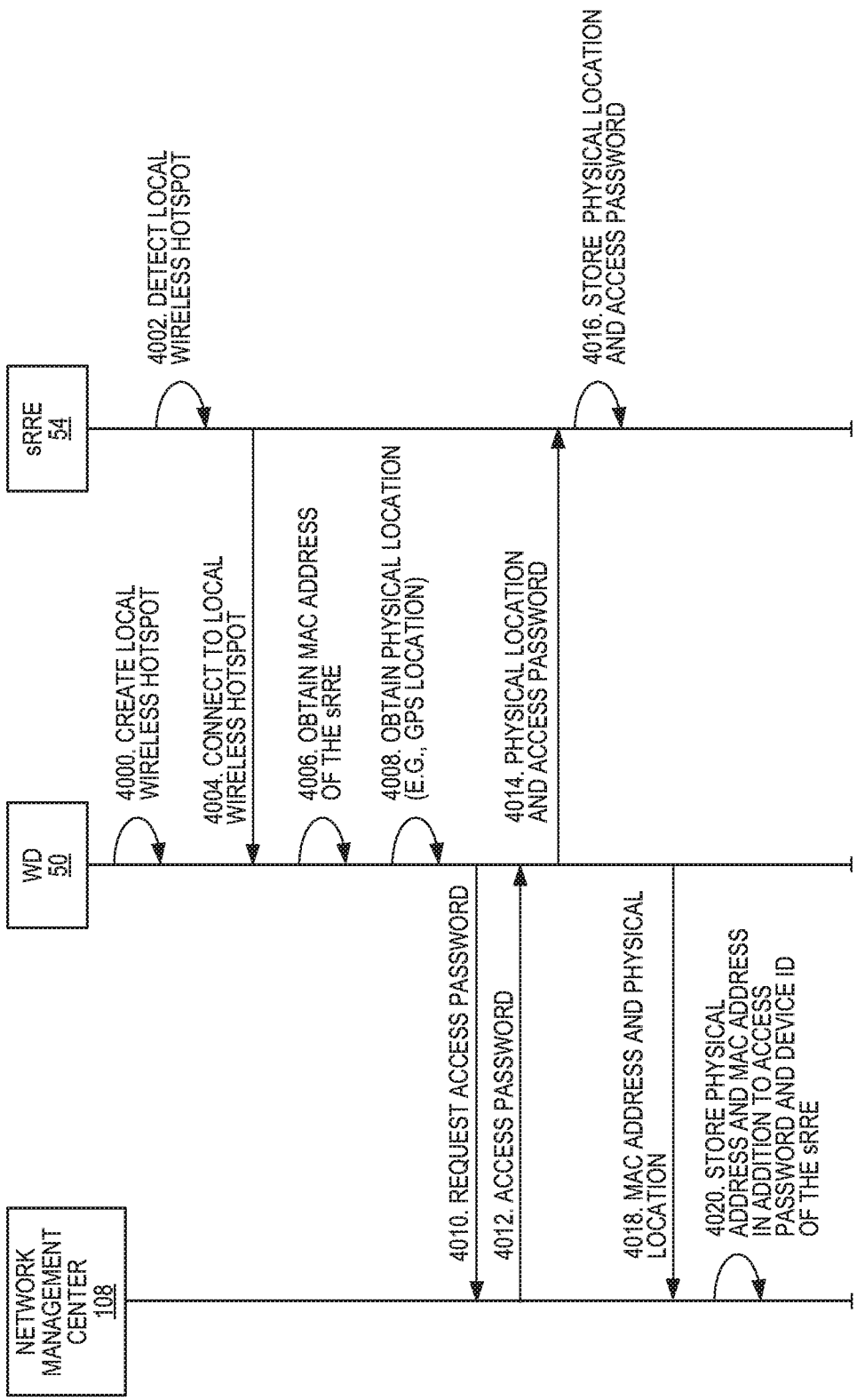
NETWORK MANAGEMENT CENTER 108
WD 50
sRRE 54
4000. CREATE LOCAL WIRELESS HOTSPOT
4002. DETECT LOCAL WIRELESS HOTSPOT
4004. CONNECT TO LOCAL WIRELESS HOTSPOT
4006. OBTAIN MAC ADDRESS OF THE sRRE
4008. OBTAIN PHYSICAL LOCATION (E.G., GPS LOCATION)
4010. REQUEST ACCESS PASSWORD
4012. ACCESS PASSWORD
4014. PHYSICAL LOCATION AND ACCESS PASSWORD
4016. STORE PHYSICAL LOCATION AND ACCESS PASSWORD
4018. MAC ADDRESS AND PHYSICAL LOCATION
4020. STORE PHYSICAL ADDRESS AND MAC ADDRESS IN ADDITION TO ACCESS PASSWORD AND DEVICE ID OF THE sRRE

FIG. 16

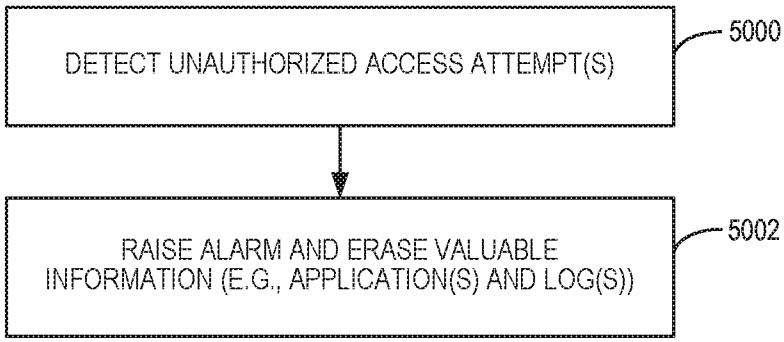
DETECT UNAUTHORIZED ACCESS ATTEMPT(S)
5000
RAISE ALARM AND ERASE VALUABLE INFORMATION (E.G., APPLICATION(S) AND LOG(S))
5002

FIG. 17

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2014/059603

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06 H04W12/12
ADD. H04W88/08 H04W92/10 H04W84/04 H04W64/00 H04L29/06

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W H04L G06F

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, COMPENDEX, 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.
Y	WO 99/01993 A2 (SIEMENS AG [DE]; HIRSCH LUCIAN [DE]) 14 January 1999 (1999-01-14) page 14, line 23 - page 25, line 22; figures 1,2	1-32
Y	EP 0 967 817 A2 (SIEMENS AG [DE]) 29 December 1999 (1999-12-29) paragraph [0008] - paragraph [0011] paragraph [0014]; figure 1	1-32
Y	EP 2 073 582 A1 (MITSUBISHI ELEC R&D CT EUROPE [NL]; MITSUBISHI ELECTRIC CORP [JP]) 24 June 2009 (2009-06-24) paragraph [0007] - paragraph [0010] paragraph [0079] - paragraph [0087]; figure 1	1-32

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 July 2014	10/07/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Grimaldo, Michele

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2014/059603

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2012/171184 A1 (HUAWEI TECH CO LTD [CN]; LI JIAN [CN]; CAI CHENGGUI [CN]; FU YONGCHENG) 20 December 2012 (2012-12-20) page 1, line 25 - page 2, line 16	1-32
A	US 2010/085949 A1 (VON BRANDT ACHIM [DE] ET AL) 8 April 2010 (2010-04-08) paragraph [0008] - paragraph [0079] paragraph [0086] - paragraph [0092]; figure 1	1-32
A	US 2012/309416 A1 (WHELAN DAVID A [US] ET AL) 6 December 2012 (2012-12-06) paragraph [0003] - paragraph [0018]	1-32
T	Anonymous: "Base transceiver station - Wikipedia, the free encyclopedia", , 21 April 2014 (2014-04-21), pages 1-5, XP055126329, Retrieved from the Internet: URL:http://en.wikipedia.org/wiki/Base_transceiver_station [retrieved on 2014-07-02] "General Architecture"	1-32

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2014/059603

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9901993 A2	14-01-1999	CN 1262020 A	02-08-2000
		EP 0993750 A2	19-04-2000
		JP 3305336 B2	22-07-2002
		JP 2000511385 A	29-08-2000
		US 6389282 B1	14-05-2002
		WO 9901993 A2	14-01-1999
EP 0967817 A2	29-12-1999	NONE	
EP 2073582 A1	24-06-2009	CN 102017684 A	13-04-2011
		EP 2073582 A1	24-06-2009
		EP 2245877 A1	03-11-2010
		JP 2011512051 A	14-04-2011
		US 2010260145 A1	14-10-2010
		WO 2009080665 A1	02-07-2009
WO 2012171184 A1	20-12-2012	CN 102204307 A	28-09-2011
		WO 2012171184 A1	20-12-2012
US 2010085949 A1	08-04-2010	NONE	
US 2012309416 A1	06-12-2012	NONE	