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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 February 2020 (27.02.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/039043 A1

(51) International Patent Classification:
G08B 13/196 (2006.01) *H04B 1/04* (2006.01)
H04N 7/18 (2006.01) *H04L 29/08* (2006.01)
H04B 1/74 (2006.01)

(21) International Application Number:
PCT/EP2019/072517

(22) International Filing Date:
22 August 2019 (22.08.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1857651 24 August 2018 (24.08.2018) FR

(71) Applicant: **VERISURE SÀRL** [CH/CH]; Chemin Jean-Baptiste Vandelle 3A, 1290 Versoix, Geneva (CH).

(72) Inventor: **HEDERSTIERNA, Christer Fredrik**; c/o Verisure Sàrl, Chemin Jean-Baptiste Vandelle 3A, 1290 Versoix, Geneva (CH).

(74) Agent: **PRINZ & PARTNER MBB PATENT- UND RECHTSANWÄLTE**; Rundfunkplatz 2, 80335 München (DE).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,

(54) **Title:** A SECURITY MONITORING SYSTEM AND A NODE AND CENTRAL UNIT THEREFOR

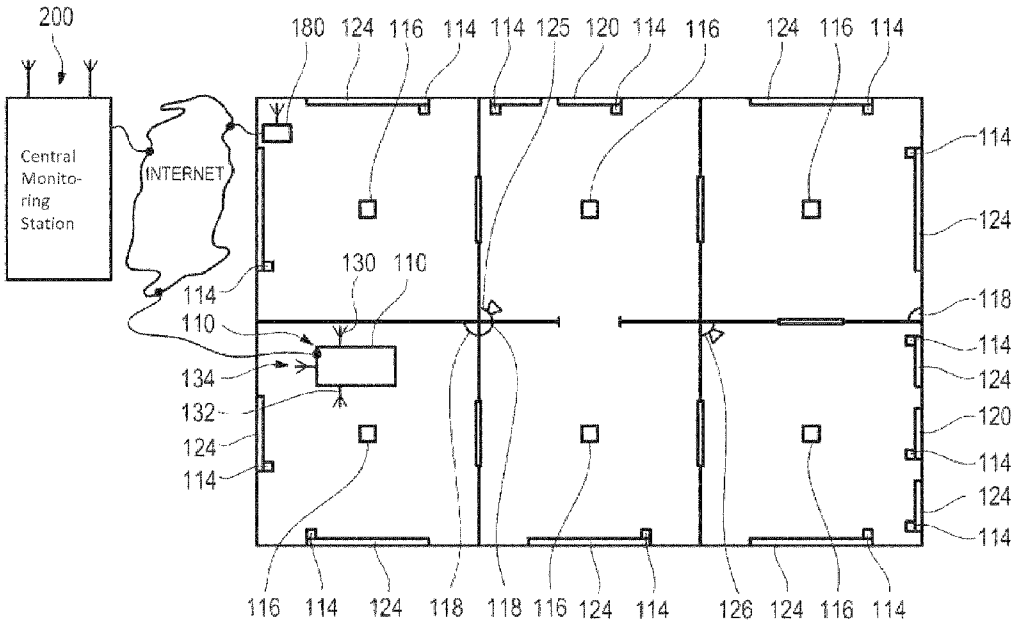

Fig. 1

(57) **Abstract:** A security monitoring system comprising: a central unit that comprises at least one radio frequency transceiver configurable with either of a first configuration and a second configuration, and a controller for controlling the radio frequency transceiver(s); a node comprising a node radio frequency transceiver operable at the first configuration, for communication with the central unit, and at the second configuration for communication with the central unit, and a controller for controlling the node radio frequency transceiver; the central unit being configured to transmit using the first configuration an offer to the node of a communication channel of the second configuration for the node to transmit data for reception by the central unit; the node being configured,on receiving the offer from the central unit, to transmit, configured in the first configuration, an acceptance message to the central unit, and thereafter to transmit data, configured in the second configuration, to the central unit; the central unit being configured, on reception of the acceptance message

[Continued on next page]

WO 2020/039043 A1

SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

from the node, to configure one of the at least one radio frequency transceiver with the second configuration to enable reception of the data transmitted by the node. The at least one radio frequency transceiver may comprise a first radio transceiver and a second radio transceiver wherein at least the second transceiver is configurable with either of the first configuration and the second configuration. The offer may be transmitted using the first transceiver, and the second transceiver may, on reception of the acceptance message from the node, be configured with the second configuration.

A security monitoring system and a node and central unit therefor

TECHNICAL FIELD

The present invention relates to a security monitoring system for monitoring premises, a node and a central unit for such a system, and a method of controlling data transmission.

BACKGROUND

Security monitoring systems for monitoring premises typically provide a means for detecting the presence and/or actions of people at the premises, and reacting to detected events. Commonly such systems include sensors to detect the opening and closing of doors and windows, movement detectors to monitor spaces for signs of movement, microphones to detect sounds such as breaking glass, and image sensors to capture still or moving images of monitored zones. Such systems may be self-contained, with alarm indicators such as sirens and flashing lights that may be activated in the event of an alarm condition being detected. Such installations typically include a central unit that is coupled to the sensors, detectors, cameras, etc. ("nodes"), and which processes receive notifications and determines a response. The central unit may be linked to the various nodes wirelessly, rather than by wires, since this facilitates installation and may also provide some safeguards against sensors/detectors effectively being disabled by disconnecting them from the central unit. Similarly, for ease of installation and to improve security, the nodes of such systems are preferably battery powered rather than mains powered.

Alternatively, a security monitoring system may include an installation at a premises, domestic or commercial, that is linked to a Central Monitoring Station (CMS) where typically human operators manage the responses required by different alarm and notification types. In such centrally monitored systems, the central unit at the premises installation typically processes notifications received from the nodes in the installation, and notifies the Central Monitoring Station of only some of these, depending upon the settings of the system and the nature of the detected events. In such a configuration, the central unit at the installation is effectively acting as a gateway between the nodes and the Central Monitoring Station.
In both centrally-managed and self-contained security monitoring systems one of the most important issues, from a practical perspective, is the battery life of the nodes of the installation – that is, the battery life of the various detectors, sensors, and cameras. Obviously, if a node's battery loses sufficient power, the node may be unable to sense a change of state or to contact the central unit, and consequently the security installation develops a weak spot where an intruder may gain access to the premises undetected. For centrally-managed systems it is usually the responsibility of the company running the system, rather than the premises owner or occupier, to change batteries, and obviously the

shorter the battery life in nodes, the more frequently site visits need to be made and the greater the administrative cost. Typically, nodes are designed in such a way as to achieve a target battery lifetime of 5 years. Consequently, controlling power consumption in the nodes is a high priority.
Further to this, it is very important to ensure a swift and timely delivery of notifications and alarms from the node to the CMS.

It is known to provide video cameras for security monitoring systems with Wi-Fi radios to enable them to transmit video data to a central unit of the monitoring system over Wi-Fi. The Wi-Fi radio, and the video camera, are turned on in the event that a PIR associated with the video camera detects movement. Unfortunately, Wi-Fi radios tend to drain batteries quite quickly, and such an arrangement typically requires large capacity batteries, and/or an external power source, if frequent battery replacement or power loss are to be avoided. Another disadvantage of using Wi-Fi in a security system is that one needs to monitor or supervise the nodes of the system. This is done by periodic messaging, and Wi-Fi consumes significant power in performing this simple task. Therefore, it is highly desirable to avoid the use of Wi-Fi (IEEE 802.11…) for communication between the nodes and central unit of a security monitoring system – at least where the nodes rely on a battery power supply. Conversely, because the Central Unit of a security monitoring system is typically mains rather than battery powered (albeit that a back-up battery power supply is typically provided) it can be acceptable to provide a Wi-Fi transceiver in the Central Unit for use in communicating with the CMS – for example, using a domestic or commercial Wi-Fi access point as a route to the Internet.

Although not directly concerned with security monitoring systems, WO01/11833 A1 discloses a multichannel wireless network designed to facilitate high-bit-rate data communication within a home, office, or similarly constrained area. A primary wireless channel (N0) is designed for relatively low bit rate (LD), high reliability and network-wide communication. A secondary wireless channel (N3) is designed for relatively high bit rate (HD) communication, but with potentially lower reliability and shorter ranges. A base station uses the primary wireless channel to configure and control operation of the wireless network, including configuring pairs of devices as requested for direct communication between the devices of the pair over the secondary wireless channel. The devices are provided with a separate physical layer for each of the two channels. As an alternative, it is proposed that an 802.11-compatible physical channel be used to carry the N0 and N3 channels using TDM. The 802.11 network operates in Point Coordination Function Mode (PCF), although the

document itself acknowledges that “PCF mode is typically inefficient and poorly-suited to the transmission of time-critical information”.

It would be beneficial if an alternative approach could be provided to enable, for example, video data to be transmitted between a node and a central unit of a security monitoring system, to enable timely action to be taken based on the information contained in the video data, in such a way as to avoid excessive power consumption at the node, thereby prolonging battery life at the node.

SUMMARY OF THE INVENTION

According to a first aspect, the present invention provides a security monitoring system comprising: a central unit that comprises at least one radio frequency transceiver that is configurable to provide a communication channel with either of a first configuration or a second configuration, and a controller for controlling the radio frequency transceiver(s);
a node comprising a node radio frequency transceiver operable in a first mode, for communication with the central unit using a communication channel according to the first configuration, and in a second mode for communication with the central unit using a communication channel according to the second configuration, and a controller for controlling the node radio frequency transceiver;
the central unit being configured to transmit using a communication channel according to the first configuration an offer to the node of a communication channel according to the second configuration for the node to transmit data for reception by the central unit;
the node being configured, on receiving the offer from the central unit, to transmit, using a communication channel according to the first configuration, an acceptance message to the central unit, and thereafter to transmit data, using a communication channel according to the second configuration, to the central unit;
the central unit being configured, on reception of the acceptance message from the node, to configure one of the at least one radio frequency transceivers to enable reception of the data transmitted by the node using a communication channel according to the second configuration;
wherein the at least one radio frequency transceiver comprises a first radio transceiver and a second radio transceiver, wherein at least the second transceiver is configurable to provide a communication channel with either of the first configuration or the second configuration,

and the central unit is configured to transmit the offer using the first transceiver, and to configure the second transceiver, on reception of the acceptance message from the node,

to enable reception of the data transmitted by the node using a communication channel according to the second configuration.

Such a system is advantageous in that low intensity data requirements, e.g. supervision, and high intensity data requirements, e.g. video, can be met by without the need to provide nodes with two separate radio solutions, thereby avoiding potentially significant cost and complexity.

Preferably, the or each node has an autonomous power supply such as a battery power supply. Also preferably, the transceiver of the or each node is a non-Wi-Fi transceiver, thereby reducing undesirable power drain and enabling node battery life to be extended compared to that obtainable when using Wi-Fi to communicate between the or each node and the Central Unit. By extending node battery life in this way, operator costs are reduced, customer satisfaction may be increased, and the security provided by the system is improved because node failure from battery exhaustion should happen less frequently.

Also preferably, communication between the Central Unit and the nodes, and vice versa, is direct rather than multi-hop from the source of a message (Central Unit or node) to its destination (node or Central Unit). Such an arrangement can offer significant node power savings compared to the use of a multi-hop system in which messages to or from some nodes from or to the Central Unit “hop” via one or more intermediate nodes en route to their destination. This avoids the battery drain caused by using other nodes as repeaters and which arises not just from the process of forwarding data but also from the signalling overhead that is necessary to enable a collection of nodes to offer multi hop communication paths.

The first configuration may comprise a first frequency and the second configuration comprise a second frequency.

According to an alternative aspect, the present invention provides a security monitoring system comprising: a central unit, comprising:
a first radio frequency transceiver operable at a first frequency, and a second radio frequency transceiver operable at the first frequency and at a second frequency, and a controller for controlling the radio frequency transceivers;
a node including a node radio frequency transceiver operable at the first frequency, for communication with the central unit, and at the second frequency for communication with the central unit, and a controller for controlling the node radio frequency transceiver;

the central unit being configured to transmit at the first frequency, using the first radio frequency transceiver, an offer to the node of a communication channel at the second frequency for the node to transmit data for reception by the second radio frequency transceiver;
the node being configured, on receiving the offer from the central unit, to transmit an acceptance message to the central unit at the first frequency, and thereafter to transmit data to the central unit at the second frequency;
the central unit being configured, on reception of the acceptance message from the node, to set the second radio frequency transceiver for reception at the second frequency to enable reception of the data transmitted by the node.
Preferably, the or each node has an autonomous power supply such as a battery power supply. Also preferably, the transceiver of the or each node is a non-Wi-Fi transceiver, thereby reducing undesirable power drain and enabling node battery life to be extended compared to that obtainable when using Wi-Fi to communicate between the or each node and the Central Unit.

Also preferably, communication between the Central Unit and the nodes, and vice versa, is direct rather than multi-hop from the source of a message (Central Unit or node) to its destination (node or Central Unit). Such an arrangement can offer significant node power savings compared to the use of a multi-hop system in which messages to or from some nodes from or to the Central Unit “hop” via one or more intermediate nodes en route to their destination.

Such systems are advantageous in that low intensity and high intensity data requirements, such as supervision and video, can be met by without the need to provide nodes with two separate radio solutions, thereby avoiding potentially significant cost and complexity.

The offer may include identifiers for a selection of alternative communication channels for the node to transmit data for reception by the second radio frequency transceiver. Under such circumstances, at least two of the alternative communication channels may use the same frequency but provide different bitrates.

The node may be configured to perform a determination of radio frequency conditions, and the node may configured to make a choice between the alternative communication channels based on the result of the determination of radio frequency conditions.

The central unit may be configured to transmit the offer to the node as a consequence of receiving notice of a security event. The central unit may receive such notice from the node to which it transmits the offer, or it may receive notice of a security event from one node but then transmit the offer to a different node.

For example, the security event may the output of a motion sensor, such as a PIR sensor, or of a microphone, or of a door or window opening sensor.

Optionally, the first and second frequencies are within the 863 to 870MHz frequency band. Optionally, the second frequency is between 868 and 870 MHz, for example between 869.4 and 869.65MHz.

The central unit may store information about frequencies and bitrates supported by the node, and may use the stored information in determining parameters of the offer to be made to the node.

The node may be configured to provide the information to the central unit when the node is first installed in the system.

The node may be configured periodically to provide the central unit with updated information about frequencies and bitrates supported by the node.

According to a further aspect of the invention, there is provided a method of controlling data transmission from a battery powered node to a central unit of a security monitoring system, the node including a non-Wi-Fi radio frequency transceiver for communication with the central unit, the non-Wi-Fi transceiver being operable, at a first frequency, and at a second frequency;
the method comprising:
receiving from the central unit at the first frequency, an offer of a communication channel at the second frequency for the node to transmit data for reception by the central unit;
transmitting an acceptance message to the central unit at the first frequency; and
subsequently
transmitting data to the central unit at the second frequency.

Preferably, communication between the Central Unit and the nodes, and vice versa, is direct rather than multi-hop from the source of a message (Central Unit or node) to its destination (node or Central Unit). Such an arrangement can offer significant node power savings

compared to the use of a multi-hop system in which messages to or from some nodes from or to the Central Unit “hop” via one or more intermediate nodes en route to their destination.

The method may include determining a response to an offer that includes identifiers for a selection of alternative communication channels for the node to transmit data for reception by the second radio frequency transceiver, the determination being based at least in part on the node’s ability to support an offered communication channel.

The method may also include performing by the node a determination of radio frequency conditions and using the result . In this case, the determination of the response to the offer may also be based on results of the determination of radio frequency conditions.

According to a further aspect of the present invention, there is provided a central unit for a security monitoring system that includes a node having a node non-Wi-Fi radio frequency transceiver for communication with the central unit, the non-Wi-Fi node radio frequency transceiver being operable at first and second frequencies, the central unit comprising: at least one radio frequency transceiver that is configurable to provide a communication channel with either of a first configuration or a second configuration, and a controller for controlling the radio frequency transceiver(s);
the central unit being configured to: transmit using a communication channel according to the first configuration an offer to the node of a communication channel of the second configuration for the node to transmit data for reception by the central unit; and, on reception of an acceptance message from the node, to configure one of the at least one radio frequency transceivers with the second configuration to enable reception of the data transmitted by the node using a communication channel according to the second configuration;
wherein the at least one radio frequency transceiver comprises a first radio transceiver and a second radio transceiver, wherein at least the second transceiver is configurable to provide a communication channel with either of the first configuration or the second configuration,
and the central unit is configured to transmit the offer using the first transceiver, and to configure the second transceiver, on reception of the acceptance message from the node, to enable reception of the data transmitted by the node using a communication channel according to the second configuration.

Preferably, the first and second transceivers of the central unit are non-Wi-Fi transceivers, thereby reducing undesirable node power drain and enabling node battery life (where, as

preferred, the or each node is battery powered) to be extended compared to that obtainable when using Wi-Fi to communicate between the or each node and the Central Unit.
Also preferably, communication between the Central Unit and the nodes, and vice versa, is direct rather than multi-hop from the source of a message (Central Unit or node) to its destination (node or Central Unit). Such an arrangement can offer significant node power savings compared to the use of a multi-hop system in which messages to or from some nodes from or to the Central Unit "hop" via one or more intermediate nodes en route to their destination.

In such a central unit the first configuration may comprise a first frequency and the second configuration may comprise a second frequency. The central unit may be configured to provide the offer of the communication channel at the second frequency in the form of an identifier or code word. The central unit may be configured to provide the offer including identifiers for a selection of alternative communication channels for the node to transmit data for reception by the second radio frequency transceiver. The central unit may be configured so that at least two of the alternative communication channels use the same frequency but provide different bitrates.

According to a further aspect of the present invention there is provided a battery-powered node for a security monitoring system having a central unit comprising at least one radio frequency transceiver configurable to provide a communication channel with either of a first configuration or a second configuration, the node comprising: a node non-Wi-Fi radio frequency transceiver operable both for communication with the central unit using a communication channel according to the first configuration, and for communication with the central unit using a communication channel according to the second configuration, and a controller for controlling the node non-Wi-Fi radio frequency transceiver;
the node being configured, on receiving an offer, transmitted from the central unit using a communication channel according to the first configuration, of a communication channel according to the second configuration for the node to transmit data using a communication channel according to the second configuration, to transmit an acceptance message to the central unit using a communication channel according to the first configuration, and thereafter to transmit data to the central unit using a communication channel according to the second configuration.
With such a node the first configuration may comprise a first frequency and the second configuration may comprise a second frequency. The node according to embodiments of the invention may comprise at least one sensor.

A node according to embodiments of the invention may comprise at least one store for storing sensor data to be transmitted to the central unit.

A node according to embodiments of the invention may be configured to determine a response to an offer that includes identifiers for a selection of alternative communication channels for the node to transmit data for reception by a second radio frequency transceiver of the central unit, the determination being based at least in part on the node's ability to support an offered communication channel.

A node according to embodiments of the invention may be configured to perform a determination of radio frequency conditions. Such a node may be configured to determine the response based also on results of the determination of radio frequency conditions.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:
Figure 1 is an overview of a security monitoring system according to a first aspect of the invention;
Figure 2 is a schematic drawing showing in more detail features of the gateway or central unit of Figure 1;
Figure 3 is a schematic drawing showing features of a node of the security monitoring system according to an embodiment of the invention;
Figure 4 illustrates a process of switching from a control channel to an offered communication channel between a node and a central unit according to an embodiment of the invention;
Figure 5 shows the structure of a typical packet of a communication protocol that may be used in embodiments of the invention;
Figure 6 shows signal flow in relation to a communication session with a non-wakeup node that may be used in embodiments of the invention;
Figure 7 shows signal flow in relation to a wakeup node that may be used in embodiments of the invention;
Figure 8 illustrates the behaviour of a wakeup node in relation to a wakeup slot that may be used in embodiments of the invention; and
Figure 9 illustrates the behaviour of a wakeup node in the receive state that may be used in embodiments of the invention.

DETAILED DESCRIPTION OF EMBODIMENTS

Hereinafter, certain embodiments will be described more fully with reference to the accompanying drawings. The invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided by way of example so that this disclosure will be thorough and complete, and will fully convey the scope of the invention, such as it is defined in the appended claims, to those skilled in the art.

Specific description

One of the principal components of node power consumption is activity of the circuitry responsible for wireless, typically RF, communication with the Central Unit 110. Generally, in high security systems, nodes are in bidirectional contact with the central unit, being able to receive as well as send information to the Central Unit 110. For example, some but not all security monitoring installations may operate on a synchronised basis, with each of the nodes having an internal clock that must be kept synchronised with the master clock in the Central Unit 110. To maintain synchronisation, the central unit may send out periodic beacon signals, and the nodes periodically listen for these and adjust their clock synchronisation as necessary. Such synchronisation can help insure that plural nodes can communicate with the central unit, in the event of detecting an incident, without the nodes' transmissions colliding. Typically such low power radio systems make use of ISM radio channels and protocols designed to reduce power consumption.

When not listening for synchronisation beacons, and when not sending an event notification, the radios of the nodes in synchronised systems are typically in a low-power consumption sleep state. Some detectors and sensors, such as magnetic switches used on doors and windows, and PIR detectors, consume virtually no power when waiting to detect an event. But other detectors, such as cameras, need to have high power functionality and shut down to avoid consuming power, typically only being powered up when trigged by low battery power functionality of the detector (when the remaining charge on the unit's battery falls below a threshold), when another sensor detects movement or when instructed to power up by the Central Unit 110.

In general, nodes can notify the central unit of events with only very modest quantities of data. The main exceptions are sensors which provide image data, image sensors – generally cameras of some kind, and those which provide sound data – microphones, which can each produce significant quantities of data. Although it is of course possible to send such large quantities of data over a low bit rate channel, this takes

considerable time and consequently consumes a lot of power. If an event has been detected by a sensor such as a PIR or a door/window opening sensor, and there is for example a video camera able to monitor a zone including the location of the event, it would be desirable to be able to transfer useable images and video frames to the central unit as soon as possible so that the nature and scale of the threat can be determined – and so that in a centrally monitored system the images/video sequence can be forwarded to the CMS 200 for analysis and action.

Security monitoring systems generally include many nodes. In general, when one node in a system senses an incident most of the other nodes in the system do not sense an incident but remain armed ready to sense another incident. The central unit receives a signal from node that has sensed an incident, and may respond to this by signalling the node or adjacent nodes, in addition to possibly communicating with the CMS 200. But it is desirable for the central unit to continue to listen for reports of other incidents from other nodes, as well as signalling to the other nodes for control and other purposes, while exchanging communications with the node(s) at the site of the reported incident. To this end, in embodiments of the invention the central unit includes at least two transceivers for simultaneous communication with the nodes of the monitoring system to provide diversity. Preferably, each of the at least two transceivers is tuneable.

Figure 1 is an overview of a security monitoring system according to a first aspect of the invention. The figure shows a stylised domestic installation 100 of a monitoring system according to an embodiment of the invention, and a monitoring centre (Central Monitoring Station or CMS) 200 that supports the domestic installation. The installation 100 includes a gateway or central unit, 110, which is connected to the monitoring centre 200 by means of a data connection 150. The data connection 150 may be provided over a phone line, a broadband internet connection, Ethernet, a dedicated data connection, or wirelessly, for example using an LTE or GSM network, and in general multiple of these options will exist for any installation, so that there is security of connection between the gateway 110 and the monitoring centre 200. For additional security, the central unit 110, or a sensor in communication with the central unit 110 and the monitoring centre may both be provided with means to support an ISM radio connection, for example in the European 863 to 870MHz frequency band, preferably one configured to resist jamming.

The domestic installation 100 involves a typical arrangement where the exterior doors 120 and windows 124 are fitted with sensors 114, for example magnetic contact sensors, to detect opening of the door or window. Each of the rooms of the building having the installation is provided with a combined fire/smoke detector 116. In addition, several

rooms have movement detectors 118, such as pyroelectric infrared (PIR) detectors, to detect movement within an observed zone within the room. The front door 120 of the building leads into a hall which also has internal doors to various rooms of the house. The hall is monitored by a video camera 125 having an associated motion detector. Similarly, the kitchen which is entered from the back door 121 is monitored by a video camera 126 which includes a motion detector. Each of the sensors, detectors and video cameras, which may throughout this specification be referred to generically as nodes, includes a wireless interface by means of which it can communicate with the central unit 110. The central unit 110 includes first and second transceivers (not shown) with associated antennas 130 and 132 for communication with the sensors, detectors and video cameras. In addition, the central unit 110 may include at least one further antenna 134 for wireless communication with the monitoring centre. Each of these antennas may be connected to a corresponding transceiver, not shown. Additionally, the central unit 110 may include a dedicated antenna arrangement for Wi-Fi, for example to connect to a domestic Wi-Fi access point 180. The Wi-Fi access point may also provide one of the means of access to the monitoring centre 200. Optionally, the central unit 110 may itself function as a Wi-Fi access point, with a connection (e.g. a wired connection) to an Internet service provider, to provide Wi-Fi coverage within the building in place of the Wi-Fi access point 180.

Some installations may include more than one central unit (CU), for example two central units, to provide a failsafe backup. In general in such multi CU installations the two CUs work together in parallel. However, in some installations the two CUs may work in parallel in communication with some of the nodes of the domestic installation and individually in communication with other nodes of the domestic installation. The latter may be the case when CU is used as a range extender in domestic installations covering larger installations. Two CUs may work in parallel but a node is only logged into one of the CUs at a time, and that CU is responsible for all communication with the node but the other CU can hear all and understand all communication between the other two – if it is not a range extension scenario.

In a domestic installation 100, the Central Unit 110 typically has knowledge of all nodes comprised in the installation 100. Each node may have a unique node identifier or serial number that is used to identify the node. Each node may have different functionalities associated with it, such as e.g. video capabilities, motion detection, still imaging, audio recording, communication speeds etc. Some or all capabilities may be communicated from the node to the Central Unit during a login procedure during setup of the installation 100. Alternatively and/or additionally, some or all capabilities may be communicated to the

Central Unit from the node upon request from the Central Unit 110. Alternatively and/or additionally, some or all capabilities may be retrieved, by the Central Unit 110, from the CMS 200.

The Central Unit 110 typically comprise at least one radio frequency transceiver. The radio frequency transceiver is configurable, by a controller, in at least two configurations e.g. a first configuration and a second configuration. The configurations may comprise frequencies used for transmission and/or reception of data and the frequencies of the at least two configurations may be different.

Figure 2 is a schematic drawing showing in more detail features of the gateway or central unit 110 of Figure 1. The gateway 110 includes a first transceiver 230 coupled to the first antenna 130, and a second transceiver 232 coupled to the second antenna 132. The transceivers 230 and 232 can both transmit and receive, but a transceiver can only perform one of these operations at a time. The transceivers 230 and 232 each operate in half duplex mode, and preferably each transceiver uses the same frequency for transmission as for reception. Generally, the two transceivers will operate on different frequencies, but they can both transmit, or both receive, on the same frequency to provide diversity. The transceivers 230 and 232 are coupled to a controller 250 by a bus. The controller 250 is also connected to a network interface 260 by means of which the controller 250 may be provided with a wired connection to the Internet and hence to the monitoring centre 200. The controller 250 is also coupled to a memory 270 which may store data received from the various nodes of the installation – for example event data, sounds, images and video data. The gateway 110 includes a power supply 262 which is coupled to a domestic mains supply, from which the gateway 110 generally derives power, and a backup battery pack 264 which provides power to the gateway in the event of failure of the mains power supply. Optionally, as shown, the central unit 110 includes a Wi-Fi transceiver 240 (using some variant of IEEE 802.11), and associated antenna arrangement 242, which may be used for communication with any of the nodes that is Wi-Fi enabled. The Wi-Fi enabled node may for example be a remote control (with user-changeable batteries) or control panel (that may be connected to the mains power supply, with battery backup, so that it is not dependent on battery power) that may for example be located close to the main entrance to the building to enable the occupier to arm or disarm the system from near the main entrance. Similarly, an interface enabling bidirectional communication over a Public Land Mobile Network (PLMN), such as GSM or LTE, may optionally be provided, and one is shown in the Figure as interface 244 and antenna arrangement 246. Optionally, a third antenna 134 and associated ISM transceiver

234 may be provided for communication with the monitoring centre 200 over, for example, the European 863 to 870MHz frequency band.

Throughout this specification, references to Wi-Fi relate to systems and elements operating according to some variant of the 802.11 standard. Conversely, systems, devices and elements referred to as ISM should not be taken to embrace Wi-Fi.

The first and second transceivers may both be tuneable ISM devices, operating for example in the European 863 to 870MHz frequency band or in the 915MHz band (which may span 902-928MHz or 915-928MHZ depending upon the country). In particular, both of these devices may be tuned, i.e. may be tuneable, to the frequencies within the regulatorily agreed sub-bands within this defined frequency band. Alternatively, the first transceiver and the second transceiver may have may have different tuning ranges provided that there is some overlap. As will be explained, at least the second transceiver 232 may be used to support a high speed channel (that is one having a higher symbol rate or bitrate than the other) that is not offered by the first transceiver – but this does not require that the first and second transceivers be technically different, as they may share the same inherent technical capabilities. But the controller of the gateway is configured to offer one or more communication channels operated over the second transceiver that may provide a higher transmission speed than is provided by communication channels operated over the first transceiver. Note that the second transceiver also may be used as a diversity transceiver operating in the same channels as operated over by the first transceiver but at any instant the first and second transceivers will operate on frequencies that are sufficiently different not to interfere with each other.

In order to help the understanding of some embodiments, the following sections will briefly describe some background information regarding wireless communication. Within wireless communications there are several parameters that determine the possibility of successful transmission and reception of a packet. The possibility that a packet is not successfully received and/or decoded is known as Packet Error Rate (PER) and the corresponding measure on bit level is Bit Error Rate (BER). The PER and BER are both stochastic distributions and a specified level, e.g. 2.4% BER for GSM, is defined as the sensitivity limit. The sensitivity limit may be different depending on protocol and standard. In case of ISM communications in the sub-GHz band the maximum allowed sensitivity is specified in ETSI EN300 220-1 v3.1.1. according to Eqn. 1:

$$10 * log(RBW) - 117\ dBm \qquad \text{Eqn. 1}$$

In Eqn. 1, RBW is the bandwidth of the receiver in KHz. The maximum allowed sensitivity will increase with increased receiver bandwidth and the reason for this is that the thermal noise power N introduced by the receiver increases as the receiver bandwidth increases, Eqn. 2:

$$N = k \cdot T \cdot RBW \qquad \text{Eqn. 2}$$

Where k is Boltzmann's constant in Joules per Kelvin (approx. 1.381×10^{-23} J/K) and T is the temperature in Kelvin. A received signal S will, with most modulation techniques, have to be above the thermal noise and a Signal to Noise Ratio, SNR, is defined in accordance with Eqn. 3:

$$SNR = \frac{S}{N} \qquad \text{Eqn. 3}$$

In digital communication, the received signal S is comprised of a series of symbols where each symbol correspond to 1 or more bits depending on the modulation order M of the modulation chosen. The number of bits per symbol n is related to the modulation order according to Eqn. 4:

$$M=2^{n} \qquad \text{Eqn. 4}$$

The receiver will decode a received signal S into bits and as mentioned earlier, the sensitivity is usually defined as a BER. A better measure of the received signal quality may be a received energy per symbol E_s or energy per bit E_b versus noise rather than the more generic SNR. From Eqn 4. we know the relation and can formulate Eqn. 5:

$$\frac{E_b}{N} = \frac{E_S}{n \cdot N} \qquad \text{Eqn. 5}$$

One important takeaway from Eqn. 5 is that the energy per bit E_b decreases with the number of bits per symbol. Further to this, the received energy per bit E_b will depend on the bit-rate. If the output power is kept constant and the bit-rate is doubled, the transmission time will be halved and consequently, so will the energy per bit E_b. From the art, the relation between BER as a function of E_b/N is known and can be accurately modelled, see e.g. "Analyze BER Performance of Wireless FSK System", Hamood Shehab Hamid et al., Microwaves & RF; Nov2009, Vol. 48 Issue 11, p80.

Figure 3 is a schematic drawing showing features of a node of the security monitoring system according to an embodiment of the invention. In this case the node is a video camera like the video camera 126 which is mounted in the kitchen, as shown in figure 1. The node includes a radiofrequency node transceiver 340 coupled to an antenna 330. A controller 350 is coupled to the transceiver and also to the image sensor 310 of the video camera. The controller is also coupled to an integral motion sensor 320 and to a memory 370. A battery 380 provides power to the node, in particular powering the controller, image sensor and motion detector. The video camera includes a lens arrangement 315 for forming an image on the image sensor 310. Optionally, the node includes an infrared light source 325 suitable for illuminating images detectable by the image sensor. The node transceiver 340 is tuneable. In particular, the node transceiver 340 can be tuned to frequencies to match those transmitted by or receivable by the first and second transceivers of the gateway 110.

The principle behind the invention will now be described. When a motion detector, for example a PIR (pyroelectric infrared) sensor, detects motion it transmits a signal to the central unit 110 using the node transceiver. Depending on the settings of the system, the central unit 110 may forward this movement detected signal to the central monitoring station. If the motion detector reporting the detection of motion is, for example, in or associated with a video camera, the central unit 110 will know this from the identity of the node that transmitted the motion detected signal. The central unit 110 will then send a message to the video camera using the first transceiver, the message (a channel definition message) requesting the video camera to transmit video data to the central unit 110 specifying a transmission frequency to which the second transceiver will be (or already is) tuned. The channel definition message may be in the form of a channel ID or code that is known to the relevant node (and possibly known by all the other nodes or some subset of the nodes) and which enables the relevant node to configure its own transceiver's transmission parameters (frequency, modulation type, bit rate, bandwidth, etc.) appropriately so that matching channel parameters are used by the relevant node and by the second transceiver of the central unit for reception of transmissions from the node). The central unit may select the channel (and hence the channel ID sent in the channel definition message) based in part on the type of data (for example video file, image file, audio file) or the likely amount of data, for example tending to offer channels capable of supporting bit rates higher than that currently offered by the first transceiver in order to permit the data to be transmitted more quickly. That is, the channel parameters may be selected to provide a high speed (e.g. higher bitrate channel to the relevant node). Such a request may be for the video camera to stream video data. More generally, the central unit may send a message to an image source, such as a

camera, requesting it to transmit image data at high speed and offering a suitable communication channel.

Trigger events other than the triggering of a movement sensor may also be used to initiate the process. For example, the activation of a node that monitors the status of an entrance to the building, for example a magnetic switch at a door or window, or detection of a sound, such as that of breaking glass, by a node comprising a microphone, will be transmitted by the relevant node to the gateway 110. The gateway 110 may, depending upon its programming and status, report the event to the CMS 200. The gateway 110 may also or alternatively use the detected event as a trigger to make an offer to a node, including e.g. a video camera, still camera or microphone, of a high speed channel to enable data to be sent from the node to the gateway at high speed. Further to this, a trigger event may be sent from CMS 200 requesting images or audio data from a particular node, this trigger may be used by the Central unit 110 to formulate an offer of one or more high speed channels to that particular node. It may also be that the installation 100 is configured such that a user of the installation 100 can request images, audio data or other relevant data from particular nodes of the installation 100 to be delivered to e.g. a mobile device of the user. The request may be generated from the mobile device and sent to the CMS 200 where it may be forwarded to the Central Unit 110. The Central Unit 110 may, if configured to do so, formulate an offer of one or more high speed channels and send that offer to the node from which the user requested data. Also, a particular node may send a message to the Central Unit 110 requesting an invitation for a high speed communication should it have relevant data to send using a high speed (e.g. higher bitrate) channel.

The provision in the central unit of a second and possibly additional transceivers in addition to the first transceiver means that security monitoring systems according systems according to the invention support channel diversity giving the central unit and the various nodes of the system multiple channels for communication in each direction and the potential to communicate in the presence of noise or attempts to jam the system.

The channel definition message from the central unit 110 requesting includes or is in the form of an offer specifying the frequency and other parameters of at least one channel. The parameters may be specified in the form of an identifier (a “channel identifier”) or code word, to reduce the size of the offer message. Each of the nodes (or possibly each of a subset of the nodes) stores the codes or channel identifiers for the parameter offers that it can support. Each offer corresponds to a set of parameters that include an RF frequency, a bit rate, and a modulation technique, e.g. GFSK, 4FSK, 4QAM, 16QAM etc., and such as

other parameters – transmission power, encoding type, etc., as may need to be specified. The offer message may include identifiers for multiple different sets of modulation parameters. The different sets of modulation parameters may have different RF transmission frequency, bandwidth and speed, and consequently, more than one transmission speed (e.g. bit rate or symbol rate) may be offered at any given RF transmission frequency.

Regulatory constraints may require operators or providers of security monitoring systems to register details of the parameters using for messaging in the systems. So it may be necessary to define, and register, each of the parameter sets used for each offer that a central unit can make to a node before any such systems are deployed. In such an environment, central units are configured only to provide identifiers for sets of parameters which have been registered. The central unit(s) and nodes of an installation each store details of the available channels and their channel identifiers. Generally the channel parameters and channel identifiers will be introduced into central units and nodes during manufacture – with any region-specific adaptations being catered for by designating particular central units and nodes to particular regions or countries.

The node receiving the offer will select one of the offers, for example based on a received code word or identifier, its selection being based at least on its own capabilities – for example by matching an offered code word or identifier with a stored code word or identifier. Optionally, the node may also determine the state of the local RF conditions at each of the RF transmission frequencies that it can support. For example, the node may use an RSSI detector to determine background noise in each of the relevant RF frequencies and/or bandwidths (that is, in each of the frequencies and/or bandwidths that the node is capable of transmitting and which are detailed in the offer from the central unit). The RSSI value will correspond to the noise power N as introduced earlier and it may optionally allow the estimation of a minimum required energy per bit E_b in order to decode a message with a desired BER. The desired BER may be a design parameter and/or a configurable parameter set by e.g. the central unit or the node. The knowledge of the noise power N and a minimum required energy per bit E_b will make it possible for the node to select the offer allowing for the highest bit-rate without compromising signalling reliability. Based on such measurements, or suitable alternative measurements, the node can chose a suitable offer that it can use to transmit the desired data, for example, a video clip file, other video data, or a still image file at to the central unit 110. The node may be configured to choose the channel offering the highest bit rate. The node may measure background noise or determine RSSI at the frequencies of the various offered channels, and may make its selection from the offered channel based on such measurements, for example choosing the highest speed

channel with an acceptably low noise or strongest RSSI. The main steps in this general process are illustrated schematically in figure 4.

At step 400, the central unit 110 receives notice of a trigger event that has been detected by a node. This is sent by the node using a communication channel according to the first configuration which may be considered to be a “normal” control channel configuration, the parameters (frequency, modulation type, bit rate, etc.) of which are predetermined. If the central unit 110 has more than one transceiver, as is preferred, the central unit may be set up to receive trigger notices only via a first transceiver or by a first and a second transceiver. If the system has more than one frequency allocated to trigger notices, the two transceivers may be tuned to receive on different trigger event notification frequencies. The node transmits the trigger notice using a communication channel according to a first configuration - at a frequency and the other parameters set for a control channel within the system. Generally the system will be set up to support multiple such channels so that adjacent systems can co-exist and the system is robust to unintentional and deliberate (jamming) interference – and the relevant node uses any agreed protocol to decide the frequency and speed at which the trigger notice should be transmitted.

The central unit 110 then determines the identity of the node that transmitted the trigger event notice and composes an appropriate offer according to a second configuration, and for example retrieves the appropriate code word(s) or identifier(s) to send to the node. The central unit may base the offer on its prior knowledge of the node’s capabilities, the central unit’s ability to support the offer, its knowledge of the current state of the RF environment, and the existence or activities of other nodes. The offer message may include an identifier for the relevant node, to enable the node to recognise that it is the intended recipient of the offer message. The offer may be encrypted such that it is only decryptable by the relevant node, e.g. using AES as is known in the art. The central unit 110 may also take into account the nature of the data that the node will provide, based on the central unit’s knowledge of the unit’s identity and hence its nature e.g. whether it is a microphone from which only audio data can be received, or a video camera from which video signals may be received, and taking account of the resolution, coding and hence bit-rate demands of the video data that the camera can provide. Thus, different nodes may receive different offers of channels (characterised by different configurations of parameters), chosen appropriate to their type and their configuration. Also, as will be described later, the Central Unit 110 may already have stored, in memory, suitable channel parameters received from the various nodes. If such parameters are stored for the relevant node, these may be taken into account by the Central Unit 110 when formulating the offer to be made. Further to this, the Central

Unit 110, may, as described earlier in relation to the node, measure the background noise of relevant frequencies in relevant bandwidths prior to making the offer. As for the node, the measured noise value will correspond to the noise power N and may optionally allow for estimation of a minimum required energy per bit E_b in order to decode a message with a desired BER which may be used to determine what channel parameters to offer to the node. The Central Unit 110 has knowledge of the signal strength of the node at the control channel (i.e. with regular speed and at the control channel frequency and modulation parameters) and may optionally use this to estimate the expected E_b/N for different modulation parameters before making the offer to the node. Additionally, there may be more than one node transmitting a trigger at substantially the same time. In this case the central unit 110 may consider capabilities of each node and prioritize one of them depending on e.g. node capabilities, expected amount of data and wireless parameters relating to that node. At step 402, the central unit 110 transmits the offer message, or invitation, of a channel of the second configuration, to the relevant node using a channel according to the first configuration. If there are two or more transceivers, the central unit may be configured to use the first of these preferentially

The node receives the offer message and determines whether it can accept the offer. If the offer message contains alternative offers of different speeds and/or at different RF frequencies, the node determines which of these overlap with its own capabilities, for example by comparing code words or channel identifiers received in the offer with code words or channel identifiers that it has stored (and each of whose channel parameter combinations it can support). The node will then determine to accept one of the offers which overlaps with its capabilities. Prior to making this election, the node may perform an RSSI check or similar at each of the overlapping RF frequencies to determine whether local signal conditions / background noise (e.g. interference or jamming) prevent or otherwise make undesirable the selection of any of the overlapping offers. Based on this determination, the node composes an acceptance message, and at step 404 the node transmits this message to the gateway using the first configuration. This message may be received by the Central Unit 110 via the first and/or the second transceiver, depending upon its settings.

The controller of the Central Unit 110 then sets the controls for a transceiver to suit the parameters corresponding to the offer selected by the node. If the central unit has two or more transceivers, one of these may be used primarily or exclusively for control messages, and the second or other transceivers used for example to receive data from nodes, in which case the node will set the second or other transceiver according to the second configuration to receive the data to be sent from the node.

At step 406, the node then sends the requested data to the Central Unit 110 on the agreed frequency, at the agreed speed, and using the agreed coding etc., that is, according to the second configuration. Thus, for example, video or audio may be sent from the node to the Central Unit 110. The Central Unit 110 may then onward transmit these data to the CMS 200 using an available connection, so that an automated system or human operator can determine an appropriate response – such as despatching human intervention (e.g. security personnel, Fire, Police, Ambulance, etc.) or the like, and/or they may be played out locally to enable an appropriate response to be determined locally. When data transmission is complete, the node sends a notice to this effect to the central unit 110 (in any appropriate form) in step 408. This enables the Central Unit 110 to repurpose the second transceiver if one is being used, or allows it to reset the sole transceiver back to the first configuration to receive trigger notices etc.. If the central unit has two transceivers, this will generally involve the Central Unit 110 switching the second transceiver back to a control channel mode until the second transceiver is needed for some other purpose. Thus, the second transceiver can again be regarded as providing diversity.

The node also switches back to the first configuration, a control channel mode, so that subsequent communications between the node and the Central Unit 110 are on an allocated control channel until another trigger event (which may or may not be related to the earlier trigger event) is notified to the Central Unit 110 in step 410. The Central Unit 110 then, in step 412, repeats the process previously described with reference to step 402. Likewise, the node formulates an acceptance message which is sent to the Central Unit 110 in step 414. Data are subsequently transmitted by the node on the offered channel in the second configuration (for example at high speed) in step 416. Again, if the central unit has two or more transceivers, these data may be received by the second transceiver which has once again set by the controller of the Central Unit 110 to the appropriate second configuration channel parameters (e.g. for high speed data transfer). Once again, once data transmission is complete, the node sends an end of transmission message to the Central Unit 110, enabling the controller of the Central Unit 110 to switch the second transceiver back to control channel mode. The node also reverts to control channel mode and waits in a state in which it can receive control messages sent by the Central Unit 110 via the first transceiver.

Thus, it can be seen, that the node sends and receives messages using the first configuration, a control channel mode, except when it has received and accepted an offer from the Central Unit 110. Thereafter, the node transmits the agreed data using the agreed channel, that is in the second configuration, until data transmission is complete. The data

transmitted by the node using the agreed offered parameters are received by the Central Unit 110 using a transceiver which has been switched to operate according to the second configuration, that is the agreed parameters of the offered channel accepted by the node. Once the data transmission is complete, both the relevant transceiver of the Central Unit 110, and the node transceiver, revert to the first configuration, e.g. the control channel settings.

It should be noted, and as is well understood by the skilled person, that the reference to a transmission may comprise e.g. transmission of a message and the subsequent reception of an acknowledgment.

All options may be configurable by e.g. the CMS 200 and can consequently exist in the node and/or Central Unit 110 and be activated depending on configuration. The offered sessions described above may comprise periodic acknowledgements of received packets by the Central Unit 110 to the node. The Central Unit 110 may send an acknowledgement on either the negotiated channel or on the control channel. In one optional embodiment, no acknowledgement is sent until the offered session is complete. The acknowledgement may comprise references to any lost packets and the node may be requested to retransmit the lost packets either using the same offered and agreed channel or using a control channel. Alternatively, in another optional embodiment, the offered session is divided into a plurality of blocks, each plurality of blocks comprises a plurality of packets and the Central Unit 110 transmits an acknowledgement after each block and the acknowledgement may comprise references to any lost packets and the node may be configured to retransmit all lost packets at the end of the session either using the same offered and agreed channel or using the control channel.

In a further optional embodiment, the Central Unit 110 may, in any acknowledgement, terminate the agreed session and request the node to revert back to the control channel and/or make another offer comprising updated modulation parameters. This may be utilized when e.g. the wireless environment changes during the course of an agreed session causing e.g. the BER to increase. Additionally and optionally, there may be a fall-back functionality configured in the node should it not receive any acknowledgement at all from the Central Unit 110. The fall-back functionality may comprise waiting for a configurable period of time and at the lapse of said time revert back to the control channel and may optionally transmit a request to the Central Unit 110 for an invitation to an alternative communication channel.

The packet structure of the communications described herein are of known structures comprising preamble, synch word and data. Depending on the transmission structure used, e.g. block transmission etc., data messages may contain packet identifiers, sender identification, recipient identifier and/or counters and the length of packets may be e.g. predetermined, configurable, negotiable etc. The packets may be encrypted and there may a Cyclic Redundancy Check, CRC, comprised in the packet.

In Fig. 5, the structure of a typical packet 400 of a suitable communication protocol is shown. The packet 400 may comprise a pre-amble 410, a sync-word 420, a payload 430 and a Cyclic Redundancy Check 440. The payload 430 is preferably encrypted with an encryption key that is known by the recipient of the packet.

There are generally two categories of nodes, and these may be termed wakeup nodes and non-wakeup nodes. The non-wakeup nodes are nodes with which communication can be initiated only by the node itself, and not by the Central Unit. Examples of non-wakeup nodes are e.g. switches such as magnetically controlled contacts used on doors and windows. Should the Central Unit 110 need to communicate with a non-wakeup node, the Central Unit 110 has to wait until it receives a message from the non-wakeup node and acknowledge that message with a message saying that the Central Unit 110 has additional message(s) to send to the non-wakeup node. This design of the communication protocol enables non-wakeup nodes to stay in a sleep or hibernation state for extended periods of time. Consequently, they only have to wake up on e.g. external events that are communicated to the Central Unit 110 or the expiry of an internal wakeup-timer that requires a periodic communication with the Central Unit 110. The internal wakeup-timer may be configurable and is typically in the range of 5-60 minutes. The communication protocol allows for extended battery life (e.g. at least 5 years from a single small battery cell) of non-wakeup nodes.

Conversely, wakeup nodes are nodes that can be woken from a monitoring state (in which their power consumption is less than in a fully awake state) to a fully awake state by the Central Unit 110, so that the Central Unit 110 can initiate communication with wakeup nodes, albeit that this requires the wake up node to enter a partially awake state – the monitoring state – in order to be able to detect the presence of a message from the central unit. Examples of wakeup nodes, i.e. nodes that can be triggered from the Central Unit 110 include e.g. camera-PIRs, nodes with video functionality, nodes with audio functionality, etc. The wakeup nodes have to wake up (that is move from a sleep state and enter a (low power consumption) monitoring state) periodically to determine if the Central Unit 110 needs to communicate with them. Because a Central Unit generally only needs to communicate with a wakeup node rather infrequently, the battery life of wakeup nodes is largely dependent on how often they have to listen for communications from the Central Unit (110) and for how

long the wakeup nodes have to stay awake before they can determine that there is no communication for them.

With reference Fig. 6, the signal flow in relation to a communication session with a non-wakeup node (a non-wakeup communication session) will be explained in further detail. The communication is initiated by the transmission from the non-wakeup node of a trigger message 510 that is received at the Central Unit, the trigger message being due to an external or an internal trigger acting on the non-wakeup node. The external trigger may be any trigger that the non-wakeup node is configured to react to, e.g. a tamper detection or, in the case of a magnet contact, the triggering of a motion sensor or reed switch. The internal triggers may be e.g. expiry of a wakeup-timer or the battery level dropping below a (configurable) threshold. In either case, the non-wakeup node transmits the trigger message 510 to the Central Unit 110, and the Central Unit 110 receives, decrypts and analyses the message.

In the signal flow of Fig. 6, the Central Unit 110 has information, data or instructions to share with the non-wakeup node and responds by sending an acknowledgement including a Listen After Talk, LAT, request 520. The acknowledgement with a LAT request 520 is received by the non-wakeup node, and the non-wakeup node, after decrypting and analysing the message, stays in a receive state waiting for an additional message(s) from the Central Unit 110. The non-wakeup node may optionally send an acknowledgement (not shown) to the Central Unit acknowledging the LAT request. The Central Unit 110 proceeds to transmit an information message 530 comprising the information, data or instructions that is wishes to share with the non-wakeup node. The non-wakeup node receives the information message 530, and after decryption and analysis of the message it may send an acknowledgement (not shown) to the Central Unit 110 confirming reception of the information message 530. Following this, the non-wakeup node reverts to a low power mode, e.g. a sleep or hibernate mode in order to conserve power. The non-wakeup node will stay in this state until the next trigger occurs at which point the non-wake-up node sends a trigger message 310, the second trigger message 510 in Fig. 6, to the Central Unit 110. In the example in Fig. 6, the Central Unit 110 has no information, data or instructions to share with the non-wakeup node and, after decryption and analysis of the second trigger message, transmits an information acknowledgement 540 to the non-wakeup node acknowledging reception of the trigger message 510. On reception of the information acknowledgement 540, the wakeup node goes back into its low power mode.

In Fig. 7 the signalling flow in relation to a wakeup node is shown. The wakeup node will wake from a sleep state into a monitoring state in wakeup slots 610, and monitor 710 a radio channel for information at periodic intervals. The time between two consecutive wakeup slots 610 is defined as the wakeup interval. The monitoring 710 is done by

determining if there is a signal present in a monitored radio bandwidth. The received signal is represented by a Receiver Signal Strength Indicator, RSSI. The monitored radio bandwidth may be a predetermined, but configurable, radio channel. The monitoring 710 will be explained in further detail in coming sections.

If no signal is detected, the wakeup node is configured to revert to a low power mode, e.g. a sleep or hibernate mode in order to conserve power. It will stay in this mode until it is time to wake up again and monitor 710 the channel for a signal, i.e. it will sleep for substantially the entire duration of the wakeup interval apart from the time spent monitoring the radio channel. The Central Unit 110 and the wakeup nodes are synchronized. If the Central Unit has information to send, it will send a wakeup message 620 during a wakeup slot 610. The wakeup node will be monitoring 710 the channel since the wakeup message 620 is sent during a wakeup slot 610, and will consequently detect a signal in the channel. The wakeup node will receive 720 the wakeup message 620, decrypt and analyse the wakeup message 620, as will be explained in more detail in later sections, and will send a wakeup acknowledgement 630. The Central Unit 110 receives the wakeup acknowledgement 630 and proceeds to send an information message 640 to the wakeup node. The wakeup node receives, decodes, and analyses the information message 640, and the signalling session is concluded by the wakeup node sending an information acknowledgement 650 to the Central Unit 110.

Referring to Fig. 8, the behaviour of a wakeup node in relation to a wakeup slot 610 will now be explained. The wakeup node is in a monitoring state 710 at the start of the wakeup slot 610 (as will be explained further below with reference to Figure 10). Generally, wakeup nodes will use transceivers rather than separate transmitters and receivers because transceivers may be smaller and cheaper than a corresponding transmitter receiver pair. The wakeup node may optionally (as shown in Fig. 8) enter the monitoring state prior to the wakeup interval 610, rather than at the start of the wakeup interval, in order to compensate for e.g. clock inaccuracy and/or drift of a timing reference of the wakeup node. Also, it is necessary for the receiver of the wakeup node to have reached a stable state, after being powered up into the monitoring state from the sleep state, for the start of the wakeup slot 610 and this may require that the receiver be powered up a little in advance of the start of the wakeup slot 610. If a relevant packet 400 is occupying the channel, the pre-amble 410 of the packet will start at the start of the wakeup interval 610. The wakeup node will, when it is in the monitoring 710 state, detect the pre-amble as an RSSI level above a predetermined configurable RSSI threshold. If there is no signal above the RSSI threshold, the wakeup node will go back to the sleep or hibernate state with the receiver fully powered down (and without the receiver having been fully powered up) until the next wakeup slot 610. If a signal is detected during the monitoring 710 of the channel, the wakeup node will switch

to a receive state 720, detect the pre-amble 410 and the following sync word 420, and proceed to receive the complete packet 400.

The receive state 720 will be described further with reference to Fig. 9. When in the receive state 720, the wakeup node may optionally be configured to perform pre-amble qualification 820, and if no pre-amble 410 is detected, directly exit the receive state 720 and go back to the sleep or hibernate state 810. Further, and still optionally, the wakeup node may be configured to perform sync word qualification 830, and if no sync word 420 is detected, directly exit the receive state 720 and go back to the sleep or hibernate state 810. Further and also optionally, the wakeup node may be configured to perform CRC qualification 840 on the received packet 400 and if the CRC 440 is not correct, directly exit the receive state 720 and go back to the sleep or hibernate state 610. Note that all the steps in relation to the receive state 720 described in Fig. 9 are mutually optional and may be combined in any foreseeable manner . Thereafter, the wakeup node will, if it is not going back to the sleep or hibernate state 810, move on to packet analysis 850.

Packet analysis 850 involves decryption 910 of the payload 430 of the packet 400, if the decryption 910 fails, i.e. the payload does not conform to an agreed format etc. the wakeup node will directly exit the packet analysis state 850 and go back to the sleep or hibernate state 810. If the decryption 910 is successful the wakeup node will perform recipient analysis 920. The recipient analysis 920 comprises analysing address identifiers of the payload 430 of the packet 400 to see if the wakeup node is one of the intended recipients for the wakeup message 620. If the wakeup node is not one of the intended recipients, the wakeup node will directly exit the packet analysis state 850 and go back to the sleep or hibernate state 810. If the wakeup node is one of the intended recipients, it will send a wakeup acknowledgement 630 confirming reception of the wakeup message 620. It may optionally, depending on the configuration of the communication protocol and/or the Central Unit, go to the sleep or hibernate state for a predetermined period of time before waking up again to receive the information message 640 from the Central Unit. The optional sleep or hibernate state 810 between the transmission of the wakeup acknowledgement 630 and reception of the information message 640 may depend on the number of intended recipients of the wakeup message 620. If there is only one intended recipient, the information message 640 may be sent by the Central Unit 110 shortly after receiving the wakeup acknowledgement 630 from the wakeup node. However, if there are a plurality of intended recipients of the wakeup message 620, there may be a, configurable, predetermined time before the information message 640 is sent. This time is preferably a time based on an integer multiple of the wakeup period, e.g. the information message will be sent at a later wakeup slot than the wakeup slot in which the wakeup message was received.

When it comes to choice of frequencies and transmission speed, regard must be had to the prevailing regulations in the region where the security system is deployed. In Europe, radio systems for security monitoring systems commonly make use of ISM (Industrial Scientific and Medical) radio frequencies around 868 MHz (the 863-870MHz band). Similar bands, but centred around different frequencies, are similarly allocated for the same purposes in other territories. For example, in the USA, Canada, Chile, Colombia, Costa Rica, Mexico, Panama, Uruguay the 915MHz band spans 902 – 928MHz, whereas in Australia, Peru and Brazil it spans 915-928MHz, and in other countries other portions of a band from 915 to 928Mhz are available. In Europe duty cycles in the ISM bands are regulated by relevant sections of the latest harmonized revision of the ETSI EN300 220 standard. This standard defines, at the time of this application, the following sub-bands and their allowable duty cycles:

g (863.0 – 868.0 MHz): 1%
g1 (868.0 – 868.6 MHz): 1%
g2 (868.7 – 869.2 MHz): 0.1%
g3 (869.4 – 869.65 MHz): 10%
g4 (869.7 – 870.0 MHz): 1%

Embodiments of the invention deployed in Europe may make use of the g1 and g2 sub-bands, where the allowable Effective Radiated Power (ERP) is 25 mW (+14 dBm), with a 1% duty cycle for communication between the Central Unit 110 and the nodes. Typically systems are configured to provide choices of pre-defined frequencies in each of the g1 and g2 bands. In such systems high speed and other offered channels may be offered in the g3 sub-band, which has an allowable ERP of 500mW (+27 dBm) with a 10% duty cycle. Again, more than one frequency may be pre-selected in this band to enable alternative options. But it will be appreciated that it the invention does not rely on the use of the g3 sub-band for the offered or high speed channel, channels could be set aside for offered/high speed use within the g1 or g2 sub-bands. If the security monitoring system is deployed in another territory, it is anticipated that the RF bands allocated security and alarm systems, or available for such use even if not specifically allocated, will likewise provide opportunities to preselect some frequencies for regular speed, control and messaging functions, while allowing others to be preselected for use as high speed channels in the context of the invention.

Typically, the regular speed channels or configuration may operate around 30 to 45 kbit/s – e.g. 38.4 kbit/s. “High speed” in the context of this disclosure may equate to 128 to 500 kbit/s e.g. 200 kbit/s.

The abovementioned frequencies and their corresponding maximum allowable duty cycles may optionally be used by the Central Unit 110 when formulating the offer to a node. The Central Unit 110 may have at least one counter per band and node keeping track of how much time each node has transmitted into each frequency band during a configurable time period. If the time spent transmitting is close to, or at, the maximum allowed duty cycle of the associated band, the Central Unit 110 may decide against making an offer of a channel in that band. Correspondingly and optionally, each node may have similar counters keeping track of their respective time spent transmitting in each band and may consequently reject certain offers if they are in a band where the node is close to, or at, the maximum allowable duty cycle.

An alternative and optional embodiment of the present invention relates to transmitting software, configuration and/or firmware updates from the Central Unit 110 to a node. The software update is sent from the CMS 200 to the Central Unit 110 and may be targeted at one or mode nodes of the installation 100. The software update may be targeted at all nodes of e.g. a particular type, model or comprising a particular functionality. In this event, the Central Unit 110, upon reception of a software update from the CMS 200, formulates an invitation for a communication channel for the targeted node(s). It may be that the reception capabilities of the targeted nodes is different from their respective transmission capabilities and the corresponding may be true for the second transceiver of the Central Unit 110.

In one embodiment, the invitation for a communication channel is sent to one node and the signalling proceeds as described with reference to earlier embodiments with the difference that the Central Unit 110 transmits at high speed using the second transceiver (in some previous embodiments the Central Unit 110 received a high speed data transmission using the second transceiver) and the node receives a high speed transmission. Correspondingly, the node may acknowledge and request retransmissions as describer earlier in relation to the Central Unit 110 receiving the data over the offered and agreed channel.

In a further optional embodiment, the offer of high speed communication is sent to a plurality of nodes. The plurality of nodes may be e.g. nodes of a particular type, model or comprising a particular functionality. The Central Unit 110 may wait for acceptance messages from the plurality of nodes and if their selected modulation parameters differ, the Central Unit 110 may choose the lowest speed and transmit a new invitation comprising the lowest speed selected by any of the plurality of nodes. Alternatively, the central unit 110 may

choose to omit some nodes from the invitation choosing to send a new invitation comprising e.g. the most commonly selected modulation parameters to the subset of the plurality of nodes who chose these particular modulation parameters in their respective acceptance to the high speed offer. When a plurality of nodes have all accepted the same modulation parameters the signalling proceeds as described with reference to earlier embodiments with the difference that the Central Unit 110 transmits at high speed using the second transceiver (in several previous embodiments the Central Unit 110 received a high speed data transmission using the second transceiver) and the plurality of nodes receives at high speed. The acknowledgement of packets may be performed per node as described in relation to earlier embodiments where the Central Unit 110 receives at high speed wherein the Central Unit 110 in this embodiment keeps track of all packets not correctly acknowledged by either of the plurality of nodes. These packets may be retransmitted, either individually to respectively node or all unacknowledged may be retransmitted to all of the plurality of nodes in which case each of those nodes will have to keep track of their respective lost packets.

In one embodiment of the installation 100, more than one Central Unit 110 is part of the installation. The Central Units are in communication with each other and are synchronized. In this embodiment, the Central Unit 110 being used to receive data over the offered channel (which as we have seen may be a high speed channel) may be chosen to be the Central Unit that has the most suitable data connection 150 to the CMS 200, for instance Ethernet over Wi-Fi over cellular. It may be that the Central Unit used to receive data over the offered communication channel is a Central Unit Light, i.e. a Central Unit having only one ISM transceiver for communication with the nodes of the system. If this is the case, the Central Unit Light will use that ISM transceiver for the offered connection as described earlier in relation to the second transceiver of the Central Unit 110 and the other Central Unit(s) 110 of the installation will monitor the regular speed control channel.

It will be appreciated that the security monitoring system need not include a central monitoring station 200, although commonly it will. The gateway or central unit 110 may have or be associated with one or more displays for the display of images, moving or still, and audio output devices such as loudspeakers. So that an operator may be alerted by status changes detected by nodes such as motion sensors, magnetic switches, and the like, and may view images and hear audio signals received from nodes.

References made to nodes having e.g. video capabilities or audio capabilities are understood to be easily replaced with nodes having other relevant functionality that will

benefit from high bit-rate transfers such as, but not limited to still imaging, thermal imaging etc.

CLAIMS

1. A security monitoring system comprising:
a central unit, comprising:
at least one radio frequency transceiver that is configurable to provide a communication channel with either of a first configuration or a second configuration, and a controller for controlling the radio frequency transceiver(s);
a node comprising a node radio frequency transceiver operable in a first mode, for communication with the central unit using a communication channel according to the first configuration, and in a second mode for communication with the central unit using a communication channel according to the second configuration, and a controller for controlling the node radio frequency transceiver;
the central unit being configured to transmit using a communication channel according to the first configuration an offer to the node of a communication channel according to the second configuration for the node to transmit data for reception by the central unit;
the node being configured, on receiving the offer from the central unit, to transmit, using a communication channel according to the first configuration, an acceptance message to the central unit, and thereafter to transmit data, using a communication channel according to the second configuration, to the central unit;
the central unit being configured, on reception of the acceptance message from the node, to configure one of the at least one radio frequency transceiver to enable reception of the data transmitted by the node using a communication channel according to the second configuration;
wherein the at least one radio frequency transceiver comprises a first radio transceiver and a second radio transceiver, wherein at least the second transceiver is configurable to provide a communication channel with either of the first configuration or the second configuration,
and the central unit is configured to transmit the offer using the first transceiver, and to configure the second transceiver, on reception of the acceptance message from the node, to enable reception of the data transmitted by the node using a communication channel according to the second configuration.

2. A security system monitoring system as claimed in claim 1, wherein the communication channel according to first configuration comprises a first frequency and the communication channel according to second configuration comprises a second frequency.

3. A security monitoring system as claimed in claim 2, wherein the central unit is configured to provide the offer of the communication channel according to the second configuration in the form of an identifier or code word.

4. A security monitoring system as claimed in claim 3, wherein the central unit is configured to provide the offer including identifiers for a multiplicity of alternative communication channels for the node to transmit data for reception by the second radio frequency transceiver.

5. A security monitoring system as claimed in claim 4, wherein at least two of the alternative communication channels use the same frequency but provide different bitrates.

6. A security monitoring system as claimed in any one of the preceding claims, wherein the node is configured to perform a determination of radio frequency conditions.

7. A security monitoring system as claimed in claim 6 as dependent on claim 4, wherein the node is configured to make a choice between the alternative communication channels based on the result of the determination of radio frequency conditions.

8. A security monitoring system as claimed in any one of the preceding claims, wherein the node includes or is connected to an image source, and the data are image data.

9. A security monitoring system as claimed in any one of the preceding claims, wherein the central unit is configured to transmit the offer to the node as a consequence of receiving notice of a security event.

10. A security monitoring system as claimed in claim 9, wherein the security event is the output of a motion sensor, a microphone, or of a door or window opening sensor.

11. A security monitoring system as claimed in any one of the preceding claims, wherein the first and second frequencies are within the 863 to 870MHz frequency band.

12. A security monitoring system as claimed in claim 11, wherein the second frequency is between 868 and 870MHz.

13. A security monitoring system as claimed in any one of the preceding claims, wherein the central unit is configured to store information about frequencies and bitrates supported by the node.

14. A security monitoring system as claimed in claim 13, wherein the node is configured to provide the information to the central unit when the node is installed in the system.

15. A security monitoring system as claimed in claim 14, wherein the node is configured periodically to provide the central unit with updated information about frequencies and bitrates supported by the node.

16. A security monitoring system as claimed in any of claims 13 to claim 15, wherein the central unit is configured to use the stored information in determining parameters of the offer made to the node.

17. A method of controlling data transmission from a battery-powered node to a central unit of a security monitoring system, the node including a non-Wi-Fi radio frequency transceiver for communication with the central unit, the non-Wi-Fi transceiver being operable at a first frequency, and at a second frequency;
the method comprising:
receiving from the central unit at the first frequency, an offer of a communication channel at the second frequency for the node to transmit data for reception by the central unit;
transmitting an acceptance message to the central unit at the first frequency; and
subsequently
transmitting data to the central unit at the second frequency.

18. A method as claimed in claim 17, including
determining a response to an offer that includes identifiers for a selection of alternative communication channels for the node to transmit data for reception by the central unit, the determination being based at least in part on the node's ability to support an offered communication channel.

19. A method as claimed in claim 17 or 18, including performing by the node a determination of radio frequency conditions and using the result .

20. A method as claimed in claim 19 as dependent on claim 18, wherein the determining of a response is also based on results of the determination of radio frequency conditions.

21. A central unit for a security monitoring system that includes a node having a node non-Wi-Fi radio frequency transceiver for communication with the central unit, the node non-Wi-Fi radio frequency transceiver being operable at first and second frequencies, the central unit comprising:
at least one radio frequency transceiver that is configurable to provide a communication channel with either of a first configuration and a second configuration, and a controller for controlling the radio frequency transceiver(s);
the central unit being configured to:
transmit using a communication channel according to the first configuration an offer to the node of a communication channel of the second configuration for the node to transmit data for reception by the central unit; and,
on reception of an acceptance message from the node, to configure one of the at least one radio frequency transceivers with the second configuration to enable reception of the data transmitted by the node;
wherein the at least one radio frequency transceiver comprises a first radio transceiver and a second radio transceiver, wherein at least the second transceiver is configurable with either of the first configuration and the second configuration,
and the central unit is configured to transmit the offer using the first transceiver, and to configure the second transceiver, on reception of the acceptance message from the node, to enable reception of the data transmitted by the node using a communication channel according to the second configuration.

22. A central unit as claimed in claim 21, wherein the first configuration comprises a first frequency and the second configuration comprises a second frequency.

23. A central unit as claimed in claim 22, wherein the central unit is configured to provide the offer of the communication channel at the second frequency in the form of an identifier or code word.

24. A central unit as claimed in claim 23, wherein the central unit is configured to provide the offer including identifiers for a selection of alternative communication channels for the node to transmit data for reception by the second radio frequency transceiver.

25. A central unit as claimed in claim 24, wherein at least two of the alternative communication channels use the same frequency but provide different bitrates.

26. A battery-powered node for a security monitoring system having a central unit comprising
at least one radio frequency transceiver configurable to provide a communication channel with either of a first configuration or a second configuration, the node comprising:
a node non-Wi-Fi radio frequency transceiver operable both for communication with the central unit using a communication channel according to the first configuration, and for communication with the central unit using a communication channel according to the second configuration, and a controller for controlling the node non-Wi-Fi radio frequency transceiver;
the node being configured, on receiving an offer, transmitted from the central unit using a communication channel according to the first configuration, of a communication channel according to the second configuration for the node to transmit data using a communication channel according to the second configuration, to transmit an acceptance message to the central unit using a communication channel according to the first configuration, and thereafter to transmit data to the central unit using a communication channel according to the second configuration.

27. A node as claimed in claim 26, wherein the communication channel according to first configuration comprises a first frequency and the communication channel according to second configuration comprises a second frequency.

28. A node for a security monitoring system as claimed in claim 26 or 27, further comprising at least one sensor.

29. A node for a security monitoring system as claimed in any one of claims 26 to 28, further comprising at least one store for storing sensor data to be transmitted to the central unit.

30. A node as claimed in any one of claims 26 to 29, wherein the node is configured to determine a response to an offer that includes identifiers for a selection of alternative communication channels for the node to transmit data for reception by a second radio frequency transceiver of the central unit, the determination being based at least in part on the node's ability to support an offered communication channel.

31. A node as claimed in any one of claims 26 to 30, wherein the node is configured to perform a determination of radio frequency conditions.

32. A node as claimed in claim 31 as dependent on claim 30, wherein the node is configured to determine the response based also on results of the determination of radio frequency conditions.

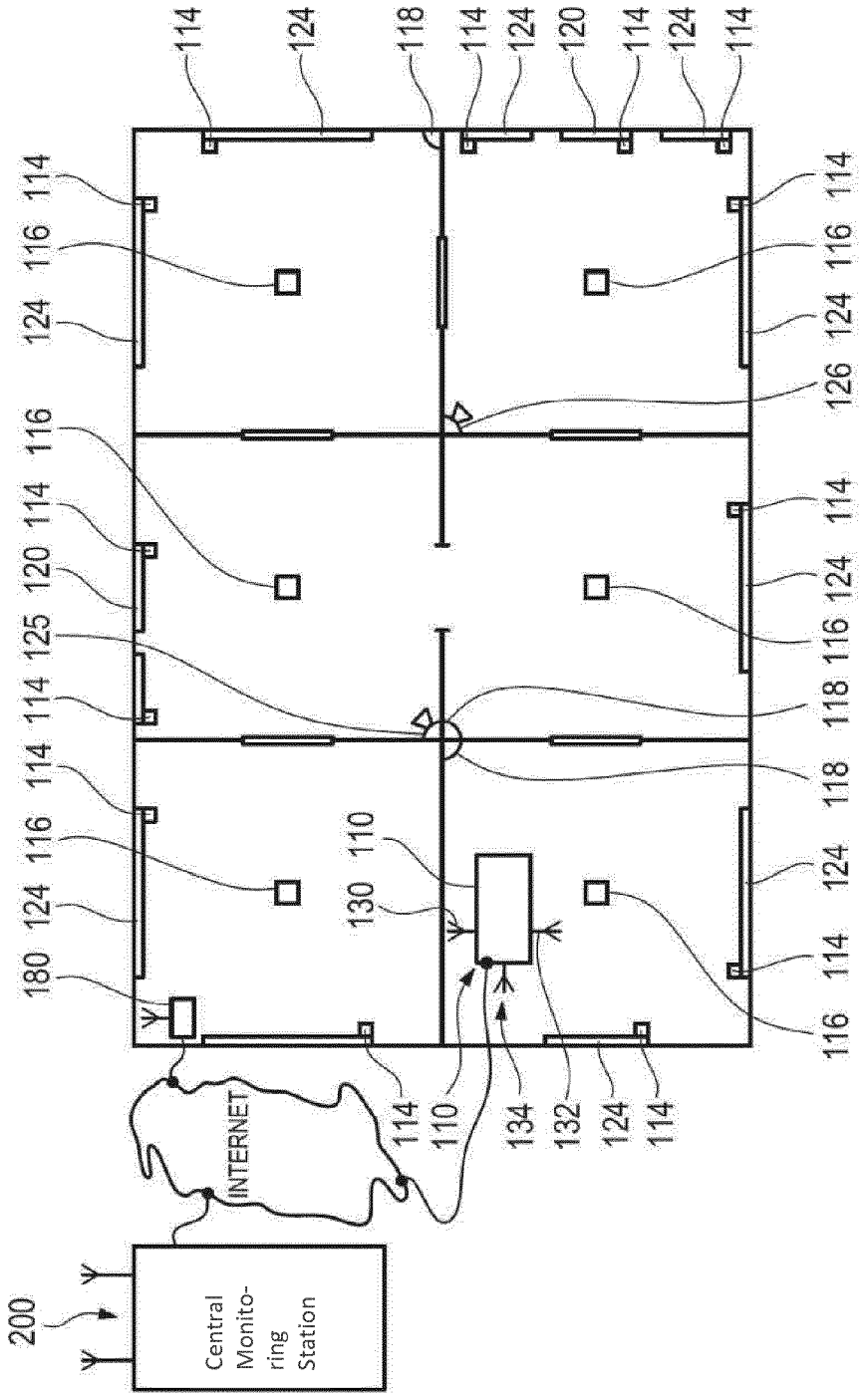
114
124
118
114
124
120
114
124
114
116
124
126
116
114
120
125
114
114
116
124
180
110
130
134
132
124
114
INTERNET
200
Central Monito-ring Station

Fig. 1

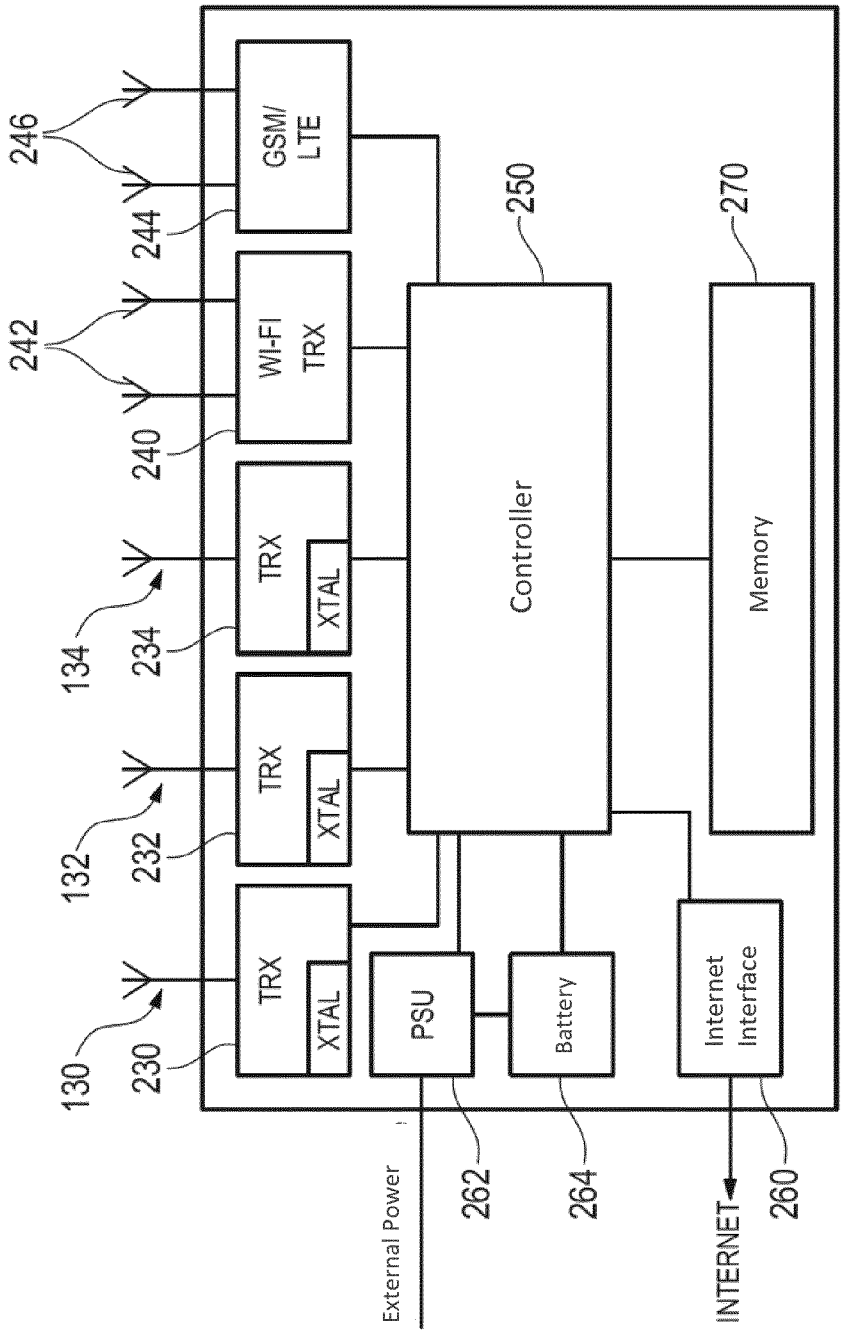
246
244
242
240
134
234
132
232
130
230
GSM/
LTE
WI-FI
TRX
TRX
XTAL
TRX
XTAL
TRX
XTAL
250
Controller
270
Memory
PSU
Battery
Internet
Interface
External Power
262
264
INTERNET
260

Fig. 2

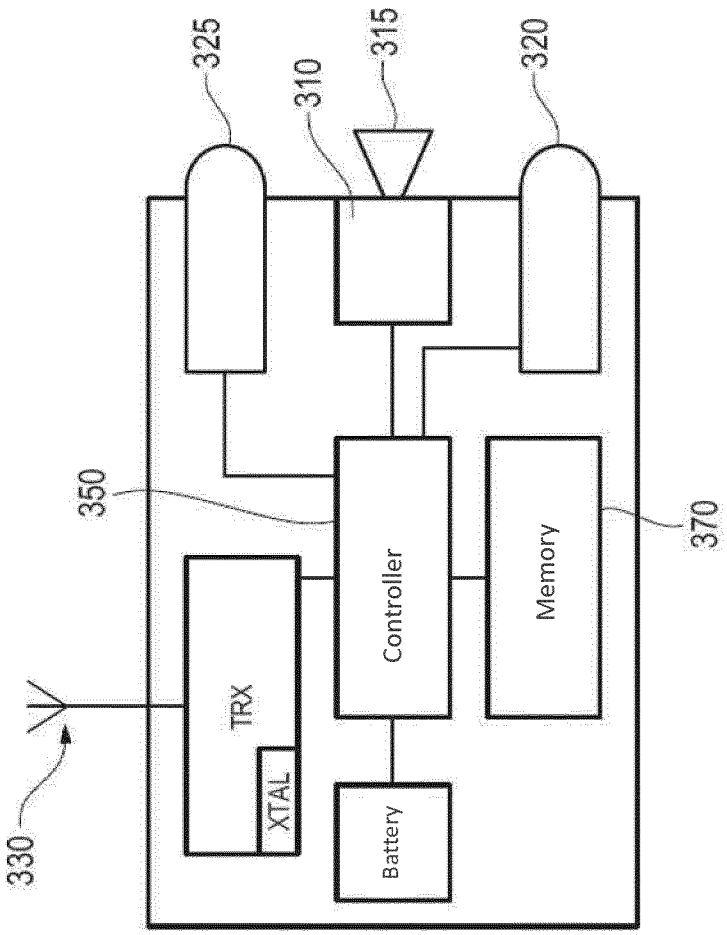
325
310
315
320
350
370
Controller
Memory
TRX
XTAL
Battery
330

Fig. 3

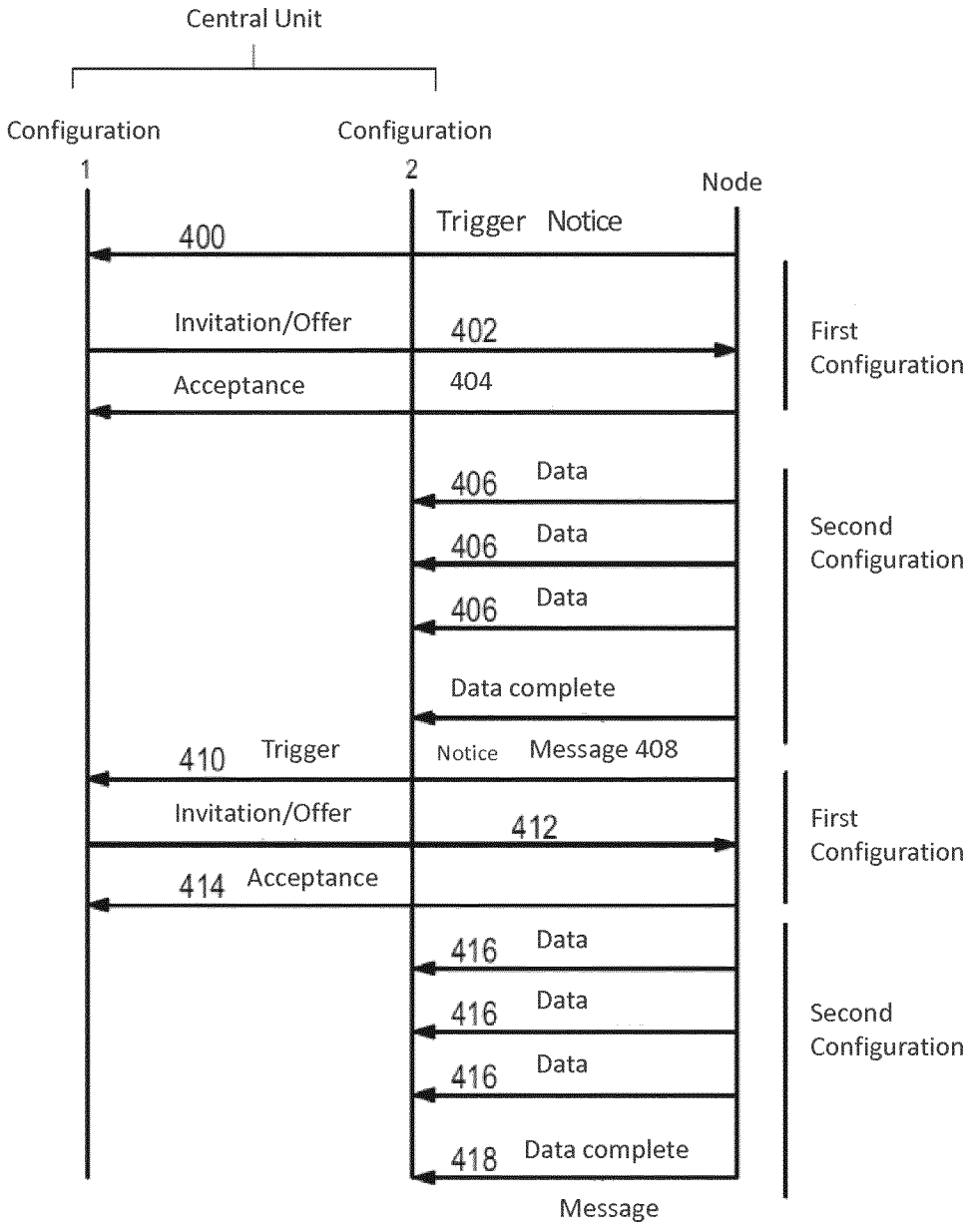
Central Unit
Configuration 1
Configuration 2
Node
400
Trigger Notice
Invitation/Offer
402
Acceptance
404
First Configuration
406
Data
406
Data
406
Data
Data complete
Second Configuration
410
Trigger
Notice
Message 408
Invitation/Offer
412
414
Acceptance
First Configuration
416
Data
416
Data
416
Data
418
Data complete
Second Configuration
Message

Fig. 4

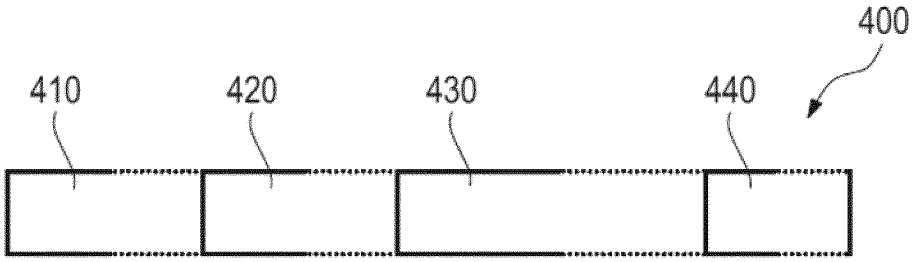

Fig. 5

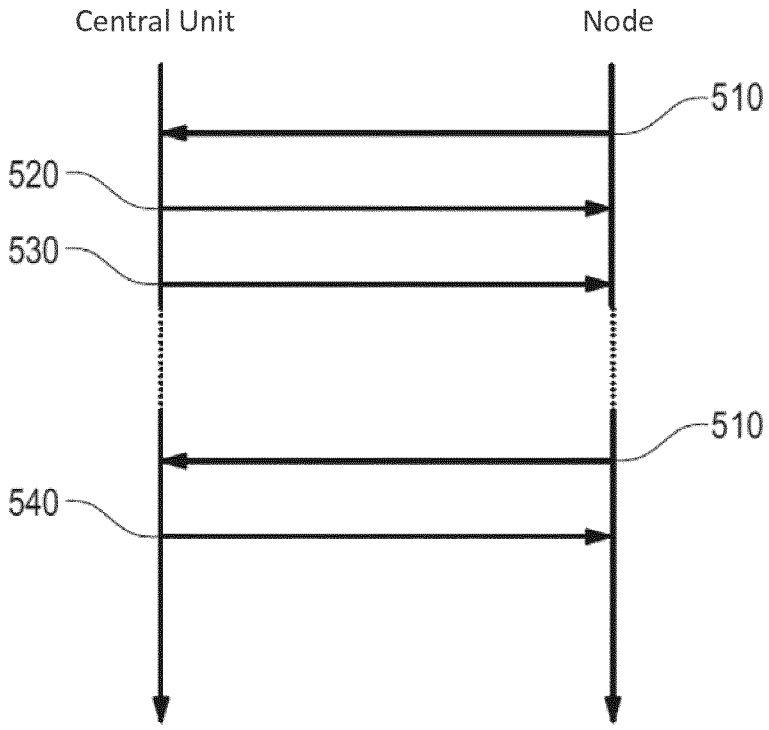

Fig. 6

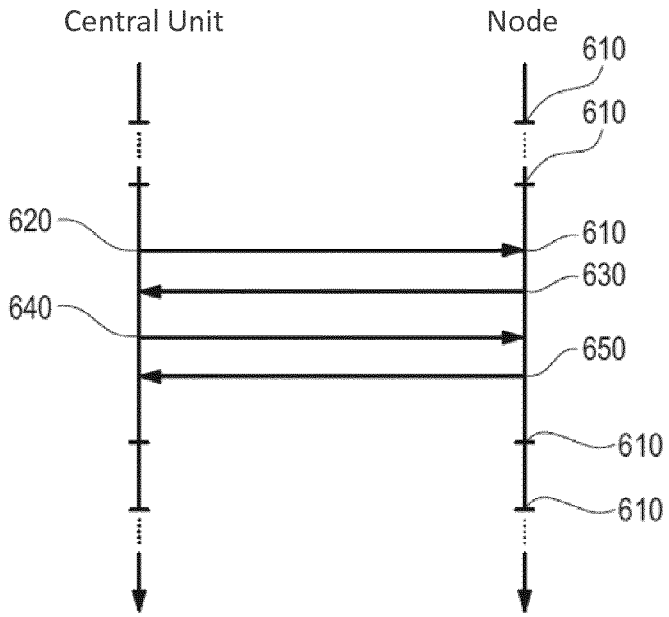
Central Unit
Node
610
610
620
610
630
640
650
610
610

Fig. 7

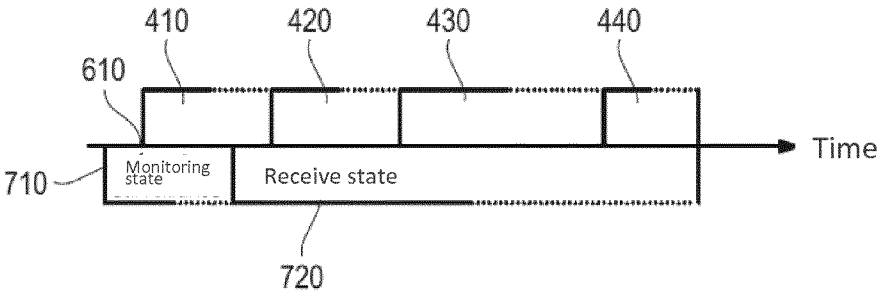
410
420
430
440
610
Time
710
Monitoring state
Receive state
720

Fig. 8

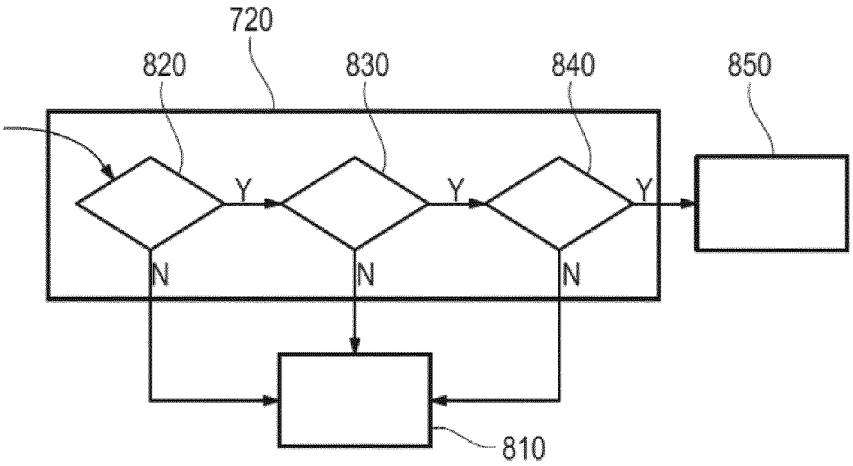

Fig. 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2019/072517

A. CLASSIFICATION OF SUBJECT MATTER
INV. G08B13/196 H04N7/18 H04B1/74 H04B1/04 H04L29/08
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G08B H04N H04B H04L

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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/11833 A1 (BERKELEY CONCEPT RES CORP [US]) 15 February 2001 (2001-02-15) page 1 - page 18 figures 2-7 -----	1-32
A	US 2016/365885 A1 (HONJO HIROFUMI [US] ET AL) 15 December 2016 (2016-12-15) paragraph [0043] - paragraph [0069] paragraph [0094] - paragraph [0107] paragraph [0134] - paragraph [0155] paragraph [0215] - paragraph [0230] paragraph [0291] - paragraph [0304] figures 1,2,6,9,14,15A,15B,23A-23F -----	1-32
A	US 8 050 206 B2 (MICROPOWER TECHNOLOGIES INC [US]) 1 November 2011 (2011-11-01) column 10 - column 27 figures 1-5 -----	1-32

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 October 2019	05/11/2019

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	Kokkinos, Titos

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2019/072517

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0111833 A1	15-02-2001	NONE	
US 2016365885 A1	15-12-2016	US 2016365885 A1	15-12-2016
		US 2017207806 A1	20-07-2017
US 8050206 B2	01-11-2011	EP 2100454 A2	16-09-2009
		US 2010141762 A1	10-06-2010
		US 2011134243 A1	09-06-2011
		US 2012147184 A1	14-06-2012
		US 2015130935 A1	14-05-2015
		US 2016127700 A1	05-05-2016
		US 2017301201 A1	19-10-2017
		US 2019246072 A1	08-08-2019
		WO 2008064270 A2	29-05-2008