

(19)



(11)

**EP 4 073 773 B1**

(12)

## EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention  
of the grant of the patent:  
**31.01.2024 Bulletin 2024/05**

(51) International Patent Classification (IPC):  
**G08B 25/00** (2006.01) **G08B 25/10** (2006.01)  
**G08B 29/24** (2006.01)

(21) Application number: **20819747.5**

(52) Cooperative Patent Classification (CPC):  
**G08B 25/007; G08B 25/004; G08B 25/10**

(22) Date of filing: **07.12.2020**

(86) International application number:  
**PCT/EP2020/084902**

(87) International publication number:  
**WO 2021/116025 (17.06.2021 Gazette 2021/24)**

### (54) SECURITY MONITORING SYSTEM

SICHERHEITSÜBERWACHUNGSSYSTEM

SYSTÈME DE SURVEILLANCE DE SÉCURITÉ

(84) Designated Contracting States:  
**AL AT BE BG CH CY CZ DE DK EE ES FI FR GB  
GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO  
PL PT RO RS SE SI SK SM TR**

(30) Priority: **11.12.2019 EP 19215371**

(43) Date of publication of application:  
**19.10.2022 Bulletin 2022/42**

(73) Proprietor: **Verisure Sàrl**  
**1290 Versoix, Geneva (CH)**

(72) Inventor: **BLOMÉ, Per Olof**  
**1290 Versoix, Geneva (CH)**

(74) Representative: **Prinz & Partner mbB**  
**Patent- und Rechtsanwälte**  
**Rundfunkplatz 2**  
**80335 München (DE)**

(56) References cited:  
**EP-A1- 2 542 011 WO-A2-2014/188282**  
**US-A- 5 148 148 US-A1- 2009 204 265**  
**US-A1- 2018 014 241 US-B2- 7 856 047**

**EP 4 073 773 B1**

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

**Description****TECHNICAL FIELD**

**[0001]** The present invention relates to a security monitoring system for monitoring premises, a node and a central unit for such a system, methods of operating the security monitoring system, the node and the central unit, and a method of compensating for differences between the operating frequency of a crystal oscillator of a central unit of a security monitoring system and a crystal oscillator of a node of the security monitoring system.

**BACKGROUND**

**[0002]** 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 of various kinds to detect the opening and closing of doors and windows, or their attempted forcing or breaking, 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. (herein generally referred to as "nodes"), and which processes received notifications and determines a response. The central unit is typically linked to the various nodes wirelessly, rather than by wires, since this facilitates installation (making it quicker and therefore potentially cheaper) and also provides 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 typically have an autonomous power supply, such as a battery, rather than mains powered.

**[0003]** Alternatively, a security monitoring system may include such 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.

**[0004]** With wireless connectivity between nodes and the central unit, the area that can be protected by a security monitoring system will depend on the range of the wireless signals. As living accommodations are getting larger and there is a need to protect also building annexes, the range of the wireless signals becomes the limiting factor.

**[0005]** 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, cameras, etc.. 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. Consequently, controlling power consumption in the nodes is a high priority.

**[0006]** In both centrally-managed and self-contained security monitoring systems it is also desirable for nodes and other elements of the system to have a long service life, of for example at least 10 to 15 years, despite the fact that the crystal controlled oscillators used both in nodes and the central unit can be expected to change their resonant frequency significantly over this timescale.

**[0007]** Further to this, it is very important to ensure a swift and timely delivery of notifications and alarms from the node to the CMS.

**[0008]** EP2542011A1 concerns a listen before talk frequency agile radio synchronisation technique. A radio frequency communication system includes a transmitter that selects a frequency channel from among multiple frequency channels available to the transmitter and to a receiver, listens to ensure that a selected channel is unused before transmitting, and sends a preamble longer in time than a receiver scan time during which the receiver is operable to scan all frequency channels available to transmitter and receiver for the preamble. This enables receivers to scan all channels to find the preamble, and lock on to the new channel to receive subsequent transmitted data while the preamble is being transmitted without prior knowledge of the transmitter's new frequency. In a further example, the preamble data transmitted comprises encoded data that the receivers can read and recognize as addressed to the intended receiver, ensuring that the transmitter re-establishes a communications link with the intended receiver or receivers.

**[0009]** The use of scanning radios in a frequency agile listen-before-talk radio environment is said to enable the transmitting radio to determine whether a channel is occupied or has a high level of noise or interference before changing

frequencies, such that the transmitter can simply select another frequency or channel and transmit once it has been determined that a channel is available. A further advantage of using a listen-before-talk approach is said to be that it exempts a transmitter from this duty cycle limitation "as it is presumed that the listen-before-talk system enforces some fairness in use of available time on a limited frequency spectrum. This makes 868MHz radios employing listen-before-talk technologies desirable in that they are not subject to the duty cycle limitations imposed to ensure other devices an opportunity to use the same frequency channels".

## SUMMARY

**[0010]** The invention is defined by the independent claims 1, 3 and 8 and by claim 13.

**[0011]** According to a first aspect, the present invention provides a method of compensating for differences between the operating frequency of a crystal oscillator of a central unit of a security monitoring system and a crystal oscillator of a node of the security monitoring system, the method comprising:

tuning a receiver of the central unit to a first frequency sub-channel of multiple frequency sub-channels that together make up a predetermined broader frequency channel;  
 listening for a preamble from the node on the first frequency sub-channel;  
 in the event that no valid preamble is received on the first frequency sub-channel within a predetermined period, tuning the receiver to a second of the multiple frequency sub-channels and listening for a preamble from the node on the second frequency sub-channel; and repeating the tuning and listening process until a valid preamble is received or until all of the multiple frequency sub-channels have been used;  
 in the event that a valid preamble is received on one of the multiple frequency sub-channels, listening for a synch word, and upon detection of a valid synch word causing a radio frequency transceiver of the central unit to transmit an acknowledgement on a radio frequency within the predetermined frequency channel;  
 detecting an offset between the radio frequency of the carrier on which the valid preamble was received and the centre frequency of the predetermined frequency channel;  
 in the event that the offset exceeds a predetermined threshold, transmitting from the central unit information regarding the offset to enable the node to adjust the operating frequency of a transceiver of the node based on the information.

**[0012]** Such a method may further comprise further comprising adjusting the operating frequency of the node (114, 118, 125, 126) based on the information regarding the offset.

**[0013]** According to a second aspect the present invention provides a central unit for a security monitoring system, the central unit having at least one radio frequency transceiver, and a controller to control the at least one radio frequency transceiver, the central unit being configurable to provide a first RF communication mode and an alternative long range communication mode, the first communication mode supporting a higher maximum bitrate than the long range mode, and the long range mode supporting a greater transmission range than the first mode; the controller being configured to:

control a radio frequency transceiver of the central unit to tune to one of multiple different radio frequency sub-channels that together make up the long-range communication channel and to listen for a preamble transmitted by a node of the security monitoring system, and in the event that no preamble is detected within a predetermined period to control said radio frequency transceiver of the central unit to tune to another of the multiple different radio frequency sub-channels to listen for a preamble transmitted by the node, and to repeat this procedure until either all the multiple different radio frequency sub-channels have been used or a preamble has been detected;  
 and, in the event that a preamble is detected, to listen for a synch word, and upon detection of a valid synch word to cause a radio frequency transceiver of the central unit to transmit an acknowledgement on a radio frequency within the long-range communication channel, and, thereafter to communicate with the node using a radio frequency within the long-range communication channel; wherein the central unit is configured, based on the frequency on which the preamble from the node was received, to estimate the accuracy of a crystal oscillator of the node, and if the estimated accuracy is less than a predetermined level to provide a feedback signal to the node, based on that estimate, to enable the node to compensate for inaccuracy of the crystal oscillator when tuning the node radio frequency transceiver.

**[0014]** In central units according to the second aspect, the controller of the central unit may be configured to transmit the acknowledgement on the radio frequency sub-channel on which the valid synch word was received.

**[0015]** In such central units the multiple different radio frequency sub-channels may be contiguous virtual sub-channels within a long-range communications channel that is defined by a pair of guard bands.

**[0016]** Such central units may be configured to use the same radio frequency transceiver to transmit messages using the first RF communication mode and using the long range communication mode.

**[0017]** In such central units, the radio frequency transceiver that is used to tune to the multiple different radio frequency sub-channels and to listen for a preamble transmitted by the node may be configured to use Digital Signal Arrival (DSA) to detect a valid preamble pattern.

**[0018]** Central units according to any variant of the second aspect may be configured to determine the RSSI for communications received from the node (114, 118, 125, 126) using the long range communication mode, and optionally in the event that the determined RSSI is above a predetermined threshold, the central unit (110) may be configured to issue an instruction to the node (114, 118, 125, 126) to switch from the long range communication mode to the first communication mode.

**[0019]** According to a third aspect, the present invention provides a node for a security monitoring system, the node having a node radio frequency transceiver configurable to provide a first RF communication mode and an alternative long range communication mode, the first communication mode supporting a higher maximum bitrate than the long range mode, and the long range mode supporting a greater transmission range than the first mode; the controller of the node being configured to:

attempt to establish communication with a central unit of the security monitoring system using the long range communication mode by:

transmitting a message comprising a preamble followed by a synch word on a frequency within a long-range communications channel, and

listening for an acknowledgement from the central unit on a frequency within the long-range communications channel;

and, in the event that an acknowledgement is received from the central unit on one of the multiple different frequencies, to communicate with the central unit using a frequency within the long-range communication channel; wherein the node controller (350) is configured to use a crystal oscillator feedback signal from the central unit to compensate for inaccuracy of the crystal oscillator (360) when tuning the node radio frequency transceiver (340).

**[0020]** With the node of the third aspect the node controller may be configured to control the node transceiver to communicate with the central unit using the frequency on which an acknowledgement was received from the central unit.

**[0021]** The node of the third aspect may be configured, on initially being triggered, to attempt to establish direct communication with the central unit using the first RF communication mode, and, if the node is unable to establish direct communication with the central unit using the first configuration, to attempt to establish direct communication with the central unit using the long range communication mode.

**[0022]** The node of the third aspect may be further configured, when attempting to establish direct communication with the central unit using the first RF communication mode, to first attempt communication using the frequency on which the node last received an acknowledgement from the central unit.

**[0023]** The node may be further configured, on establishing direct communication with the central unit to receive an acknowledgement from the central unit to exchange security keys and system settings using the communication mode that was used by the node to establish direct communication with the central unit, and subsequently to communicate with the central unit directly using that communication mode.

**[0024]** According to a fourth aspect there is provided a security monitoring system comprising a central unit according to the second aspect, and one or more nodes according to the third aspect.

**[0025]** In security monitoring systems of the fourth aspect, the controller of the central unit may be configured to transmit the acknowledgement on the radio frequency sub-channel on which the preamble and valid synch word were received, the node controller being configured to control the node transceiver to transmit on the centre frequency of the long-range communications channel.

**[0026]** In security monitoring systems of the fourth aspect, the node controller may be configured to control the node transceiver to transmit on the centre frequency of the long-range communications channel.

**[0027]** In security monitoring systems of the fourth aspect, the multiple different radio frequency sub-channels may be contiguous virtual sub-channels within a long-range communications channel that is defined by a pair of guard bands.

**[0028]** The multiple different radio frequency sub-channels may be provided by at least 6 different radio virtual sub-channels, for example 8 or 10 sub-channels.

**[0029]** Each of the sub-channels may span a frequency range of no more than 5kHz, for example each of the sub-channels may span a frequency range of between 1.5 and 3 kHz.

**[0030]** In any of these security monitoring systems the node may be configured to attempt to establish communication with the central unit using the first communication mode prior to attempting to establish communication with the central unit using the long range communication mode, and only on failing to establish communication with the central unit using the first communication mode to attempt to establish communication with the central unit using the long range communication mode.

**[0031]** In any of these security monitoring systems the central unit may be configured to use the same radio frequency

transceiver to transmit messages using the first RF communication mode and using the long range communication mode.

**[0032]** In any of these security monitoring systems the preambles transmitted by the node in the long range mode may be at least 10 bytes long, for example at least 12 bytes or at least 15 or 16 bytes long.

**[0033]** In any of these security monitoring systems the data rate of the long range communication mode may be 20% or less, for example 10%, of the data rate of the first RF communication mode

**[0034]** In any of these security monitoring systems the long range communication mode may operate in the ISM g3 band of 869.4 - 869.65 MHz, in the ISM band of 869.65 to 869.7 MHz, or in the ISM g4 band of 869.7 to 870.0 MHz.

**[0035]** In any of these security monitoring systems the first RF communication mode may operate in the ISM g1 band of 868.0 - 868.6 MHz or in the ISM g2 band of 868.7 to 869.2 MHz.

**[0036]** In any of these security monitoring systems the central unit radio frequency transceiver that is used to tune to one of the multiple different radio frequency sub-channels and to listen for a preamble transmitted by the node is preferably configured to use Digital Signal Arrival (DSA) to detect a valid preamble pattern. This enables the central unit to recognise preamble patterns quickly, meaning that frequency lock between the central unit and the node can be achieved more quickly.

**[0037]** According to a fifth aspect, a non claimed example provides a method of operating a security monitoring system, the system comprising:

a central unit, having at least one radio frequency transceiver, and a control unit to control the at least one radio frequency transceiver, the central unit being configurable to provide a first RF communication mode and an alternative long range communication mode, the first communication mode supporting a higher maximum bitrate than the long range mode, and the long range mode supporting a greater transmission range than the first mode;

a node comprising a node radio frequency transceiver operable in the first communication mode, for direct communication with the central unit, and in the long range communication mode for direct communication with the central unit, and a controller for controlling the node radio frequency transceiver;

the method comprising:

attempting, using the controller of the node, to establish communication with the central unit using the long range communication mode by:

transmitting a message comprising a preamble followed by a synch word on a frequency within the long-range communication channel, and

listening for an acknowledgement from the central unit on a frequency within the long-range communication channel;

and, in the event that an acknowledgement is received from the central unit on a frequency within the long-range communication channel, to communicate with the central unit using a frequency within the long-range communication channel; and

controlling, using the control unit of the central unit, a central unit radio frequency transceiver to tune to one of the multiple different radio frequency sub-channels that together make up the long-range communication channel and to listen for a preamble transmitted by the node, and in the event that no preamble is detected within a predetermined period controlling the central unit radio frequency transceiver to tune to another of the multiple different radio frequency sub-channels to listen for a preamble transmitted by the node, and repeating this procedure until either all the multiple different radio frequency sub-channels have been used or a preamble has been detected;

and, in the event that a preamble is detected, listening for a synch word, and upon detection of a valid synch word causing a radio frequency transceiver of the central unit to transmit an acknowledgement on a radio frequency within the long-range communication channel; the method further comprising the central unit estimating, based on the frequency on which the message from the node was received, the accuracy of a crystal oscillator of the node, and if the estimated accuracy is less than a predetermined level providing a feedback signal to the node, based on that estimate; and the node controller using the feedback signal provided by the central unit to compensate for inaccuracy of the crystal oscillator when tuning the node radio frequency transceiver.

**[0038]** According to a sixth aspect, a non claimed example provides a method of operating a central unit of a security monitoring system,

the central unit having at least one radio frequency transceiver, and a controller to control the at least one radio frequency transceiver, the central unit being configurable to provide a first RF communication mode and an alternative long range communication mode, the first communication mode supporting a higher maximum bitrate than the long range mode, and the long range mode supporting a greater transmission range than the first mode;

the method comprising:

controlling a radio frequency transceiver of the central unit to tune to one of the multiple different radio frequency sub-channels that together make up a long-range communication channel and to listen for a preamble transmitted by the node, and in the event that no preamble is detected within a predetermined period controlling said radio frequency transceiver of the central unit to tune to another of the multiple different radio frequency sub-channels and listening for a preamble transmitted by the node, and repeating this procedure until either all the multiple different radio frequency sub-channels have been used or a preamble has been detected;  
and, in the event that a preamble is detected, listening for a synch word, and upon detection of a valid synch word causing a radio frequency transceiver of the central unit to transmit an acknowledgement on a radio frequency within the long-range communication channel, and, thereafter communicating with the node using a radio frequency within the long-range communication channel; the method further comprising estimating, based on the frequency on which the preamble from the node was received, the accuracy of a crystal oscillator of the node, and if the estimated accuracy is less than a predetermined level to providing a feedback signal to the node, based on that estimate, to enable the node to compensate for inaccuracy of the crystal oscillator when tuning the node radio frequency transceiver.

**[0039]** In the method of any of the fifth or sixth aspects of the invention, the multiple different radio frequency sub-channels are preferably contiguous virtual sub-channels within a communications channel that is defined by a pair of guard bands.

**[0040]** According to a seventh aspect, a non claimed example provides a method of operating a node of a security monitoring system, the node having a node radio frequency transceiver configurable to provide a first RF communication mode and an alternative long range communication mode, the first communication mode supporting a higher maximum bitrate than the long range mode, and the long range mode supporting a greater transmission range than the first mode; the method comprising:  
attempting to establish communication with the central unit using the long range communication mode by:

transmitting a message comprising a preamble followed by a synch word on a frequency within the long-range communication channel., and  
listening for an acknowledgement from the central unit on a frequency within the long-range communication channel.;  
and, in the event that an acknowledgement is received from the central unit on a frequency within the long-range communication channel., communicating with the central unit using a frequency within the long-range communication channel; the method further comprising the node controller using a crystal oscillator feedback signal from the central unit to compensate for inaccuracy of the crystal oscillator when tuning the node radio frequency transceiver.

**[0041]** In any of the first to seventh aspects, the node's attempt to communicate with the central unit may be a consequence of the node being triggered by an event such as detection of the opening of a door or window, detection of movement, etc.. Alternatively, the node's attempt to communicate may occur when checking in with the central unit for example a periodic checking in for updates or for synchronisation.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0042]** 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; and

Figure 3 is a schematic drawing showing features of a node of the security monitoring system according to an embodiment of the invention.

## DETAILED DESCRIPTION OF EMBODIMENTS

**[0043]** 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

**[0044]** Generally, in high security systems, nodes are in bidirectional contact with the central unit, being able to receive information from, as well as to send information to, the Central Unit 110. For example, some 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 ensure 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.

**[0045]** When not listening for synchronisation beacons, and when not sending an event notification, the radios of the nodes 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 triggered by low battery power functionality of the detector, or when they or another associated sensor detects movement or when instructed to power up by the Central Unit 110.

**[0046]** 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, meaning that the transceiver must be powered up for at least the duration of the transmission, and consequently consumes a lot of power. Also, there are, at many frequencies, regulations controlling how much time a device is allowed to wirelessly transmit within a certain period of time. 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.

**[0047]** 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 the 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 preferably 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. Preferably one of the transceivers is dedicated to the long-range communication mode, while another of the transceivers is dedicated to providing a higher data-rate channel (e.g. a standard communication link).

**[0048]** 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) 200 that supports the domestic installation. The installation 100 includes a gateway or central unit, 110, also referred to as a control unit, 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 and diversity of connection between the gateway 110 and the monitoring centre 200. For additional security, the central unit 110, sensors and nodes of the system, and the monitoring centre may all 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.

**[0049]** 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, and/or magnetic contact and shock sensors (that also include an accelerometer for example to detect attempts to break the window or door). Each of the rooms of the building having the installation may be provided with a combined fire/smoke detector 116. In addition, several rooms have movement detectors 118, such as passive 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 or integrated 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 preferably 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 transceiver with an antenna 134 for wireless communication with the monitoring centre. Additionally, the central unit 110 may include a dedicated antenna arrangement, and associated transmitter/receiver or transceiver, 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. One or more of the nodes of the system, for example nodes including an image sensor such as a video camera, may also include Wi-Fi functionality in addition to an ISM or similar transceiver.

**[0050]** 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. That is, if there are two CUs, they 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 while the other CU can hear all and understand all communication between the other two - if it is not a range extension scenario.

**[0051]** 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.

**[0052]** 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 optionally a second transceiver 232 coupled to a second antenna 132. The transceivers 230 and 232 can each both transmit and receive, but a transceiver cannot both transmit and receive at the same time. Thus, the transceivers 230, 232 each operate in half duplex. Preferably a transceiver will use the same frequency to transmit and receive (although of course if the two transceivers are to operate simultaneously but in opposite modes, they will operate on different frequencies). The transceivers 230, 232 may be arranged such that one transceiver 230 uses a first frequency for transmit and receive and the second transceiver 232 uses the same first frequency for transmit and receive, i.e. the transceivers are arranged to operate in a diversity-like arrangement. Alternative, the second transceiver may, depending on configuration, be arranged to use a second frequency for transmit and/or receive. 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 central unit 110 also includes a crystal oscillator 251, which is preferably a temperature controlled or oven controlled crystal oscillator. This is used for system clocking and also frequency control of the transceivers. 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, 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 be a remote control or control panel 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, or it may for example be an image-capture device such as a video camera. Similarly, an interface enabling bidirectional communication over a Public Land Mobile Network (PLMN), such as GSM or LTE, may optionally be provided. Optionally, a third antenna 134 and associated ISM transceiver 234 may be provided, for example for communication with the monitoring centre 200 over, for example, the European 863MHz to 870MHz frequency band.

**[0053]** The first and second transceivers may both be tuneable ISM devices, operating for example in the European 863MHz 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, if present, may have different tuning ranges and optionally there is some overlap between these ranges.

**[0054]** Also, at least the second transceiver 232 may be used to support a long range channel, having a significantly

lower 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 longer range 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 particular, the second transceiver may be used to support what may be termed a long-range channel according to a second configuration while the first transceiver is used to support a regular range channel according to a first configuration. If the central unit only has one transceiver for communication with the nodes of the security monitoring system, that transceiver may be switched between the first and second configurations as required, under the control of a central unit controller, as will be explained.

**[0055]** 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:

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

**[0056]** In Eqn. 1, RBW is the bandwidth of the receiver. The maximum allowed sensitivity will increase with increased receiver bandwidth and the reason for this is that the thermal noise power N introduced to the receiver increases as the receiver bandwidth increases, Eqn. 2:

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

**[0057]** Where k is Boltzmann's constant in Joules per Kelvin (approx.  $1.381 \times 10^{-23}$  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:

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

**[0058]** The receiver will, as mentioned earlier, decode a received signal S into bits and the sensitivity is usually defined in BER. An alternative measure of the received signal quality may be a received energy per bit  $E_b$  versus noise Eqn. 5:

$$\frac{E_b}{N} \quad \text{Eqn. 5}$$

**[0059]** The relation between the BER and  $E_b/N$  is known in the art 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.

**[0060]** In order to maximize the link-budget of a wireless communication, the fraction presented in Eqn. 5 above has to be maximized. This is achieved either by increasing the energy per bit  $E_b$  or by decreasing the noise N. One straight forward approach would be to increase the energy per bit  $E_b$  by increasing the transmit power, but this is not always possible due to regulatory constraints, for example the regulations governing the use of the ISM bands in Europe specify a maximum transmit power. Energy is power over time and if a transmission burst of a power P consists of n bits and the transmission time is  $t_{trans}$ , the energy per bit  $E_b$  can be described according to Eqn. 6:

$$E_b = \frac{P \cdot t_{trans}}{n} \quad \text{Eqn. 6}$$

**[0061]** As seen in Eqn. 6, increasing the transmission time  $t_{\text{trans}}$  is an alternative way of increasing the energy per bit  $E_b$ . This is achieved simply by decreasing the bitrate of the transmission, since doing so will require an increased transmission time  $t_{\text{trans}}$  in order to transfer the same number of bits  $n$ .

**[0062]** Eqn. 2 teaches that the noise will increase with the receiver bandwidth, RBW, and Eqn. 6 teaches that decreasing the bitrate will increase the energy per bit,  $E_b$ . Consequently, a low bitrate received in a narrow bandwidth will increase the link budget, thereby potentially increasing the range of the link.

**[0063]** Generally, electronic devices in general and electronic devices comprising radio frequency circuitry in particular, uses one or more oscillator to generate base frequencies used for e.g. internal clocking. The oscillator is typically connected to a frequency synthesizer that is used to generate signals of frequencies relevant to the electronic device. Consequently, the oscillator is typically the most significant source of frequency errors in an electronic device. The following section will detail this and from the explanation above it is clear that regardless of terminology used, e.g. clock, oscillator etc., the same basic group of components and function is meant.

**[0064]** Having a narrow receiver bandwidth will make the receiving node more sensitive to frequency drift (both its own and that of the central unit's transmitter). Frequency drift arises from oscillator inaccuracy in the oscillator feeding the synthesizer of the RF circuitry. Typically this is a crystal oscillator, XO, or in less price sensitive devices, a temperature controlled crystal oscillator, TCXO, or even an oven controlled crystal oscillator, OCXO. The oscillator frequency will have an inherent error of a first Parts Per Million, PPM, a temperature drift of a second PPM and drift due to aging of a third PPM. The worst case frequency error is the sum of the first, second and third PPM. If the operating frequency is e.g. 869.5 MHz, the bitrate 2.4 kbps (such as might be used for a long-range channel) and the receiver bandwidth is 5 kHz (such as also might be used for a long-range channel), an oscillator frequency inaccuracy of just above 5 PPM would be enough for the RBW to lie outside the band of interest. Typically, the Central Unit of the security monitoring system comprises a relatively, compared to the node, accurate oscillator (and hence clock), typically being temperature controlled or oven controlled but with receiver bandwidths below 5kHz it will be challenging, or at least costly, for the Central Unit to have an accurate enough oscillator to ensure accurate enough transmission frequency to fit within the receiver window given its narrow receiver bandwidth (RBW). The frequency error will, as the skilled person understands, in a worst case be the sum of the worst case frequency error of the node added to worst case frequency error of the Central Unit (when the two frequencies have drifted apart). To further complicate matters, commercial constraints mean that the nodes must be produced at low cost, while high accuracy oscillators are expensive. Moreover, and very significantly, security monitoring system installations are typically expected to have installed lifetimes of 10 years or more, e.g. 15 years. Over this kind of timescale, even the most expensive crystal controlled oscillators can be expected to exhibit significant frequency drift, due to aging of the crystal, particularly for example in installations where the air quality is poor. Consequently, over the design lifetime of an installation, something needs to be done to address oscillator frequency drift.

**[0065]** Consequently, something needs to be done to address the issue of frequency drift, especially that from crystal ageing, in systems with narrow receiver bandwidths, in order to enable installed systems to work reliably for lifetimes of between 10 and 15 years.

**[0066]** 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 350 is coupled to a crystal controlled oscillator 360, which may also be coupled to the transceiver. 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.

**[0067]** In security monitoring systems according to embodiments of the invention the central unit is able to use at least two communication modes for communicating with the nodes of the system - one regular-range communication protocol (with a first configuration), and one long-range communication protocol (with a second configuration). The regular-range communication protocol comprises one or more one regular-range communication channel, and the long-range communication protocol comprises one or more long-range communication channels. Security monitoring systems according to embodiments of the invention may be configured to use only one of the regular-range communication channels for the regular-range communication protocol and only one of the long-range communication channels for the long range-communication protocol. The long-range communication channels defined by the long-range communication protocol have a lower bitrate and a smaller receiver bandwidth than the corresponding regular-range communication channels defined by the regular-range protocol.

**[0068]** The most effective way of improving range is to increase sensitivity. If one aims to improve sensitivity over that provided by a standard e.g. 38.4kbit/s data rate channel by 10dB, one typically needs to reduce bitrate considerably.

To get a suitable improvement in sensitivity, a bitrate of low kilobits per second will generally be required, for example of 5 kbps or less, e.g. 2.4kbps. To give a receiver, such as a receiver in the central unit, optimal sensitivity, the modulation index is preferably kept close to  $h=1$ , so with a bitrate of 2.4kbps the deviation could be set to around 1.2kHz. This gives quite a narrow occupied bandwidth of approximately 3.9kHz.

**[0069]** This quite narrow bandwidth put tough requirements on the accuracy of clock synchronization between nodes and the central unit. Using 2.4kbps we would need to have an accuracy of 0.5-1ppm or better than 600-900Hz. This would require expensive, accurate oscillators and there are still real challenges to handle ageing and long-term stability. Further out there will also be a rapid decline in sensitivity depending on the ability for the receiver to track the carrier and adjust filters.

The problems with the high requirements on the clock synch mean that it would be difficult or even impossible to achieve clock synch between the central unit and the nodes even with the most accurate oscillators. Thus a different approach would seem to be required.

A standard 25kHz narrow band channel was defined and the approximate occupied BW of the signal was set to 4kHz.

**[0070]** The solution adopted for embodiments of the present invention was to implement a kind of asynchronous automatic frequency hopping in a long-range receiver (generally of course this is the receiver function of a transceiver) in the central unit. A certain number of channels were defined that would be constantly cycled. The receiver's task is to quickly find the channel that corresponds to the frequency offset between the transceiver of the node and that of the central unit, without any prior knowledge other than the target centre frequency of the narrow band channel (to which the transceiver of the node would nominally be tuned). By making the preamble long enough to catch the worst case that the transmit channel was just missed, the asynchronous jumping scheme should not miss any packets.

**[0071]** A target channel frequency was set in the centre of the long-range channel, and depending on the accuracy of the clock synch between node clock and central unit clock there is an unknown frequency offset. This unknown offset we want to translate into a known subchannel. To achieve this the long-range channel is divided into a number of virtual channels (virtual in the sense that they are contiguous analogue sub-channels which are not separated by guard bands), based on the channel resolution needed to get good enough sensitivity. The long-range communication mode uses a narrow band frequency modulated signal. Nodes of the system will typically use a standard crystal and will generally attempt to transmit as close as possible to the centre of the long-range channel being used (of course determined based on the frequency of their own crystal oscillator).

The (long-range) receiver of the central unit will then continuously look for preambles on the sub-channels and as soon as there is a lock on a preamble the central unit will try to find a valid synch word. If the (long-range) receiver of the central unit is successful in receiving the message it will send an acknowledgement to the node, preferably on the same sub-channel as was used to receive the valid synch word. This ack can be sent promptly, and the assumption is that the node's crystal oscillator will be stable in this time frame and the node should be able to receive the ack (packet) from the central unit. With the chosen bandwidth to cover set at approximately 20kHz, 10 sub-channels with a 2kHz channel spacing can be used to cover the entire bandwidth. Clearly these parameters can be adjusted appropriately based on the particular system and system performance required. So for example fewer than 10 sub-channels, e.g. 5, 6, 7, 8, or 9 sub-channels may be used. Equally, more than 10 sub-channels may be provided, e.g. 11, 12, 13, 14 or 15 channels may be provided. Similarly, the channel spacing need not be 2kHz but may for example be anywhere in the range 1.5 to 3kHz.

**[0072]** The central unit is thus controlled to scan continuously through the set of pseudo channels and to try to detect the channel that the node is using based on the individual offset and inaccuracy of its crystal. When a valid preamble is found the cycling of the central unit through channels is stopped, and a clock synch is performed and the synch word is checked to see if it is a message of the system (i.e. it is determined whether or not the synch word is a valid one for the system).

Upon detection of a valid packet, or that preamble, synch, + CRC are correct an acknowledgement is sent, for example in accordance with ETSI regulations, on the same frequency and at the actual channel / frequency of the received packet.

**[0073]** The biggest challenge here is that the channels are not well defined with guard bands, but are simply a collection of analogue channels scattered over the discrete channel that we have defined, and the central unit's (long range) receiver has to decide which is the strongest channel and be able to lock on to the preamble on that channel.

The challenge with this approach is the time it takes to scan through all virtual sub channels and quickly determine if there is a valid preamble or not. To solve this we use digital signature (sometimes referred to as Digital Signal Arrival DSA) of a valid preamble so the receiver in only two bits can decide if the preamble is valid or not, and if not the receiver should jump to the next sub channel. The lack of guard bands is a challenge but we mitigate this by restriction the dynamics to only use long range on weak signals. After a valid preamble detect we still have enough preamble bits to do a full clock recovery and frequency offset measurement.

**[0074]** The configured regular-range communication channels may be used by all nodes whose link budgets allow for regular-range communication. This will often be possible for those nodes corresponding to the inside of a given premises, e.g. a house or an apartment. But nodes that are placed too far from the Central Unit, or for which signal attenuation is

likely to be higher than normal for other reasons (e.g. as a consequence of attenuation by walls/floors, etc. between the central unit and the relevant node), to be able to communicate using the regular-range communication protocol can be arranged to communicate using the configured long-range communication channel. This may be e.g. nodes mounted in a detached or semi-detached garage, outhouse, pool house etc. There are also situations where although the central unit and all the nodes of an installation are within 10, 20 or 30 metres, one or more of the nodes may be so located that RF signals between the node and the central unit suffer considerably increased attenuation compared to signals passing between the central unit and most of the other nodes of the installation. For example, the affected nodes may be on another floor to the central unit, for example in a basement or attic, and the construction of the intervening ceiling(s)/floor(s) may be such that RF signals are attenuated significantly on passage therethrough. Typically this can occur where the construction includes structural metalwork or reinforcement, or high density concrete or the like. Similar problems may occur even between rooms on the same floor, either through the use of structural metalwork or reinforcement, high density concrete, or even having intervening walls lined with books or files, for example. Also, there may be particular use cases for certain nodes that cause the link budget to deteriorate, one non limiting example could be sensors placed inside refrigerators, freezers or other appliances that have a shielding effect on radio waves.

**[0075]** In security monitoring systems according to embodiments of the invention that have both a long-range transceiver and a regular-range transceiver, the Central Unit will generally be arranged to monitor continuously the configured long-range communication channel and the configured regular-range communication channel (unless the relevant transceiver is itself transmitting). This means that in such systems there is at least one receiver (generally a transceiver operating in receive mode) of the Central Unit(s) in the security monitoring system listening to each configured channel.

**[0076]** When a new node is installed into a security monitoring system, it typically needs to login with the Central Unit of the system. A login procedure typically comprises exchanging security keys and system settings etc. The login procedure is typically initiated by the node desiring to log in, the node transmitting, sequentially on each of the communication channels available to the node, a login beacon (a "HELLO" message) comprising a message made up of a preamble, a synch word and a payload. After each login beacon is broadcast, the node waits (in receive mode) for a response from the Central Unit, if no response is received, the node changes communication channel and sends a new login beacon. If a response is received from the Central Unit, the node proceeds with the login procedure on the communication channel on which the response was received.

**[0077]** The initial login is, from a frequency perspective, open loop. The node has no concept of its frequency relative to the Central Unit other than perhaps e.g. a calibrated offset from the factory. If the RBW of the receiving device is in the region above 50 kHz this is typically no major issue but if the RBW is below 10 kHz there is a risk that the login beacon will be transmitted at a frequency outside the intended communication channel. It should be noted that there is no necessity for the transceivers in the node and in the central unit to operate with the same receiver bandwidth. For example, if the central unit increases its transmitted power, the node can reduce its RBW. The Rx/Tx link budgets node/CU should be balanced with regards to the complete receiver chain.

**[0078]** Login by a node to the configured long-range channel may be attempted upon failure to login on the available regular-range channels. Alternatively, the Central Unit may instruct a node (that has already been logged in to the Central Unit) to change to the configured long-range communication channel, in which case a frequency or frequency offset relating to the currently occupied frequency may be communicated from the Central Unit to the node. For example, the central unit may order the change based on CMS instructions. For example, when an alarm system suffers from recurrent supervision issues with a particular node (the node fails to communicate with the central unit for a certain period of time), this may be highlighted by service personnel of the CMS, and one possible solution would be to change to a long range configuration.

**[0079]** Also the CU may have functionality in itself to determine if there should be a change of protocol. In particular, the central unit may be configured to determine the RSSI of signals received from the various nodes of the system. If the central unit determines that the RSSI from a node using the long distance communication mode is higher than a certain threshold (signifying a higher than expected received signal strength), the central unit may instruct the relevant node to switch from the long range mode to the standard mode. Such a transition of course means that the relevant node will benefit from a higher bandwidth communication channel to the central unit, meaning that alerts and other messages can be sent from that node to the central unit in less time, resulting in less battery drain in the node and hence potentially longer battery life.

**[0080]** In embodiments of the invention, a node may be configured to "remember" long-range as the preferred protocol - for example having learnt it on initial installation. This would mean that in the case of battery change or loss of communication with the central unit, these cases triggering a new login sequence from the node, the node would in this case start the new login sequence using a long-range (second configuration) rather than a regular (first configuration) channel. Additionally, or alternatively, the nodes of the system may be configured to "remember" the communication parameters of their last communication session, whether long range or standard, and to use those remembered parameters when next trying to communicate with the central unit.

**[0081]** Generally, the Central Unit is the master and the frequency that it uses as the long-range communication

channel is what should be used. Nodes receiving messages on the long-range communication channel are configured to adjust their frequency to that of the Central Unit, for example this would be the case where communication and login is established but a small frequency error is detected by the node in receiving the CU transmission. This error is compensated in the node, each transceiver having a register indicating the frequency offset between the center frequency of the tuned RBW and the measured frequency of the received message.

**[0082]** If the Central Unit receives a message from a node, it may optionally acknowledge the message on the same centre frequency as the message was received on but have the acknowledgement specify a frequency offset from the current frequency that the node should use for all future communications. This may be employed as a typical acknowledgement on all acknowledgements sent from the Central Unit on the long-range communication channel.

**[0083]** Alternatively, and preferably, the central unit may be configured to utilize the narrow bandwidth of the modulation of the long-range signals from the nodes. When the long-range receiver of the central unit locks to the preamble from the node, the receiver gets a rough estimate of the crystal accuracy of the node compared to the crystal on the central unit. It can also determine an estimate of the distance in Hz between the centre frequency of the long-range transceiver of the central unit and the node transceiver's centre frequency. This information can be stored and compared with a predetermined threshold value, and if outside certain boundaries the discrepancy can be looped back to the node with a suggestion (or instruction) for the to update the offset of its crystal (to reduce the frequency offset between the transceiver of the node and the relevant transceiver of the central unit). Importantly, this technique can be used both to track and improve communication in semi fast crystal changes, but also to compensate more generally for ageing in the crystals. Ageing happens in all crystals, in nodes and in central units, but it is the difference between receiver and transmitter that is critical and by aligning all nodes to the crystal of the central unit the effects of ageing would no longer be an issue. The crystal inaccuracy of the central unit would not impact the system, only the accuracy in the measurement of the frequency offset by the central unit, and the resolution of frequency compensation and the nodes ability to handle rapid changes in the environment, like temperature. It will be appreciated that this approach to compensating for the effects of crystal ageing, and in particular differences between the effects of crystal ageing in nodes and in the central unit, is of general relevance and is not confined in its application to systems that include multiple communication modes (i.e. it is not solely applicable to systems that provide both standard and long-range communication channels).

#### Installation limitation

**[0084]** Typically in conventional security monitoring systems a minimum received signal strength (RSSI) limit is set, and for a node to be installed in the system the node must be close enough to the central unit to receive signals from the central unit at above that signal level. For example, such a limit may be set at e.g. -82dBm. Most significantly, we want to have a margin of at least 20dB in order to be able to cope with fading link conditions.

**[0085]** The power budgets may be set so that standard and long range operation would overlap, by for example approximately 10dB, so there would be a high probability that standard mode would work most of the time and long-range could therefore be used largely as a fall-back. Since the long-range channel is not only lower bitrate, but also adds frequency diversity, it effectively adds some extra robustness to the link.

#### Frequency band

**[0086]** The band 869.4-869.65MHz enables 10% duty cycle and a maximum power of 500mW ERP, which is 12dB above the other alarm channels used. Although the use of only one long-range channel has been described, more than one channel can be provided if required.

#### Energy budget

**[0087]** One of the major challenges with lower bitrate is to comply with the target energy budget. The lower bitrate will consume more power for the same traffic data so essentially there is a need to decrease the amount of data that need to be transferred to comply with energy budget. A sensible target battery life for nodes is 5 years of service, and the major limiting factors are: background current consumption in sleep mode, periodic update, and tamper detect. Alarm interactions are rare occasions in comparison.

#### Frequency band and additional channels

**[0088]** Although the described implementation of long-range uses only one channel 869.4-869.425MHz, it could be beneficial to implement support for more channels, for example to limit impact on other systems in areas where there are many competing RF sources. It should, for example, be possible to run as many as 10 channels in the same band. The band 869.65-869.7MHz is an alarm only band restricted to 25mW ERP and this band would be suitable for running

the long-range channel, and two channels should be supportable in this band.

**[0089]** 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. The skilled person will know how to form packets that will enable the implementation of the embodiments described herein.

**[0090]** Long packets should only be allowed under good network conditions, at least unless forward error correction is implemented. Since the long-range channel is targeting weak link conditions, it is reasonable to accept a limitation of the maximum payload length.

**[0091]** 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%

**[0092]** 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 preselected in this band to enable alternative options. But it will be appreciated that the invention does not rely on the use of the g3 sub-band, channels could be set aside 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 long-range channels in the context of the invention.

**[0093]** Typically, the regular speed channels or configuration may operate around 30 to 45 kbit/s - e.g. 38.4 kbit/s. "Long range" may equate to 0.6 to 14.4 kbit/s e.g. 4.8 kbit/s or 2.4kbit/s.

**[0094]** Sending the same amount of data over the long range radio will take longer time due to, among other reasons, the lower bit rate. The longer the radio is active the more battery will be consumed. This means that in general if we can get packets through on standard radio we should use that.

#### Channel Agility

**[0095]** To support fast switches to long-range channels, the system should be configured to support the changing of channel without requiring a login, since a full login sequence usually requires many packets being sent in both directions. Thus, for example a node switching channel (or sub-channel) should continue its operation on the new channel as if nothing has changed. And a gateway (central unit) should accept a node changing channel without requiring a login.

#### Node behaviour

**[0096]** Optional hello cycle / Cold start schema:

when a node enters its Hello-cycle to scan for central units it should include its available long-range channels.

**[0097]** Channel stickiness: a node should preferably be configured to stay on the channel where it last received an ACK - i.e. on the channel where it last had a working link.

**[0098]** Optional node fall-back schema:

When a node does not receive a required ACK in response to transmitting a message (preamble, synch word, data), it

shall use the following sequence for trying to send the message (packet). The list starts while on a standard channel:

1. Retry packet x times (e.g. 10 times) on current channel
2. Retry packet y times (e.g. 3 to 5 times) on available node long-range channels
3. Retry once on all standard channels
4. Restart Hello cycle

Central Unit behaviour

**[0099]** There are typically different requirements during the installation and normal operations mode.

Operations Mode

**[0100]** During normal operation of the system the preference is always to use Standard rates if possible. This is primarily to conserve battery but will also have other benign effects such as polluting the frequency band less and faster re-logins if required.

**[0101]** If a node is on long-range, but the RSSI (measured by the central unit) indicates that it should work on Standard rates, the central unit may be configured to issue a push to move that node to Standard.

Installation mode

**[0102]** One of the benefits of the long-range proposal is that it can make the system installation experience (and the new-node installation experience) easier and less complicated for the installers. This means that systems may be so configured that the process of installing a long range node does not differ for the installer in any significant way from installing a standard range node.

**[0103]** During installation, the Central Unit and Long Range Node may therefore be configured to work together automatically to steer the node to the best protocol based on the acceptance criteria. The node may therefore predictably follow the behaviour laid out above, while the Central Unit will try to make more informed decisions.

**[0104]** A node with  $RSSI_{node} < \text{lowest RSSI level acceptable for installing a standard range node (Sinst)}$  will be pushed to Long Range so make sure that the RSSI acceptance criteria are fulfilled and to receive RSSI values on Long Range.

**[0105]** When the Central Unit exits Installation mode it will run an evaluation on the current RSSI if the node is on a Long Range channel:

Push to long range, if  $RSSI < S_{inst}$

evaluate standard RSSI {

No Action - otherwise

**[0106]** Although in general security monitoring systems according to embodiments of the invention will be so configured that nodes will initially attempt to communicate with the central unit using a standard communication channel rather than a long range channel, they may instead be so configured that they initially attempt to communicate using a long-range channel. Subsequently, the central unit may move such a node to a standard communication channel if the measured RSSI indicates a suitably high signal strength. But because of the higher bit rate provided by standard communication channels it is generally preferred to configure the system and nodes for the nodes always to attempt initially to communicate using a standard communication channel.

**[0107]** Also, nodes that last successfully communicated with the central unit using a long range channel may, because of channel stickiness, also initially attempt to communicate with the central unit using the stored long-range channel and then frequency hop through the other long range channels to establish communication over any long-range sub-channel. Subsequently, the central unit may move such a node to a standard communication channel if the measured RSSI indicates a suitably high signal strength.

Interactive mode

**[0108]** Consider now the provision of long-range functionality in the case of a magnetic contact node. Typically, magnetic contact nodes may be configured as listen after talk (LAT) nodes. This means that the central unit can only talk to this

node after the node has first talked to the central unit, and only during a short period from when the node talked to the central unit.

**[0109]** LAT stands for Listen After Talk. Meaning the node listens for packets from the Central Unit a short period after it has sent its own packets to the Central Unit.

5 **[0110]** A LAT based node will only talk to the Central Unit under two main conditions:

1. If something happens with the node. i.e. the magnet contact is violated.
2. During periodic updates to verify that the node is still alive.

10 **[0111]** The periodic update for a magnet may be around 7 minutes, but for a Long Range node it will have to be more infrequent due to battery consumption.

**[0112]** With the introduction of Long Range there is now a requirement of more frequent RSSI reports as well as having to be able to issue the push command to nodes if they need to be moved between Long Range and Standard.

15 **[0113]** To solve this, it is proposed to introduce a mode for the node which might be termed Interactive mode. During installation for the nodes where this requirement is valid, the Central Unit will lower the periodic report rate on the nodes to make sure the central unit can talk to them in a timely manner.

**[0114]** This method may also be used for the same kind of nodes to enable quicker and more deterministic FOTA (Firmware Over The Air) updates.

20 **[0115]** For the Central Unit to perform the push between Long Range and Standard, the central unit may issue instructions to nodes according to one or other of the following two options, although of course alternative methods may be used instead:

Retain Credentials

25 **[0116]** This option allows the node to not do a full login on the new channel. Instead it will simply switch frequency and continue as if nothing has happened. This can be enabled using channel agility functionality.

Immediate Send Enabling

30 **[0117]** This option requires the node to immediately send a periodic status report once it has switched frequency. This can be set by the Central Unit as a way to immediately verify that a switch has worked. A failed ack on the periodic status will force the node into its Hello cycle.

35 **[0118]** It will be appreciated that in accordance with non claimed alternatives, 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.

## 40 Claims

1. A method of compensating for differences between the operating frequency of a crystal oscillator (251) of a central unit (110) of a security monitoring system and a crystal oscillator (360) of a node (114, 118, 125, 126) of the security monitoring system, the method comprising: tuning a receiver (230, 232, 234) of the central unit (110) to a first frequency sub-channel of multiple frequency sub-channels that together make up a predetermined broader frequency channel;

listening for a preamble from the node (114, 118, 125, 126) on the first frequency sub-channel;

50 in the event that no valid preamble is received on the first frequency sub-channel within a predetermined period, tuning the receiver (230, 232, 234) to a second of the multiple frequency sub-channels and listening for a preamble from the node (114, 118, 125, 126) on the second frequency sub-channel; and repeating the tuning and listening process until a valid preamble is received or until all of the multiple frequency sub-channels have been used;

55 in the event that a valid preamble is received on one of the multiple frequency sub-channels, listening for a synch word, and upon detection of a valid synch word causing a radio frequency transceiver (230, 232, 234) of the central unit (110) to transmit an acknowledgement on a radio frequency within the predetermined frequency channel;

detecting an offset between the radio frequency of the carrier on which the valid preamble was received and

the centre frequency of the predetermined frequency channel;  
 in the event that the offset exceeds a predetermined threshold, transmitting from the central unit (110) information regarding the offset to enable the node (114, 118, 125, 126) to adjust the operating frequency of a transceiver (340) of the node based on the information.

2. The method of claim 1, further comprising adjusting the operating frequency of the node (114, 118, 125, 126) based on the information regarding the offset.

3. A central unit (110) for a security monitoring system, the central unit having at least one radio frequency transceiver (230, 232, 234), and a controller (250) to control the at least one radio frequency transceiver (230, 232, 234), the central unit (110) being configurable to provide a first RF communication mode and an alternative long range communication mode, the first communication mode supporting a higher maximum bitrate than the long range mode, and the long range mode supporting a greater transmission range than the first mode;  
 the controller (250) being configured to:

control a radio frequency transceiver (230, 232, 234) of the central unit to tune to one of multiple different radio frequency sub-channels that together make up the long-range communication channel and to listen for a preamble transmitted by a node (114, 118, 125, 126) of the security monitoring system, and in the event that no preamble is detected within a predetermined period to control said radio frequency transceiver (230, 232, 234) of the central unit (110) to tune to another of the multiple different radio frequency sub-channels to listen for a preamble transmitted by the node (114, 118, 125, 126), and to repeat this procedure until either all the multiple different radio frequency sub-channels have been used or a preamble has been detected; and, in the event that a preamble is detected, to listen for a synch word, and upon detection of a valid synch word to cause a radio frequency transceiver (230, 232, 234) of the central unit (110) to transmit an acknowledgement on a radio frequency within the long-range communication channel, and, thereafter to communicate with the node using a radio frequency within the long-range communication channel;  
 wherein the central unit (110) is configured, based on the frequency on which the preamble from the node (114, 118, 125, 126) was received, to estimate the accuracy of a crystal oscillator (360) of the node, and if the estimated accuracy is less than a predetermined level to provide a feedback signal to the node (114, 118, 125, 126), based on that estimate, to enable the node (114, 118, 125, 126) to compensate for inaccuracy of the crystal oscillator (360) when tuning the node radio frequency transceiver (340).

4. The central unit of claim 3, wherein the controller (250) unit of the central unit (110) is configured to transmit the acknowledgement on the radio frequency sub-channel on which the valid synch word was received.

5. The central unit of claim 3 or claim 4, wherein the central unit (110) is configured to use the same radio frequency transceiver (230, 232, 234) to transmit messages using the first RF communication mode and using the long range communication mode.

6. The central unit of any one of claims 3 to 5, wherein the radio frequency transceiver (230, 232, 234) of the central unit (110) that is used to tune to the multiple different radio frequency sub-channels and to listen for a preamble transmitted by the node (114, 118, 125, 126) is configured to use Digital Signal Arrival, DSA, to detect a valid preamble pattern.

7. The central unit of any one of claims 3 to 6, wherein the central unit (110) is configured to determine the RSSI for communications received from the node (114, 118, 125, 126) using the long range communication mode, and optionally wherein in the event that the determined RSSI is above a predetermined threshold, the central unit (110) is configured to issue an instruction to the node (114, 118, 125, 126) to switch from the long range communication mode to the first communication mode.

8. A node (114, 118, 125, 126) for a security monitoring system, the node having a node radio frequency transceiver (340) configurable to provide a first RF communication mode and an alternative long-range communication mode, the first communication mode supporting a higher maximum bitrate than the long-range mode, and the long-range mode supporting a greater transmission range than the first mode; the controller (350) of the node being configured to:  
 attempt to establish communication with a central unit (110) of the security monitoring system using the long range communication mode by:

transmitting a message comprising a preamble followed by a synch word on a frequency within a long-range

communications channel, and

listening for an acknowledgement from the central unit (110) on a frequency within the long-range communications channel;

and, in the event that an acknowledgement is received from the central unit (110) on one of the multiple different frequencies, to communicate with the central unit (110) using a frequency within the long-range communication channel;

wherein the node controller (350) is configured to use a crystal oscillator feedback signal from the central unit to compensate for inaccuracy of the crystal oscillator (360) when tuning the node radio frequency transceiver (340).

9. The node of claim 8, wherein the node controller (350) is configured to control the node transceiver (340) to communicate with the central unit (110) using the frequency on which an acknowledgement was received from the central unit (110).

10. The node of claim 8 or claim 9, wherein the node is configured, on initially being triggered, to attempt to establish direct communication with the central unit (110) using the first RF communication mode, and, if the node (114, 118, 125, 126) is unable to establish direct communication with the central unit (110) using the first configuration, to attempt to establish direct communication with the central unit using the long range communication mode.

11. The node of claim 10, the node (114, 118, 125, 126) further being configured, when attempting to establish direct communication with the central unit (110) using the first RF communication mode, to first attempt communication using the frequency on which the node (114, 118, 125, 126) last received an acknowledgement from the central unit (110).

12. The node of any one of claims 8 to 11, the node further being configured, on establishing direct communication with the central unit (110) to receive an acknowledgement from the central unit to exchange security keys and system settings using the communication mode that was used by the node to establish direct communication with the central unit, and subsequently to communicate with the central unit directly using that communication mode.

13. A security monitoring system comprising a central unit as claimed in any one of claims 3 to 7, and one or more nodes as claimed in any one of claims 8 to 12.

14. A security monitoring system as claimed in claim 13, a central unit as claimed in any one of claims 3 to 7, or a node (114, 118, 125, 126) as claimed in any one of claims 8 to 12, wherein the multiple different radio frequency sub-channels are contiguous virtual sub-channels within a long-range communications channel that is defined by a pair of guard bands.

15. A central unit, node or security monitoring system of any one of claims 3 to 14, wherein the data rate of the long range communication mode is 20% or less, for example 10%, of the data rate of the first RF communication mode.

## Patentansprüche

1. Verfahren zum Ausgleichen von Unterschieden zwischen der Betriebsfrequenz eines Quarzoszillators (251) einer Zentraleinheit (110) eines Sicherheitsüberwachungssystems und eines Quarzoszillators (360) eines Knotens (114, 118, 125, 126) des Sicherheitsüberwachungssystems, wobei das Verfahren Folgendes umfasst: Abstimmen eines Empfängers (230, 232, 234) der Zentraleinheit (110) auf einen ersten Frequenzunterkanal von mehreren Frequenzunterkanälen, die zusammen einen vorbestimmten breiteren Frequenzkanal bilden;

Warten auf eine Präambel von dem Knoten (114, 118, 125, 126) auf dem ersten Frequenzunterkanal; in dem Fall, dass innerhalb eines vorbestimmten Zeitraums keine gültige Präambel auf dem ersten Frequenzunterkanal empfangen wird, Abstimmen des Empfängers (230, 232, 234) auf einen zweiten der mehreren Frequenzunterkanäle und Warten auf eine Präambel von dem Knoten (114, 118, 125, 126) auf dem zweiten Frequenzunterkanal; und Wiederholen des Abstimm- und Wartevorgangs, bis eine gültige Präambel empfangen wird oder bis alle der mehreren Frequenzunterkanäle genutzt worden sind;

in dem Fall, dass auf einem der mehreren Frequenzunterkanäle eine gültige Präambel empfangen wird, Warten auf ein Synchronwort, und bei Erfassung eines gültigen Synchronworts wird ein Hochfrequenz-Sender/Empfänger (230, 232, 234) der Zentraleinheit (110) dazu veranlasst, eine Bestätigung auf einer Hochfrequenz

innerhalb des vorbestimmten Frequenzkanals zu senden;

Erfassen eines Versatzes zwischen der Hochfrequenz des Trägers, auf dem die gültige Präambel empfangen wurde, und der Mittenfrequenz des vorbestimmten Frequenzkanals;

in dem Fall, dass der Versatz einen vorbestimmten Schwellenwert überschreitet, werden Informationen von der Zentraleinheit (110) hinsichtlich des Versatzes gesendet, um den Knoten (114, 118, 125, 126) in die Lage zu versetzen, die Betriebsfrequenz eines Senders/Empfängers (340) des Knotens anhand der Informationen einzustellen.

2. Verfahren nach Anspruch 1, bei dem ferner die Betriebsfrequenz des Knotens (114, 118, 125, 126) anhand der Informationen hinsichtlich des Versatzes eingestellt wird.

3. Zentraleinheit (110) für ein Sicherheitsüberwachungssystem, wobei die Zentraleinheit wenigstens einen Hochfrequenz-Sender/Empfänger (230, 232, 234) sowie eine Steuerung (250) zur Steuerung des wenigstens einen Hochfrequenz-Senders/Empfängers (230, 232, 234) aufweist, wobei die Zentraleinheit (110) so eingerichtet werden kann, dass sie einen ersten HF-Kommunikationsmodus und einen alternativen Weitstreckenkommunikationsmodus bereitstellt, wobei der erste Kommunikationsmodus eine höhere maximale Bitrate als der Weitstreckenmodus unterstützt und der Weitstreckenmodus eine größere Übertragungsreichweite als der erste Modus unterstützt, wobei die Steuerung (250) so eingerichtet ist, dass sie:

einen Hochfrequenz-Sender/Empfänger (230, 232, 234) der Zentraleinheit so steuert, dass er sich auf einen von mehreren verschiedenen Hochfrequenzunterkanälen einstellt, die zusammen den Weitstreckenkommunikationskanal bilden, und auf eine von einem Knoten (114, 118, 125, 126) des Sicherheitsüberwachungssystems gesendete Präambel wartet, und in dem Fall, dass innerhalb eines vorbestimmten Zeitraums keine Präambel erfasst wird, den Hochfrequenz-Sender/Empfänger (230, 232, 234) der Zentraleinheit (110) so steuert, dass er sich auf einen anderen der mehreren verschiedenen Hochfrequenzunterkanäle einstellt, um auf eine von dem Knoten (114, 118, 125, 126) gesendete Präambel zu warten, und diesen Vorgang wiederholt, bis entweder alle der mehreren verschiedenen Hochfrequenzunterkanäle genutzt worden sind oder eine Präambel erfasst worden ist; und in dem Fall, dass eine Präambel erfasst wird, auf ein Synchronwort wartet, und bei Erfassung eines gültigen Synchronworts einen Hochfrequenz-Sender/Empfänger (230, 232, 234) der Zentraleinheit (110) veranlasst, eine Bestätigung auf einer Hochfrequenz innerhalb des Weitstreckenkommunikationskanals zu senden, und danach mit dem Knoten unter Verwendung einer Hochfrequenz innerhalb des Weitstreckenkommunikationskanals kommuniziert; wobei die Zentraleinheit (110) so eingerichtet ist, dass sie anhand der Frequenz, auf der die Präambel von dem Knoten (114, 118, 125, 126) empfangen wurde, die Genauigkeit eines Quarzoszillators (360) des Knotens schätzt, und wenn die geschätzte Genauigkeit unter einem vorbestimmten Niveau liegt, ein Rückkopplungssignal an den Knoten (114, 118, 125, 126) liefert, das auf dieser Schätzung beruht, um den Knoten (114, 118, 125, 126) in die Lage zu versetzen, eine Ungenauigkeit des Quarzoszillators (360) beim Abstimmen des Knoten-Hochfrequenz-Senders/Empfängers (340) auszugleichen.

4. Zentraleinheit nach Anspruch 3, wobei die Steuereinheit (250) der Zentraleinheit (110) so eingerichtet ist, dass sie die Bestätigung auf dem Hochfrequenzunterkanal sendet, auf dem das gültige Synchronwort empfangen wurde.

5. Zentraleinheit nach Anspruch 3 oder Anspruch 4, wobei die Zentraleinheit (110) so eingerichtet ist, dass sie zum Senden von Nachrichten unter Verwendung des ersten HF-Kommunikationsmodus und unter Verwendung des Weitstreckenkommunikationsmodus den gleichen Hochfrequenz-Sender/Empfänger (230, 232, 234) verwendet.

6. Zentraleinheit nach einem der Ansprüche 3 bis 5, wobei der Hochfrequenz-Sender/Empfänger (230, 232, 234) der Zentraleinheit (110), der zum Einstellen auf die mehreren verschiedenen Hochfrequenzunterkanäle und zum Warten auf eine von dem Knoten (114, 118, 125, 126) gesendete Präambel verwendet wird, zur Verwendung von Digital Signal Arrival (Digitalsignalkunft (DSA)) eingerichtet ist, um ein gültiges Präambelmuster zu erfassen.

7. Zentraleinheit nach einem der Ansprüche 3 bis 6, wobei die Zentraleinheit (110) so eingerichtet ist, dass sie den RSSI für von dem Knoten (114, 118, 125, 126) empfangene Mitteilungen unter Verwendung des Weitstreckenkommunikationsmodus ermittelt, und wahlweise wobei in dem Fall, dass der ermittelte RSSI oberhalb eines vorbestimmten Schwellenwerts liegt, die Zentraleinheit (110) so eingerichtet ist, dass sie dem Knoten (114, 118, 125, 126) eine Anweisung gibt, von dem Weitstreckenkommunikationsmodus in den ersten Kommunikationsmodus zu wechseln.

8. Knoten (114, 118, 125, 126) für ein Sicherheitsüberwachungssystem, wobei der Knoten einen Knoten-Hochfrequenz-Sender/Empfänger (340) aufweist, der so eingerichtet werden kann, dass er einen ersten HF-Kommunikationsmodus und einen alternativen Weitstreckenkommunikationsmodus bereitstellt, wobei der erste Kommunikationsmodus eine höhere maximale Bitrate als der Weitstreckenmodus unterstützt und der Weitstreckenmodus eine größere Übertragungsreichweite als der erste Modus unterstützt, wobei die Steuerung (350) des Knotens so eingerichtet ist, dass sie:

versucht, unter Verwendung des Weitstreckenkommunikationsmodus eine Verbindung mit einer Zentraleinheit (110) des Sicherheitsüberwachungssystems herzustellen, durch:

Senden einer Nachricht, die eine Präambel, gefolgt von einem Synchronwort, umfasst, auf einer Frequenz innerhalb eines Weitstreckenkommunikationskanals, und  
Warten auf eine Bestätigung von der Zentraleinheit (110) auf einer Frequenz innerhalb des Weitstreckenkommunikationskanals,  
und in dem Fall, dass von der Zentraleinheit (110) eine Bestätigung auf einer der mehreren verschiedenen Frequenzen empfangen wird, unter Verwendung einer Frequenz innerhalb des Weitstreckenkommunikationskanals mit der Zentraleinheit (110) kommuniziert,  
wobei die Knotensteuerung (350) so eingerichtet ist, dass sie ein Quarzoszillatorkopplungssignal von der Zentraleinheit dazu verwendet, eine Ungenauigkeit des Quarzoszillators (360) beim Abstimmen des Knoten-Hochfrequenz-Senders/Empfängers (340) auszugleichen.

9. Knoten nach Anspruch 8, wobei die Knotensteuerung (350) dazu eingerichtet ist, den Knoten-Sender/Empfänger (340) so zu steuern, dass er unter Verwendung der Frequenz, auf der eine Bestätigung von der Zentraleinheit (110) empfangen wurde, mit der Zentraleinheit (110) kommuniziert.

10. Knoten nach Anspruch 8 oder Anspruch 9, wobei der Knoten dazu eingerichtet ist, bei anfänglicher Ansteuerung zu versuchen, unter Verwendung des ersten HF-Kommunikationsmodus eine direkte Verbindung mit der Zentraleinheit (110) herzustellen, und wenn der Knoten (114, 118, 125, 126) nicht in der Lage ist, unter Verwendung der ersten Konfiguration eine direkte Verbindung mit der Zentraleinheit (110) herzustellen, zu versuchen, unter Verwendung des Weitstreckenkommunikationsmodus eine direkte Verbindung mit der Zentraleinheit herzustellen.

11. Knoten nach Anspruch 10, wobei der Knoten (114, 118, 125, 126) ferner dazu eingerichtet ist, bei dem Versuch, unter Verwendung des ersten HF-Kommunikationsmodus eine direkte Verbindung mit der Zentraleinheit (110) herzustellen, zuerst eine Verbindung unter Verwendung der Frequenz zu versuchen, auf der der Knoten (114, 118, 125, 126) zuletzt eine Bestätigung von der Zentraleinheit (110) empfangen hat.

12. Knoten nach einem der Ansprüche 8 bis 11, wobei der Knoten ferner dazu eingerichtet ist, beim Herstellen einer direkten Verbindung mit der Zentraleinheit (110) eine Bestätigung von der Zentraleinheit zu empfangen, um Sicherheitsschlüssel und Systemeinstellungen unter Verwendung des Kommunikationsmodus auszutauschen, der von dem Knoten zur Herstellung einer direkten Verbindung mit der Zentraleinheit verwendet wurde, und anschließend unter Verwendung dieses Kommunikationsmodus direkt mit der Zentraleinheit zu kommunizieren.

13. Sicherheitsüberwachungssystem mit einer Zentraleinheit nach einem der Ansprüche 3 bis 7 und einem oder mehreren Knoten nach einem der Ansprüche 8 bis 12.

14. Sicherheitsüberwachungssystem nach Anspruch 13, Zentraleinheit nach einem der Ansprüche 3 bis 7 oder Knoten (114, 118, 125, 126) nach einem der Ansprüche 8 bis 12, wobei die mehreren verschiedenen Hochfrequenzunterkanäle benachbarte virtuelle Unterkanäle innerhalb eines Weitstreckenkommunikationskanals sind, der durch ein Paar Sicherheitsbänder definiert ist.

15. Zentraleinheit, Knoten oder Sicherheitsüberwachungssystem nach einem der Ansprüche 3 bis 14, wobei die Datenrate des Weitstreckenkommunikationsmodus 20% oder weniger, zum Beispiel 10%, der Datenrate des ersten HF-Kommunikationsmodus beträgt.

## Revendications

1. Procédé de compensation de différences entre la fréquence de fonctionnement d'un oscillateur à quartz (251) d'une unité centrale (110) d'un système de surveillance de sécurité et d'un oscillateur à quartz (360) d'un noeud (114,

118, 125, 126) du système de surveillance de sécurité, le procédé comprenant : le réglage d'un récepteur (230, 232, 234) de l'unité centrale (110) sur un premier sous-canal de fréquence parmi plusieurs sous-canaux de fréquence qui ensemble forment un canal de fréquence plus large prédéterminé ;

l'attente d'un préambule provenant du noeud (114, 118, 125, 126) sur le premier sous-canal de fréquence ; dans le cas où aucun préambule valide n'est reçu sur le premier sous-canal de fréquence dans une période prédéterminée, le réglage du récepteur (230, 232, 234) sur un deuxième sous-canal parmi les plusieurs sous-canaux de fréquence et l'attente d'un préambule provenant du noeud (114, 118, 125, 126) sur le deuxième sous-canal de fréquence ; et la répétition de la procédure de réglage et d'attente jusqu'à ce qu'un préambule valide a été reçu ou l'ensemble des plusieurs sous-canaux de fréquence a été utilisé ; dans le cas où un préambule valide est reçu sur l'un des plusieurs sous-canaux de fréquence, l'attente d'un mot de synchronisation, et lors de la détection d'un mot de synchronisation valide, un émetteur-récepteur à haute fréquence (230, 232, 234) de l'unité centrale (110) est amené à transmettre une confirmation sur une haute fréquence dans le canal de fréquence prédéterminé ; la détection d'une déviation entre la haute fréquence du porteur sur lequel le préambule valide a été reçu et la fréquence centrale du canal de fréquence prédéterminé ; dans le cas où la déviation dépasse un seuil prédéterminé, la transmission par l'unité centrale (110) d'informations concernant la déviation pour permettre au noeud (114, 118, 125, 126) de régler la fréquence de fonctionnement d'un émetteur-transmetteur (340) du noeud sur la base des informations.

2. Procédé selon la revendication 1, comprenant en outre le réglage de la fréquence de fonctionnement du noeud (114, 118, 125, 126) sur la base des informations concernant la déviation.

3. Unité centrale (110) pour un système de surveillance de sécurité, l'unité centrale présentant au moins un émetteur-récepteur à haute fréquence (230, 232, 234) et une commande (250) pour commander ledit au moins un émetteur-récepteur à haute fréquence (230, 232, 234), l'unité centrale (110) étant apte à être réalisée de manière à fournir un premier mode de communication HF et un mode de communication alternatif à longue portée, le premier mode de communication supportant un débit binaire maximum plus élevé que le mode à longue portée, et le mode à longue portée supportant une portée de transmission plus élevée que le premier mode ; la commande (250) étant réalisée de manière :

à commander un émetteur-récepteur à haute fréquence (230, 232, 234) de l'unité centrale de sorte qu'il se règle sur l'un des plusieurs sous-canaux à haute fréquence différents qui forment ensemble le canal de communication à longue portée, et à attendre un préambule transmis par un noeud (114, 118, 125, 126) du système de surveillance de sécurité, et dans le cas où aucun préambule n'est détecté dans une période prédéterminée, à commander l'émetteur-récepteur à haute fréquence (230, 232, 234) de l'unité centrale (110) de sorte qu'il se règle sur un autre sous-canal parmi les plusieurs sous-canaux à haute fréquence différents pour attendre un préambule transmis par le noeud (114, 118, 125, 126), et répète cette procédure jusqu'à ce que l'ensemble des plusieurs sous-canaux à haute fréquence différents a été utilisé ou un préambule a été détecté ; et, dans le cas où un préambule est détecté, à attendre un mot de synchronisation, et lors de la détection d'un mot de synchronisation valide, à amener un émetteur-récepteur à haute fréquence (230, 232, 234) de l'unité centrale (110) à transmettre une confirmation sur une haute fréquence dans le canal de communication à longue portée, et ensuite à communiquer avec le noeud en utilisant une haute fréquence dans le canal de communication à longue portée ;

l'unité centrale (110) étant réalisée de manière à estimer, sur la base de la fréquence sur laquelle le préambule provenant du noeud (114, 118, 125, 126) a été reçu, la précision d'un oscillateur à quartz (360) du noeud, et si la précision estimée est inférieure à un niveau prédéterminé, à fournir un signal de retour au noeud (114, 118, 125, 126) basé sur cette estimation, pour permettre au noeud (114, 118, 125, 126) de compenser l'imprécision de l'oscillateur à quartz (360) lors du réglage de l'émetteur-récepteur à haute fréquence (340) du noeud.

4. Unité centrale selon la revendication 3, l'unité de commande (250) de l'unité centrale (110) étant réalisée de manière à transmettre la confirmation sur le sous-canal à haute fréquence sur lequel le mot de synchronisation valide a été reçu.

5. Unité centrale selon la revendication 3 ou la revendication 4, l'unité centrale (110) étant réalisée de manière à utiliser le même émetteur-récepteur à haute fréquence (230, 232, 234) pour transmettre des messages en utilisant le premier mode de communication HF et en utilisant le mode de communication à longue portée.

6. Unité centrale selon l'une des revendications 3 à 5, l'émetteur-récepteur à haute fréquence (230, 232, 234) de l'unité centrale (110) qui est utilisé pour le réglage sur les plusieurs sous-canaux à haute fréquence différents et pour attendre un préambule transmis par le noeud (114, 118, 125, 126) étant réalisé de manière à utiliser Digital Signal Arrival (arrivé de signal numérique - DSA) pour la détection d'un modèle de préambule valide.
7. Unité centrale selon l'une des revendications 3 à 6, l'unité centrale (110) étant réalisée de manière à déterminer le RSSI pour les communications reçues du noeud (114, 118, 125, 126) en utilisant le mode de communication à longue portée, et en option, dans le cas où le RSSI déterminé est supérieur à une valeur seuil prédéterminée, l'unité centrale (110) étant réalisée de manière à émettre une instruction au noeud (114, 118, 125, 126) pour passer du mode de communication à longue portée au premier mode de communication.
8. Noeud (114, 118, 125, 126) pour un système de surveillance de sécurité, le noeud présentant un émetteur-récepteur (340) à haute fréquence de noeud qui est apte à être réalisé de manière à fournir un premier mode de communication HF et un mode de communication alternatif à longue portée, le premier mode de communication supportant un débit binaire maximum plus élevé que le mode à longue portée, et le mode à longue portée supportant une portée de transmission plus élevée que le premier mode ; la commande (350) du noeud étant réalisée de manière à : tenter d'établir une communication avec une unité centrale (110) du système de surveillance de sécurité en utilisant le mode de communication à longue portée :  
  
en transmettant un message comprenant un préambule suivi d'un mot de synchronisation sur une fréquence dans un canal de communication à longue portée, et  
en attendant une confirmation de l'unité centrale (110) sur une fréquence dans le canal de communication à longue portée ;  
et, dans le cas où une confirmation provenant de l'unité centrale (110) est reçue sur l'une des plusieurs fréquences différentes, à communiquer avec l'unité centrale (110) en utilisant une fréquence dans le canal de communication à longue portée ;  
la commande de noeud (350) étant réalisée de manière à utiliser un signal de retour d'un oscillateur à quartz provenant de l'unité centrale pour compenser une imprécision de l'oscillateur à quartz (360) lors du réglage de l'émetteur-récepteur à haute fréquence de noeud (340).
9. Noeud selon la revendication 8, la commande de noeud (350) étant réalisée de manière à commander l'émetteur-récepteur de noeud (340) de sorte qu'il communique avec l'unité centrale (110) en utilisant la fréquence sur laquelle une confirmation provenant de l'unité centrale (110) a été reçue.
10. Noeud selon la revendication 8 ou la revendication 9, le noeud, lors du déclenchement initial, étant réalisé de manière à tenter d'établir une communication directe avec l'unité centrale (110) en utilisant le premier mode de communication HF et, si le noeud (114, 118, 125, 126) n'est pas en mesure d'établir une communication directe avec l'unité centrale (110) en utilisant la première configuration, à tenter d'établir une communication directe avec l'unité centrale en utilisant le mode de communication à longue portée.
11. Noeud selon la revendication 10, le noeud (114, 118, 125, 126), lors de la tentative d'établir une communication directe avec l'unité centrale (110) en utilisant le premier mode de communication HF, étant en outre réalisé de manière à tenter d'abord une communication en utilisant la fréquence sur laquelle le noeud (114, 118, 125, 126) a reçu en dernier une confirmation de l'unité centrale (110).
12. Noeud selon l'une des revendications 8 à 11, le noeud, lors de l'établissement d'une communication directe avec l'unité centrale (110), étant en outre réalisé de manière à recevoir une confirmation de l'unité centrale pour échanger des clés de sécurité et des paramètres du système en utilisant le mode de communication utilisé par le noeud pour établir une communication directe avec l'unité centrale, et ensuite à communiquer directement avec l'unité centrale en utilisant ce mode de communication.
13. Système de surveillance de sécurité comprenant une unité centrale selon l'une des revendications 3 à 7 et un ou plusieurs noeuds selon l'une des revendications 8 à 12.
14. Système de surveillance de sécurité selon la revendication 13, unité centrale selon l'une des revendications 3 à 7, ou noeud (114, 118, 125, 126) selon l'une des revendications 8 à 12, les plusieurs sous-canaux à haute fréquence différents étant des sous-canaux virtuels contigus dans un canal de communication à longue portée qui est défini

par une paire de bandes de garde.

15. Unité centrale, noeud ou système de surveillance de sécurité selon l'une des revendications 3 à 14, le débit de transfert de données du mode de communication à longue portée correspondant à 20% ou moins, par exemple à 10% du débit de transfert de données du premier mode de communication HF.

5

10

15

20

25

30

35

40

45

50

55

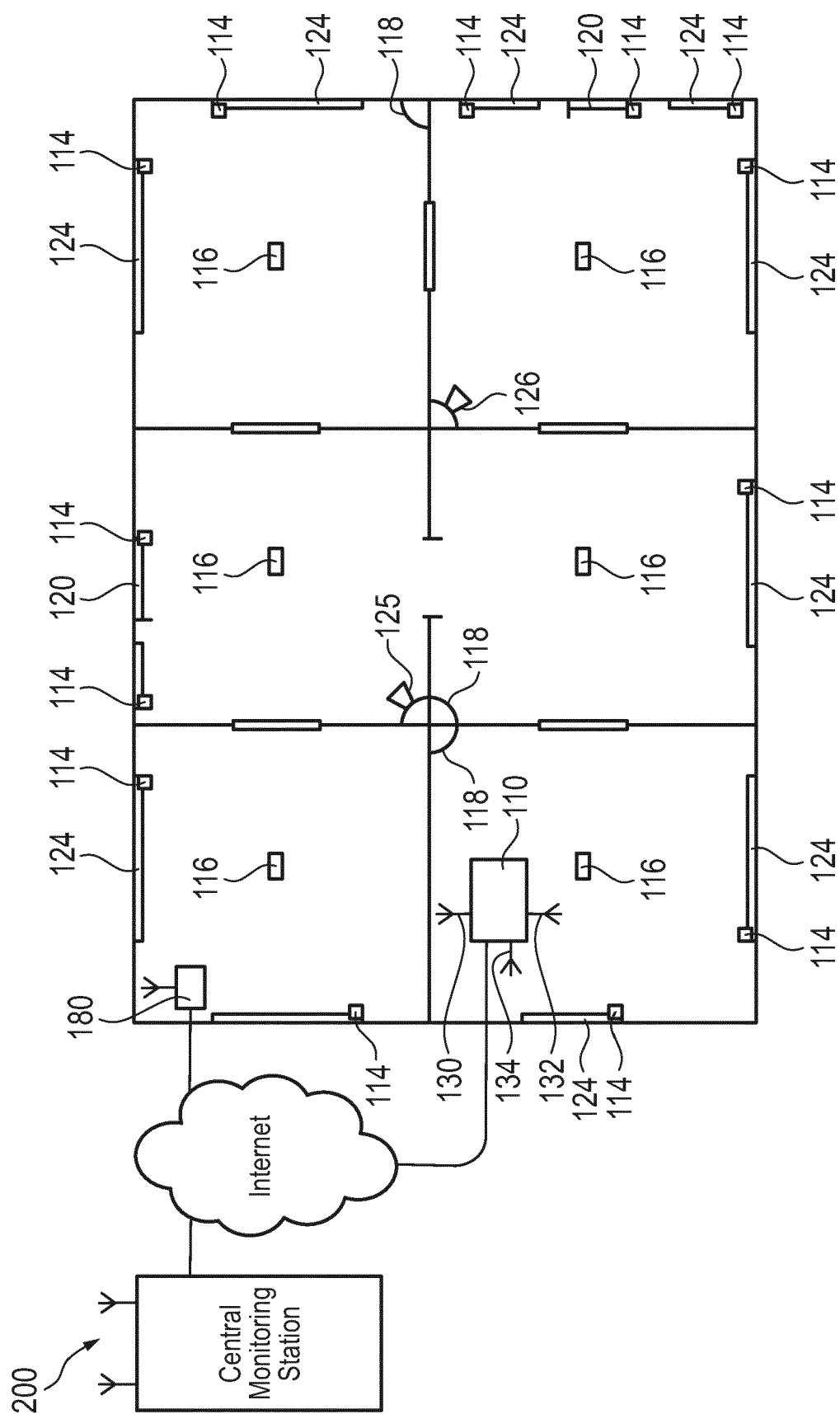


Fig. 1

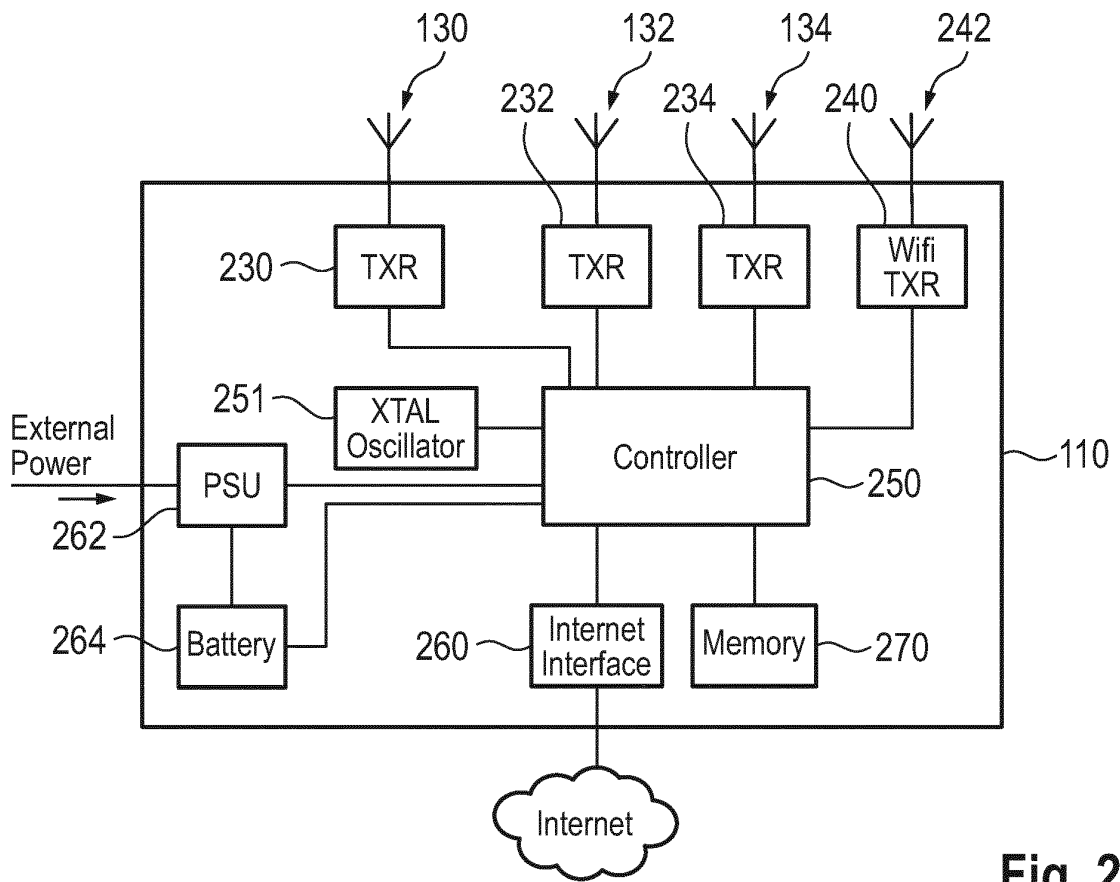


Fig. 2

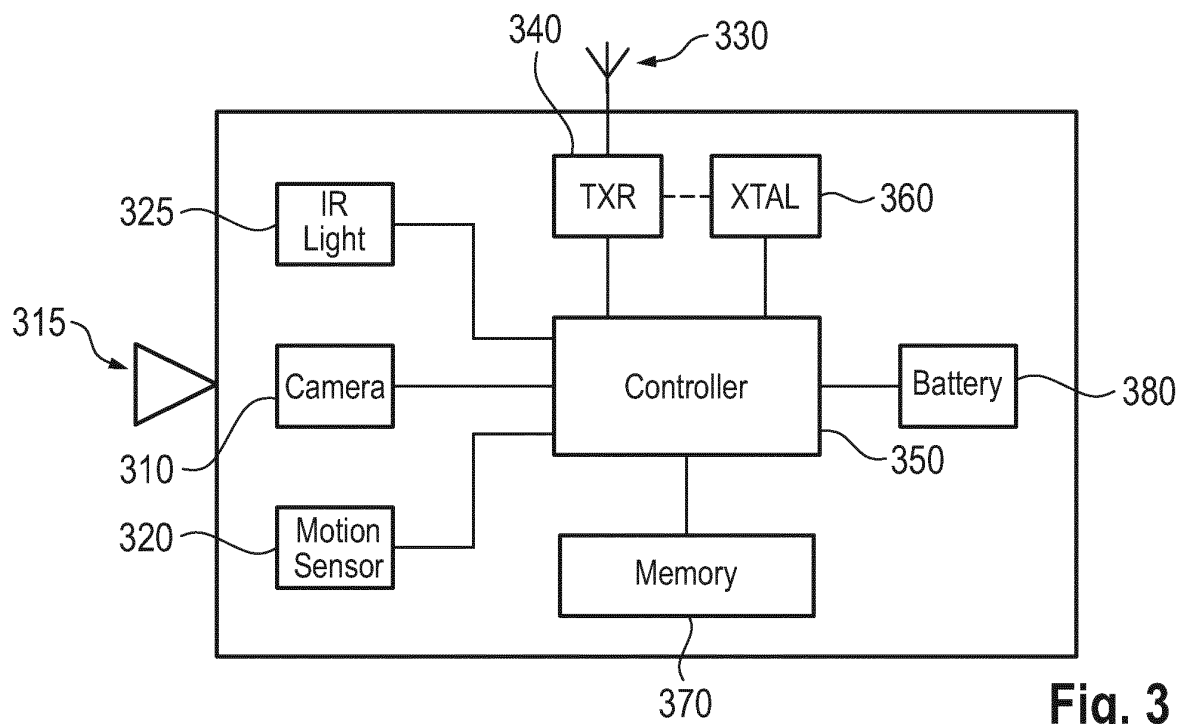


Fig. 3

**REFERENCES CITED IN THE DESCRIPTION**

*This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.*

**Patent documents cited in the description**

- EP 2542011 A1 [0008]

**Non-patent literature cited in the description**

- **HAMOOD SHEHAB HAMID et al.** Analyze BER Performance of Wireless FSK System. *Microwaves & RF*,, November 2009, vol. 48 (11), 80 [0059]