(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 828 849 A1**

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
02.06.2021 Bulletin 2021/22

(51) Int Cl.:
G08B 13/196 *(2006.01)*

(21) Application number: **19211597.0**

(22) Date of filing: **26.11.2019**

(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
Designated Extension States:
BA ME
KH MA MD TN

(71) Applicant: **Verisure Sàrl**
1290 Versoix (CH)

(72) Inventors:
- **Wells, Andrew**
  1290 Versoix, Geneva (CH)
- **Westergren, Christian**
  1290 Versoix, Geneva (CH)
- **Ryd, Patrik**
  1290 Versoix, Geneva (CH)
- **Winge, Carl Olof**
  1290 Versoix, Geneva (CH)
- **Blomé, Per Olof**
  1290 Versoix, Geneva (CH)
- **Hederstierna, Christer Fredrik**
  1290 Versoix, Geneva (CH)
- **Hackett, Nicholas J.**
  1290 Versoix, Geneva (CH)

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

(54) A SECURITY MONITORING SYSTEM

(57) A security monitoring system for a building or a secured space within a building, the system being operatively connected to a monitoring station, the system including:
a control unit for controlling, arming and disarming the security monitoring system, and having a radio frequency transceiver, and a controller for controlling the radio frequency transceiver;
a camera node having: a node controller;
an image sensor for capturing images;
a node radio frequency transceiver, for communication with the control unit;
the node controller being configured to:
transmit a captured image as an image file using the node radio frequency transceiver, wherein the transmission of the image file to the control unit is subject to a predetermined maximum transmission duration; and
wherein the node controller is further configured to determine the resolution and compression of the image file based on the predetermined maximum transmission duration and an estimate up of the uplink bandwidth between the camera node and the control unit in order to enable the image file to be transmitted to the control unit within the predetermined maximum transmission duration;

the control unit being configured:
to perform measurement of RSSI and to transmit a measured RSSI value to the camera node;
in response to receiving an event notification from a node of the system, to transmit, using the radio frequency transceiver, a control message to the camera node for the camera node to transmit a captured image;
the control unit being further configured, on reception of a captured image file from the camera node, to transmit the received image file to the monitoring station.

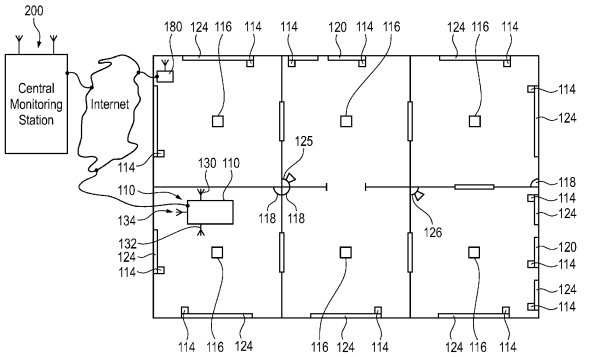

Fig. 1

EP 3 828 849 A1

Description

Technical field

[0001] The present invention relates to a security monitoring system for monitoring premises, a camera node and a control unit for such a system, and methods of operating a camera node, a control, and a 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 to detect the opening and closing of doors and windows, movement detectors to monitor spaces for signs of movement, microphones to detect sounds such as breaking glass, and image sensors to capture still or moving images of monitored zones. Such systems may be self-contained, with alarm indicators such as sirens and flashing lights that may be activated in the event of an alarm condition being detected. Alternatively, a security monitoring system may include an installation at a premises, domestic or commercial, that is linked to a Central Monitoring Station (CMS) where typically human operators manage the responses required by different alarm and notification types.

Such installations typically include a central unit (also known as a control unit) that is coupled to the sensors, detectors, cameras, etc. ("nodes"), and which processes received notifications and determines a response. The central unit is commonly linked to the various nodes wirelessly, rather than by wires, since this facilitates installation and may also provide some safeguards against sensors/detectors effectively being disabled by disconnecting them from the central unit. Similarly, for ease of installation and to improve security, the nodes of such systems typically include an autonomous power supply, such as a battery, rather than being mains powered.

In 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.

[0003] 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. 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 or otherwise have their actions 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.

Further to this, it is very important to ensure a swift and timely delivery of notifications and alarms from the node to the CMS so that necessary and appropriate actions and interventions can be organised. Perhaps surprisingly, from a practical perspective, delaying the initial delivery of a notification of an incident to the CMS by even a second or less can have very significant consequences - and this is because of the effective quantisation of the availability of response options. For example, there will always be a limited number of available first responders, and response vehicles (collectively "first responder resources"), and in general once a first responder resource has been allocated to a first incident, that resource will not be available for allocation to another incident until stood down from the first. In other words, even a momentary delay in delivering the initial incident report to the CMS can lead to delays of minutes or hours in delivering the necessary response to the incident - and of course the consequence of a delayed response may quite literally be fatal.

[0004] It is known to provide video cameras for security monitoring systems with Wi-Fi radios to enable them to transmit video data to a central unit of the monitoring system over Wi-Fi. The Wi-Fi radio, and the video camera, are turned on in the event that a PIR associated with the video camera detects movement. Unfortunately, Wi-Fi radios tend to drain batteries quite quickly, and such an arrangement typically requires large capacity batteries, and/or an external power source, if frequent battery replacement or power loss are to be avoided. Another disadvantage of using Wi-Fi in a security system is that one needs to monitor or supervise the nodes of the system. This is done by periodic messaging, and Wi-Fi consumes significant power in performing this simple task.

[0005] It would be beneficial if an alternative approach could be provided to enable, for example, video data to be transmitted at high speed between a node and a central unit of a security monitoring system, to enable timely action to be taken based on the information contained in the video data, in such a way as to avoid excessive power consumption at the node, thereby prolonging battery life at the node.

Summary of the invention

[0006] According to a first aspect, the present invention provides a camera node for a security monitoring system for a building or a secured space within a building , the system including a control unit for controlling, arming and disarming the security monitoring system; the camera

node comprising:

a node controller;
an image sensor for capturing images;
a node radio frequency transceiver, for communication with the control unit;
the node controller being configured to:

transmit a captured image as an image file using the node radio frequency transceiver, wherein the transmission of the image file to the control unit is subject to a predetermined maximum transmission duration; and
wherein the node controller is further configured to determine the resolution and compression of the image file based on the predetermined maximum transmission duration and an estimate up of the uplink bandwidth between the camera node and the control unit in order to enable the image file to be transmitted to the control unit within the predetermined maximum transmission duration.

[0007] Such a camera node is advantageous in that it enables useful image data of the best available quality to be delivered to the central monitoring station within a known acceptable delay from the triggering of an event.

[0008] According to a further aspect of the invention, there is provided a method of operating a camera node of a security monitoring system for a building or a secured space within a building , the system including a control unit for controlling, arming and disarming the security monitoring system;
the camera node including:

a node controller;
an image sensor for capturing images;
a node radio frequency transceiver, for communication with the control unit;
the method comprising:

the node controller transmitting a captured image as an image file using the node radio frequency transceiver, wherein the transmission of the image file to the control unit is subject to a predetermined maximum transmission duration; and
determining the resolution and compression of the image file based on the predetermined maximum transmission duration and an estimate up of the uplink bandwidth between the camera node and the control unit in order to enable the image file to be transmitted to the control unit within the predetermined maximum transmission duration.

[0009] According to a further aspect of the present invention, there is provided a control unit for a security monitoring system for a building or a secured space within a building, the system being operatively connected to a monitoring station, and the system including a camera node having:

a node controller;
an image sensor for capturing images;
a node radio frequency transceiver, for communication with the control unit;
the control unit having:

a radio frequency transceiver for communication with the camera node, and a controller for controlling the radio frequency transceiver;
the control unit being configured:

to perform measurement of RSSI and to transmit a measured RSSI value to the camera node;
in response to receiving an event notification from a node of the system, to transmit, using the radio frequency transceiver, a control message to the camera node for the camera node to transmit a captured image;
the control unit being further configured, on reception of a captured image file from the camera node, to transmit the received image file to the monitoring station.

[0010] According to a further aspect of the present invention there is provided a method of operating a control unit for a security monitoring system for a building or a secured space within a building, the system being operatively connected to a monitoring station, and the system including a camera node having:

a node controller;
an image sensor for capturing images;
a node radio frequency transceiver, for communication with the control unit;
the control unit having:

a radio frequency transceiver for communication with the camera node, and a controller for controlling the radio frequency transceiver;
the method comprising:

performing measurement of RSSI and transmitting a measured RSSI value to the camera node;
in response to receiving an event notification from a node of the system, transmitting, using the radio frequency transceiver, a control message to the camera node for the camera node to transmit a captured image;
on reception of a captured image file from the camera node, transmitting the received image file to the monitoring station.

[0011] According to a further aspect of the present invention there is provided a security monitoring system for a building or a secured space within a building, the system being operatively connected to a monitoring station, the system including:

a control unit for controlling, arming and disarming the security monitoring system, and
having a radio frequency transceiver, and a controller for controlling the radio frequency transceiver;
a camera node having:

a node controller;
an image sensor for capturing images;
a node radio frequency transceiver, for communication with the control unit;
the node controller being configured to:

transmit a captured image as an image file using the node radio frequency transceiver, wherein the transmission of the image file to the control unit is subject to a predetermined maximum transmission duration; and
wherein the node controller is further configured to determine the resolution and compression of the image file based on the predetermined maximum transmission duration and an estimate up of the uplink bandwidth between the camera node and the control unit in order to enable the image file to be transmitted to the control unit within the predetermined maximum transmission duration;
the control unit being configured:

to perform measurement of RSSI and to transmit a measured RSSI value to the camera node;
in response to receiving an event notification from a node of the system, to transmit, using the radio frequency transceiver, a control message to the camera node for the camera node to transmit a captured image;
the control unit being further configured, on reception of a captured image file from the camera node, to transmit the received image file to the monitoring station.

[0012] According to a further aspect of the present invention there is provided a method of operating a security monitoring system for a building or a secured space within a building, the system being operatively connected to a monitoring station, the system including:

a control unit for controlling, arming and disarming the security monitoring system, and
having a radio frequency transceiver, and a controller for controlling the radio frequency transceiver;
a camera node having:

a node controller;
an image sensor for capturing images;
a node radio frequency transceiver, for communication with the control unit;
the method comprising:

the node controller transmitting a captured image as an image file using the node radio frequency transceiver, wherein the transmission of the image file to the control unit is subject to a predetermined maximum transmission duration; and
determining the resolution and compression of the image file based on the predetermined maximum transmission duration and an estimate up of the uplink bandwidth between the camera node and the control unit in order to enable the image file to be transmitted to the control unit within the predetermined maximum transmission duration;
the control unit performing measurement of RSSI and transmitting a measured RSSI value to the camera node;
and
on reception of a captured image file from the camera node, the control unit transmitting the received image file to the monitoring station.

Brief description of the drawings

[0013] 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 control unit of Figure 1; and
Figure 3 is a schematic drawing showing features of a two-transceiver camera node of the security monitoring system according to an embodiment of the invention.

Specific description

[0014] One of the principal components of node power consumption is activity of the circuitry responsible for wireless, typically RF, communication with the control unit 110. Generally, in high security systems, nodes are in bidirectional contact with the central unit, being able to receive as well as send information to the control 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 syn-

chronised with the master clock in the control unit 110. To maintain synchronisation, the control 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 control unit, in the event of detecting an incident, without the nodes' transmissions colliding. Power consumption considerations also influence the choice of RF communication mode, and regular speed transmission is typically possible between the nodes and the control unit, and vice versa. Typically such low power radio systems make use of ISM radio channels and protocols designed to reduce power consumption.

[0015] 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 shut down to avoid consuming power, typically only being powered up when trigged by low power functionality of the detector, when another sensor detects movement or when instructed to power up by the control unit 110.

[0016] The use of regular speed transmission is possible and in many cases advantageous because, in general, nodes can notify the central unit of events with only very modest quantities of data. The main exceptions are sensors which provide image data, image sensors - generally cameras of some kind, and those which provide sound data - microphones, which can each produce significant quantities of data. Although it is of course possible to send such large quantities of data over a low bit rate channel, this takes considerable time and consequently consumes a lot of power. If an event has been detected by a sensor such as a PIR or a door/window opening sensor, and there is for example a video camera able to monitor a zone including the location of the event, it would be desirable to be able to transfer useable images and video frames to the central unit as soon as possible so that the nature and scale of the threat can be determined - and so that in a centrally monitored system the images/video sequence can be forwarded to the CMS 200 for analysis and action. Currently such analysis is typically performed by human operators, but it is likely that in the near future artificial intelligence will be used to supplement, and eventually perhaps replace or largely replace .human operators. But in any event, the need exists for images and video sequences to be available for analysis at the CMS as soon as possible after an incident is first detected.

[0017] 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 control unit, 110, which is connected to the monitoring centre 200 by means of a data connection 150. The data connection 150 may be provided over a phone line, a broadband internet connection, Ethernet, a dedicated data connection, or wirelessly, for example using an LTE or GSM network, and in general multiple of these options will exist for any installation, so that there is security of connection between the gateway 110 and the monitoring centre 200. For additional security, the central unit 110, or a sensor in communication with the central unit 110 and the monitoring centre may both be provided with means to support an ISM radio connection, for example in the European 863 to 870MHz frequency band, preferably one configured to resist jamming.

[0018] The domestic installation 100 involves a typical arrangement where the exterior doors 120 and windows 124 are fitted with sensors 114, for example magnetic contact sensors, to detect opening of the door or window. Each of the rooms of the building having the installation may be provided with a combined fire/smoke detector 116, as shown in the Figure. 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 motion detector. Similarly, the kitchen which is entered from the back door 121 is monitored by a video camera 126 which includes a motion detector. Each of the sensors, detectors and video cameras, which may throughout this specification be referred to generically as nodes, includes a wireless interface by means of which it can communicate with the central unit 110. The central unit 110 includes first and second antennas 130 and 132 for communication with the sensors, detectors and video cameras. In addition, the central unit 110 may include at least one further antenna 134 for wireless communication with the monitoring centre. Each of these antennas may be connected to a corresponding transceiver, not shown. Additionally, the central unit 110 may include a dedicated antenna arrangement for Wi-Fi, for example to connect to camera nodes 125 and also 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.

[0019] Some installations may include more than one control unit (CU), for example two control 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 installa-

tion 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.

[0020] In a domestic installation 100, the control 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 control unit during a login procedure during setup of the installation 100. Alternatively and/or additionally, some or all capabilities may be communicated to the control unit from the node upon request from the control unit 110. Alternatively and/or additionally, some or all capabilities may be retrieved, by the control unit 110, from the CMS 200.

[0021] Figure 2 is a schematic drawing showing in more detail features of a gateway or control unit 110 of Figure 1. The control unit 110 includes a first transceiver 230 coupled to the first antenna 130. The transceiver 230 can both transmit and receive, but cannot both transmit and receive at the same time. Thus, the transceiver 230 operates in half duplex, and may use the same frequency for transmit and receive, or different frequencies. The transceiver 230 is 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, as well as stored programs to control the operation of the control unit. In general, the control unit acts as a router providing a path to the central monitoring station for audio and video (more generally image) data - the storing of such data at the control unit is optional. The control unit 110 includes a power supply 262 which may be coupled to a domestic mains supply, from which the control unit 110 generally derives power, and a backup battery pack 264 which provides power to the control unit in the event of failure of the mains power supply.

The control unit 110 also includes a second transceiver 240 which, unlike the first transceiver, supports the use of Wi-Fi protocols (using some variant of IEEE 802.11), and associated antenna arrangement 242, which may be used for communication with any of the nodes that is Wi-Fi enabled, for example with one or camera nodes. A Wi-Fi enabled camera node may include or be associated with a motion detector and have video and/or still picture capabilities. Such a Wi-Fi node (whether a camera node or not) may, and preferably will, include both means for Wi-Fi communication and means for regular (non-Wi-Fi) ISM communication.

The control unit 110 may also include an interface enabling bidirectional communication over a Public Land Mobile Network (PLMN), such as GSM or LTE, and one is shown in the Figure as interface 244 with antenna arrangement 246. Optionally, a third antenna 134 and associated ISM transceiver 234 may be provided for communication with the monitoring centre 200 over, for example, the European 863 to 870MHz frequency band.

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

[0022] The first transceiver is tuneable ISM device, operating for example in the European 863 to 870MHz frequency band or in the 915MHz band (which may span 902-928MHz or 915-928MHz depending upon the country). The first transceiver may be tuned, i.e. is tuneable, to the frequencies within the regulatorily agreed subbands within this defined frequency band. As will be explained, first transceiver 230 generally provides a control channel for communication between the control unit and the nodes of the system, but may also be used for other purposes. Whereas the Wi-Fi transceiver 240 is used to support a high speed channel (that is one having a higher symbol rate or bitrate than the control channel provided by the first transceiver) that is not supported by the first transceiver. But the controller of the gateway may be configured to offer one or more communication channels operated over the first transceiver that provide a higher transmission speed than is provided by control channel provided by the first transceiver.

[0023] Figure 3 is a schematic drawing showing features of a Wi-Fi enabled node of the security monitoring system according to an embodiment of the invention. In this case the node is a camera node like the video camera 126 which is mounted in the kitchen, as shown in figure 1, although it could instead be a camera to produce only still images or sequences of still images. The Wi-Fi node includes one radiofrequency node transceiver 340, coupled to an antenna 330, primarily for the exchange of control messages with the control unit. This transceiver may be referred to as the secondary transceiver. The camera node also includes a primary radiofrequency node transceiver 350, coupled to an antenna 355, which supports the use of Wi-Fi protocols and which hence can communicate with the second transceiver of the control unit 110. A controller 360 is coupled to the primary and secondary transceivers of the node, and also to the image sensor 310 of the video camera. The controller 360 may also be coupled to a motion sensor 320, which may be an integral motion sensor, as shown, or one mounted remotely, and to a memory 370. An autonomous power

supply, for example a battery, 380, provides power to the node, in particular powering the controller, transceivers, image sensor and integral motion sensor (if present). The autonomous power supply may include one or more elements to enable energy to be obtained from the environment - such as one or more photovoltaic elements, an RF energy harvesting arrangement, and even a compact wind turbine arrangement. The video camera also includes a lens arrangement 315 for forming an image on the image sensor 310. Optionally, the node includes an infrared light source 325, and possibly a source of visible light, suitable for illuminating images detectable by the image sensor. The secondary 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 transceiver of the gateway 110. Likewise, the secondary node transceiver 350 is tuneable. In particular, the secondary node transceiver 350 can be tuned to frequencies to match those transmitted by or receivable by the second transceiver of the control unit 110.

[0024] When a motion detector, for example a PIR (passive infrared) sensor of or associated with a camera node, detects motion it transmits a signal to the control unit 110 using the secondary node transceiver in control channel mode. Depending on the settings of the system, the control unit 110 may forward this movement detected signal to the central monitoring station. If the motion detector reporting the detection of motion is, for example, in or associated with a video camera, the control unit 110 will know this from the identity of the node that transmitted the motion detected signal. The control unit 110 may then send a message to the video camera using the control unit's first transceiver in control channel mode, the message requesting the video camera to transmit video data to the central unit 110 at high speed (e.g. higher bitrate than is used for control signals). Such a request may be for the video camera to stream video data. More generally, the control unit may send a message to an image source, such as a camera, requesting it to transmit image data, in the form of an image file, at high speed. Alternatively, if the

[0025] Trigger events other than the triggering of a movement sensor may also be used to initiate the process. For example, the activation of a node that monitors the status of an entrance to the building or to a controlled space in the building, for example a magnetic switch at a door or window, or detection of a sound, such as that of breaking glass, by a node comprising a microphone, will be transmitted by the relevant node to the control unit 110. The control unit 110 may, depending upon its programming and status, report the event to the CMS 200. Alternatively, a trigger event may be sent from CMS 200 requesting images or audio data from a particular node, this trigger may be used by the control unit 110 to instruct that particular node to transmit the requested images or audio data.

First Example

[0026] A first approach to reducing the time needed to transmit in particular image data to the central monitoring station will now be described.

[0027] If a motion detector of or associated with a camera node detects motion, the camera is activated to capture an image(s) or video. The camera node will then prepare two images or clips. One of the images or clips will be a relatively low resolution (e.g. standard VGA or QVGA) in the form of an image file of modest file size (**e.g**. 30kB once compressed), while the other image will be of significantly higher resolution (**e.g**. 1080P or 4K,) and in the form of an image file of considerably (which might have a file size possibly in the range 600kB - 2MB) greater size (although the size of the image file once compressed might be in the range of 4 to 10 times the size of the compressed low resolution image file . The smaller image file, (hereinafter the second image file) is transmitted using the secondary transceiver of the node, while the larger image file (hereinafter the first image file) is transmitted using the node's Wi-Fi primary transceiver. The node controller provides the two image files with the same ID.

The system may be configured such that when the control unit receives an event notification from the motion sensor, the control unit sends a message to the camera node (over a non-Wi-Fi channel) instructing the camera node to transmit image data.

The idea is that although it is better for the CMS (more particularly the analyst in the CMS) to receive the more detailed image file, it may be that the smaller file sent using the secondary transceiver may actually arrive sooner than that sent via the Wi-Fi transceiver, for example due to congestion of the Wi-Fi network or interference (intentional or not) with transmission over the Wi-Fi network) - and hence the CMS may be able to make an earlier decision based on the smaller image file than would be the case if the CMS had to await the bigger file sent via Wi-Fi.

It will be appreciated that where the system is configured such that when the control unit receives an event notification from the motion sensor, the control unit sends a message to the camera node (over a non-Wi-Fi channel) instructing the camera node to transmit image data the node's secondary transceiver will already be active - having been used to receive the message from the control unit, the secondary transceiver is likely to be able to begin transmitting its smaller image file before the node's Wi-Fi transceiver has been activated, configured and registered with the Wi-Fi transceiver (effectively the Wi-Fi bases station) of the control unit. It may therefore be the case that even though the node controller nominally initiates the two transmission processes at the same time, the smaller image file transmitted by the node's secondary transceiver may actually arrive before the larger image file sent via Wi-Fi, even if the current radio environment supports high speed transmission over a Wi-Fi channel.

The control unit 110 forwards to the CMS the first to arrive of the first or second image files. Subsequently, if the first arrived file was the smaller second image file, on arrival of the larger first image file, the control unit will forward the first image file to the CMS. Conversely, of course, the control unit does not forward the smaller second image file to the CMS if the larger first image file with the same ID has already been forwarded to the CMS.

[0028] At the CMS, the human (or AI) analyst reacts to the arrival of the first to arrive image file. If another image file with the same ID arrives at the CMS while the relevant event is still being handled by the analyst, the CMS system substitutes the later arriving image file for the first. The system of the CMS may be configured to notify the operator of the availability of a higher resolution image file. For example, a work station of a human operator may provide an on-screen warning and/or an audible announcement of the updating of the available image.

Second Example

[0029] In an alternative approach, with a camera node which has a primary transceiver which supports a first maximum bandwidth, and a secondary transceiver that supports a second maximum bandwidth lower than the first and which is used for exchanging control signals with the control unit, the secondary transceiver may be used to provide redundancy enabling an image file to be transmitted to the control unit even though that image file sent using the primary transceiver has failed to reach the control unit.

A camera node may be configured to transmit, possibly in response to receiving a message from the control unit to transmit image data, the image file using just the primary transceiver, or may be configured, as in the first example, to transmit image data by transmitting the image file using both the primary and secondary transceivers. The control unit may be configured to respond to receiving an image file by transmitting an acknowledgement ("ack") message, so that the camera node knows whether or not the transmission of an image file was successful. If the camera node fails to receive an expected ack message in respect of the transmission of an image file using the primary transceiver, it may be configured to attempt to transmit the image file (or a smaller image file) using the secondary transceiver instead. With the camera node set up as in the first example, if an ack message is received in respect of an image file transmitted using the secondary transceiver but not in respect of an image file transmitted using the primary transceiver, the camera node may be configured to transmit the higher resolution image file using the secondary transceiver. Although the lower bandwidth of the secondary transceiver will mean that transmission of the larger file will take longer than it should have taken using the primary transceiver, if transmission problems are affecting the higher bandwidth channel the larger file might actually reach the CMS more quickly using the lower bandwidth transceiver instead of the primary transceiver.

So, for example, in a camera node having a Wi-Fi enabled primary transceiver and a non-Wi-Fi control channel transceiver, an image file intended for transmission using the primary transceiver may instead be sent using the control channel transceiver in the event that an expected ack message in response to attempted transmission of the image file using the primary transceiver is not received.

It will be appreciated that a low resolution image can enable a person/ not a person decision to be made - e.g. distinguishing between the presence of a non-human animal or other source of movement, such as vegetation being moved by the wind, whereas a higher resolution image file may enable a description to be given of the person or persons captured by the image, or to enable the identity of the person or persons captured by the image - e.g. to enable the householder to be told that one or other children of the house are present. And clearly it is therefore useful to provide a higher resolution file to the CMS even after the supply of a low resolution image (e.g. despite the availability of a low resolution thumbnail).

Third Example

[0030] In an alternative approach, a camera node having one transceiver that supports one or more control channels and another, primary transceiver that supports a higher bitrate, is arranged to maintain the primary transceiver in an inactive state (e.g. powered down, turned off) until either the control channel transceiver (which may be termed the secondary transceiver) receives a message from the control unit of the system following the latter's reception of an event notification from a node of the system, or the primary transceiver is activated as the result of a motion (or other) sensor of or associated with the camera node being triggered causing the camera to capture one or more images or video sequences.

The message from the control unit of the system includes credentials for use by the primary transceiver in accessing a higher bitrate channel for the transmission of an image file.

For example, where the primary transceiver is configured for accessing a Wi-Fi channel, the message from the control unit may contain the SSID, PSK and channel ID to enable the primary transceiver to reduce the lead time needed to access a transmission channel. Although Wi-Fi enabled devices typically store the SSID and corresponding PSK of the last Wi-Fi connection that they used, generally the channel identifier is not stored - because in general Wi-Fi devices switch between different channels of an SSID very frequently. It is therefore normal for a Wi-Fi enabled device to have to hunt for a free channel with the correct SSID before being able to start to transmit data. By having the system control unit, which in this instance is also working as a Wi-Fi base station, provide

not only the relevant SSID and PSK but also the identifier of an available channel, potentially several seconds of delay are avoided. It also needs to be borne in mind that there may be months or potentially years between events in which the system control unit will message a particular camera node for image data. There is therefore a possibility that, when a camera node next needs to activate its primary transceiver, the SSID and or the PSK may have changed since the transceiver was last activated - so that the SSID and/or PSK in the memory of the camera node may no longer be correct. It will be appreciated that in general, most installed Wi-Fi devices maintain some level of connectivity with the Wi-Fi Base Station/ Access Point. In this example, and generally for all the examples, the camera node turns off its Wi-Fi transceiver completely when not in use.

By providing the secondary control channel (non-Wi-Fi), we can send all the access credentials, including channel ID, to the camera node, meaning that the camera node doesn't need to waste several precious seconds scanning for an available channel before being able to send its image file. The secondary control channel also enables the control unit to transmit any changes in the Wi-Fi credentials as and when they occur, so that the updated credentials are stored in a memory of the camera node for use when the camera node next needs to use its Wi-Fi transceiver. Consequently, even if since the last time the Wi-Fi transceiver of the camera node was in use there have been changes to the credentials needed to access a suitable Wi-Fi channel, the camera node will quickly be able to access a suitable channel. Clearly, the transmissions of the Wi-Fi access credentials must be secure from eavesdroppers, so they are encrypted appropriately. Thus, the following way of working is also supported in this example:

1. PIR detects motion
2. Image is captured by camera
3. The Wi-Fi credentials needed should be stored (the last know ones are stored) in the node and available for use when needed

    a. If the Wi-Fi channel changes while the primary node receiver is off, then the updated Wi-Fi credentials should have been communicated by the CU to the node via 868 during this time, so that they are available when needed

4. The node Wi-Fi connects with the network
5. The image is sent via Wi-Fi without waiting for there to be an exchange via 868 which ends in the control message from the CU asking for the image.

Fourth Example

[0031] In an alternative approach, which can work even if the camera node only has one transceiver (but which works equally well in transceivers having two transceivers as in the other examples), a target delivery time is determined within which a camera image will be delivered to the central monitoring station. The camera node uses an estimate of uplink bandwidth to determine the parameters for the image file to ensure that the image file will be delivered in time at a level of quality satisfying a known quality requirement.

The control unit and the camera node periodically exchange control messages over a control channel, for example they may exchange control messages every 10 minutes. The control channel will typically be provided in the 868 MHz band. When sending such a control message, each of the control unit and the camera node will determine an RSSI level and supply the determined level to its counterpart. These supplied RSSI levels are stored until the next control packet is received.

When the control unit wants the camera node to transmit an image file, the control unit may send a message requesting an image file, and that message may include an RSSI measurement from the control unit. The camera node can then use this supplied RSSI measurement to estimate uplink bandwidth. The camera node may perform an RSSI check or similar at each of several RF frequencies to determine whether local signal conditions / background noise (e.g. interference or jamming) prevent or otherwise make undesirable the selection of particular ones of the several RF frequencies. Based on this determination, the camera node may compose an acceptance message, and the node transmits this message to the control unit at a usual control signal frequency/speed. The controller of the control unit 110 then sets the controls for the second transceiver to suit the parameters corresponding to the choice made by the node. The control unit 110 may then onward transmit these data to the CMS 200 using an available connection, so that an automated system or human operator can determine an appropriate response - such as despatching human intervention (e.g. security personnel, Fire, Police, Ambulance, etc.) or the like, and/or they may be played out locally to enable an appropriate response to be determined locally. When high speed data transmission is complete, the node sends notice to the control unit 110 (in any appropriate form) to enable the control unit 110 to repurpose the second transceiver. This will generally involve the control unit 110 switching the second transceiver back to a regular speed mode until the second transceiver is needed for some other purpose. Thus, the second transceiver can again be regarded as providing diversity.

[0032] The controller of the camera node may then determine a resolution and compression ratio to be used to produce an image file which can be delivered to the CMS within the target delivery at an acceptable resolution. For example, the controller of the camera node may refer to a table which, for a given target delivery time maps uplink bandwidth to target image file size and hence compression ratio. Clearly, if the uplink bandwidth is low, for a given resolution, the compression ratio may need to be high to ensure timely delivery . With higher uplink band-

width a lower compression ratio and/or higher resolution may be used - and the table will include the relevant parameters. The goal is to deliver something as quickly as possible.

The important input is the target size estimated based on the uplink. When we have the target size we can, based on experience, guess a good quality value for the compression. If we miss the target we can do a second one and if that also misses the target we can use linear extrapolation (even it is not 100% linear). As a rule of thumb its always better to compress than resample. It keeps more information in the image.

It can be seen that the camera node is configured to transmit a captured image as an image file using a node radio frequency transceiver, the transmission of the image file to the control unit being subject to a predetermined maximum transmission duration, the node controller being configured to determine the resolution and compression of the image file based on the predetermined maximum transmission duration and an estimate up of the uplink bandwidth between the camera node and the control unit in order to enable the image file to be transmitted to the control unit within the predetermined maximum transmission duration.

[0033] It may also be that the installation 100 is configured such that a user of the installation 100 can request images, audio data, or other relevant data from particular nodes of the installation 100 to be delivered to e.g. a mobile device of the user. The request may be generated from the mobile device and sent to the CMS 200 where it may be forwarded to the control unit 110. The control unit 110 may, if configured to do so, formulate an instruction and send that instruction to the node from which the user requested data.

[0034] The message from the control unit 110 requesting high speed transmission of video may specify the parameters of at least one high speed channel. The parameters may include the SSID and PSK for connection to the Wi-Fi transceiver of the control unit, and may also include an identifier for a particular channel provided by the SSID.

[0035] 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.

[0036] 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%
g**1** (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%

[0037] 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 control 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 channels may be offered in the g3 sub-band, which has an allowable ERP of 500mW (+27 dBm) with a 10% duty cycle. Again, more than one frequency may be pre-selected in this band to enable alternative options. But it will be appreciated that it the invention does not rely on the use of the g3 sub-band for the high speed channel, channels could be set aside for high speed use within the g1 or g2 sub-bands. If the security monitoring system is deployed in another territory, it is anticipated that the RF bands allocated security and alarm systems, or available for such use even if not specifically allocated, will likewise provide opportunities to preselect some frequencies for regular speed, control and messaging functions, while allowing others to be preselected for use as high speed channels in the context of the invention.

[0038] Typically, the regular speed channels or configuration may operate around 30 to 45 kbit/s - e.g. 38.4 kbit/s. The "High speed" may equate to 128 to 500 kbit/s e.g. 200 kbit/s.

[0039] The abovementioned frequencies and their corresponding maximum allowable duty cycles may optionally be used by the Control Unit 110 when formulating the offer to a node. The control unit 110 may have at least one counter per band and node keeping track of how much time each node has transmitted into each frequency band during a configurable time period. If the time spent transmitting is close to, or at, the maximum allowed duty cycle of the associated band, the Control Unit 110 may decide against making an offer of a high speed chan-

nel in that band. Correspondingly and optionally, each node may have similar counters keeping track of their respective time spent transmitting in each band and may consequently reject certain offers if they are in a band where the node is close to, or at, the maximum allowable duty cycle.

[0040] In one embodiment of the installation 100, more than one Control Unit 110 is part of the installation. The Control Units are in communication with each other and are synchronized. In this embodiment, the Control Unit 110 being used for high speed data may be chosen to be the Control Unit that has the most suitable data connection 150 to the CMS 200, for instance Ethernet over Wi-Fi over cellular.

[0041] References made to nodes having e.g. video capabilities or audio capabilities are understood to be easily replaced with nodes having other relevant functionality that will benefit from high bit-rate transfers such as, but not limited to still imaging, thermal imaging etc.

Claims

1. A camera node for a security monitoring system for a building or a secured space within a building , the system including a control unit for controlling, arming and disarming the security monitoring system;
   the camera node comprising:

   a node controller;
   an image sensor for capturing images;
   a node radio frequency transceiver, for communication with the control unit;
   the node controller being configured to:

   transmit a captured image as an image file using the node radio frequency transceiver, wherein the transmission of the image file to the control unit is subject to a predetermined maximum transmission duration; and
   wherein the node controller is further configured to determine the resolution and compression of the image file based on the predetermined maximum transmission duration and an estimate up of the uplink bandwidth between the camera node and the control unit in order to enable the image file to be transmitted to the control unit within the predetermined maximum transmission duration.

2. The camera node of claim 1, wherein the node controller is configured to transmit the image file only in response to receiving a control message from the control unit.

3. The camera node of claim 1 or claim 2, wherein the estimate of uplink bandwidth is based on one or more RSSI measurements.

4. The camera node of claim 3, wherein the node controller is configured to cause the camera node to perform measurement of RSSI, and the estimate of uplink bandwidth is based on a result of a measurement made by the camera node.

5. The camera node of claim 3 or claim 4, wherein the node controller is configured to cause the camera node to store an RSSI measurement received from the control unit, and the estimate of uplink bandwidth is based on an RSSI measurement received from the control unit.

6. The camera node of any one of claims 3 to 5, wherein the node controller is configured to determine an RSSI value and to transmit the determined value to the control unit.

7. A method of operating a camera node of a security monitoring system for a building or a secured space within a building , the system including a control unit for controlling, arming and disarming the security monitoring system;
   the camera node including:

   a node controller;
   an image sensor for capturing images;
   a node radio frequency transceiver, for communication with the control unit;
   the method comprising:

   the node controller transmitting a captured image as an image file using the node radio frequency transceiver, wherein the transmission of the image file to the control unit is subject to a predetermined maximum transmission duration; and
   determining the resolution and compression of the image file based on the predetermined maximum transmission duration and an estimate up of the uplink bandwidth between the camera node and the control unit in order to enable the image file to be transmitted to the control unit within the predetermined maximum transmission duration.

8. The method of claim 8, wherein the node controller is configured to transmit the image file only in response to receiving a control message from the control unit.

9. The method of claim 7 or claim 8, further comprising controlling the transceiver to determine an RSSI value and to transmit the determined RSSI value to the

control unit.

10. A control unit for a security monitoring system for a building or a secured space within a building, the system being operatively connected to a monitoring station, and the system including a camera node having:

a node controller;
an image sensor for capturing images;
a node radio frequency transceiver, for communication with the control unit;
the control unit having:

a radio frequency transceiver for communication with the camera node, and a controller for controlling the radio frequency transceiver;
the control unit being configured:

to perform measurement of RSSI and to transmit a measured RSSI value to the camera node;
in response to receiving an event notification from a node of the system, to transmit, using the radio frequency transceiver, a control message to the camera node for the camera node to transmit a captured image;
the control unit being further configured, on reception of a captured image file from the camera node, to transmit the received image file to the monitoring station.

11. A method of operating a control unit for a security monitoring system for a building or a secured space within a building, the system being operatively connected to a monitoring station, and the system including a camera node having:

a node controller;
an image sensor for capturing images;
a node radio frequency transceiver, for communication with the control unit;
the control unit having:

a radio frequency transceiver for communication with the camera node, and a controller for controlling the radio frequency transceiver;
the method comprising:

performing measurement of RSSI and transmitting a measured RSSI value to the camera node;
in response to receiving an event notification from a node of the system, transmitting, using the radio frequency transceiver, a control message to the camera node for the camera node to transmit a captured image;
on reception of a captured image file from the camera node, transmitting the received image file to the monitoring station.

12. A security monitoring system for a building or a secured space within a building, the system being operatively connected to a monitoring station, the system including:

a control unit for controlling, arming and disarming the security monitoring system, and
having a radio frequency transceiver, and a controller for controlling the radio frequency transceiver;
a camera node having:

a node controller;
an image sensor for capturing images;
a node radio frequency transceiver, for communication with the control unit;
the node controller being configured to:

transmit a captured image as an image file using the node radio frequency transceiver,
wherein the transmission of the image file to the control unit is subject to a predetermined maximum transmission duration; and
wherein the node controller is further configured to determine the resolution and compression of the image file based on the predetermined maximum transmission duration and an estimate up of the uplink bandwidth between the camera node and the control unit in order to enable the image file to be transmitted to the control unit within the predetermined maximum transmission duration;
the control unit being configured:

to perform measurement of RSSI and to transmit a measured RSSI value to the camera node;
in response to receiving an event notification from a node of the system, to transmit, using the radio frequency transceiver, a control message to the camera node for the camera node to transmit a captured image;
the control unit being further con-

figured, on reception of a captured image file from the camera node, to transmit the received image file to the monitoring station.

13. The security monitoring system of claim 12, wherein the node controller of the camera node is configured to transmit the image file only in response to receiving a control message from the control unit.

14. A method of operating a security monitoring system for a building or a secured space within a building, the system being operatively connected to a monitoring station, the system including:

a control unit for controlling, arming and disarming the security monitoring system, and
having a radio frequency transceiver, and a controller for controlling the radio frequency transceiver;
a camera node having:

a node controller;
an image sensor for capturing images;
a node radio frequency transceiver, for communication with the control unit;
the method comprising:

the node controller transmitting a captured image as an image file using the node radio frequency transceiver, wherein the transmission of the image file to the control unit is subject to a predetermined maximum transmission duration; and
determining the resolution and compression of the image file based on the predetermined maximum transmission duration and an estimate up of the uplink bandwidth between the camera node and the control unit in order to enable the image file to be transmitted to the control unit within the predetermined maximum transmission duration;
the control unit performing measurement of RSSI and transmitting a measured RSSI value to the camera node; and
on reception of a captured image file from the camera node, the control unit transmitting the received image file to the monitoring station.

15. The method of claim 14, including:

transmitting, in response to receiving an event notification from a node of the system, using the radio frequency transceiver of the control unit, a control message to the camera node for the camera node to transmit a captured image, in response to receiving a control message from the control unit; and
the node controller of the camera node only transmitting the image file in response to receiving the control message from the control unit.

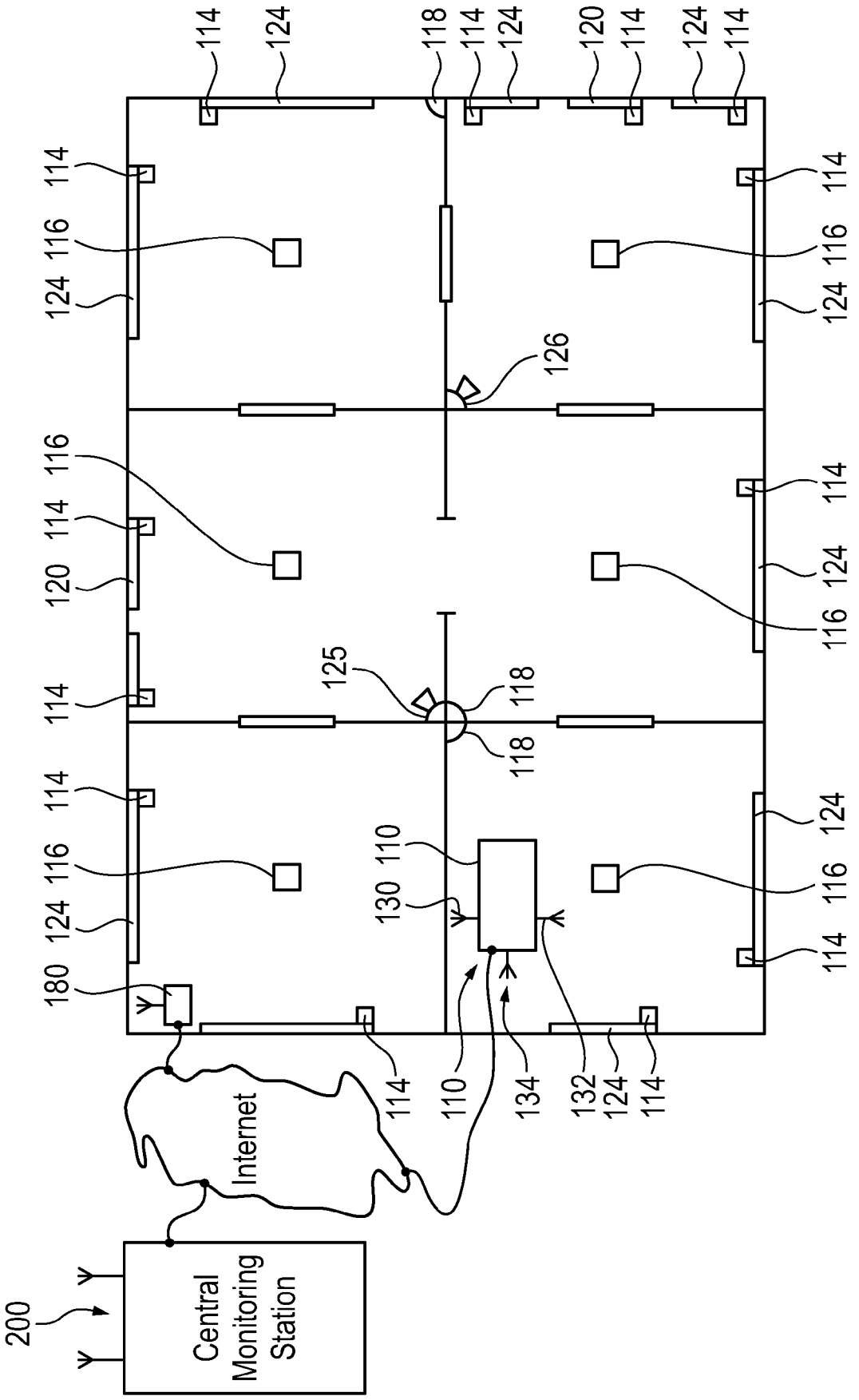
114
124
118
114
124
120
114
124
114
114
116
124
116
124
126
116
114
114
120
124
116
116
125
118
118
114
114
124
110
116
130
124
116
180
114
110
134
132
124
114
Internet
200
Central Monitoring Station

Fig. 1

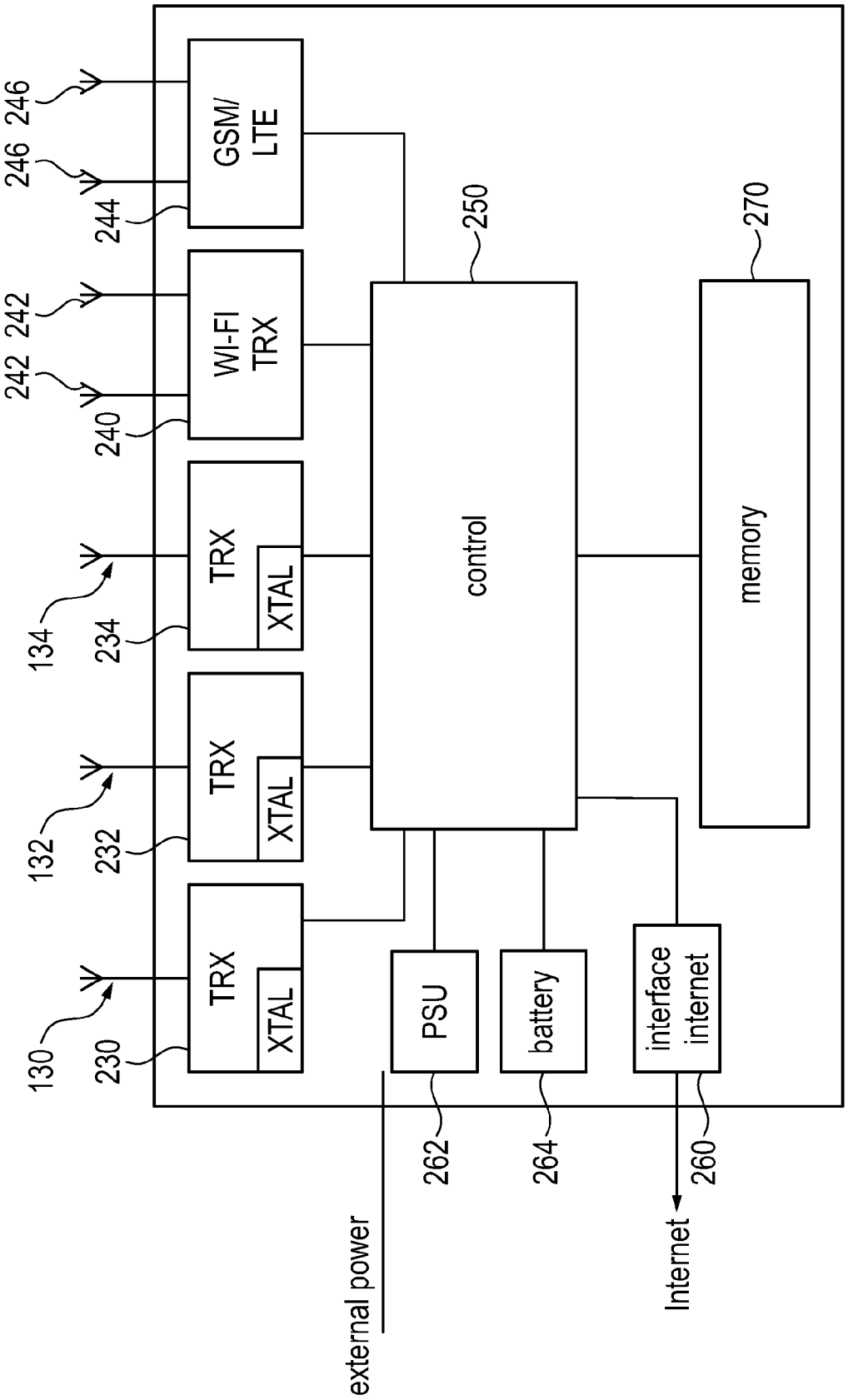
246
246
244
GSM/
LTE
242
242
240
WI-FI
TRX
134
234
TRX
XTAL
132
232
TRX
XTAL
130
230
TRX
XTAL
250
control
270
memory
PSU
battery
interface
internet
262
264
260
external power
Internet

Fig. 2

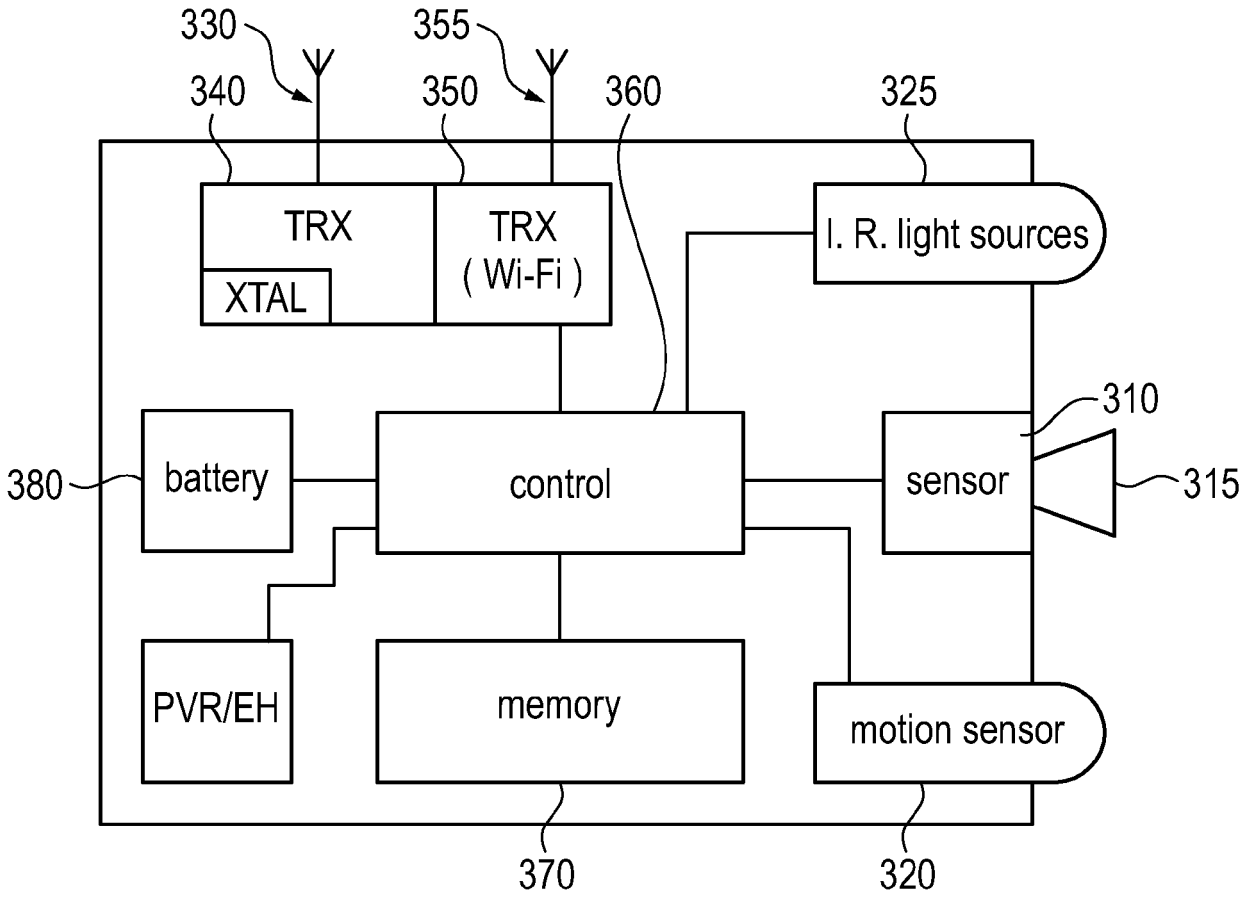
330
355
340
350
360
325
TRX
XTAL
TRX
(Wi-Fi)
I. R. light sources
310
380
battery
control
sensor
315
PVR/EH
memory
motion sensor
370
320

Fig. 3

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 19 21 1597

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X Y	US 2009/189981 A1 (SIANN JON [US] ET AL) 30 July 2009 (2009-07-30) * paragraph [0003] - paragraph [0033] * * paragraph [0042] - paragraph [0075] * * paragraph [0097] - paragraph [0126] * * paragraphs [0130], [0217] *	1,2,7,8, 10-15 3-6,9	INV. G08B13/196
Y	US 2019/197896 A1 (BAKHISHEV TEYMUR [US] ET AL) 27 June 2019 (2019-06-27) * paragraphs [0051], [0052], [0087], [0088] *	3-6,9	
Y	US 9 756 570 B1 (RAMACHANDRA MANJUNATH [IN]) 5 September 2017 (2017-09-05) * column 3, line 29 - column 6, line 53 *	1,7, 10-12,14	
Y	US 2016/171853 A1 (NAIDOO SURENDRA N [US] ET AL) 16 June 2016 (2016-06-16) * paragraph [0030] - paragraph [0042] * * paragraph [0064] - paragraph [0071] *	1,7, 10-12,14	
			TECHNICAL FIELDS SEARCHED (IPC) G08B

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	31 March 2020	Dascalu, Aurel

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 19 21 1597

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

31-03-2020

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009189981 A1	30-07-2009	EP 2238758 A2	13-10-2010
		US 2009189981 A1	30-07-2009
		US 2011096168 A1	28-04-2011
		US 2016173833 A1	16-06-2016
		WO 2009094591 A2	30-07-2009
US 2019197896 A1	27-06-2019	US 2019197896 A1	27-06-2019
		US 2020082719 A1	12-03-2020
US 9756570 B1	05-09-2017	CN 107544657 A	05-01-2018
		EP 3264225 A1	03-01-2018
		US 9756570 B1	05-09-2017
US 2016171853 A1	16-06-2016	US 2014232861 A1	21-08-2014
		US 2016171853 A1	16-06-2016

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82