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

(11) **EP 4 092 643 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
23.11.2022 Bulletin 2022/47

(21) Application number: **21174825.6**

(22) Date of filing: **19.05.2021**

(51) International Patent Classification (IPC):
G08B 13/196 *(2006.01)*

(52) Cooperative Patent Classification (CPC):
G08B 13/19697

(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
Designated Validation States:
KH MA MD TN

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

(72) Inventor: **WESTERGREN, Christian**
1290 Versoix, Geneva (CH)

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

(54) A SECURITY MONITORING SYSTEM

(57) Provided is a security monitoring system including: a system controller;
a video camera, coupled to a motion sensor, arranged to monitor a surveillance area;
a portable token storing a token ID; the video camera being configured on receipt of a motion detection signal from the motion sensor to send an alert to the system controller;
the system controller being configured in an armed state, on receipt of an alert from the video camera, to start an event timer and to send an instruction to the video camera to broadcast a token activation signal, the instruction including an event identifier;
the video camera further being configured to, on receipt of the instruction from the system controller, broadcast a token activation signal including the event identifier;
the portable token being configured to respond to receipt of a token activation signal from the video camera by broadcasting a response including the token ID and the event identifier;
the system controller further being configured: on receipt of a response from the token to: compare the event identifier included in the response with the event identifier included in the instruction to the video camera; compare the token ID included in the response with one or more stored token IDs; and to suspend the event timer if both comparisons provide a match; if either no response is received or one or both comparisons do not provide a match, to determine an alarm event on expiry of the event timer.

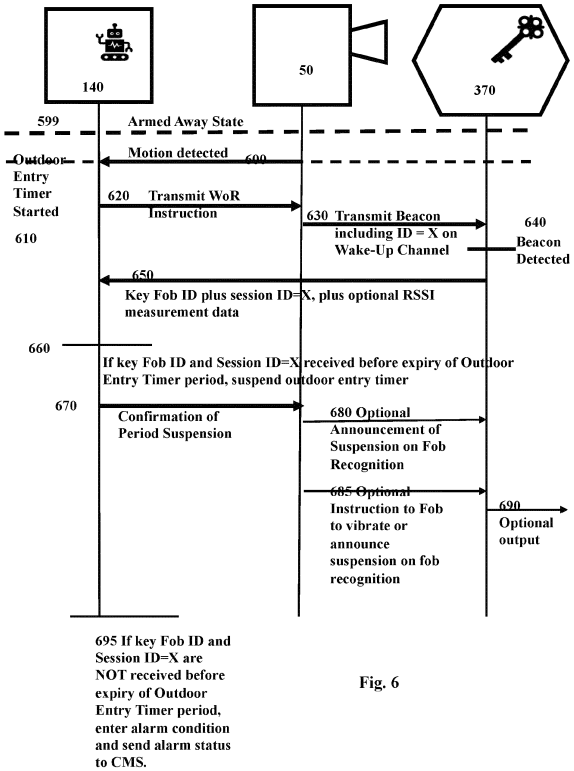


Fig. 6

EP 4 092 643 A1

Description

Technical field

[0001] The present invention relates to a security monitoring system for monitoring premises, a video camera for use with such a system and methods of configuring and operating such a monitoring system.

Background

[0002] Security monitoring systems for monitoring premises, often referred to as alarm systems, 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 (both within and outside buildings) 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 control unit (which may also be termed a central unit), generally mains powered, that is coupled to the sensors, detectors, cameras, etc. ("nodes"), and which processes received notifications and determines a response. The central unit may be linked to the various nodes by wires, but increasingly is instead linked 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 source, such as a battery power supply, rather than being mains powered.

[0003] As an alternative to self-contained systems, a security monitoring system may include an installation at a premises, domestic or commercial, that is linked to a Central Monitoring Station (CMS) where, typically, human operators manage the responses required by different alarm and notification types. In such centrally monitored systems, the central unit at the premises installation typically processes notifications received from the nodes in the installation, and notifies the Central Monitoring Station of only some of these, depending upon the settings of the system and the nature of the detected events. In such a configuration, the central unit at the installation is effectively acting as a gateway between the nodes and the Central Monitoring Station. Again, in such installations the central unit may be linked by wires, or wirelessly, to the various nodes of the installation, and these nodes will typically be battery rather than mains powered.

[0004] While security monitoring systems are normally developed to protect premises, such as houses or apartments, some installations include one or more cameras, typically video cameras, arranged to monitor external spaces such as terraces, gardens and forecourts. Typically, in such installations the (video) camera is associated with one or more movement sensors, the camera and the movement sensor(s) being arranged to cover a common surveillance area. When the system is armed, movement within the monitored surveillance area triggers the movement sensor, turning on the camera and alerting the central unit which in turn may signal an alarm condition to a central monitoring station.

[0005] Such external monitoring arrangements are a frequent source of false alarms, triggered by owners/occupiers of the protected premises who forget that the external area is monitored. False alarms can be expensive for system operators as they may require security personnel to be dispatched, and they can also annoy owners/occupiers so that they become dissatisfied with the system provider. Frequent false alarms may also lead to the owner/occupier leaving the monitoring systems unarmed - with the potential risk that real security breaches will not be detected by the security monitoring system.

[0006] -It would be desirable to be able to reduce or even eliminate this problem while still retaining a high level of security.

[0007] Embodiments of the invention provide potential solutions to the problems, in systems with external surveillance areas, of false alarms being triggered by authorised persons.

Summary of the invention

[0008] According to a first aspect, there is provided a security monitoring system including: a system controller; a video camera, coupled to a motion sensor, arranged to monitor a surveillance area; a portable token storing a token ID; the video camera being configured on receipt of a motion detection signal from the motion sensor to send an alert to the system controller; the system controller being configured in an armed state, on receipt of an alert from the video camera, to start an event timer and to send an instruction to the video camera to broadcast a token activation signal, the instruction including an event identifier; the video camera further being configured to, on receipt of the instruction from the system controller, broadcast a token activation signal including the event identifier; the portable token being configured to respond to receipt of a token activation signal from the video camera by broadcasting a response including the token ID and the event identifier; the system controller further being configured: on receipt of a response from the token to: compare the event identifier included in the response with the event identifier included in the instruction to the video camera; compare the token ID included in the response with one or more stored token IDs; and to suspend the event timer if both comparisons provide a match; if either no response is received or one or both comparisons do not provide a match, to determine an alarm event on expiry of the event timer.

[0009] The video camera and motion sensor may be arranged to survey a surveillance area and the video camera configured to broadcast the token activation signal as a radio signal having an effective range that does not extend significantly beyond the surveillance area.

[0010] Optionally, the portable token includes a processor coupled to a token movement sensor, and the token is configured to respond to token activation signals only if the processor determines that the token is moving.

[0011] Preferably, the portable token includes a wake on radio receiver, and the video camera is configured to broadcast token activation signals as wake on radio signals to which the token is responsive.

[0012] The portable token may be configured to include RSSI data in its response to the token activation signal from the video camera, and the system controller may be configured to use the RSSI data included in the token response in determining whether to trust the received response. Furthermore, the system controller may be configured to regard the token response as invalid if the RSSI data included in the token response suggest that the response has come from outside the usual range of radio signals from the camera. Preferably, radio frequency transceivers of the portable token, the video camera and the system controller are configured to operate in the industrial, scientific and medical, ISM, radio bands.

[0013] Preferably, the video camera is configured, on instruction from the system controller to transmit video images captured by the video camera using Wi-Fi.

[0014] The system controller is optionally configured, in an armed state, to disarm the security monitoring system if both comparisons provide a match.

[0015] Alternatively, the system controller may be configured in an armed state, if both comparisons provide a match, to disarm the security monitoring system only in respect of the monitoring of the surveillance area.

[0016] According to a second aspect, there is provided video camera for use in a security monitoring system according to any variant of the first aspect, the video camera including an image sensor, a radio frequency transmitter, a radio frequency receiver, and a processor operatively connected to the image sensor, the radio frequency transmitter and the radio frequency receiver, the processor being configured, on receipt of a motion trigger signal from a motion sensor to: transmit, using the radio frequency transmitter, a flag signal to the system controller of the security monitoring system; in response to receiving, via the radio frequency receiver, an instruction from the controller to cause the radio frequency transmitter to transmit a token activation signal.

[0017] Preferably, the token activation signal is a wake on radio signal. Optionally, the motion sensor is part of the video camera.

[0018] Preferably, the video camera's radio frequency transmitter and radio frequency receiver are configured to operate within the industrial, scientific and medical, ISM, radio bands, such as the 868 MHz band.

[0019] A video camera according to the second aspect may further comprise an RF transmitter configured to transmit Wi-Fi signals, and the video camera's processor may be configured, on instruction from the controller of a security installation to activate the RF transmitter to transmit via Wi-Fi video images captured by the video camera.

[0020] According to a third aspect, there is provided a method of configuring a security monitoring system, the method comprising: providing a system controller; a remote video camera coupled to a motion sensor; and a portable token storing a token ID; the video camera being configured on receipt of a motion detection signal from the motion sensor to send an alert to the system controller; the system controller being configured, on receipt of an alert from the video camera, to start an event timer and to send an instruction to the video camera to broadcast a token activation signal, the instruction including an event identifier; the video camera further being configured to, on receipt of the instruction from the system controller, broadcast a token activation signal including the event identifier; the portable token being configured to respond to receipt of a token activation signal from the video camera by broadcasting a response including the token ID and the event identifier; the system controller further being configured: on receipt of a response from the token to: compare the event identifier included in the response with the event identifier included in the instruction to the video camera; compare the token ID included in the response with one or more stored token IDs; and to suspend the event timer if both comparisons provide a match; if either no response is received or one or both comparisons do not provide a match, to determine an alarm event on expiry of the event timer.

[0021] According to a fourth aspect, there is provided a method of operating a security monitoring system, the security monitoring system including: a system controller; a video camera, coupled to a motion sensor, arranged to monitor a surveillance area; and a portable token storing a token ID; the method comprising: monitoring the surveillance area using the video camera and motion sensor; on receipt by the video camera of a motion detection signal from the motion sensor sending an alert to the system controller; on receipt of an alert from the video camera, the system controller starting an event timer and sending an instruction to the video camera to broadcast a token activation signal, the instruction including an event identifier; the video camera, on receipt of the instruction from the system controller, broadcasting a token activation signal including the event identifier; the portable token responding to receipt of the token activation signal from the video camera by broadcasting a response including the token ID and the event identifier; the system controller: on receipt of a response from the token, comparing the event identifier included in the response with the event identifier included in the instruction to the video camera; comparing the token ID included in the response with one or more stored token IDs; and suspending the event timer if both comparisons provide a match; if either

no response is received or one or both comparisons do not provide a match, determining an alarm event on expiry of the event timer.

[0022] Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a schematic drawing showing a stylised building with an external space which is monitored by a security monitoring system according to an embodiment of the invention;
Figure 2 is a schematic drawing showing major elements of a camera 50 (here a video camera) according to an aspect of the disclosure;
Figure 3 schematically shows the main components of various devices of a security monitoring system;
Figure 4 is a simplified schematic sequence diagram illustrating a method according to an aspect of the invention;
Figure 5 is another sequence diagram illustrating what happens when an unauthorised intruder enters the area monitored by security monitoring camera;
Figure 6 is a timing diagram showing the sequence of events and actions of the various elements of the security system that characterise a method, according to an embodiment of the invention;
Figure 7 is a flow chart illustrating one possible process for a portable authentication device 370 according to an embodiment of the invention; and
Figure 8 is a simplified schematic illustrating 2-stage detection.

Specific description

[0023] Figure 1 is an overview of a security monitoring system according to a first aspect of the invention. The Figure shows a rough plan view of a domestic dwelling 110, which may be a building such as a house or a secured space, such as an apartment, in a building and which is protected by a security monitoring system 100. The dwelling has a front door 120, in a doorway that is a main entrance giving access to the protected interior of the dwelling. The door 120 is fitted with a door sensor 130 to detect the opening of the door. The door sensor 130 is typically, but not necessarily, a magnetically triggered switch which is fitted to the opening side of the door, opposite to the hinge side. It will be appreciated that the door sensor is an example of a detector to detect the breaching of the entrance represented by the doorway. It will also be appreciated that the breaching of an entrance may also be detected using a motion sensor such as a PIR sensor, a video camera or other image sensor, a floor-mounted pressure sensor, or some other contact or non-contact sensor, any of which may be used to detect the breaching of an entrance into a building, garden, farm, etc., and which may therefore generate an alarm trigger signal to indicate the breaching of a monitored entrance.

[0024] The door sensor 130 includes an RF transmitter, not shown, that transmits an entry violation signal to a central unit 140 of the monitoring system 100 in the event that the door is opened. Inside the dwelling, close to the front door 120, a disarm node 150 is mounted on a wall. The disarm node 150 has a user interface, including a touch screen or keypad to receive a user input to disarm the system, and a radio frequency transmitter, not shown, to transmit, in consequence of the user input, a disarm instruction to the control unit 140. A similar disarm node 160 is also mounted on a wall of the kitchen near to a back door 170 which also gives access to the protected interior of the dwelling. The dwelling is also provided with Windows, 180, and these are provided with one or more sensors to detect window opening, glass breakage, tampering or the like.

[0025] The security installation 100 also includes an exterior monitoring camera, here a video camera, 50 with which is associated to transceiver 55 and a movement detector, such as a PIR detector 60. Although the transceiver 55 and the movement detector 60 are shown as mounted outside the casing of the video camera 50, commonly both the transceiver and the movement detector will be integrated into the camera and enclosed within the video cameras casing. The movement detector 60 and the video camera 50 are mounted to survey a monitored area, in this case a back garden associated with the domestic dwelling hundred and 10. The back garden being accessible through a garden gate 70. The owner or occupier of the domestic dwelling 110 may, for example keep removable valuables, such as scooter 80, in the back garden, and the exterior monitoring camera can help protect such removable valuables. In the example shown to the exterior monitoring camera 50 is not secured to the structure of the domestic dwelling 110, but rather is mounted remotely so that it can better survey both the rear exterior of the property and also the back garden. The video camera 50 is activated in the event that the movement detector 60 detects movement, for example when the garden gate 70 is opened and someone enters the garden. Upon activation, the video camera 50 uses the transceiver 55 to communicate with the central unit 140. If the security monitoring system is in an armed state, the central unit may be configured to enter an alarm state and, for example, communicate with a remote central monitoring station 190 wirelessly, or with a wired connection, for example via the Internet 195. The central unit 140 may instruct the video camera 50 to transmit images using the transceiver 55, and then forward the images to the central monitoring station for review. Upon review at the central monitoring station, you may be decided to dispatch security personnel and/or raise an alarm with the police.

[0026] Unfortunately, it is easy for an occupier of the dwelling to arm the security monitoring system prior to exiting the dwelling, and then to open the back gate 70 to retrieve the scooter 80, forgetting that by entering the back garden after having armed the security monitoring

system she will trigger an alarm condition. The present disclosure provides methods and apparatus to reduce the risk of such accidental triggering of alarm conditions.

[0027] Figure 2 illustrates schematically the major elements of a camera 50 (here a video camera) according to an aspect of the disclosure. The camera includes a camera module 200 that includes an image sensor and a lens. The camera module 200 is controlled by a processor 210, which includes RAM memory 215. Operatively coupled to the processor 210 is a further memory arrangement 220 for long term storage of program data and image data (although these may of course be stored in separate memories). The camera 50 is powered by a battery power supply 230. Optionally, a photovoltaic arrangement 240 may be provided to provide supplementary power and to charge a rechargeable battery within the battery power supply.

[0028] The processor 210 is also operatively coupled to the camera's RF transceiver 55. In the example shown two transceivers 55' and 55" are provided, and at least one of these transceivers uses the industrial, scientific and medical (ISM) radio bands, and RF transceivers is configured to provide Wi-Fi functionality. The two transceivers may be identical, or one may support ISM while the other supports Wi-Fi. Preferably, RF communication between the central unit and the nodes (including cameras 50), detectors and sensors of security monitoring systems according to embodiments of the invention use the industrial, scientific, and medical (ISM) radio bands, such as in Europe the 868MHz band. Within the 868 MHz band are several sub-bands dedicated to "non-specific SRD" which are of interest. When the camera 50 has image data, especially video image data, to send to the central unit 140, a transceiver 55 preferably uses Wi-Fi to transmit the data provided there is sufficient battery charge and sufficient available bandwidth. Each of the transceivers has an associated antenna arrangement.

[0029] Figure 2 also shows the motion sensor 60, which may be a PIR sensor, incorporated within the camera 50 and operatively coupled to the processor. Also shown are an optional microphone 250 and loudspeaker 260, both of which are operatively coupled to the processor 210. The loudspeaker may be used to provide feedback to an authorised user, as will be discussed later, and to enable communications from the central monitoring station 190 to be heard in the vicinity of the camera 50. Finally, the camera may include an indicator light 265, to provide optical feedback under the control of the processor 210. Of course, the camera may also be associated with an infrared or other light source, not shown, for use in illuminating the monitored area and effectively improving the quality of images obtained by the camera 50.

[0030] Figure 3 shows schematically shows the main components of various devices of the security monitoring system and that may be involved in arming and, more particularly, disarming the system, specifically the main elements of the central unit 140, and disarm node 150, and a key fob or token 370.

[0031] The central unit 140 includes a processor 300 with an associated memory 310 which stores, among other things, identities for the key fobs that are registered to the system, identities for the door sensors and disarm nodes of the system together with an association between each disarm node and the door sensor for the access door closest to the relevant disarm node. These identities and associations are stored in a database 315 within the memory 310. The central unit includes at least one RF transceiver 320, with associated antenna 322, for communication with the various nodes and sensors of the monitoring system. Typically, there will be a second transceiver 330 as shown, also with an associated antenna 332, for communication with the central monitoring station 190, as a backup or alternative to a wired data connection to the Internet via a network interface 340. The antennas of the various transceivers will typically all be internal to the central unit. The processor 300 is connected to, and controls, the memory 310, transceivers 320, 330 and the network interface 335. The central unit generally draws power from the domestic power supply (generally referred to as a mains power supply) which feeds a power supply 336 within or associated with the central unit. The central unit also includes a backup battery power supply which automatically becomes operational in the event that the external power supply fails. The internal battery power supply is based on rechargeable cells 337 that are kept continuously topped up by the power supply 350. The central unit may also include a user interface 325, including a display 326, a keypad or keyboard 327, a loudspeaker 328, and a microphone 329. The keypad or keyboard may be a provided by making the display a touch-sensitive display, or as a unit distinct from the display. The central unit may be arranged to accept through the keypad or keyboard a code or codes to arm and disarm the system. The central unit may also include a near field communication (NFC) antenna and a corresponding NFC chip or equivalent circuitry which can be used, for example, to detect the presence of a "disarm dongle" provided to the user of the system and which can communicate with the central unit using Near Field Communication. The key fobs may also be provided with an NFC antenna and chip or equivalent circuitry, so that they can be used as "disarm dongles" with the central unit and with NFC-enabled disarm nodes.

[0032] The disarm node 150 includes a processor 350 with an associated memory 351 that stores an ID of the disarm node. The disarm node also includes a user interface 352 comprising indicators, e.g. LEDs, 353, a keypad, 354, and optionally a display 355 which may be present instead of or in addition to the LED indicators. A transceiver 360, with an associated antenna 361 (which will typically be internal, rather than external as illustrated), is controlled by the processor 350, and is used for communicating with the central unit 140 and the key fob 370. The transceiver 360 will typically be configured to operate in the 868MHz ISM bands (or equivalent available ISM bands in countries outside Europe). The disarm

node includes a battery power supply 362, and in general this will be the only power supply as typically it is preferred not to have to connect disarm nodes to the mains power supply. A loudspeaker 363 is provided so that audible messages and instructions can be given to a user at the disarm node. These audible messages and instructions may be automated ones, generated by the central unit or by the disarm node itself, but additionally the loudspeaker 363 can be used to relay messages from a central monitoring station 190. The disarm node may also store audio files for these messages and instructions on its internal memory, to avoid problems caused by use of a low-bandwidth channel (e.g., an 868MHz RF channel) between the central unit and the disarm node. A disarm node storing such audio files may then receive instructions from the central unit to play out particular messages, and do so using the stored audio files. For example, the loudspeaker may be used to provide a disarm success or failure message. The disarm node may also store audio files for these messages and instructions on its internal memory, to avoid problems caused by the use of a low-bandwidth channel (e.g. an 868MHz RF channel) between the central unit and the disarm node. A disarm node storing such audio files may then receive instructions from the central unit to play out particular messages and do so using the stored audio files. Conveniently, the disarm node also includes a microphone 364 to permit a user at the disarm node to hold a conversation with a human operative in, for example, a central monitoring station 190, or even with the emergency services - for example if patched through by the central monitoring station. As an alternative, the disarm node may not include a microphone but a co-located external microphone provided to enable a user to speak to operatives in the Central Monitoring Station or the emergency services. Preferably, the disarm node 150 is secured to the building protected by the security monitoring system, for example attached to an internal wall at a height convenient for user operation - for example fixed at a height between 1 metre and 1.5 metres from the floor.

[0033] The system is arranged to permit the system to be armed and disarmed from a disarm node. The disarm node also includes a Near Field Communication antenna and chip 365 to enable a disarm dongle, such as an NFC-enabled fob, to be used to disarm or arm the system by bringing the dongle within a few centimetres of the disarm node - e.g., by bringing the fob into contact with the disarm node.

[0034] The disarm node may also be configured to encrypt its radio transmissions, and to decrypt received signals, so that secure communications with the central unit are possible. The encryption may be based on a secret shared between the central unit 140 and the disarm node 150.

[0035] The key fob 370 includes a processor 375, with an associated memory 376 that stores an identifier for the fob, a transceiver 377, and a battery 378 that provides power to the processor and the transceiver. Transceiver 377 is typically a conventional polling transceiver designed for low power consumption. Such a polling transceiver, when in a resting state, periodically powers just the front end of its receiver circuit to listen for polling signals. If a polling signal is detected, possibly subject to some power level minimum, the rest of the receiver circuit is energised to receive transmissions. Such a polling transceiver may listen for no more than about 100 - 125 ms each second, unless polling signals are detected. The transceiver, of whatever kind, is controlled by the processor and enables radio communication with the central unit 140, the disarm node 150 and the transceiver 55 of camera 50. The key fob also includes a motion sensor 379, such as an accelerometer, which is used to determine whether the key fob is being carried by someone or whether it is stationary. E.g. whether it has been deposited inside the house. may also include one or more buttons 380 which a user can use to issue commands or responses. The key fob may also include one or more visual indicators 385, for example one or more LEDs, to indicate a status, to confirm a button press, or the like. A single multi-coloured indicator, such as an LED, may be used to provide multiple different indications while keeping component count low and enabling the key fob dimensions to be made compact. The key fob may also include one or both of a loudspeaker and a haptic transducer 390 for providing user feedback.

[0036] The key fob is preferably configured to encrypt its radio transmissions, and to decrypt received signals, so that secure communications with the central unit are possible. The encryption may be based on a secret shared between the central unit and the key fob.

[0037] Figure 4 is a simplified schematic sequence diagram illustrating a method according to an aspect of the invention. In particular, it illustrates in a simplified way how a security monitoring system according to an aspect of the invention responds when an authorised person (someone carrying a registered key fob 370) enters a zone monitored by external security monitoring camera 50.

[0038] Let us imagine that an occupant of a premises (e.g. house) monitored by a security monitoring system according to an embodiment of the invention arms the system and then leaves the house, but then wants to collect her bicycle or scooter from the back garden. The occupant opens the garden gate 70 and enters the area monitored by the security monitoring camera 50. The opening of the garden gate 70 triggers, 400, the motion detector 60 associated with the camera 50, causing a motion trigger signal to be supplied to the processor 210 of the camera. The processor 210 then activates one of the transceivers 55 to transmit, 410, a motion trigger signal to the central unit 140. On receiving the motion trigger signal from camera 50, the central unit 140 starts, 420, an outdoor entry timer. The central unit 140 also transmits, 430, a start wake on radio instruction to the camera 50. On receiving the start wake on radio instruction, the camera 50 uses one of its transceivers 55 to transmit,

440, a low power out of band wake up signal whose strength is sufficient to wake up any key fob 370 that is within the monitored area. Because the occupant is carrying a key fob 370, her key fob wakes up and transmits, 450, a signal including the fob ID (which can be considered to be the start of a Login cycle). The signal from the key fob is received by the central unit 140, and if the fob ID is registered with the central unit 140, the central unit pauses, 460, the outdoor entry timer. The outdoor entry timer may be paused for (in effect extended by) a configurable period chosen to be long enough to accommodate the usual coming and going of an occupier. For example, if the occupier keeps a bicycle in the back garden, the paused period should be long enough to enable the occupier to unlock her bicycle, stow the lock, don her helmet, and leave the garden shutting the gate behind her. This period might be of the order of one or two minutes. Meanwhile, the security monitoring system remains armed - so that opening a door or window, for example, will trigger the usual armed away response from the central unit. After the expiry of the paused period, the central unit may revert to its usual armed state, so that subsequently detected motion in the monitored area will again cause the central unit to start an outdoor entry timer.

[0039] Alternatively, the central unit 140 may be configured to disarm the security monitoring system at step 460 - so that, for example, if the fob-carrying occupier were to enter the house from the back garden through the back door 170, the monitoring system would not generate an alarm. If this behaviour is programmed into the central unit 140 then it is preferred for the relevant disarm node, here 160, to respond to the detection by the sensor 130 of the opening of the back door 170 by providing some kind of audible or visual indication signifying that the security monitoring system was disarmed as the result of the occupier's presence in the back garden having been detected by virtue of their registered fob. For example, the disarm node could voice a welcome back message confirming that "the monitoring system was armed but that it had been disarmed when we recognised you in the back garden". A further option would be to configure the central unit to re-arm the system (to its previous armed state) in the event that no entry is attempted to the house within a certain period after the disarming of the system, and no motion has been detected in the monitored area for a certain time. In this way, if the occupier had just entered the back garden to take her bicycle or scooter and then left, the premises would once again by protected by the security monitoring system.

[0040] The security monitoring installation according to embodiments of the invention may include plural external cameras 50, each with its own respective monitored area, and the central unit can be configured to disarm the monitoring system, or suspend the outdoor entry timer, only in respect of the monitored area within which a key fob 370 has responded to a wake on radio wake up signal. If the system is configured to disarm just in respect of the relevant monitored area, it may be configured to re-arm the monitoring system in respect of the previously disarmed monitored area following a period of no motion triggers being received from the relevant camera 50.

[0041] Figure 5 is a sequence diagram showing, by way of contrast, what happens when an unauthorised intruder enters the area monitored by security monitoring camera 50. On entering the monitored area, the intruder triggers the motion detector 60 associated with the camera 50, causing a motion trigger signal to be supplied, 500, to the processor 210 of the camera. The processor then activates one of the transceivers 55 to transmit, 510, a motion trigger signal to the central unit 140. On receiving the motion trigger signal from camera 50, the central unit 140 starts, 520, an outdoor entry timer. The central unit 140 also transmits, 530, a start wake on radio instruction to the camera 50. On receiving the start wake on radio instruction, the camera 50 uses one of its transceivers 55 to transmit, 540, a low-power, out of band wake up signal. Because the intruder is not carrying an authorised key fob 370, no response is received to the wake on radio signal, and consequently the outdoor entry timer expires. On expiry, 550, of the outdoor entry timer, the central unit 140 determines an alarm event, notifies the central monitoring station 190, and instructs the camera 50 to start transmitting image data which may be supplied to the central monitoring station 190. The central unit 140 may also trigger a siren or other alarm indicator at the premises and/or may trigger announcements, for example, from the speaker of the camera 50 to advise the intruder that they have been spotted.

[0042] Figure 6 is a timing diagram showing the sequence of events and actions of the various elements of the security system that characterise a method, according to an embodiment of the invention, of suspending an outdoor entry timer when the presence of an authorised user is detected. The diagram concerns the operations of the entrance breach detector - e.g., the camera 50 including movement detector 60, the central unit 140, and the portable authentication device 370.

[0043] The method starts, 599, with the security monitoring system in an armed away state (the described method could equally be performed with the system in an armed at home status, but generally the issue of owner-induced false alarms caused by unintentional triggering of external monitored areas arises when systems are in the armed away state) at 599. At 600 the motion sensor senses an event, for example the opening of the garden gate, in the monitored external area, and this results in the camera's processor 210 causing an RF transceiver 55 of the camera to transmit an entry violation message. This entry violation message, which includes the camera's ID, is received at a transceiver of the control unit 140.

[0044] The central unit 140 starts, at 610, an entry period timer, which is set for the duration of the period within which a disarm process needs to be completed before the control unit causes the system to enter an alarm con-

dition - for example in the range 20 to 90 seconds (a period set based on the time needed for an occupant/user to disarm the arm - possibly including unlocking the back door, entering the house, and using the disarm node. The central unit identifies the detector that transmitted the motion detection message (which can be considered a form of entry violation message) from the camera ID contained in the received message. The central unit 140 includes the ID code for that camera in a message which it transmits, at 620, to the camera 50 to cause the camera to transmit, at 630, a beacon signal or polling signal to wake up the transceiver in any portable authentication device (or at least any portable authentication device which is moving or which has not had its transceiver shut down following a period of non-movement) within the vicinity of the targeted camera 50, and preferably includes a special identifier to be included in the beacon signal or polling signal, and details of a packet countdown (to be described later) to be used. The special identifier will typically be a random or pseudo random number whose value changes at each use. The portable authentication device 370 listens for beacon signals on one or more channels whose parameters are known to each of the portable authentication devices - for example by having been pre-programmed, but more preferably having been communicated to the or each portable authentication device when that portable authentication device first registered with the central unit (although of course the central unit could periodically update these parameters through an exchange of messages with the portable authentication device(s)). The characteristics of the beacon or polling signal transmitted by the camera 50 are preferably chosen to make the effective range of the beacon signal small - preferably of the order of a few metres, e.g. no more than 5 metres (but of course depending upon the extent of the monitored area and the range over which an authorised person is likely to roam) for detection by a portable authentication device 370, so that it will only be effective in waking a portable authentication device 370 in the immediate vicinity of the camera 50. These characteristics will be discussed in more detail later.

[0045] The transceiver 377 of a portable authentication device 370 that is within a few metres of the camera 50 (and that is not currently in a shut-down state following a period of non-movement as determined based on signals from the motion sensor 379) detects, 640, the beacon signal and wakes up. The transceiver 377 receives and decodes the beacon signal, retrieving the special identifier (if used). The controller 375 of the portable authentication device 370 then causes the transceiver 377 of the portable authentication device to transmit, at 650, a message including the portable authentication device ID and the special identifier (if used) to the central unit 140.

[0046] The central unit 140 checks that the special identifier (if used) is valid (meaning that it is one issued within the current period of the outdoor entry timer) and also checks to see whether the portable authentication device ID corresponds to one registered with the central unit. If both checks are passed (if a special identifier is being used), the central unit at 660, may suspend the system if the message from the portable authentication device 370, containing the portable authentication device id and the special identifier (if used), was received before expiry of the outdoor entry timer. The control unit 140 may also at this stage send, 670, a further message to the camera 50 to cause the camera to provide, 680, a notification of the fact that the presence of an authorised key fob 370 has been detected and that the outdoor entry period timer has been suspended. For example, the camera may activate an appropriate indicator light 265 and/or provide a "Welcome" sound or announcement through the loudspeaker 260. The camera 50 may also be instructed to send, 685, a further message to the portable authentication device 370 to cause the fob to generate, 690, a signal indicating successful recognition - for example, by illuminating an indicator on the portable authentication device, making an announcement or sound, or vibrating in a characteristic way.

[0047] As will be described later, the disarm request message sent by the portable authentication device 370 to the control unit 140 may also include a report on the RSSI levels of messages received by the portable authentication device 370 from the camera 50, and the control unit 140 may use the information about measured RSSI levels in such a report in determining whether or not to trust the received disarm request - i.e. whether to disregard the disarm request as invalid on the basis that it is likely to have come from a rogue actor (outside the usual range of the camera) rather than from an authorised user within range of the camera.

[0048] At 695, if no appropriate message is received from a portable authentication device 370 within the outdoor entry timer and no appropriate disarm credentials are received before expiry of the outdoor entry timer, the control unit identifies 140 an alarm state. If the system is backed up by a central monitoring station (CMS) 190, the central unit 140 will send a status change message to the CMS 190, typically with the identifier of the camera that first indicated movement (as an example of an entrance breach) event. The CMS 190 may then cause the central unit 140 to activate the camera (plus possibly other video cameras) or other image capture devices, audio capture devices, etc. and provide data feeds from these to the CMS 190. The CMS may also invoke human intervention as appropriate.

[0049] Figure 7 is a flow chart illustrating one possible process for a portable authentication device 370 according to an embodiment of the invention to determine whether to respond to a received transmission. At 1000 the portable authentication device receives an RF transmission at its transceiver (the transceiver not having been shut down following a determination that the portable authentication device is stationary). As a first step, 1100, the portable authentication device determines whether the received transmission is a disarm instruction - that

is, including a disarm transmission identifier of some kind, for example being a wake beacon (for example, from a camera 50 as previously described) or disarm success or failure message. If the determination is negative, i.e., it is not a disarm instruction, the process moves to step 1200.

[0050] If the determination is positive, the process proceeds to step 1300 in which the movement status of the portable authentication device 370 is checked. If the portable authentication device is determined to be stationary, the process moves to step 1400. If the portable authentication device is configured to shut down its transceiver following a period of non-movement, when the fob 370 is deemed to be stationary, the portable authentication device will subsequently not receive any RF transmission (until after the portable authentication device is detected as having moved again) and hence this process does not take place. But if the portable authentication device is determined to be moving, at 1600, the process proceeds to step 1800.

[0051] At step 1400, the processor 375 determines whether the portable authentication device 370 should be deemed to be stationary, for example by checking a count (or some other measure of elapsed time) since the portable authentication device was last determined to be moving. If the count is less than a predetermined threshold count, the portable authentication device 370 is determined, 1500, to be a "live" portable authentication device which can be used to provide a disarm instruction to the central unit (that is, the portable authentication device is not deemed to be stationary), and the process proceeds to step 1800. If the portable authentication device is deemed to be stationary, then no disarm message will be transmitted by the portable authentication device 370, and the process ends at 1700.

[0052] The period of inactivity that is accepted as indicating that a portable authentication device 370 is "live" may be set differently in different installations, but typically this period will be no more than about 60 seconds. A cut off at 30 seconds will often be long enough for most users, although for system installations where the occupants or users of the secured space are elderly or infirm 30 seconds may not be long enough. Preferably the cut off period is kept relatively short, at no more than a minute or so.

[0053] If at step 1300 the portable authentication device is determined to be moving 1600, the process proceeds to step 1800.

[0054] At step 1800, the portable authentication device generates a transmission message that includes the portable authentication device ID, and the disarm transmission identifier (if used), and such other parameters as the system requires (for example, a report of measured RSSI).

[0055] At step 1200, when the transmission is determined not to be a disarm instruction, the portable authentication device may be programmed simply to read the transmission and act on the contents, or to check for a certain flag or flags and to respond differently based on the flag(s) determined to be present. So, for example, the monitoring system may be so arranged that the portable authentication device 370 is configured to receive an instruction other than a disarm instruction via the transceiver, including a flag, from the control unit to perform an action; and wherein in the event that the other instruction includes the flag, the processor is configured to cause the portable authentication device to perform the instructed action whether or not, when the instruction is received, the portable authentication device is determined to be stationary. Portable authentication devices 370 configured in this way can be activated by an RF signal, from the control unit or from a disarm node, enabling the status of all portable authentication devices in range to be checked and/or updated. It would also be possible to perform an audit of all the portable authentication devices in range of, say, the central unit. If such a portable authentication device 370 were to include one or more of a visual indicator 385, an audio transducer 390, a haptic transducer 390, and were further configured to generate an output using one or more of these when so instructed by a received instruction including the flag, a mislaid portable authentication device could be made to announce itself. Of course, this approach would only work with all portable authentication devices if they were either not configured to shut down their transceivers following a period of non-movement, or if none of them had shut down their transceiver when the RF signal from the control unit or disarm node was transmitted.

[0056] Portable authentication devices 370 according to the invention may be configured to listen for instructions related to hands free disarm (including transmissions from external cameras 50 as previously described) only on a particular channel or channels, with given frequency and given modulation, but to listen to another channel or channels on a different frequency and possibly with different modulation for other kinds of instructions.

[0057] Disarm instructions received from a disarm node do not typically contain a portable authentication device ID - because, if more than one portable authentication device is registered with the central unit, it cannot be assumed which if any portable authentication device is being carried by the person who opened the door whose opening has been sensed. But other message may be targeted to a particular portable authentication device or to a group of portable authentication devices that is a subset of all the registered portable authentication devices. Consequently, a portable authentication device according to embodiments of the invention may also be arranged to check the contents of received messages for the presence of that portable authentication device's ID. In this way, the control unit 140 can target an individual portable authentication device 370 or group of portable authentication devices. For example, in the event that a portable authentication device has been mislaid, a "announce myself' message could be transmitted by the cen-

tral unit flagged with the ID of the particular portable authentication device that has been mislaid. If other portable authentication devices receive the message, they do not respond to it, because it is flagged as an "announce myself' message and does not contain their ID. Whereas the missing portable authentication device sees that the message is flagged as an "announce myself' message, recognises its own ID, and announces its presence using one or more of its inbuilt indicators (for example one or more LEDs, or providing a haptic announcement - by "buzzing" or vibrating).

[0058] In general, monitoring systems according to embodiments of the invention will not be configured to transmit only disarm messages to portable authentication devices, but will also be configured to send other types of messages to portable authentication devices 370. In systems that do only send portable authentication devices 370 disarm messages, a portable authentication device just needs to recognise a received message as a disarm message and respond with the disarm transmission identifier (if used) and the portable authentication device ID (although, as will be explained later, portable authentication devices may be required to perform RSSI measurements and include these, or a report based on these, as part of the response). But in systems where there are additional message types, message types will typically fall into two classes: targeted messages that are targeted at a subset of one or more of all the registered portable authentication devices, that include one or more portable authentication device IDs, and in respect of which a reaction is sought only from the portable authentication device(s) having an ID included in the message; and group or general messages, in respect of which a reaction is sought from any portable authentication device that receives the message - and which therefore do not need to include a portable authentication device ID (and which hence will generally not include any portable authentication device ID). For example, a central unit may be configured to instruct the portable authentication device involved in a hands free disarm event to provide a disarm success indicator on a successful disarm event. Such an instruction will preferably include the ID of the portable authentication device that transmitted the disarm request to the central unit (the portable authentication device ID having been included in that disarm request).

[0059] Messages may be sent to portable authentication devices 370 at least from the control unit (of which, in some systems, there may be more than one), disarm nodes 150, and external monitoring cameras 50. Where there are multiple message types, they may be labelled Disarm Message, Group, and Targeted - labels which can be considered to be class flags. If finer granularity is required, a further level of flags may be provided - so that a message type is indicated by a primary flag (Disarm Message, Group, or Targeted), and (at least for Group and Targeted) a secondary flag that indicates the specific message type within the class. Alternatively, a single level of flags may be provided, with typically multiple flags for each of the Group and Targeted classes.

[0060] Within the 868/869 MHz band in Europe, the sub-band between 869.7 and 870Mhz is particularly interesting for use when transmitting short-range beaconing signals from the disarm nodes because it provides a relatively wide channel, the beacon channel, which allows the use of a high data rate, e.g. 250 kbit/s, which is helpful in reducing the effective range of the beacon signal. The effective radiated power ceiling of 5mW also poses no significant constraint for this application. For these reasons, this sub-band between 869.7 and 870Mhz is the preferred frequency band for the short-range transmissions from the disarm node - and which are used for communication with portable authentication devices, e.g., for the transmission of wake up messages.

[0061] Although, for the reasons just given, we prefer to transmit the beacons from the disarm node closest to the entrance which gave rise to the alarm trigger signal, alternatives are possible.

[0062] For example, a sensor that detects the breaching of an entrance transmits an alarm trigger signal, including a sensor identifier, that is detected by the control unit. The control unit recognises the sensor identifier and uses this to retrieve the identifier for the disarm node that is associated with the relevant sensor. The control unit then transmits a message, which may be a wake up message, including the relevant disarm node identifier which has the effect of causing the relevant disarm node to listen for signals from fobs (portable identification devices). The control unit then transmits a fob wake up signal receivable by any fob adjacent any of the disarm nodes. Any fob that receives the fob wake up signal from the control unit then responds by transmitting a response signal, including its own identifier, that is only detectable by a disarm node within no more than about 2 metres of the fob (using appropriately selected transmission characteristics of power, data rate, etc. to ensure a short effective transmission range). A disarm node receiving the fob response signal then transmits a signal, including the fob identifier, to the control unit which then determines whether the fob identifier is for a registered fob. In this way only the disarm node whose identifier was included in the transmission from the control unit detects the fob response.

[0063] As a further alternative, the disarm node may be configured to generate an alarm trigger signal that is transmitted to the control unit in response to receiving an entrance breach signal from a sensor configured to detect the breaching of an entrance to the building or secured space. That is, the sensor transmits a signal in respect of a detected breach, which signal is received by the associated disarm node rather than by the control unit. The control unit then transmits a fob wake up signal receivable by any fob adjacent any of the disarm nodes. Any fob that receives the fob wake up signal from the control unit then responds by transmitting a response signal, including its own identifier, that is only detectable

by a disarm node within no more than about 2 metres of the fob. A disarm node receiving the fob response signal then transmits a signal, including the fob identifier, to the control unit which then determines whether the fob identifier is for a registered fob. In this way only the disarm node whose identifier was included in the transmission from the control unit detects the fob response. However, this approach is less preferred than the alternatives already mentioned, because if the signal from the sensor detecting the breach of an entrance is only received by the control unit through the disarm node, rather than directly, the security of the system is reduced - the disarm node becomes a point of weakness, because if it is disabled or its signals blocked in some way by a bad actor, the control unit will not receive any alarm trigger signal in respect of the breach. For this reason, it would be desirable to include anti-tampering features in the disarm node, such as sensors to detect and report on attempts to open the disarm node, and possible also implementing a "heartbeat" function in which the disarm node periodically "checks-in" with the control unit - the failure of the control unit to receive the heartbeat, or the reception of a tamper message from the disarm node causing the control unit to determine an alarm condition which is reported to the central monitoring station (if present) and to provide alarm signals (audio and optical) through the alarm installation - as well as sending reports to the user's phone - email, as appropriate. Such extra security features may also be present in disarm nodes according to any of the other embodiments and variants.

[0064] Achieving effective battery life of nodes and sensors in alarm and monitoring systems is a constant concern, because battery failure disables the relevant node or sensor, which can lead to loss of security, and battery replacement may involve a site visit by the system supplier - which is expensive and inconvenient. For a portable authentication device, loss of battery power means that the portable authentication device stops working, which is inconvenient for the user, and the cause of the failure may not be apparent to the user so that the user may require a site visit to identify and fix the problem. Consequently, we are interested in reducing power consumption in all of the battery powered components of the system, including the portable authentication device. For this reason the use of a wake on radio receiver in the portable authentication device is attractive although acceptable battery life can also be obtained using a more conventional radio receiver that periodically wakes to listen (poll) for beacon signals.

[0065] One way of reducing portable authentication device power consumption during the wake up process is for the portable authentication device to use 2-stage detection, an example of which is illustrated in Figure 8. A first detection stage of the transceiver of the portable authentication device may be used to perform a first step which involves just checking an RSSI level. For example, the transceiver in the portable authentication device may perform periodically a brief RSSI check polling the beacon channel, using just the RF front end of the transceiver, for example for a first period of less than a few milliseconds, preferably a fraction of a millisecond, e.g. around 0.5 milliseconds, and then revert to its rest state if the sensed RSSI level is below some pre-set threshold. If the sensed RSSI level is above threshold, the portable authentication device listens for a brief period for a synch word from the disarm node - for example for a second period of a few milliseconds, for example for less than 10 milliseconds, e.g. 5ms. If no synch word is detected, the transceiver reverts to its rest state. But if a synch word is detected, the transceiver starts the full radio receiver which remains powered up, for example for a third period of between say 8 to 16ms, for example 10ms, to receive the full wake up packet. Each packet will typically last of the order of 220μs, and the disarm node may transmit for 2 to 4 seconds, e.g. for 3 seconds - meaning that the portable authentication device should be able to receive 20 to 30 packets. Clearly, the choice of duration for the various periods is a trade-off between power consumption, user experience and accuracy - but the timings given represent a reasonable compromise as a starting point to be adjusted as necessary.

[0066] RSSI detection can be achieved by activating just front end components of the transceiver, avoiding the need to power up all of the transceiver. If the detected RSSI level is below a threshold, the portable authentication device determines that there is unlikely to be valid data available and halts its RSSI check until the next cycle. The cycle period determines the length of time for which the disarm node needs to transmit its beacon and also sets a lower bound on how quickly hands-free disarm is likely to occur on average. The portable authentication device wake up interval, which is controlled by a clock in the portable authentication device, will typically be chosen based on the duration of the disarm node beacon. For example, if the disarm node transmits its beacon for 2 seconds, then a portable authentication device wake up interval of one second would provide a good likelihood that a f portable authentication device within range of a broadcasting disarm node would be able to wake and retrieve the necessary information from the beacon signal. A portable authentication device wake up of interval (period between polling events) of 2 seconds will often be frequent enough when the disarm node is configured to transmit its beacon signal for 3 seconds. The portable authentication device wake up interval can conveniently be set at between a quarter and two thirds of the beacon duration. By having the portable authentication device check the RSSI for a very brief period, for example a few milliseconds, at each polling event, good battery life can generally be obtained. A shorter relative cycle time is not technically problematic, but it is likely to use proportionally more battery power and hence shorten battery life commensurately. The cycle time could be more than one half of the beacon duration, provided the system enables the portable authentication device to capture the beacon quickly after wake up, so that the necessary special ID

(if used) can be recovered by the portable authentication device.

[0067] The disarm node transmits a beacon signal, on the beacon channel, which preferably includes the special codeword (shown as ID in Figure 8) received from the control unit for this hands free disarm event. Typically, the beacon signal will be made up of a sequence of packets, each beginning with a preamble, followed by a synch word, then an identifier which is the special ID from the central unit. Preferably, each packet includes a countdown value, the countdown value decreasing by one in each subsequent packet (to zero in the final packet of the sequence) and indicating the number of packets until the end of the sequence of packets.

[0068] The beacon signal is recognised as such by the portable authentication device, because it is the only message of that kind with the relevant format in that channel, causing the portable authentication device to transmit a response including the special codeword (special I.D.).

[0069] By including sequence information in the beacon from the disarm node, it becomes possible for the portable authentication device to determine when the beacon transmission will end. Using this information, the portable authentication device can delay transmitting its response to the central unit until after the disarm node has finished transmitting - so that it is easier for the central unit to detect the response from the portable authentication device without local interference. This means that portable authentication device transmit power can be kept low, prolonging the life of the portable authentication device's battery, while still enabling the control unit to receive the portable authentication device 's response. In addition, when the portable authentication device captures beacon packets, it can calculate how long it will be before the sequence ends. If the captured packets are early in the sequence, the portable authentication device can "snooze" or power down while waiting for the sequence to end, and then wake again in order to transmit its response to the central unit just after the sequence ends.

[0070] The portable authentication device will listen to multiple packets to be able to use statistics to get a reliable RSSI figure, and may report on the RSSI figure for each of the packets detected.

[0071] As a refinement, the portable authentication device controller 375 may use movement information from the portable authentication device's built-in movement sensor 379 to control the polling by the portable authentication device's transceiver 377. That is, polling may be suspended in the event that the processor deems that the portable authentication device is stationary - e.g. if movement sensor detects no movement, and the processor determines that a count since the portable authentication device was last determined to be moving is more than a predetermined threshold count, the portable authentication device is deemed to be stationary and polling may be suspended completely or the frequency of polling reduced (the preferred option, since that means that "lost" portable authentication devices can be made to announce themselves when they next poll). For example, the frequency of polling may be reduced to between a half and a twentieth, or less, of the usual frequency. Conversely, if the processor determines that the portable authentication device is still moving, or has recently been moving (so that the portable authentication device is not deemed to be stationary), the usual polling frequency is maintained. The processor of the portable authentication device may be configured to cease generating the running count of the time since the portable authentication device was last in motion after the count of the time since the fob was last in motion reaches the predetermined threshold value, as this can reduce portable authentication device energy consumption, which is good for improving battery life.

[0072] In order to reduce the effective range of the radio beacon, it is transmitted from the disarm node at a low power (e.g. -20dBm or less) with a high data rate (for example, 250kbps or more, say 400 kbps) and with a low modulation index, to give an effective range of no more than about 5 metres. By using a suboptimal modulation index we achieve three things: quickly send a lot of packets, reduce sensitivity to decrease range and to fit inside the given spectrum. We limit the output power from the disarm node to limit range. To make it harder to receive from a greater distance we have a high data rate and low modulation index. However the main reason is not the poor link budget but the speed. The higher the bitrate the more packets can be used for estimation. Sensitivity is in the range of around -90dBm at this settings and we try to be in line of sight, meaning that the distance from the transmitter is given as the fading of the channel with distance, using the Friis formula .

[0073] Encryption, for example based on shared keys, is preferably used for all transmissions from and to the control unit in each of the embodiments of the invention.

[0074] As mentioned previously, a further option to improve security, which may be used with any or all of the preceding options to further enhance the security of the system, is for the portable authentication device to include in the response message sent to the control unit details of the results of RSSI determinations made by the portable authentication device. In particular, the disarm node may be configured to send a series of wake up messages upon being prompted by the control unit to send a disarm instruction, preferably including a unique disarm transmission identifier, to the portable authentication device . And the portable authentication device may be configured to determine the RSSI level of each of the messages of the series that are received from the disarm node. The portable authentication device may be configured to include in the disarm request sent to the central unit a report based on the determined RSSI levels. For example, the portable authentication device may be configured to send a summary of the RSSI levels measured, such as the number of messages/packets meas-

ured or measured above a certain level, maximum RSSI level, average RSSI level, etc.

[0075] Inclusion of the RSSI data can be used by the system to reduce the susceptibility of the system to "relay attacks" of the type used to fool passive entry systems (PES) of cars.

[0076] The portable authentication device would report RSSI values as, for example, max/min values, and an average, and the central unit may hold factory pre-set values for a "real" disarm, and/or these may be supplemented or replaced with real world values obtained during commissioning/testing of the system.

[0077] Instead of the identity of the portable authentication device being checked by the control unit, it would also be possible for the disarm node(s) to include a list of registered portable authentication devices and for the disarm node(s) rather than the control unit to perform the check of authentication device identity on receipt of the authentication devices response to the wake up signal/beacon. The disarm node would, on successful authentication transmit an alarm deactivation message to the control unit. Such an approach would of course require that the control unit update the disarm node(s) with additions and deletions to the list of registered authentication devices. This is a less preferred approach because of the need for the increased burden of keeping up to date lists in both the control unit and the disarm node(s).

[0078] Also, although as thus far described any disarm transmission identifier or event ID has been generated by the central unit and then transmitted to a disarm node for inclusion in a wake up message from the disarm node, other alternatives are of course possible. For example, the disarm node could itself generate a disarm transmission identifier or event ID and either provide this to the central unit for the central unit to check any received fob transmission for the presence of the correct disarm transmission identifier or event ID or itself check any received fob transmission for the presence of the correct disarm transmission identifier or event ID and transmit the result of the check to the central unit. In general, it is preferable for the disarm transmission identifier or event ID to be generated and checked by the central unit, rather than devolving either or both these functions to a disarm node, because this reduces the risk of a bad actor adopting the guise of a disarm node to fool the system.

Claims

1. A security monitoring system including:

a system controller;
a video camera, coupled to a motion sensor, arranged to monitor a surveillance area;
a portable token storing a token ID;
the video camera being configured on receipt of a motion detection signal from the motion sensor to send an alert to the system controller;
the system controller being configured in an armed state, on receipt of an alert from the video camera, to start an event timer and to send an instruction to the video camera to broadcast a token activation signal, the instruction including an event identifier;
the video camera further being configured to, on receipt of the instruction from the system controller, broadcast a token activation signal including the event identifier;
the portable token being configured to respond to receipt of a token activation signal from the video camera by broadcasting a response including the token ID and the event identifier;
the system controller further being configured:
on receipt of a response from the token to:

compare the event identifier included in the response with the event identifier included in the instruction to the video camera;
compare the token ID included in the response with one or more stored token IDs; and to suspend the event timer if both comparisons provide a match;
if either no response is received or one or both comparisons do not provide a match, to determine an alarm event on expiry of the event timer.

2. A security monitoring system as claimed in claim 1, wherein the video camera and motion sensor are arranged to survey a surveillance area and the video camera is configured to broadcast the token activation signal as a radio signal having an effective range that does not extend significantly beyond the surveillance area.

3. A security monitoring system as claimed in claim 1 or claim 2, wherein the portable token includes a processor coupled to a token movement sensor, and the token is configured to respond to token activation signals only if the processor determines that the token is moving.

4. A security monitoring system as claimed in any one of the preceding claims, wherein the portable token includes a wake on radio receiver, and the video camera is configured to broadcast token activation signals as wake on radio signals to which the token is responsive.

5. A security monitoring system as claimed in any one of the preceding claims, wherein the portable token is configured to include RSSI data in its response to the token activation signal from the video camera.

6. A security monitoring system as claimed in claim 5, wherein the system controller is configured to use

the RSSI data included in the token response in determining whether to trust the received response.

7. A security monitoring system as claimed in claim 6, wherein the system controller is configured to regard the token response as invalid if the RSSI data included in the token response suggest that the response has come from outside the usual range of radio signals from the camera.

8. A security monitoring system as claimed in any one of the preceding claims, wherein radio frequency transceivers of the portable token, the video camera and
the system controller are configured to operate in the industrial, scientific and medical, ISM, radio bands.

9. A security monitoring system as claimed in any one of the preceding claims, wherein the video camera is configured, on instruction from the system controller to transmit video images captured by the video camera using Wi-Fi.

10. A security monitoring system as claimed in any one of the preceding claims, wherein the system controller is configured, in an armed state, to disarm the security monitoring system if both comparisons provide a match.

11. A security monitoring system as claimed in any one of claims 1 to 9, wherein the system controller is configured in an armed state, if both comparisons provide a match, to disarm the security monitoring system only in respect of the monitoring of the surveillance area.

12. A video camera for use in a security monitoring system as claimed in any one of the preceding claims, the video camera including an image sensor, a radio frequency transmitter, a radio frequency receiver, and a processor operatively connected to the image sensor, the radio frequency transmitter and the radio frequency receiver, the processor being configured, on receipt of a motion trigger signal from a motion sensor to:

transmit, using the radio frequency transmitter, a flag signal to the system controller of the security monitoring system;
in response to receiving, via the radio frequency receiver, an instruction from the controller to cause the radio frequency transmitter to transmit a token activation signal.

13. The video camera as claimed in claim 12, wherein the token activation signal is a wake on radio signal.

14. The video camera as claimed in claim 12, wherein the motion sensor is part of the video camera.

15. The video camera as claimed in any one of claims 12 to 14, wherein the video camera's radio frequency transmitter and radio frequency receiver are configured to operate within the industrial, scientific and medical, ISM, radio bands.

16. The video camera as claimed in claim 15, wherein the radio frequency receiver and the radio frequency receiver are configured to operate in the 868 MHz band.

17. The video camera as claimed in any one of claims 12 to 16, further comprising an RF transmitter configured to transmit Wi-Fi signals.

18. The video camera as claimed in claim 17, wherein the processor is configured, on instruction from the controller of a security installation to activate the RF transmitter to transmit via Wi-Fi video images captured by the video camera.

19. A method of configuring a security monitoring system, the method comprising:

providing a system controller;
a remote video camera coupled to a motion sensor; and
a portable token storing a token ID;
the video camera being configured on receipt of a motion detection signal from the motion sensor to send an alert to the system controller;
the system controller being configured, on receipt of an alert from the video camera, to start an event timer and to send an instruction to the video camera to broadcast a token activation signal, the instruction including an event identifier;
the video camera further being configured to, on receipt of the instruction from the system controller, broadcast a token activation signal including the event identifier;
the portable token being configured to respond to receipt of a token activation signal from the video camera by broadcasting a response including the token ID and the event identifier;
the system controller further being configured:
on receipt of a response from the token to:

compare the event identifier included in the response with the event identifier included in the instruction to the video camera;
compare the token ID included in the response with one or more stored token IDs;
and to suspend the event timer if both comparisons provide a match;

if either no response is received or one or both comparisons do not provide a match, to determine an alarm event on expiry of the event timer.

20. A method of operating a security monitoring system, the security monitoring system including:

a system controller;
a video camera, coupled to a motion sensor, arranged to monitor a surveillance area; and
a portable token storing a token ID; the method comprising:

monitoring the surveillance area using the video camera and motion sensor;
on receipt by the video camera of a motion detection signal from the motion sensor sending an alert to the system controller;
on receipt of an alert from the video camera, the system controller starting an event timer and sending an instruction to the video camera to broadcast a token activation signal, the instruction including an event identifier;
the video camera, on receipt of the instruction from the system controller, broadcasting a token activation signal including the event identifier;
the portable token responding to receipt of the token activation signal from the video camera by broadcasting a response including the token ID and the event identifier;
the system controller: on receipt of a response from the token, comparing the event identifier included in the response with the event identifier included in the instruction to the video camera;
comparing the token ID included in the response with one or more stored token IDs; and suspending the event timer if both comparisons provide a match;
if either no response is received or one or both comparisons do not provide a match, determining an alarm event on expiry of the event timer.

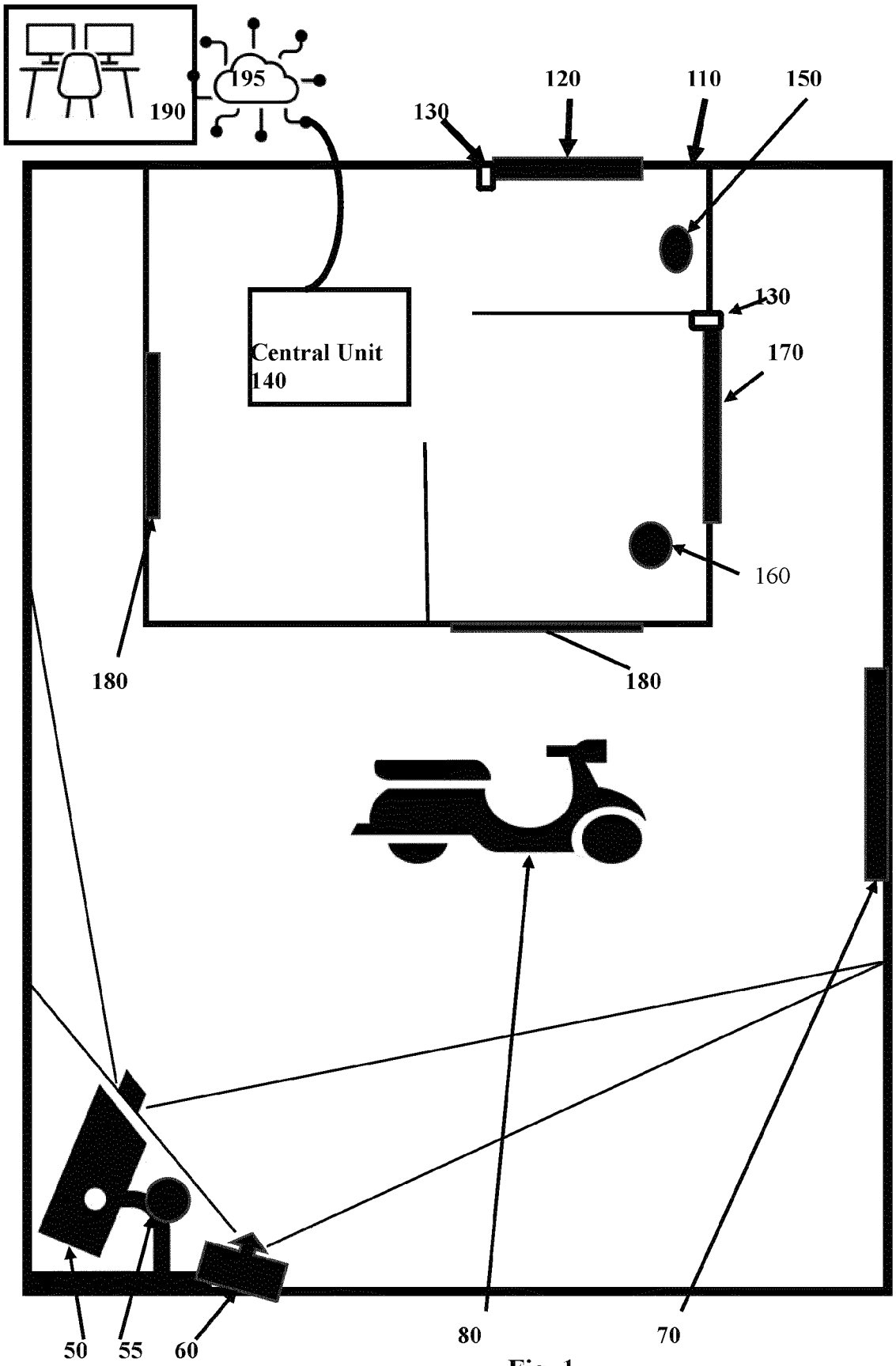
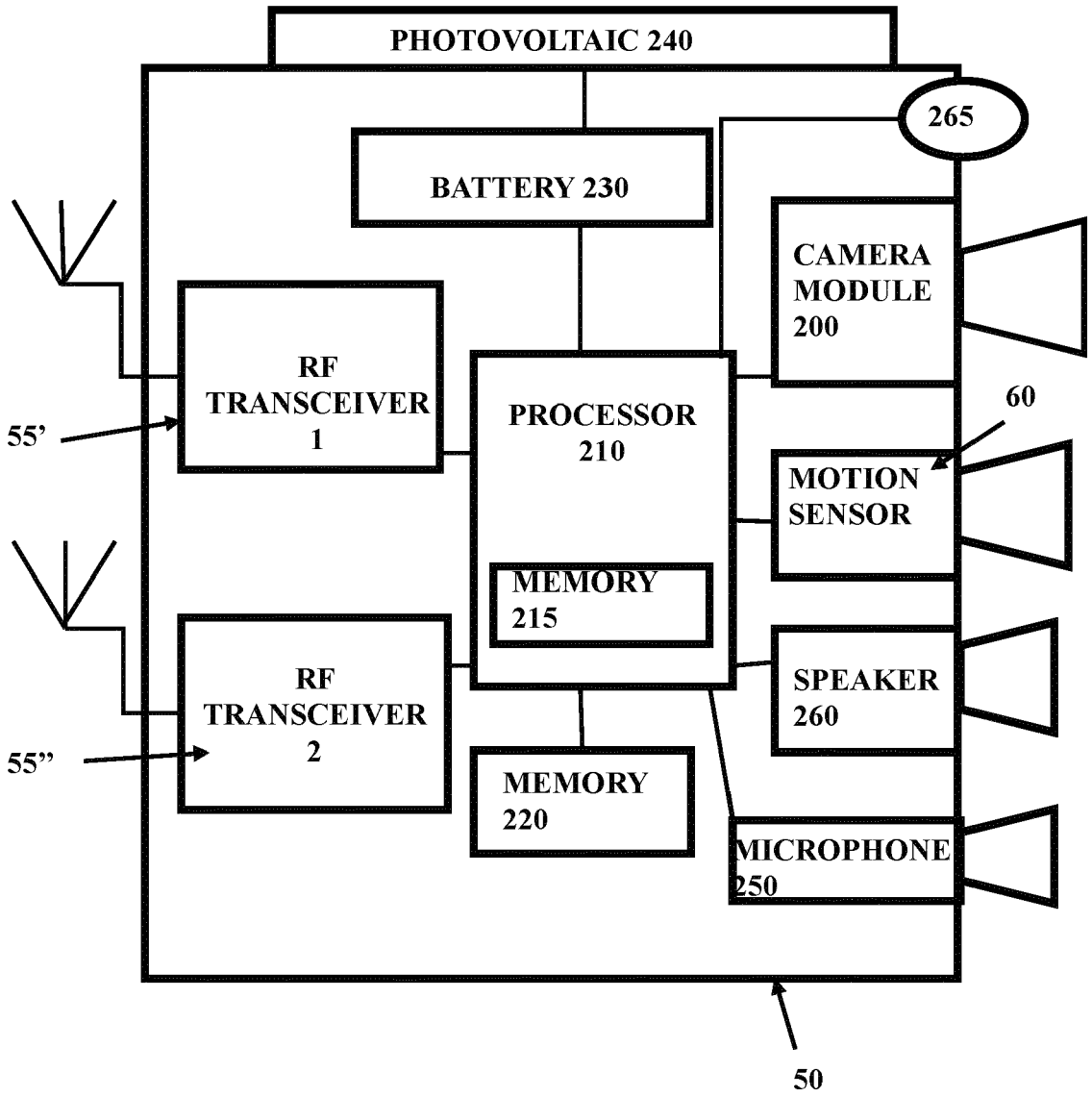

190
195
130
120
110
150
130
Central Unit
140
170
160
180
180
50
55
60
80
70

Fig. 1

Fig. 2


PHOTOVOLTAIC 240
265
BATTERY 230
CAMERA MODULE 200
RF TRANSCEIVER 1
PROCESSOR 210
60
55'
MOTION SENSOR
MEMORY 215
RF TRANSCEIVER 2
SPEAKER 260
55"
MEMORY 220
MICROPHONE 250
50

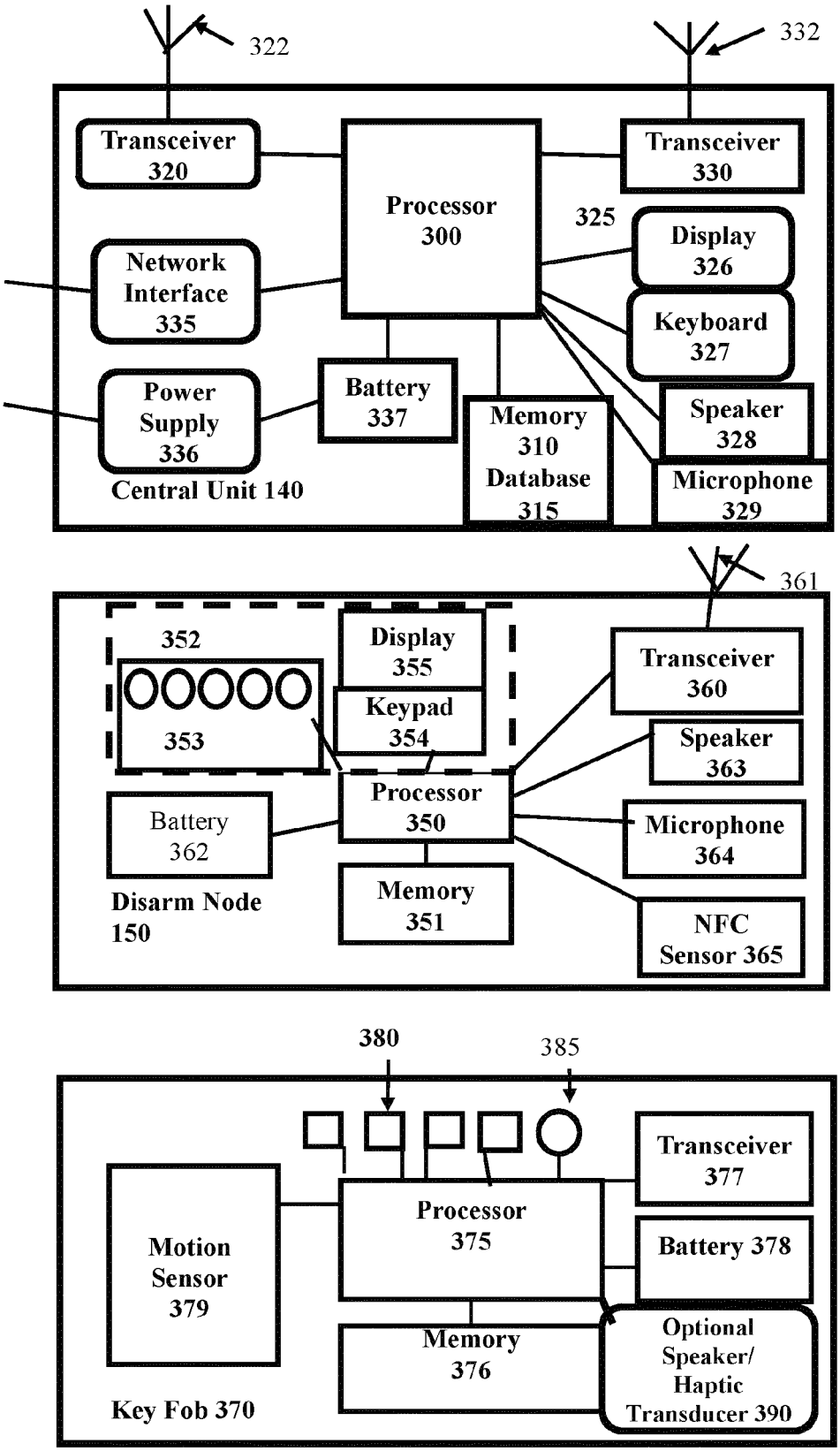

322
332
Transceiver 320
Processor 300
Transceiver 330
325
Display 326
Network Interface 335
Keyboard 327
Power Supply 336
Battery 337
Memory 310 Database 315
Speaker 328
Microphone 329
Central Unit 140
361
352
Display 355
Transceiver 360
Keypad 354
353
Speaker 363
Processor 350
Battery 362
Microphone 364
Memory 351
Disarm Node 150
NFC Sensor 365
380
385
Transceiver 377
Processor 375
Motion Sensor 379
Battery 378
Memory 376
Optional Speaker/ Haptic Transducer 390
Key Fob 370

Fig. 3

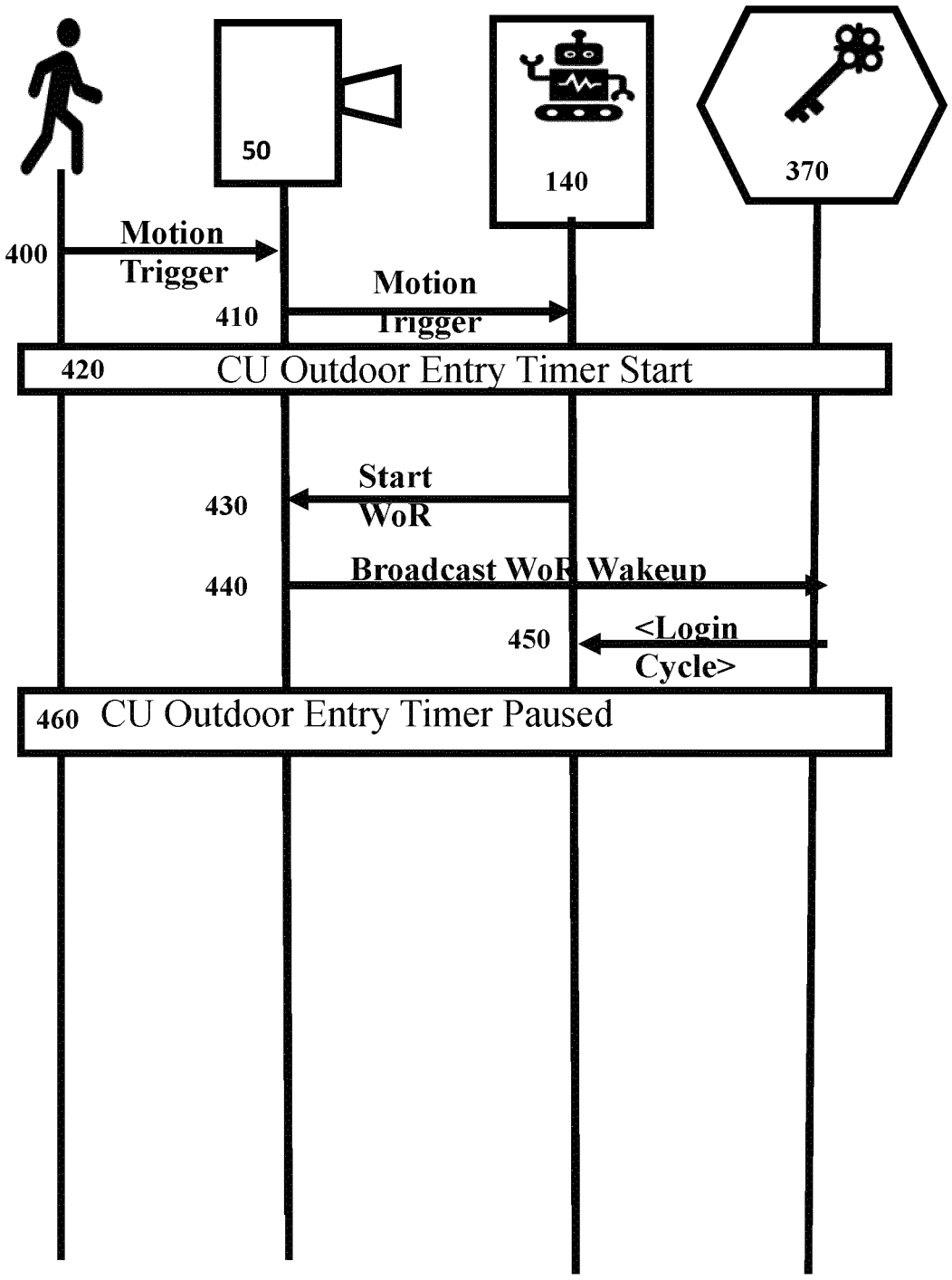

50
140
370
400
Motion Trigger
410
Motion Trigger
420
CU Outdoor Entry Timer Start
430
Start WoR
440
Broadcast WoR Wakeup
450
<Login Cycle>
460
CU Outdoor Entry Timer Paused

Fig. 4

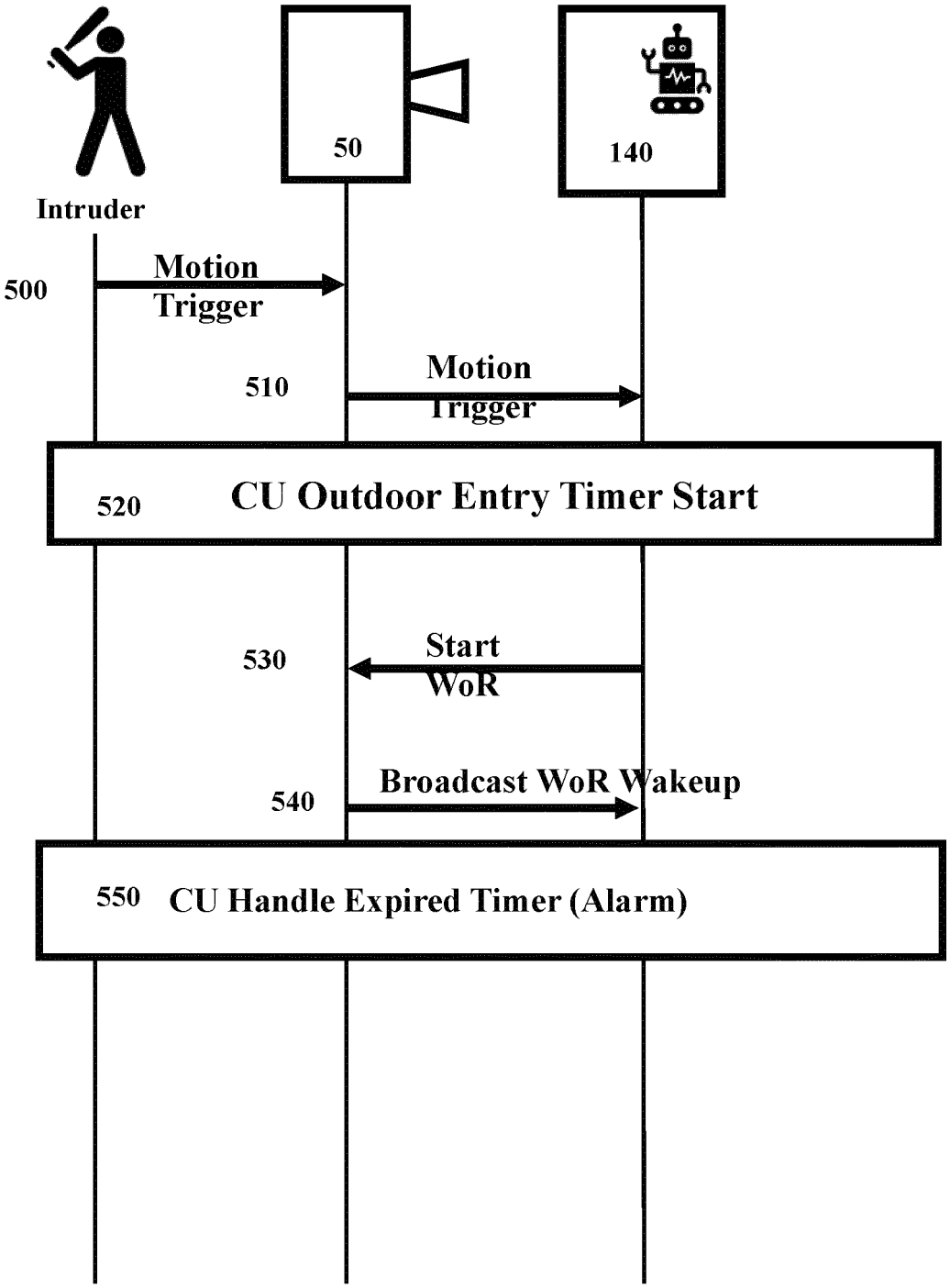

Intruder
50
140
500
Motion Trigger
510
Motion Trigger
520
CU Outdoor Entry Timer Start
530
Start WoR
540
Broadcast WoR Wakeup
550
CU Handle Expired Timer (Alarm)

Fig. 5

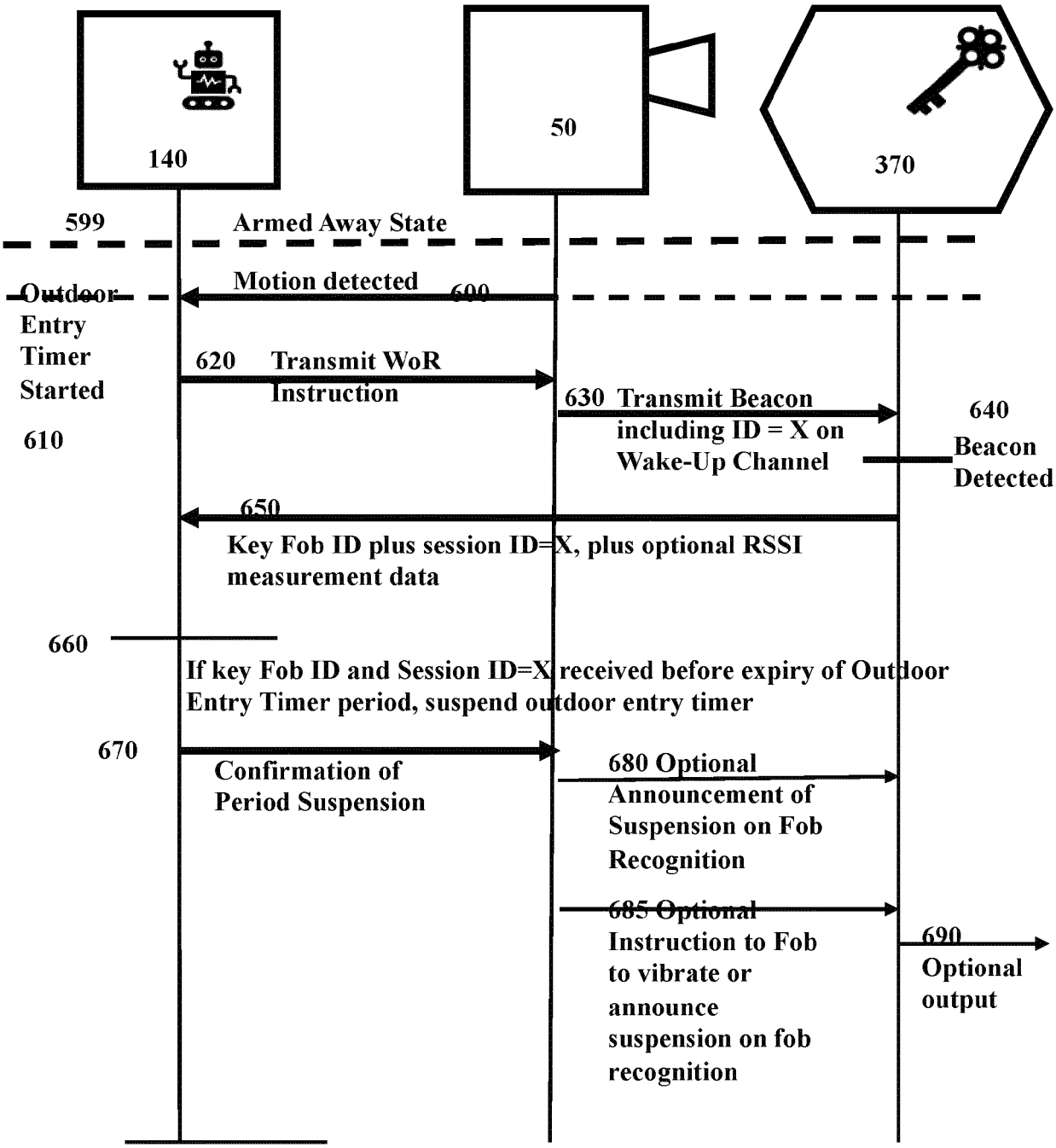

140
50
370
599
Armed Away State
Outdoor Entry Timer Started
610
Motion detected
600
620 Transmit WoR Instruction
630 Transmit Beacon including ID = X on Wake-Up Channel
640 Beacon Detected
650
Key Fob ID plus session ID=X, plus optional RSSI measurement data
660
If key Fob ID and Session ID=X received before expiry of Outdoor Entry Timer period, suspend outdoor entry timer
670
Confirmation of Period Suspension
680 Optional Announcement of Suspension on Fob Recognition
685 Optional Instruction to Fob to vibrate or announce suspension on fob recognition
690 Optional output
695 If key Fob ID and Session ID=X are NOT received before expiry of Outdoor Entry Timer period, enter alarm condition and send alarm status to CMS.

Fig. 6

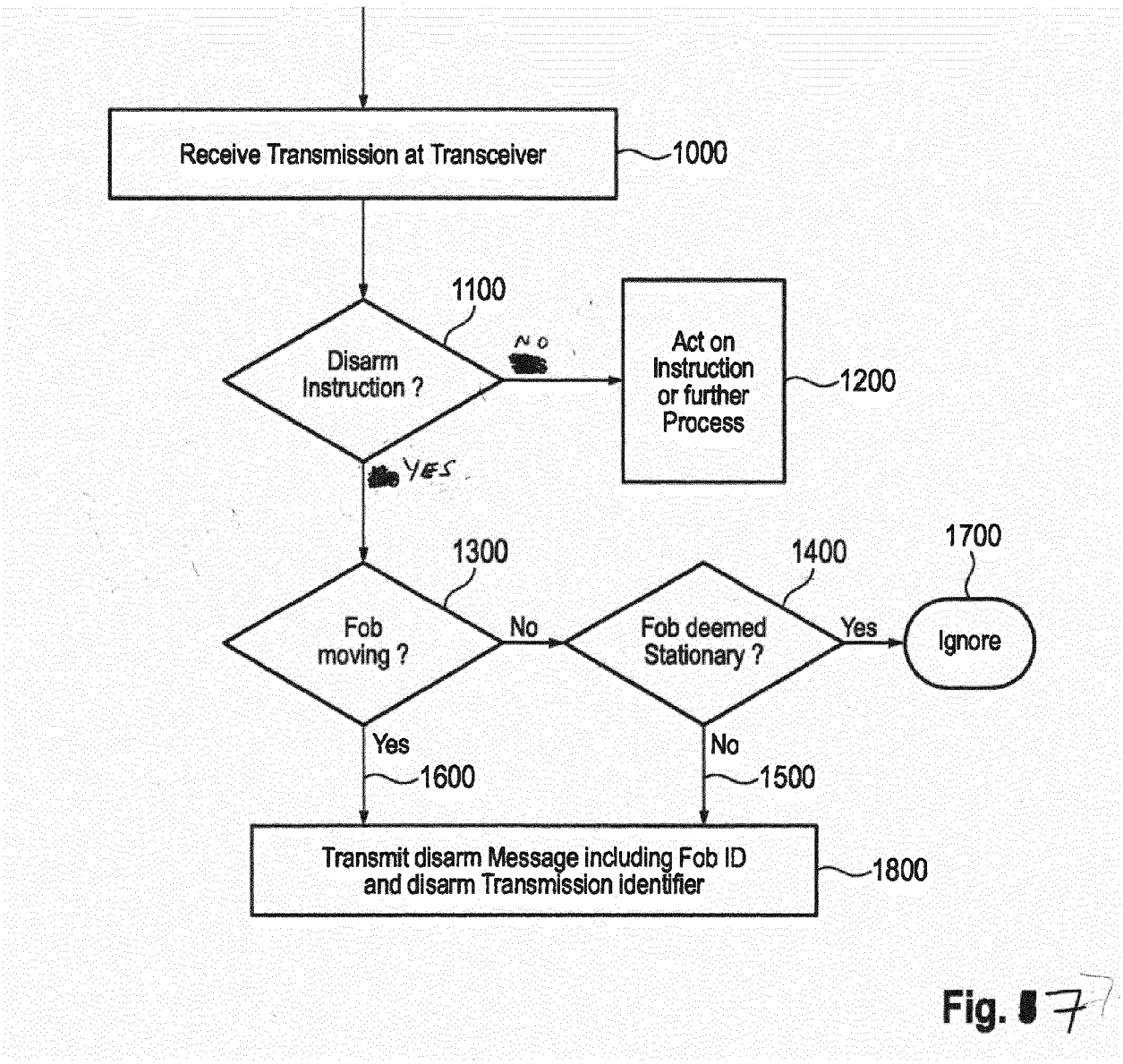

Receive Transmission at Transceiver
1000
1100
Disarm Instruction ?
No
Act on Instruction or further Process
1200
Yes
1300
Fob moving ?
No
1400
Fob deemed Stationary ?
Yes
1700
Ignore
Yes
1600
No
1500
Transmit disarm Message including Fob ID and disarm Transmission identifier
1800

Fig. 17

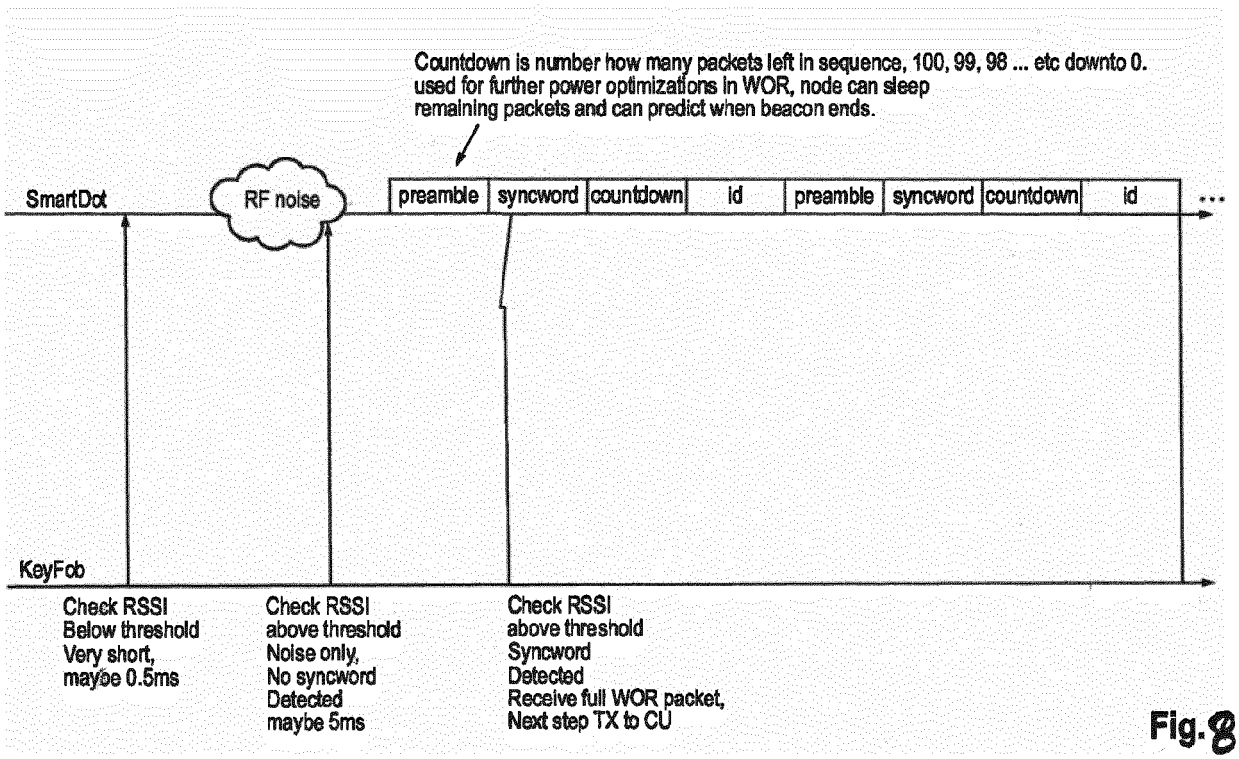

Countdown is number how many packets left in sequence, 100, 99, 98 ... etc downto 0.
used for further power optimizations in WOR, node can sleep
remaining packets and can predict when beacon ends.
SmartDot
RF noise
preamble
syncword
countdown
id
preamble
syncword
countdown
id
...
KeyFob
Check RSSI
Below threshold
Very short,
maybe 0.5ms
Check RSSI
above threshold
Noise only,
No syncword
Detected
maybe 5ms
Check RSSI
above threshold
Syncword
Detected
Receive full WOR packet,
Next step TX to CU

Fig. 8

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 21 17 4825

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	US 2014/139678 A1 (MORIARTY ANTHONY D [AU] ET AL) 22 May 2014 (2014-05-22) * paragraphs [0013], [0039], [0040]; figures 1,4 *	1-20	INV. G08B13/196
A	US 2016/035198 A1 (COVIELLO FRANCIS JOSEPH [US]) 4 February 2016 (2016-02-04) * paragraphs [0030], [0031], [0070] *	1-20	
A	US 2014/136701 A1 (BILLAU RONALD L [US] ET AL) 15 May 2014 (2014-05-15) * paragraph [0126] *	1-20	
A	US 2003/062997 A1 (NAIDOO SURENDRA N [US] ET AL) 3 April 2003 (2003-04-03) * paragraph [0085] *	1-20	

TECHNICAL FIELDS SEARCHED (IPC)

G08B
G07C
H04N

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	28 October 2021	Coffa, Andrew

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 21 17 4825

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.

28-10-2021

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014139678 A1	22-05-2014	US 2014139678 A1	22-05-2014
		WO 2014078843 A1	22-05-2014
US 2016035198 A1	04-02-2016	US 2016035198 A1	04-02-2016
		US 2017032639 A1	02-02-2017
		US 2017221330 A1	03-08-2017
US 2014136701 A1	15-05-2014	US 2014132763 A1	15-05-2014
		US 2014136701 A1	15-05-2014
		US 2017195633 A1	06-07-2017
US 2003062997 A1	03-04-2003	CA 2389958 A1	18-03-2003
		US 2003062997 A1	03-04-2003
		WO 03026305 A1	27-03-2003

EPO FORM P0459

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