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

(11) **EP 4 207 123 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
05.07.2023 Bulletin 2023/27

(21) Application number: **21218141.6**

(22) Date of filing: **29.12.2021**

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

(52) Cooperative Patent Classification (CPC):
G08B 25/008

(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) Inventors:
- **HACKETT, Nicholas J.**
1290 Versoix, Geneva (CH)
- **PIEDBOIS, Julien**
1290 Versoix, Geneva (CH)

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

(54) **PREMISES SECURITY MONITORING SYSTEM**

(57) Provided is a method of automatically switching a security monitoring system of premises into a nocturnal armed at home mode, the premises providing accommodation for a household, and the accommodation comprising sleeping accommodation and living accommodation, the two accommodations being separate, the method comprising:
using radio-based presence and location sensing to detect perturbations of radio signals;
determining that the perturbations of radio signals signify that the household has vacated the living accommodation and occupied the sleeping accommodation;
using time of day and stored information about the households' daily routine,
applying one or more rules to determine whether use of the nocturnal armed mode is appropriate, and if it is appropriate switching the security monitoring system into the nocturnal armed at home mode, in which detection of movement or presence in the living accommodation constitutes an alarm event but in which detection of movement or presence in the sleeping accommodation does not constitute an alarm event.

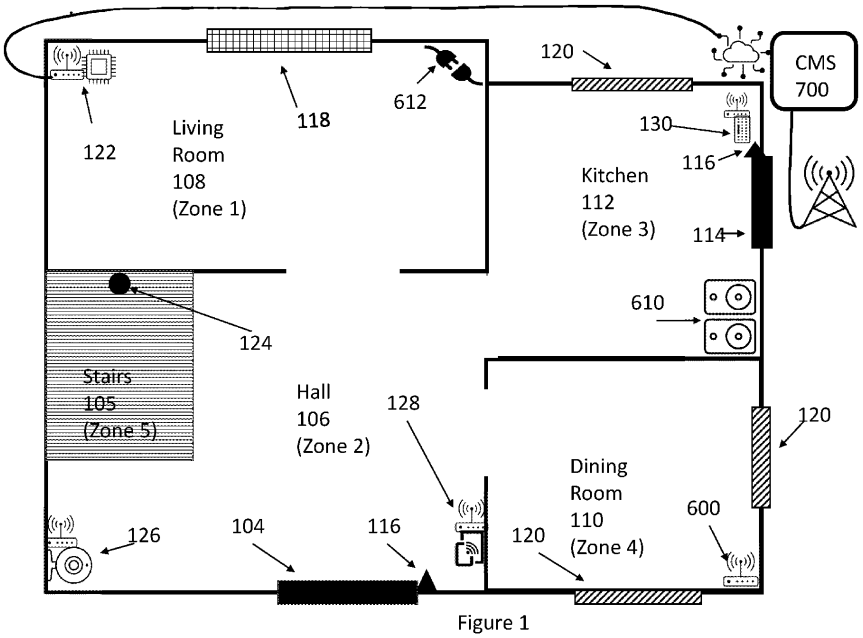

Figure 1

EP 4 207 123 A1

Description

Field

[0001] The present invention relates generally to security monitoring systems for premises, and in particular to installations of such systems including a radio-based location sensing arrangement to detect human presence and location based on detecting perturbations of radio signals, local management devices for such systems, and corresponding methods.

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 or local management device), generally mains powered, that is coupled to the sensors, detectors, cameras, etc. ("nodes"), and which processes received notifications and determines a response. The local management device or 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 remotely located monitoring station where, typically, human operators manage the responses required by different alarm and notification types. These monitoring stations are often referred to as Central Monitoring Station (CMS) because they may be used to monitor a large number of security monitoring systems distributed around the monitoring station, the CMS located rather like a spider in a web. In such centrally monitored systems, the local management device or 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 - in particular whether it is fully or only partially armed, 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] It is known for security monitoring systems to include more than one armed mode in addition to a disarmed mode. The ubiquitous armed mode is sometimes referred to as the "armed away" mode - in which the security monitoring system both secures the perimeter of the premises, and also monitors the interior of the premises with the possibility of an alarm event being triggered not only by a detected breach of the secured perimeter (for example upon the opening of a door or window provided typically with a node that senses opening based on a change in a magnetic field) but also upon motion been detected within the premises. A second armed mode, sometimes referred to as "armed at home", secures the perimeter, so that opening of a monitored door or window constitutes an alarm event, but typically movement within the house is not monitored and hence movement does not give rise to an alarm event. But depending upon the arrangement of sensors in the secured premises, there may be a third armed mode, which may be referred to as "night mode", and in which the perimeter is secured and movement within the sleeping accommodation of the premises is not monitored but movement within the living accommodation of the premises is monitored. If the security monitoring system has motion sensors in the living accommodation (e.g. on the ground floor, or "downstairs") but not in the sleeping accommodation (e.g. upstairs) then this night mode may simply be the same as the "armed away" mode.

[0005] The idea behind using the "night mode" (whether it is the armed away mode or a variant of "armed at home") is of course to provide a warning of and to any intruders who break into, or move around within, the living accommodation - which is commonly on the ground floor and hence more readily accessible than the sleeping accommodation that is commonly on an upper floor, while permitting occupants of the sleeping accommodation to move within and between bedrooms and bathrooms without triggering an alarm. Although many burglaries take place during the day, many also take place at night when there is more likelihood that the living accommodation will be vacant, but the sleeping accommodation occupied - and hence when the sounding of an alarm both to alert the legitimate occupants and hopefully deter the intruders has increased value. But sadly, many occupants of premises protected by security monitoring systems fail to arm them at night! There seem to be two reasons for this failure to arm. The first is that many occupants are scared by the risk of a false alarm, that is an alarm event triggered by a legitimate occupant - either by wandering downstairs (i.e., from the sleeping accommodation into

the living accommodation) in the night, perhaps for a midnight snack, forgetting that the system is armed and having neither a disarm dongle nor remembering the PIN to disarm the system, or by failing to vacate the monitored zone before that zone becomes "live". The second is that occupants just forget to set the alarm when they go to bed. And even if they do remember subsequently, they are reluctant to leave a warm comfortable bed to go downstairs "just" to arm the alarm.

[0006] User security would obviously be improved if users could be persuaded to use the "night-time" arming mode regularly, but so far the best efforts of suppliers of security monitoring systems to persuade users to do so have failed.

[0007] There therefore exists a need to find a way to increase the usage of the "night-time" arming mode of security monitoring systems. It will be appreciated that some households sleep during the day, rather than at night, at least sometimes - and the same concern exists for such households, albeit that the "night-time" mode is then the correct mode to employ during the day.

[0008] The present invention seeks to address this problem, at least in part.

[0009] Embodiments of the invention are based on the insight that in an installation in premises in which sleeping accommodation and living accommodation are separated (e.g. on different floors, in different zones of a single-storey premises, or in different wings, etc.), radio-based presence and location sensing may be used to switch the security monitoring installation from an armed perimeter state to a kind of armed away state (in effect secured perimeter plus movement/presence sensing within a particular portion of the premises but not in another portion) automatically on detecting that everyone has retired to bed. This automatic switching to what might be considered a nocturnal armed at home mode may provide greater user convenience and improved security, both by making it more likely that the system will actually be armed at night, and also by using radio-based presence and location sensing to monitor the living accommodation when the occupants are only present in the sleeping accommodation.

[0010] Such systems and installations could also be configured to use radio-based presence and location sensing to sense new movement from the sleeping quarters towards or into the living accommodation as a trigger to switch from the nocturnal mode to a/the "daytime" armed at home, permitting a householder to go from the sleeping quarters to the living accommodation, e.g. to the kitchen for a late night snack, without triggering the alarm. The system/installation could also be configured to re-arm automatically back to the nocturnal mode when the occupant goes back to bed.

[0011] This switching from the nocturnal armed at home mode to a normal or "daytime" armed at home mode when sensing new movement from the sleeping quarters towards or into the living accommodation could also (in addition or as an alternative to the use of radio-based sensing for this task) be done using one or discrete motion sensors, e.g., line of sight sensors such as PIRs to detect human movement from the sleeping accommodation towards and/or into the living accommodation. For example, one or more such sensors could be mounted to monitor the head of the stairs and other parts of the stairs that lead from the sleeping accommodation to the living accommodation. Preferably any such motion sensors, or the security monitoring system, are configured to respond only to human presence/movement and not, for example, to respond to the presence/movement of pets.

Summary

[0012] According to a first aspect, there is provided a security monitoring system for a dwelling, the dwelling including a first part providing living accommodation for occupants of the dwelling and, distinct from the first part, a second part providing sleeping accommodation for occupants of the dwelling, the system having a local management device, a plurality of alarm event sensors, and a radio-based location sensing arrangement to detect human presence and location within the first part and the second part of the dwelling based on detecting perturbations of radio signals, wherein the system is configured, to perform a determination that the occupants of the dwelling have all vacated the living accommodation for the sleeping accommodation (e.g. "retired for the day" or "gone to bed") based on presence information from the location sensing arrangement, and at least the time of day, and based on the determination automatically to arm the security monitoring system for the first part but not for the second part, so that if presence or movement is detected in the first part an alarm event is determined, but not if presence or movement is detected only in the second part.

[0013] By arming the security monitoring system, for a part, a zone, or overall, means that the local management device or central unit of the security monitoring system is set such that signals received by the local management device or central unit from alarm event sensors (e.g., PIR motion sensor) within the relevant area may trigger an alarm event (depending upon the identity of the sensor and the rules associated with it in the local management device). That is, typically the alarm event sensors in a security monitoring system are not "aware" of the arm state of the system, so that they typically respond to being triggered in the same way whatever the arm state of the system. What changes with arming into different armed states or disarming is the behaviour of the local management device: if the system is armed in respect of the area protected by the triggered sensor, the central unit will process the signal received from the sensor and this may (and generally will) give rise to an alarm event; but if the system is not armed in respect of the area protected by the triggered sensor, the central unit will just ignore the signal received from the sensor (generally after first

processing the signal) so that no alarm event is raised.

[0014] According to a second aspect there is provided a security monitoring system for a dwelling, the dwelling including a first part providing living accommodation for occupants of the dwelling and, distinct from the first part, a second part providing sleeping accommodation for occupants of the dwelling, the system having a local management device, a plurality of alarm event sensors, and a radio-based location sensing arrangement to detect human presence and location within the first part and the second part of the dwelling based on detecting perturbations of radio signals, wherein the local management device stores information about the occupants' daily routine and is configured, automatically to switch the system into a nocturnal armed at home mode in which detection of movement or presence in the first part constitutes an alarm event but in which detection of movement or presence in the second part does not trigger an alarm, in the event that information from the location sensing arrangement indicates that the occupants have vacated the living accommodation for the sleeping accommodation, and the time of day and the occupants' daily routine suggest that use of the nocturnal armed mode is appropriate (e.g. based on rules applied by the local management device).

[0015] According to a third aspect there is provided a security monitoring system for a dwelling, the dwelling including a first part providing living accommodation for occupants of the dwelling and, distinct from the first part, a second part providing sleeping accommodation for occupants of the dwelling, the system having a local management device, a plurality of alarm event sensors, and a radio-based location sensing arrangement to detect human presence and location within the first part and the second part of the dwelling based on detecting perturbations of radio signals, wherein the local management device stores information about the occupants' daily routine and is configured to: switch the system automatically into a nocturnal armed at home mode in which detection of movement or presence in the first part constitutes an alarm event but in which detection of movement or presence in the second part does not constitute an alarm event, in the event that information from the location sensing arrangement indicates that the occupants have vacated the living accommodation for the sleeping accommodation, and the time of day and the stored information about the occupants' daily routine suggest that use of the nocturnal armed mode is appropriate (e.g. based on rules applied by the local management device); but not to treat detected presence or movement in the first part as an alarm event if it is determined that someone has moved from the second part into the first part.

[0016] According to a fourth aspect there is provided a security monitoring system for a dwelling, the dwelling including a first part providing living accommodation for occupants of the dwelling and, distinct from the first part, a second part providing sleeping accommodation for occupants of the dwelling, the system having a local management device, a plurality of alarm event sensors, and a radio-based location sensing arrangement to detect human presence and location within the first part and the second part of the dwelling based on detecting perturbations of radio signals, wherein the local management device stores information about the occupants' daily routine and is configured to: switch the system automatically into a nocturnal armed at home mode, in which perimeter alarm event sensors are, if not already armed, armed to provide a secured perimeter, and detection of movement or presence in the first part constitutes an alarm event but in which detection of movement or presence in the second part does not constitute an alarm event, in the event that information from the location sensing arrangement indicates that the occupants have vacated the living accommodation for the sleeping accommodation, and the time of day and the stored information about the occupants' daily routine suggest that use of the nocturnal armed mode is appropriate (e.g. based on rules applied by the local management device); but not to treat detected presence or movement in the first part as an alarm event if it is determined that someone has moved from the second part into the first part without the perimeter alarm event sensors having detected breaching of the secured perimeter.

[0017] In a fifth aspect there is provided a security monitoring system for a dwelling, the dwelling including a first part providing living accommodation for occupants of the dwelling and, distinct from the first part, a second part providing sleeping accommodation for occupants of the dwelling, the system having a local management device (which may also be referred to herein as a central unit), a plurality of alarm event sensors coupled to the local management device, and a radio-based location sensing arrangement to detect human presence and location within the first and second parts of the dwelling based on detecting perturbations of radio signals, wherein the local management device stores information about the occupants' daily routine and is configured to switch the system automatically into a nocturnal armed at home mode, in which perimeter alarm event sensors are, if not already armed, armed to provide a secured perimeter, in the event that information from the location sensing arrangement indicates that the occupants have vacated the living accommodation for the sleeping accommodation, and the time of day and the stored information about the occupants' daily routine suggest that use of the nocturnal armed mode is appropriate (e.g. based on rules applied by the local management device); the nocturnal armed at home mode being a mode in which detection of movement or presence in the first part constitutes an alarm event, but in which detection of movement or presence in the second part does not constitute an alarm event; and the local management unit is further configured, in the nocturnal armed at home mode, not to treat detected presence or movement in the first part as an alarm event if it is determined that someone has moved from the second part into the first part without the perimeter alarm event sensors having detected breaching of the secured

perimeter.

[0018] In a sixth aspect, there is provided a security monitoring system installation in a dwelling, the dwelling including a first part providing living accommodation for occupants of the dwelling and, distinct from the first part, a second part providing sleeping accommodation for occupants of the dwelling, the system having a plurality of alarm event sensors, and a radio-based location sensing arrangement to detect human presence and location within the first and second parts of the dwelling based on detecting perturbations of radio signals, coupled to a local management device, wherein the local management device is configured to store information about the occupants' daily routine and is further configured to switch the system automatically into a nocturnal armed at home mode, in which perimeter alarm event sensors are, if not already armed, armed to provide a secured perimeter, in the event that information from the location sensing arrangement indicates that the occupants have vacated the living accommodation for the sleeping accommodation, and the time of day and the stored information about the occupants' daily routine are such that use of the nocturnal armed mode is appropriate based on rules stored in the local management device; the nocturnal armed at home mode being a mode in which detection of movement or presence in the first part constitutes an alarm event, but in which detection of movement or presence in the second part does not constitute an alarm event.

[0019] It should also be appreciated that each of the first through sixth aspects also provides a corresponding local management device.

[0020] In an seventh aspect there is provided a local management device for a security monitoring system installation in a dwelling, the dwelling including a first part providing living accommodation for occupants of the dwelling and, distinct from the first part, a second part providing sleeping accommodation for occupants of the dwelling, the system including a radio-based location sensing arrangement to detect human presence and location within the first part and the second part of the dwelling based on detecting perturbations of radio signals, the local management device configured to: be coupled to a plurality of alarm event sensors; store information about the occupants' daily routine; and automatically switch the system into a nocturnal armed at home mode in which detection of movement or presence in the first part constitutes an alarm event but in which detection of movement or presence in the second part does not constitute an alarm event, in the event that information from the location sensing arrangement indicates that the occupants have vacated the living accommodation for the sleeping accommodation, and the time of day and the stored information are such that use of the nocturnal armed mode is appropriate based on rules stored in the local management device.

[0021] Each of the first through seventh aspects also provides a method of automatically switching a security monitoring system of premises into a nocturnal armed at home mode.

[0022] In an eighth aspect there is provided a method of automatically switching a security monitoring system of premises into a nocturnal armed at home mode, the premises providing accommodation for a household, and the accommodation comprising sleeping accommodation and living accommodation, the two accommodations being separate, method comprising:

using radio-based presence and location sensing to detect perturbations of radio signals;
determining that the perturbations of radio signals signify that the household has vacated the living accommodation and occupied the sleeping accommodation; using time of day and stored information about the households' daily routine, applying one or more rules to determine whether use of the nocturnal armed mode is appropriate, and if it is appropriate switching the security monitoring system into the nocturnal armed at home mode, in which detection of movement or presence in the living accommodation constitutes an alarm event but in which detection of movement or presence in the sleeping accommodation does not constitute an alarm event.

[0023] The method may further comprise, as part of switching the system into the nocturnal armed at home mode, configuring the system to provide a secured perimeter, in the event that the system is not already providing a secured perimeter, and optionally further comprising, in the nocturnal armed at home mode, if no signal has been received indicating that the secure perimeter has been breached, determining that someone has moved from the sleeping accommodation into the living accommodation, and thereafter ceasing to treat the detection of movement or presence in the living accommodation constitutes as an alarm event.

[0024] The method may further comprise using radio-based location sensing presence and location sensing to perform people counting, and optionally determining the presence of one or more intruders based on detecting a change in the people count when the system is in the nocturnal armed mode

Brief description of the drawings

[0025] 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 plan of a single floor of premises in which a first security monitoring system has been installed, the system including a radio-based presence and location sensing system;
Figure 2 illustrates schematically the principles of radio-based presence and location sensing; and
Figure 3 illustrates schematically features of a local management device of the system of Figure 1.

Specific description

[0026] Figure 1 shows schematically a security monitoring system installation 100 in a dwelling, having a perimeter. In this example, the dwelling is a multi-storey house. A front door 104 serves as the main entrance to the premises. The Figure shows just one floor of the dwelling, in this instance a ground floor, which accommodates the living space, while the sleeping space is provided on one or more other (upper) floors accessed via stairway 105. The living space includes an entrance hall 106, onto which the front door 104 opens, off which are a rear living room 108, a front dining room 110, and a rear kitchen 112.

[0027] The kitchen 112 includes the back door 114 of the premises. The front 104 and back 114 doors are each provided with a sensor arrangement 116 that is triggered by the opening of the relevant door - for example, a sensor arrangement 116 including a magnetically triggered sensor such as a reed relay or a magnetometer.

[0028] The living room 108 is provided with glazed doors 118, which may be in the style of "French Windows" or the like, which permit access to a rear garden, but which are not intended, or used, for regular access to the interior of the premises. These doors 118 may not be provided with any sensing arrangement to detect their opening (to reduce the cost of installing the security monitoring system), but preferably are. Similarly, windows 120 to the kitchen 112 and dining room 110 may also not be provided with any sensing arrangement to detect their opening (but preferably are) - again as a means of reducing the cost of installing the security monitoring system.

[0029] The security monitoring system includes a controller or central unit (which may also be referred to as a local management device) 122 which is operatively coupled to the door opening sensors 116 and any other sensors of the system preferably wirelessly using radio frequency (RF) communication rather than via a wired connection. In addition, the central unit 122 is operatively connected, for example via a wired and/or wireless Internet connection, to a remote monitoring station 700 to which alarm events are communicated for review and for appropriate intervention or other action to be taken - and preferably the remote monitoring station 700 (also referred to as a central monitoring station, CMS, given that one such station typically supports several or many security monitoring installations) is staffed by human operatives who can for example review images, video, and/or sound files, plus other alert types and details, in order to decide whether to deploy private security staff, law enforcement agents, a fire brigade, or medical staff such as paramedics or an ambulance - as well as optionally reporting events and situations to one or more individuals associated with the security monitoring system (e.g. a householder or owner).

[0030] The security monitoring system also includes one or more motion sensors, typically line-of-sight motion sensors such as PIR sensors. In the illustrated example, a motion sensor 124 is shown as being installed only at the head of the stairs 105 that lead to the upper floor(s).

[0031] Preferably, as shown, the security monitoring system includes at least one camera, preferably a video camera with an associated (integral or separate) motion sensor, activation of which may cause the camera (or the motion sensor) to report an event to the central unit. In response, the central unit 122 may or may not instruct the camera to transmit images (still or video), for example using a Wi-Fi transceiver, to the central unit for onward reporting to the CMS 700.

[0032] The upper floor(s) of the premises may or may not include one or more motion sensors, and there may be a motion-triggered video camera, typically at the head of the stairs. Depending upon the proximity of climbable features externally, such as rainwater downpipes, soil stacks, trees, outbuildings, some or all of the windows on the upper floors may also be provided with sensors to detect their whether they are opened or closed, and sometimes also to show the degree of their opening if open (e.g. based on one or more magnets and one or more magnetometers or other sensors responsive to a magnetic field). But typically, the bedrooms and bathrooms, and often the landings and walkways between them, will not be provided with motion sensors - the idea being that such sensors will not be armed in the armed at home mode, because we don't want the alarm being triggered at night by occupants of the bedrooms, nor by those occupants walking between bedrooms or between bedrooms and bathrooms.

[0033] The security monitoring system also includes a user interface or control panel 128 in the hall 106 fairly close to the front door 104. This control panel 128 is provided so that a user can arm and disarm the security monitoring system using either a code or PIN (e.g. a 4 or 6 digit PIN) or a token (using a short-range communication technology e.g. RFID, NFC, BTLE). The control panel may also be used to set the security monitoring system to an armed at home state, optionally directly from an armed away state. The control panel 128 preferably includes a visual display, such as a screen (optionally a touch sensitive display) to provide users with system information, status updates, event reports, and even possibly face to face communication with personnel in the central monitoring station (for which purpose the control panel 128 may have a built-in video camera and optionally lighting). Although the same type of user interface may also be provided adjacent the back door (within the premises), typically a rather simpler device - known as a disarm node 130, may be provided to enable a user to disarm or arm the system, again optionally using a PIN, code, or dongle/device. Such a disarm node 130 may include one or more indicator lights, featuring e.g. RGB LEDs, to provide visual feedback on arming status (armed away, armed at home, and possibly other armed states), alarm event status, as well as at least an audio output device to provide warning and advisory tones or

messages. Preferably the disarm node 130 includes both an audio output device (e.g. one or more loudspeakers and optionally an alarm sounder) and a microphone so that a user can talk with a CMS operator if necessary. Like the sensors 116 and 124, the control panel 128 and disarm node 130 are preferably provided with at least one radio transceiver for communication with the control unit 122, as well as having at least built-in autonomous power supplies (e.g., each having a battery power supply). The various nodes of the security monitoring system, other than the central unit 122, are preferably battery powered and communicate using RF transceivers that consume little power (hence, not relying on Wi-Fi, 802.11 protocols, as these tend to be very power hungry) for control signals and for event reporting and that typically rely on radio frequencies in approved ISM frequency bands - such as between 860 and 900 MHZ. As already mentioned, any video cameras will typically include in addition a Wi-Fi transceiver for use in transmitting image and video data, on request, to the central unit.

[0034] Conventionally, when such a security monitoring system is in the disarmed state, opening of the front or back doors, or triggering any of the motion sensors 124 doesn't constitute an alarm event. The relevant sensor 116, 124 will typically be configured to report a sensed event to the central unit 122 irrespective of the arm state of the security monitoring system (since typically the nodes of a security monitoring system are not aware of the arming state of the system), but the central unit 122 will disregard such reported events when the system is disarmed. In the fully armed state, which may be termed the "armed away" state, event notifications from perimeter sensors (in the illustrated example the door opening sensors 116 on the front 104 and back 114 doors, but typically also including one or more sensors to detect the opening of windows 120) and internal movement or presence sensors, typically result in the central unit 122 determining an alarm event which may then be reported to the central monitoring station 700. As previously explained, typically, such security monitoring system also have a second armed state in which only the security of the perimeter is monitored - so that only events reported by one or other of the door sensors 116 (or window sensors if present) count as potential alarm events to be reported by the central unit 122 to the remote monitoring station 700 - and this may be termed the "armed at home" state. The armed at home state is intended to be used when the premises are occupied. In the armed at home state the central unit 122 will routinely be arranged not to request any internal (video) camera to share images with the central unit 122 - so that user privacy is maintained.

[0035] There may be more than one variant of the armed at home state - so that, for example during the daytime only the perimeter may be monitored, but at night (or upon the occupants retiring to bed) the system may be set to a nocturnal armed at home state in which movement within the living accommodation (but not the sleeping accommodation) can also give rise to an alarm event potentially to be reported to the CMS 700 (including images from any camera within the monitored zone) - but the triggering of any movement sensors for the area of the sleeping accommodation, e.g. on a landing, will not give rise to alarm events. The illustrated installation provides such a nocturnal armed at home state, as well as a "daytime" armed at home state in which only the perimeter is secured.

[0036] The installation shown in Figure 1 also includes a radio-based location sensing arrangement to detect human presence throughout the premises (both the ground floor "living accommodation" and the "sleeping accommodation" on the upper floor(s), that is configured to sense presence and location based on detecting perturbations of radio signals. Figure 1 shows various Wi-Fi capable devices which are distributed around the ground floor, signals from which are used by a radio-based location sensing arrangement which is provided as part of the security monitoring system.

[0037] The radio-based presence sensing, which here is conveniently be based on the monitoring of Wi-Fi signals (but which could be based on radio signals from other radio communications standards or protocols), and which for convenience we will refer to as WFS, is here performed by the central unit 122 which operates as a Wi-Fi Access Point (AP) and which serves as a Wi-Fi sensing receiver. The Figure shows the presence of various radio transceivers that are used to provide radio-based presence detection in each of the interior spaces of the ground floor of premises. The WFS system may be configured to recognise location "zones" which may map to rooms, or map to floors in premises comprising a plurality of floors, but may also map to regions within rooms, and exterior zones may be identified corresponding to particular sections of the grounds or surroundings of a dwelling or other structure - e.g. terrace, front garden, parking area, etc.

[0038] To ensure that the WFS effectively covers the whole area of interest (for example, the ground of the premises, as shown here) we need to provide a sufficient number of suitable located Wi-Fi stations (STAs) as WFS illuminators so that Wi-Fi signals received at the central unit AP 122 traverse the whole area of interest. If we want to provide WFS cover to multiple floors we may need to provide an appropriate WFS receiver on each floor, together an appropriate number of suitably positioned illuminator devices, although depending on the building's construction signals from illuminators on one floor may be used by WFS receivers on other floors.

[0039] Because Wi-Fi transceivers are quite power hungry, we will generally want the STAs used as WFS illuminators to be mains powered (but preferably also with some back-up power supply such as an internal battery power source) rather than solely battery powered. That may lead us to replace some battery powered but Wi-Fi capable devices of an existing non-WFS security monitoring system with mains powered equivalents - so, for

example, a battery powered video camera might be replaced by a mains powered equivalent 126, and a battery powered control unit may be replaced by a mains powered equivalent 128 that is Wi-Fi capable (although the control unit 128 will typically still use something other than a Wi-Fi transceiver (e.g. a low power ISM transceiver) to communicate with the central unit 122).

[0040] Alternatively (or additionally) we may simply add new mains powered Wi-Fi capable devices such as smart plugs, smart bulbs, Wi-Fi range extenders (for example of the type that simply plug in to a socket of the mains electricity supply), to provide a Wi-Fi network that covers the whole of the area of interest and that is used for WFS. The household may have more than one Wi-Fi network, but generally only one of these will be used for WFS - and conveniently the central unit 122 will be an AP of that network.

[0041] The central unit AP 122 preferably works in infrastructure mode in conjunction with the various other Wi-Fi stations (STAs) to form either an infrastructure Basic Service Set (BSS) or, in conjunction with another AP connected (e.g via ethernet) to the same Local Area Network as the central unit 122 - such as broadband router 600, to provide an Extended Service Set (ESS).

[0042] For ease of explanation, we will assume initially that the central unit AP 122 provides just a BSS and not an ESS, and that only the central unit AP 122 serves as a Wi-Fi sensing receiver. Some or all of the STAs in the BSS act as illuminators to provide signals which the CU 122 analyses in order to perform WFS. As shown, these other STAs include the broadband router 600 in the dining room, the control unit 128 and a Wi-Fi-enabled camera 126 in the hall, and optionally the disarm node 130 in the kitchen. Preferably, because of the power consumption concerns, both the Wi-Fi enabled camera and the disarm node 130 are fed with power from a mains electricity supply as well as having an autonomous internal power supply. In addition, the kitchen is provided with an STA in the form of for example a "smart speaker" 610, and the living room with a "smart plug" 612. If the disarm node 130 only has an internal power supply, and is not mains fed, it is preferably not configured as a Wi-Fi STA but instead some other Wi-Fi STA device (such as the smart speaker 610) may be installed to suitably extend WFS coverage within the kitchen and the living room - for example, a Wi-Fi range extender or smart plug or the like which is plugged into a conveniently located power socket.

[0043] With the arrangement shown in Figure 1 the control unit 122 (or more generally the security monitoring system, given that some entity other than the central unit may be responsible for determining presence and location of presence) may be configured, whatever the arming state of the system, to use the radio-based presence sensing to detect and locate presence within the monitored area(s). The system (typically the central unit) may for example records, e.g. in a database, the location (e.g. the relevant zone identifier) and time of the inferred presence. The system (e.g. central unit) receives information data from the radio-based presence sensing arrangement relating to detected presence and these data will be processed to determine the location(s) (e.g. zone identifier(s)) of any human presence and also preferably information data relating to the person count in each zone determined to be occupied. These data, and their timings, are recorded in the database. The system (e.g., the central unit) is therefore continuously aware when and where there is presence in the monitored areas.

[0044] Although Figure 1 only illustrates a single floor of premises, it will be appreciated that if it is desired to provide a WFS capability for other floors of the premises - as we do here, because the sleeping accommodation is provided on the upper floor(s) while the ground floor is devoted to living accommodation - it is necessary to ensure suitable Wi-Fi network coverage of those floors, typically by providing a corresponding access point, together with a plurality of Wi-Fi STAs as illuminators, for each floor - although sometimes useful WFS capability can be achieved between floors. Understandably, attenuation of signals within a building is critically dependent upon the type of construction and the materials used, and these factors need to be considered when designing and installing any WFS system.

[0045] We will now provide a brief introduction to radio-based presence detection, which may for example be based on analysing the signal dynamics and signal statistics of radio signals and/or detecting changes in channel state information (CSI). A radio (or wireless) signal as used herein refers to a signal transmitted from a radio transmitter and received by a radio receiver, wherein the radio transmitter and radio receiver operate according to a standard or protocol. Such standards include, but are not limited to, IEEE 802.11. (which includes the Wi-Fi standards), IEEE 802.15 (which includes Zigbee), Bluetooth SIG, IEEE 802.16, IEEE 802.20, UMTS, GSM 850, GSM 900, GSM 180, GSM 19011, GPM ITU-R 5.13, GPM ITU-R 5.150, ITU-R 5.280, 3GPP 4G (including LTE), 3GPP 5G, 3GPP NR, AND IMT-2000. However, the radio transmitters and receivers providing and using radio signals for WFS may operate in nontelecommunications or Industrial, Scientific and Medical (ISM) spectral regions without departing from the scope of the invention.

[0046] Essentially the idea is to use radio signals to probe a zone or zones of interest, and to analyse and extract statistics from these signals, in particular looking at the physical layer and/or data link layer such as MAC address measurements that expose the frequency response of a radio channel (e.g., CSI or RSSI measurements). These measurements are processed to detect anomalies and variations over time, and in particular to detect changes signifying the entrance of a person and/or movement of a person within a monitored zone. The zone(s) to be monitored need to be covered sufficiently by radio signals, but the sources of the radio signals may either already be present before a monitoring system is established - for example from the plurality of Wi-Fi or

Bluetooth capable devices that are now dotted around the typical home or office, or the sources may be added specifically to establish a monitoring system. Often some established (i.e., already located or installed) radio devices are supplemented by some extra devices added as part of establishing a radio-based presence detection system. Among the types of devices (preinstalled or specifically added) that may be used as part of such a detection system are Wi-Fi access points, Wi-Fi routers, smart speakers, Wi-Fi repeaters, as well as video cameras and video doorbells, smart bulbs, etc. Because presence (or intrusion) is detected by detecting a change in the properties or character of radio signals compared to some previous reference signal(s), it is preferred to establish what might be termed the monitoring network between radio devices that are essentially static (i.e., that remain in the same position for extended periods) rather than relying on devices that are repeatedly moved - such as smart phones, headphones, laptops, and tablet devices. It is not strictly speaking essential for all the devices whose signals are used by the monitoring system to be part of the same network - for example, signals from Wi-Fi access points of neighbouring premises could be used as part of a monitoring system in different premises. Again, a primary consideration is the stability of the signals from the signal sources that are used. Wi-Fi access points provided by broadband routers are seldom moved and rarely turned off, consequently they can generally be relied upon as a stable signal source - even if they are in properties neighbouring the property containing the zone or zones to be monitored.

[0047] The idea is illustrated very schematically in Figure 2, here with an installation 200 including just a single source (or illuminator) 202 and just a single receiver 204, for simplicity, although in practice there will typically be multiple sources (illuminators) and sometimes plural receivers. The installation 200 has been established to monitor a monitored zone 206. In Figure 2A we see that in steady state, and in the absence of a person, radio signals are transmitted from the source 202, spread through the monitored zone 206, and are received by the receiver 204. Of course, in most installations there will be walls, ceilings, floors, and other structures that will tend to reflect, at least in part, signals from the source. Furniture and other objects may block and attenuate the signals, the reflected signals will give rise to multiple paths, and the signals may interfere with each other, and there may be scattering and other behaviours, such as phase shifts, frequency shifts, all leading to complexity in the channels experienced by the radio signals that arrive at the receiver 204. But while the environment is static and unchanging, the receiver will tend to see a consistent pattern of radio signals. And this is true whether or not the source transmits continuously or transmits periodically. But this consistent pattern of received signals is changed by the arrival of an intruder 208, as shown in Figure 2B. From Figure 2B we see that, at the very least, the presence of a person in the monitored zone blocks at least some of the signals from the source, and that affects the pattern of radio signals received by the receiver 204. The changed pattern of signals received by the receiver enables the presence of the intruder to be detected by a presence monitoring algorithm that is supplied with information derived from the received signals. It will be appreciated that the nature and extent of the perturbation of the signals passing from the source 202 to the receiver 204 is likely to change as the intruder 208 enters, passes through, and leaves the monitored area 206, and that this applies also to reflected, refracted, and attenuated signals. These changes may enable the location of a person within the zone, and their speed of movement, to be determined. Indeed, these techniques have been shown even to be capable of detecting gestures, and patterns of human respiration, as well as enabling "people counting".

[0048] It will be realised that signals that are received from an illuminator device (or from more than one illuminator device) after having passed through a monitored space (or volume), have in effect been filtered by the environment to which they have been exposed. We can therefore imagine the monitored volume as a filter having a transfer coefficient, and we can see that a received signal is at least in part defined by the properties, or channel response, of the wireless channel through which it propagated. If the environment provided by the monitored volume changes, for example by the addition of a person, then the transfer coefficient of the filter, and the channel response or properties, will also change. The changes in the transfer coefficient, and in the channel response, consequent on the change in the environment of the monitored space, can be detected and quantified by analysing radio signals received by the wireless sensing receiver(s). Both the introduction of an object, e.g. a person, into the monitored space, and movement of that object within the monitored space will change the environment and hence change the effective transfer coefficient and the channel response.

[0049] The radio-based sensing system can be trained by establishing a base setting in which the monitored zone is unoccupied, which is then labelled as unoccupied for example using a smartphone app or the like, and then training occupied states by a person entering, standing, and then walking through each of the zones one by one. Presence at different locations in each of the zones may be captured and labelled in the system in the same way. This process may be repeated with two people, and then optionally with more people. In essence this is a supervised machine learning approach, but other approaches to training may be used.

[0050] The system may need to be retrained for the base setting if bulky furniture or other large objects (particularly if made of metal) are added to or moved within the monitored space, because these can be expected to change the propagation properties of the relevant zone/space. The data for unoccupied states are preferably retained within a database of "unoccupied" states,

even when there are changes to the arrangement of furniture etc. It may not be necessary to retrain for the occupied states if the system can determine a delta function between the previous base state and the new one, because the delta function may also be applicable in occupied states. But if not, it may be sufficient to retrain only a subset of the occupied states previously learnt. The system may also be configured to self-learn to accommodate changes in the characteristics of the zones when unoccupied, and to add newly determined unoccupied state data to the database.

[0051] Although the Figure 2 example uses just a single source (illuminator) and a single receiver, as already mentioned generally multiple sources (illuminators) will be used in order to achieve satisfactory coverage of the zone or zones to be monitored. Multiple zones may be monitored by a single receiver through the use of multiple strategically placed sources, but each zone, or some zones of multiples zones may have a dedicate receiver that does not serve other zones. Likewise, a radio signal source (illuminator) may provide illuminating signals for a single monitored zone or for multiple monitored zones. Also, a presence monitoring system (and a security monitoring system including such a presence monitoring system) may use mesh network arrangement, for example a Wi-Fi mesh network, in which multiple devices act as receivers for illuminating signals - either for a single monitored zone or for multiple monitored zones.

[0052] Now, considering once again the installation of Figure 1, and assuming that the location and presence sensing arrangement also covers the sleeping accommodation of the premises, it will be appreciated that by combining a radio-based location sensing arrangement with a premises security monitoring system it is possible for the security monitoring system to be aware of human presence and the location(s) of any humans present. The security monitoring system can thus be configured automatically to switch the system into a nocturnal armed at home mode, in which detection of movement or presence in the living accommodation constitutes an alarm event but in which detection of movement or presence in the sleeping accommodation does not constitute an alarm event, in the event that information from the location sensing arrangement indicate that the occupants have vacated the living accommodation for the sleeping accommodation. The time of day and stored information about the occupants' daily routine may be used in determining that use of the nocturnal armed mode is appropriate based on rules stored in the local management device. In this way, the security monitoring system can provide enhanced security because it can automatically switch to a premises monitored nocturnal armed at home mode rather than a user having to remember to arm the system appropriately each time the "household" (however many people that is) retires to bed.

[0053] Information about the occupants' daily routine may conveniently be provided by user input at a user interface of the security monitoring system, either as part of the control unit 128 or, for example by means of a dedicated app or a web page, and stored by the system (e.g. in the central unit 122). Thus, preferably the installation or the central unit is further configured to accept user input of information about occupants' daily routine, optionally in the form of usual bedtime(s), optionally for specified days of the week.

[0054] Such information about user's daily routines, in particular usual bedtimes, is preferably provided on initial installation of the system or on handover to new owners/tenants/occupiers (e.g. when the house is sold, or when a new academic year begins). "Normal bedtimes" may be provided with a range or span (e.g. half an hour, an hour, or more than an hour) depending on the regularity of household hours, typically specified for particular days of the week and taking account of weekends, holidays, and regular events or activities.

[0055] The local management unit may be configured to acquire information about the occupants' daily routine based on information from the radio-based location sensing arrangement, including the number of occupants detected and their movements, user interactions with the security monitoring system, and taking account of time of day. Preferably the system is also configured to adapt the stored information based on observation of the household's behaviour, for example using machine learning.

[0056] The stored information about user's daily routines should be updated or replaced if the composition of the household changes, e.g. if the number of people making up the household changes - for example following sale of the house, or with a new intake of tenants, or if the occupants' schedules change markedly for any other reason.

[0057] In an embodiment there is provided a local management device for a security monitoring system installation in a dwelling, the dwelling including a first part providing living accommodation for occupants of the dwelling and, distinct from the first part, a second part providing sleeping accommodation for occupants of the dwelling, the system including a radio-based location sensing arrangement to detect human presence and location within the first part and the second part of the dwelling based on detecting perturbations of radio signals, the local management device configured to: be coupled to a plurality of alarm event sensors;

store information about the occupants' daily routine; and

automatically switch the system into a nocturnal armed at home mode in which detection of movement or presence in the first part constitutes an alarm event but in which detection of movement or presence in the second part does not constitute an alarm event, in the event that information from the location sensing arrangement indicates that the occupants have vacated the living accommodation for the sleeping accommodation, and the time of day and the stored information are such that use of the nocturnal armed mode is appropriate based on rules stored in the local management device.

[0058] The local management device may be further configured to switch the system automatically into a nocturnal armed at home mode, in which perimeter alarm event sensors are, if not already armed, armed to provide a secured perimeter. This is useful if the occupier(s) have forgotten or chosen not to put the system into the "daytime" armed at home mode before going to bed.

[0059] The local management device may be configured, in the nocturnal armed at home mode, not to treat detected presence or movement in the first part as an alarm event if it is determined that someone has moved from the second part into the first part without the perimeter alarm event sensors having detected breaching of the secured perimeter.

[0060] The installation may further comprise one or more line of sight motion detectors coupled to the local management device and positioned to detect human movement from the second part into the first part. For example, where the living accommodation is on one floor and the sleeping accommodation on another floor, the sleeping accommodation including a landing or passageway that leads from the bedrooms and bathrooms to the stairs, a first such detector could be provided to detect anyone leaving the sleeping area for the stairs, and a second such detector could be provided on or at the stairs to detect anyone leaving the sleeping accommodation. In a sense, the stairs and the approach to the stairs within the zone that provides the sleeping accommodation constitute a buffer zone or zone of transition between the sleeping and living accommodation. By monitoring entrance into this zone (from the sleeping zone), it is possible to determine when someone is moving from the sleeping zone into the living zone - and to do so before the person can trigger an alarm event by being detected in the living zone. It will be appreciated that the monitoring of the buffer zone may be done either using WFS or using line of sight (or other) motion sensing arrangements, or both, and the system can be configured to use the relevant information to automatically disarm the system into a secured-perimeter only armed state. Clearly, the same technique may be used in reverse by confirming that the person has left the living accommodation and returned to the sleeping accommodation, so that the system can re-arm back into nocturnal mode. Even when the living and sleeping accommodation are provided on a single floor there will generally be a buffer zone or zone of transition between the living and sleeping accommodations, unless the sleeping accommodation is distributed within the living accommodation (in the latter case it will generally not be possible to employ the invention). Any such buffer or intermediate zone can typically be provided with line-of-sight or other motion detectors to produce a result as just described.

[0061] The radio-based location sensing arrangement is preferably trained to identify perturbations of radio signals corresponding to human movement from the sleeping accommodation into the living accommodation. So, for example, a processor of the local management device or central unit 122 may be trained, e.g. using supervised learning based on controlled human presence and movement, to recognise patterns of perturbations in radio signals that correspond to human movement from the sleeping accommodation into the living accommodation. This training, or at least the initial training (as the system may be configured to use unsupervised machine learning thereafter) preferably happens upon installation of the security monitoring system. If the system includes appropriately positioned motion sensors (as just described)

[0062] The local management device may be configured, on determining that someone is about to enter the living accommodation from the sleeping accommodation (e.g., someone is has entered the buffer zone from the sleeping accommodation), or has moved from the second part into the first part, to disarm the security monitoring system to a mode in which only a detected breach of the perimeter is treated as an alarm event.

[0063] The local management device may be further configured to use data from the radio-based location sensing arrangement to perform people counting, and optionally to use determine the presence of one or more intruders based on a detected change in the people count when the system is in the nocturnal armed mode. For example, the techniques and methods described in US2020/0302187A1, assigned to Origin Wireless, can be used to count occupants and determine their locations in installations, systems and methods according to embodiments of the invention.

[0064] In installations or systems according to embodiments of the invention the plurality of alarm event sensors may include one or more motion sensors to detect movement in the first part, and optionally one or more motion sensors to detect movement in a buffer zone intermediate the first part and the second part, and/or optionally one or more motion sensors to detect movement in the second part.

[0065] The radio-based sensing arrangement is preferably configured to process communication signals received from one or more radio transmitters operating according to one or more communication standards or protocols, and optionally the one or more radio transmitters that are in a common wireless network with the local management device.

[0066] Preferably, the local management device includes a radio receiver of the radio-based presence and location sensing system, and optionally the local management device includes a processor and a memory holding software instructions that when run on the processor cause the local management device to process radio signals to derive location and presence data.

[0067] Preferably, the sensing arrangement to detect human presence uses changes in channel state information or received signal strength in determining presence.

[0068] Preferably, the local management device is configured to function as an access point of a radio network whose signals are used by the radio-based presence and location sensing system. Optionally, the radio

network for which the local management device functions as an access point includes at least one further access point.

[0069] Preferably, the radio network is a Wi-Fi network, and optionally the one or more radio transmitters include one or more of the following: a Wi-Fi access point, a Wi-Fi extender, a smart plug or smart socket, a smart speaker, a smart bulb, a control panel of the security monitoring system, a Wi-Fi-enabled video camera.

[0070] Preferably, the local management device is further configured to perform processing of signals as part of the radio-based location sensing arrangement.

[0071] In an embodiment, there is provided a method of automatically switching a security monitoring system of premises into a nocturnal armed at home mode, the premises providing accommodation for a household, and the accommodation comprising sleeping accommodation and living accommodation, the two accommodations being separate, the method comprising: using radio-based presence and location sensing to detect perturbations of radio signals; determining that the perturbations of radio signals signify that the household has vacated the living accommodation and occupied the sleeping accommodation; using time of day and stored information about the households' daily routine, applying one or more rules to determine whether use of the nocturnal armed mode is appropriate, and if it is appropriate switching the security monitoring system into the nocturnal armed at home mode, in which detection of movement or presence in the living accommodation constitutes an alarm event but in which detection of movement or presence in the sleeping accommodation does not constitute an alarm event.

[0072] The method may further comprise, as part of switching the system into the nocturnal armed at home mode, configuring the system to provide a secured perimeter, in the event that the system is not already providing a secured perimeter, and optionally in the nocturnal armed at home mode, if no signal has been received indicating that the secure perimeter has been breached, determining that someone has moved from the sleeping accommodation into the living accommodation, and thereafter ceasing to treat the detection of movement or presence in the living accommodation constitutes as an alarm event.

[0073] The method may further comprise using radio-based location sensing presence and location sensing to perform people counting, and optionally determining the presence of one or more intruders based on detecting a change in the people count when the system is in the nocturnal armed mode.

[0074] Figure 3 is a schematic drawing showing in more detail features of the gateway or central unit 122 of Figures 1. The gateway 122 includes a first transceiver 430 coupled to the first antenna 480, and optionally a second transceiver 432 coupled to a second antenna 482. The transceivers 430 and 432 can each both transmit and receive, but a transceiver cannot both transmit and receive at the same time. Thus, the transceivers 430, 432 each operate in half duplex. Preferably a transceiver will use the same frequency to transmit and receive (although of course if the two transceivers are to operate simultaneously but in opposite modes, they will operate on different frequencies). The transceivers 430, 432 may be arranged such that one transceiver 430 uses a first frequency for transmit and receive and the second transceiver 432 uses the same first frequency for transmit and receive, i.e. the transceivers are arranged to operate in a diversity-like arrangement. Alternative, the second transceiver may, depending on configuration, be arranged to use a second frequency for transmit and/or receive. The transceivers 430 and 432 are coupled to a controller 450 by a bus. The controller 450 is also connected to a network interface 460 by means of which the controller 450 may be provided with a wired connection to the Internet and hence to the monitoring centre 700. The controller 450 is also coupled to a memory 470 which may store data received from the various nodes of the installation for example event data, sounds, images and video data. The central unit 122 also includes a crystal oscillator 451, which is preferably a temperature controlled or oven-controlled crystal oscillator. This is used for system clocking and also frequency control of the transceivers. The gateway 122includes a power supply 362 which is coupled to a domestic mains supply, from which the gateway 122 generally derives power, and a backup battery pack 464 which provides power to the gateway in the event of failure of the mains power supply. Preferably, as shown, the central unit 122 also includes a Wi-Fi transceiver 440, and associated antenna arrangement 442, which may be used for communication with any of the nodes that is Wi-Fi enabled. The Wi-Fi enabled node may be a remote control or control panel that may for example be located close to the main entrance to the building (e.g., control panel 128 or disarm node 130) to enable the occupier to arm or disarm the system from near the main entrance, or it may for example be an image-capture device such as a video camera. Similarly, an interface enabling bidirectional communication over a Public Land Mobile Network (PLMN), such as GSM or L TE, may optionally be provided. Optionally, a third antenna 484 and associated ISM transceiver 434 may be provided, for example for communication with the monitoring centre 700 over, for example, the European 863MHz to 870MHz frequency band. Optionally, the third transceiver 434 may be a Sigfox transceiver configured to use the Sigfox network to contact the central monitoring station especially in the event that jamming of other radio channels is detected.

[0075] The first 430 and second 432 transceivers may both be tuneable ISM devices, operating for example in the European 863MHz to 870MHz frequency band or in the 915MHz band (which may span 902-928MHz or 915-928MHZ depending upon the country). In particular, both of these devices may be tuned, i.e. may be tuneable, to the frequencies within the regulatorily agreed sub-

bands within this defined frequency band. Alternatively, the first transceiver and the second transceiver, if present, may have different tuning ranges and optionally there is some overlap between these ranges.

[0076] The controller 450 is configured to run a sensing application using a WFS software agent 800, which may be stored in memory 470. The WFS software agent 400 uses WFS radio APIs in the Wi-Fi transceiver 440 to interact with the Wi-Fi radio, the APIs enabling extraction of desired channel environment measurement information and provides the ability to assert any related controls to configure WFS features. This behaviour will be described in more detail shortly. The sensing application on the CU will report a presence state change when the appropriate thresholds are triggered, along with the address of the device whose received data triggered the algorithm. The WFS agent provides a monitoring system which enables the security monitoring system to detect presence and movement in a monitored space, without the necessity to use line of sight motion detectors.

[0077] As an alternative to incorporating the radio sensing application into the central unit, this functionality can be provided on an access point, e.g. a Wi-Fi access point, AP such as router 300, of the premises, with the AP configured to report the result of presence detection to the central unit 122. In another example, a Wi-Fi range extender could instead be used as sensing master for its connected nodes and configured to report to the central unit 122 which would be the overall master in terms of reporting the "alarm".

[0078] A brief explanation will now be given of how Wi-Fi Sensing works, and how Wi-Fi Sensing can be integrated into a security monitoring system, and in particular how WFS can be integrated into a central unit of a security monitoring system.

[0079] Wi-Fi Sensing can be performed with any Wi-Fi device and can be used on any available communication path. Each communication path between two devices gives the chance to extract information about the surrounding environment. Wi-Fi sensing is based on an ability to estimate the wireless channel and hence the surrounding environment. Because Wi-Fi networks comprise many devices spread throughout a geographical area, they are well suited to exploiting these devices' transmissions in effect to provide a radar system. Depending on the number of devices, the radar system may be monostatic, bistatic, or multistatic. In monostatic WFS, a single device measures its own transmitted Wi-Fi signals. In bistatic WFS, the receiver and transmitter are two different devices (for instance, an AP and a STA in infrastructure mode). In multistatic WFS, the received signals from multiple Wi-Fi transmitters are used to learn about a shared environment.

[0080] At least one Wi-Fi transmitter and one Wi-Fi receiver are required to perform WFS measurements, and these can be located in the same device (to create a kind of monostatic radar) or in different devices. The measurement is always performed by a Wi-Fi Sensing-enabled receiver on the Wi-Fi signal transmitted by a transmitter, and which may or may not originate from a Wi-Fi sensing-capable device. The device that transmits the signal that is used for measurements is called the "illuminator," as its transmissions enable collection of information about the channel - that is, it illuminates the channel.

[0081] Different modes of Wi-Fi Sensing measurements are recognised - Passive, Triggered, Invoked, and Pushed, and these depend upon what triggers the illuminator device to transmit a Wi-Fi signal. Preferably the agent improves the usefulness of the standard beacon interval by using optimised timings.

[0082] In passive mode, WFS relies on transmissions that are part of regular Wi-Fi communication. The Wi-Fi Sensing receiver(s) rely only on transmissions between itself and the illuminator device(s). Passive transmissions do not introduce overhead, but the Wi-Fi sensing device lacks control over the rate of transmissions, transmission characteristics (bandwidth, number of antennas, use of beamforming), or environmental measurements.

[0083] Triggered measurement happen when a Wi-Fi Sensing device is triggered to transmit a Wi-Fi packet for the purpose of WFS measurements, either in response to a received Wi-Fi packet or by the higher layers (for instance, in WFS software).

[0084] Invoked measurement involves utilizing a packet transmission that is in response to a packet received from the Wi-Fi Sensing receiver device.

[0085] In pushed mode, a transmission is initiated by the illuminator device for measurement. A pushed transmission can be either a unicast or a multicast/broadcast message. Multicast/broadcast messages can be used for measurements by multiple WFS receivers simultaneously if the devices are not in power-save mode. Triggered transmissions introduce overhead because additional over-the-air transmissions are required. Pushed transmissions introduce less overhead compared to invoked transmissions, because the exchange is unidirectional rather than bidirectional. Triggered transmissions allow for a system to control both the rate and occurrence of measurements.

[0086] A WFS network is made up of one or more WFS illuminators and one or more WFS receivers. A WFS system is made up of three main components and that are present in Wi-Fi Sensing illuminators and receivers:

first is the Wi-Fi radio, which encompasses the radio technology specified in IEEE 802.11 standards, the interfaces and the APIs connecting the radio to the higher layers;

second is the Wi-Fi Sensing software agent, consisting of a signal processing algorithm and interfaces, the agent interacting with the Wi-Fi environment, and turning radio measurement data into motion or context-aware information; and

thirdly, an application layer operates on the Wi-Fi sensing output and forms the services or features which are ultimately presented to an end user - such

as a security monitoring service provided by a security monitoring system that detects presence using WFS.

[0087] A WFS system can be built based on existing Wi-Fi standards, hardware, software and infrastructure.

[0088] The fundamental component required to enable Wi-Fi sensing on the radio is the interface to enable control and extraction of periodic channel or environmental measurement data. Regardless of device type, operating band or Wi-Fi generation, the core APIs to enable Wi-Fi sensing are similar, as the required data and control are common.

[0089] The WFS software Agent can reside on any Wi-Fi device; for example, in the infrastructure mode, the agent may reside on the AP, in which case channel measurements from all the STAs associated with the AP can be collected. The software agent may also be located on a STA. But in the security management system applications this would mean that the STA would either need to be the controller of the security management system (e.g. the CU), or would have to be reporting to the controller of the security management system (e.g. the CU). Generally, we therefore prefer to run the software agent on the CU, and given that the CU is conveniently also an access point, it makes sense for us to run the software agent on the CU acting as AP rather than merely as an STA.

[0090] The WFS software Agent uses the WFS radio APIs to interact with the Wi-Fi radio, the APIs enabling extraction of desired channel environment measurement information and providing the ability to assert any related controls to configure WFS features.

[0091] The WFS Agent has two main subsystems: Configuration and Control; and a Sensing Algorithm. The Configuration and Control subsystem interact with the radio, using a standard set of APIs. The Configuration and Control subsystem performs tasks including sensing capability identification, pushed illumination coordination, and radio measurement configuration. The sensing algorithm subsystem includes intelligence needed to extract the desired features from the radio measurement data and may differ according to the desired sensing application.

[0092] The WFS software Agent is needed on any sensing receiver but is merely optional on an illuminator - only being required if the illuminator also acts as a receiver. If included on an illuminator, only the configuration and control subsystem is needed. By having the agent on the illuminator, additional enhancements are enabled, including sensing capability identification and co-ordinated pushed illumination. If the illuminator is not running an agent, it is still technically able to participate in the sensing network, but only the most basic features that currently exist in Wi-Fi standards will be supported.

[0093] The WFS software Agent processes and analyses the channel measurement information and makes sensing decisions, such as detecting motion. This information is then shared with the application layer via the Wi-Fi Sensing agent I/O interface. As well as interfacing with the radio and the application layer, the Wi-Fi Sensing agent also interfaces with the existing Wi-Fi services on the system. This interface is necessary for the agent to provide feedback for sensing optimizations that can be used in radio resource management decisions, such as band steering or AP selection requests.

[0094] The application layer of a WFS system creates the sensing service and in effect presents the information to the end user (in our case to the security management system).

[0095] The application layer can potentially reside on any networked device: in some embodiments of the present invention, it will reside in the central unit 122 along with the WFS agent, but in other embodiments the application layer may exist in an external server or even in the central monitoring station. We prefer, however, to provide the application layer on the central unit to avoid potential problems with signalling delays (for example due to accidental or deliberate network interruption) between the central unit (or other WFS receiver) and a remotely located entity. The application layer receives input from one or multiple Wi-Fi sensing software agents. It combines the information and delivers it to the security management system which may then in turn provide it to the CMS and/or to a cloud service by means of which push notifications may be sent to a registered user device such as a smartphone - allowing users to receive real-time notifications and the ability to view historic data.

[0096] A typical Wi-Fi home network follows one of two common deployment scenarios. The first consists of a single AP that serves as the internet gateway for all the devices in the house. The second consists of multiple APs forming an ESS and extending coverage throughout the home. Depending on the use case, the Wi-Fi Sensing receiver may be the AP and/or other devices in the network. Not all the devices in a home deployment need to be Wi-Fi Sensing capable.

[0097] Wi-Fi Sensing can be deployed in all types of Wi-Fi networks and topologies, operating in different frequency bands (2.4, 5, 6, and 60 GHz) and different bandwidths. The sensing resolution and performance depends on the use case requirements. In general, it is enhanced with the increase in the number of participating devices and higher bandwidths. Applications that require lower resolutions and longer range, such as home monitoring, can be deployed using Wi-Fi networks operating in 2.4GHz and 5GHz. Applications that require higher resolutions and lower range, such as gesture recognition, require 60GHz Wi-Fi networks.

[0098] In multi-AP and/or multi-band deployments, there may be an advantage to having a Wi-Fi sensing device connected to a specific AP or operating in a specific frequency band. Radio resource management (RRM) events, such as AP and/or band steering, should be conducted in coordination with the Wi-Fi Sensing agent/operation.

[0099] The devices involved with Wi-Fi Sensing will depend upon the deployment environment and the specific use case. The sensing measurements also need to be processed by the device with enough computation power. The coordination of sensing, including participating devices, is a role particularly suited to an AP. Typically the central unit of a security monitoring system will have ample processing power, as well as being able to function as an AP, to handle this task efficiently and speedily.

[0100] The nature of Wi-Fi networks is such that it should be possible able to add additional Wi-Fi sensing capable devices to the network to enhance accuracy, coverage and/or localization. These additional devices do not necessarily need to be Wi-Fi Sensing capable or dedicated Wi-Fi sensing devices to participate; however, optionally they may also identify their Wi-Fi sensing capabilities and supported features to the AP. Internet of Things (IoT) devices for home deployment can typically also be used as part of a WFS installation supporting a WFS-enabled security monitoring system: example include Wi-Fi controllable plugs and sockets, light bulbs, thermostats, smart speakers, and video door bells. However, even when a device connects to the AP and reports that it is Wi-Fi sensing capable, the Wi-Fi Sensing agent may elect not to make use of that device.

[0101] WFS for a security monitoring system may be run over a dedicated Wi-Fi network, the premises having at least one other Wi-Fi network for other purposes. But for reasons of simplicity and economy it may often be preferred to operate a single Wi-Fi network to serve all a household's (or small business's) needs including WFS for a security monitoring service. If a single-network solution is adopted, performance degradation due to airtime usage and sensing overhead must be minimized and hence Wi-Fi transactions required for conducting sensing measurements and sensing management and processing must be optimized for efficiency.

[0102] For each Wi-Fi Sensing application, at least one network device executes the sensing software, or Wi-Fi Sensing Agent. The Wi-Fi Sensing agent is typically placed on the AP, but it can be placed on any STA (although, as previously mentioned, we prefer to run the Wi-Fi Sensing agent on the AP). Following authentication and association of a device with the Wi-Fi network, the Wi-Fi Sensing agent should discover the device and its sensing capabilities. Depending on the capabilities of the device, its role in the Wi-Fi sensing network would be determined. If the new device is another Wi-Fi Sensing-capable AP, then coordination among the agents is required.

[0103] The WFS agent needs to have a mechanism to determine which devices are capable and needs to participate in the sensing for each application on a device-specific basis.

A WFS agent also needs to be capable of configuring the radio for measurements and triggering transmissions on a periodic basis for sensing measurements, and to enable/disable measurements or adjust configuration parameters for Wi-Fi sensing-capable devices. Optionally, the Wi-Fi Sensing agent is also able to request specific radio resource management operations, such as AP or band steering. The WFS agent is also preferably able to detect and process specific sensing events and communicate the relevant information to the application layer (e.g., the security monitoring system) for specific handling and user presentation.

[0104] One of the parameters that impacts the quality of the received signal in a wireless network is the amount of interference present. Interference can be caused by other Wi-Fi devices operating in the same band, which causes cochannel interference, or in an adjacent channel, which causes adjacent channel interference. It can also be caused by non-W-Fi devices, which can be other communication systems or unintentional transmissions that create electromagnetic noise in the band. Interference can impact Wi-Fi Sensing performance in two ways. Firstly, it may interfere with the sensing transmissions and thereby reduce the number of measurements made in a given time interval. As such, it introduces jitter in time instants during which the measurements are made. Secondly channel-state measurements may capture the impact of transient interference, such as for a non-Wi-Fi device, as opposed to motion in the environment.

[0105] Wireless systems deploy various techniques to avoid or reduce the impact of interference, and these techniques also help to improve WFS performance. These techniques aim at maximizing the reuse of spectrum, while minimizing the overlap of spectrum used by nearby networks: for example, Dynamic Channel Allocation (DCA); Auto Channel Selection (ACS); optimized RF planning; (e.g., non-overlapping channels and use of reduced channel width when applicable), and power control.

[0106] As already mentioned, increasing the number of illuminators may result in a higher sensing performance: with more transmitters that are located sufficiently apart from one another, motion in a larger area can be detected; when motion is detected using transmissions on one or more transmitters, information is provided that can be used to determine localization of the motion; and sensing accuracy is improved with a higher number of measurements taken across a larger number of transmitters in most scenarios.

[0107] The IEEE 802.1 1a preamble is useful for Wi-Fi Sensing. The preamble contains a short training field (STF), a guard interval and a long training field (LTF). The STF is used for signal detection, automatic gain control (AGC), coarse frequency adjustment and timing synchronization. The LTF is used for fine frequency adjustment and channel estimation. Since only 52 subcarriers are present, the channel estimation will consist of 52 frequency points. Newer OFDM PHY versions (HT/VHT/HE) maintain the IEEE 802.11a preamble for backward compatibility and refer to it as the legacy preamble. The legacy preamble spans a 20MHz bandwidth and consists of a legacy STF (L-STF) and legacy LTF

(L-LTF). As more recently defined OFDM PHY versions (HT/VHT/HE) introduce wider channel bandwidths (up to 160MHz) for backward compatibility, the legacy preamble is duplicated on each 20MHz channel. This allows the receiver to compute 52, 104, 208 or 416 valid L-LTF frequency points, which represent the channel estimation between the two devices.

[0108] Also potentially useful for Wi-Fi Sensing are the MIMO training fields present in HT, VHT and HE LTFs. The MIMO fields are modulated using the full bandwidth (20MHz to 160MHz) and are traditionally used by the receiver to estimate the mapping between the constellation outputs and the receive chains. Since these fields span the full bandwidth, they provide more frequency points. For example, a 20MHz L-LTF contains 52 subcarriers, while a 20MHz HT/VHT-LTF contains 56 subcarriers. The latest introduction of the HE PHY has the potential to enhance Wi-Fi Sensing. In addition to enabling operation in the 6GHz spectrum, the HE PHY has increased the number of subcarriers per 20MHz bandwidth by 4x, which effectively allows for better object resolution.

[0109] The IEEE 802.1 1ad amendment defines a Directional-Multi-Gigabit (DMG) PHY for operation in the 60GHz band. While there are three different modulation schemes (Control, Single-Carrier and OFDM) defined, Control and the Single Carrier PHY are the primary PHY used in 802.1 1ad (and is also part of the subsequent 802.1 1ay amendment). Regardless of the modulation scheme, every packet starts with a preamble that consists of a short training field (STF) and a channel estimation field (CEF). The STF is used for timing estimation and AGC adjustment. CEF is used for channel estimation. Similar to the OFDM-based PHYs, the necessary channel estimation for Wi-Fi Sensing is available following successful reception and processing of the preamble of a packet and can be provided to the higher layers. The wide channel bandwidth available in 802.11ad/ay can significantly improve the performance of Wi-Fi Sensing in terms of the resolution; however, the limited communication range in 60GHz band restricts the sensing range and coverage. As such, in many situations the central unit of a security monitoring system may relay instead on frequency bands with longer range, sufficient to cover the majority of households. However, for smaller-scale installations the use of the 60GHz band may be attractive and therefore embodiments of the invention may use this band for WFS.

[0110] When it comes to identifying peer devices in a WFS installation, the MAC layer mechanisms may be used to obtain information about the connected devices and the roles they play in Wi-Fi sensing. The MAC layer also initiates and drives transmissions required for channel estimation among the devices in the Wi-Fi Sensing network.

[0111] Various aspects of peer identification arise with Wi-Fi Sensing. The first is identifying the devices and the channel estimation mapped to the physical environment between any two devices. Typically, an STA is identified by a 48-bit MAC address. A MAC address is sufficient identification for STAs associated with a Wi-Fi network; however, if the association is lost during the lifetime of the application, then randomized MAC addresses may be used. In this case, a different or more involved mechanism would be required to identify each STA. This identification must match the corresponding channel estimate measurement obtained from the PHY. The second is identifying the device network role and its connection type, such as whether it is an AP or an STA, or whether it is part of a mesh or a P2P connection. This information is used by the Wi-Fi Sensing agent to decide the best method for conducting measurements.

[0112] The third aspect is the identification of WFS device capabilities, such as sensing capabilities, supported measurement rate, and the availability and willingness of the device to participate in sensing measurements. This information is required from all devices in the network for the Wi-Fi Sensing agent to select devices participating in the sensing measurements.

[0113] As already noted, there are different types of transmissions that can be used for illumination of the Wi-Fi channel and obtaining measurements between two devices. Passive transmissions rely on existing Wi-Fi traffic and do not introduce any new MAC layer requirements. Triggered transmissions, however, rely on additional transmissions. Depending on whether existing packet exchange procedures are used for triggered transmissions or new exchanges are defined, the requirements on the MAC layer will be different. An example of one existing packet exchange that can be used for triggering invoked transmissions is null data packet (NDP) and ACK exchange. NDP transmission by the Wi-Fi Sensing receiver can be used to invoke a Wi-Fi Sensing transmitter to respond with an ACK, which may then be used to compute a channel estimation. The disadvantage of using ACK packets for channel estimation, in 2.4/5GHz bands, is that the ACKs are only transmitted in legacy mode. Another example of how an invoked measurement can be triggered is by use of the implicit unidirectional beamforming procedure, first defined in the IEEE 802.1 In standard. In this procedure, an STA requests beamforming training by sending a MAC frame with the training request (TRQ) bit set to 1. This triggers the receiving device to send an NDP announcement, followed by an NDP to illuminate the channel. The benefit of this invoked measurement is that it is not limited to the legacy preamble for channel measurements and uses the MIMO training fields, as well.

[0114] In pushed measurements, a transmission is triggered by the illuminator to be received by one or multiple Wi-Fi Sensing receivers. Beacon frames are an example of using existing MAC packet exchanges for pushed measurements.

[0115] Also as already noted, to support different use cases, either the AP or STA may take the role of sensing receiver; additionally, there may be multiple sensing re-

ceivers required to support the application. Moreover, there may be multiple illuminators involved in the measurements. MAC layer coordination is used to coordinate the sensing transmissions among the illuminators and the sensing receivers in an efficient way. MAC layer scheduling may also be used to enable periodic measurements on which some use cases rely. Coordination and scheduling at the MAC layer should enable different options for conducting sensing measurements among multiple illuminators and sensing receivers, with minimal added overhead, while accounting for the power save state of the devices.

[0116] To interact with the MAC and PHY, the WFS agent has an interface to pass the WFS control information to the radio and extract the measurement data. The interface should be PHY agnostic and is, therefore, defined in a generic manner and extendable to cover different radio driver implementations, including drivers from different chipset vendors. The interface definition should allow for potential additional features or capabilities provided by a specific PHY or a chipset, as well as a path for growing the technology. Definition of a standard interface/API enables radio firmware and driver developers to ensure compliance and enables reuse of components or common codes, which may be placed into a library. Most Wi-Fi drivers are based on either the wireless-extensions framework or the more recent and actively developed cfg80211 / nl80211 framework. As the system integration components are largely provided, these frameworks enable Wi-Fi driver developers to focus on the hardware aspects of the driver. These frameworks also offer significant potential as a location for defining a WFS API. The WFS interface should provide the WFS agent with STA identification and enable the WFS agent to track the physical device in the network (i.e., the AP to which it is connected), as well as the device's capability and availability to participate in the measurements.

[0117] The WFS agent requires control of the STAs that will participate in the sensing measurements, as well as what measurement type (passive vs triggered) will be performed. The WFS interface should provide such control, either on a global system scale or on a per STA basis so that the WFS agent can conduct WFS measurements in the most efficient manner.

[0118] Based on the specific WFS application or use case, different measurement rates may be required. The measurement rate is typically decided by the WFS agent, and the interface should support its control. However, to provide the lowest jitter and best efficiency possible, it is best to rely on the MAC layer for scheduling. WFS applications may have different measurement parameter requirements (bandwidth, antenna configuration, etc.). The configuration of measurement parameters allows the application to obtain only the data it requires to maintain efficiency. The measurement parameters should be configurable independently for each STA.

[0119] The WFS interface should be flexible enough for the radio to specify whether the data payload is in time-domain or frequency-domain, the numerical format, etc. By having this knowledge, the Wi-Fi Sensing agent can correctly interpret the data.

Claims

1. A security monitoring system installation in a dwelling, the dwelling including a first part providing living accommodation for occupants of the dwelling and, distinct from the first part, a second part providing sleeping accommodation for occupants of the dwelling, the system having a local management device, a plurality of alarm event sensors, and a radio-based location sensing arrangement to detect human presence and location within the first part and the second part of the dwelling based on detecting perturbations of radio signals, wherein the local management device stores information about the occupants' daily routine and is configured, automatically to switch the system into a nocturnal armed at home mode in which detection of movement or presence in the first part constitutes an alarm event but in which detection of movement or presence in the second part does not constitute an alarm event, in the event that information from the location sensing arrangement indicates that the occupants have vacated the living accommodation for the sleeping accommodation, and the time of day and the stored information are such that use of the nocturnal armed mode is appropriate based on rules stored in the local management device.

2. A local management device for a security monitoring system installation in a dwelling, the dwelling including a first part providing living accommodation for occupants of the dwelling and, distinct from the first part, a second part providing sleeping accommodation for occupants of the dwelling, the system including a radio-based location sensing arrangement to detect human presence and location within the first part and the second part of the dwelling based on detecting perturbations of radio signals, the local management device configured to:

   be coupled to a plurality of alarm event sensors;
   store information about the occupants' daily routine;
   and automatically switch the system into a nocturnal armed at home mode in which detection of movement or presence in the first part constitutes an alarm event but in which detection of movement or presence in the second part does not constitute an alarm event, in the event that information from the location sensing arrangement indicates that the occupants have vacated the living accommodation for the sleeping ac-

commodation, and the time of day and the stored information are such that use of the nocturnal armed mode is appropriate based on rules stored in the local management device.

3. An installation as claimed in claim 1 or a local management device as claimed in claim 2, wherein the local management device is further configured to switch the system automatically into a nocturnal armed at home mode, in which perimeter alarm event sensors are, if not already armed, armed to provide a secured perimeter.

4. An installation or local management device as claimed in claim 3, wherein the local management device is further configured, in the nocturnal armed at home mode, not to treat detected presence or movement in the first part as an alarm event if it is determined that someone has moved from the second part into the first part without the perimeter alarm event sensors having detected breaching of the secured perimeter.

5. An installation as claimed in claim 3, further comprising one or more line of sight motion detectors coupled to the local management device and positioned to detect human movement from the second part into the first part.

6. An installation or local management device as claimed in claim 3, wherein the radio-based location sensing arrangement has been trained to identify perturbations of radio signals corresponding to human movement from the second part into the first part.

7. An installation or local management device as claimed in any one of claims 2 to 6, wherein the local management device is further configured, on determining that someone is moving from the second part into the first part or has so moved, to disarm the security monitoring system to a mode in which only a detected breach of the perimeter is treated as an alarm event.

8. An installation or local management device as claimed in any one of the preceding claims, wherein the local management device is further configured to accept user input of information about occupants' daily routine, optionally in the form of usual bedtime(s), optionally for specified days of the week.

9. An installation or local management device as claimed in any one of the preceding claims, wherein the local management device is further configured to use data from the radio-based location sensing arrangement to perform people counting, and optionally to use determine the presence of one or more intruders based on a detected change in the people count when the system is in the nocturnal armed mode.

10. The installation or local management device as claimed in any one of the preceding claims, wherein the local management unit is further configured to acquire information about the occupants' daily routine based on information from the radio-based location sensing arrangement, including the number of occupants detected and their movements, user interactions with the security monitoring system, and taking account of time of day.

11. An installation as claimed in any one of the preceding claims, wherein the plurality of alarm event sensors includes:
one or more motion sensors to detect movement in the first part; and optionally one or more motion sensors to detect movement in a buffer zone intermediate the first part and the second part.

12. The installation or local management device as claimed in any one of the preceding claims, wherein the radio-based sensing arrangement is configured to process communication signals received from one or more radio transmitters operating according to one or more communication standards or protocols, and optionally the one or more radio transmitters that are in a common wireless network with the local management device.

13. The installation or local management device as claimed in any one of the preceding claims, wherein the local management device includes a radio receiver of the radio-based presence and location sensing system, and optionally the local management device includes a processor and a memory holding software instructions that when run on the processor cause the local management device to process radio signals to derive location and presence data.

14. The installation or local management device as claimed in any one of the preceding claims, wherein the sensing arrangement to detect human presence uses changes in channel state information or received signal strength in determining presence.

15. The installation or local management device as claimed in any one of the preceding claims, wherein the local management device is configured to function as an access point of a radio network whose signals are used by the radio-based presence and location sensing system.

16. The installation of claim 15, wherein the radio network for which the local management device func-

tions as an access point includes at least one further access point.

17. The installation of claim 15 or claim 16, wherein the radio network is a Wi-Fi network, and optionally the one or more radio transmitters include one or more of the following: a Wi-Fi access point, a Wi-Fi extender, a smart plug or smart socket, a smart speaker, a smart bulb, a control panel of the security monitoring system, a Wi-Fi-enabled video camera.

18. The installation or local management device of any one of claims 12 to 17, wherein the local management device is further configured to perform processing of signals as part of the radio-based location sensing arrangement.

19. A method of automatically switching a security monitoring system of premises into a nocturnal armed at home mode, the premises providing accommodation for a household, and the accommodation comprising sleeping accommodation and living accommodation, the two accommodations being separate, the method comprising:

using radio-based presence and location sensing to detect perturbations of radio signals;
determining that the perturbations of radio signals signify that the household has vacated the living accommodation and occupied the sleeping accommodation;
using time of day and stored information about the households' daily routine,
applying one or more rules to determine whether use of the nocturnal armed mode is appropriate, and if it is appropriate switching the security monitoring system into the nocturnal armed at home mode, in which detection of movement or presence in the living accommodation constitutes an alarm event but in which detection of movement or presence in the sleeping accommodation does not constitute an alarm event.

20. The method of claim 19, further comprising, as part of switching the system into the nocturnal armed at home mode, configuring the system to provide a secured perimeter, in the event that the system is not already providing a secured perimeter, and optionally further comprising in the nocturnal armed at home mode, if no signal has been received indicating that the secure perimeter has been breached, determining that someone has moved from the sleeping accommodation into the living accommodation, and thereafter ceasing to treat the detection of movement or presence in the living accommodation constitutes as an alarm event.

21. The method as claimed in claim 19 or 20, further comprising using radio-based location sensing presence and location sensing to perform people counting, and optionally determining the presence of one or more intruders based on detecting a change in the people count when the system is in the nocturnal armed mode.

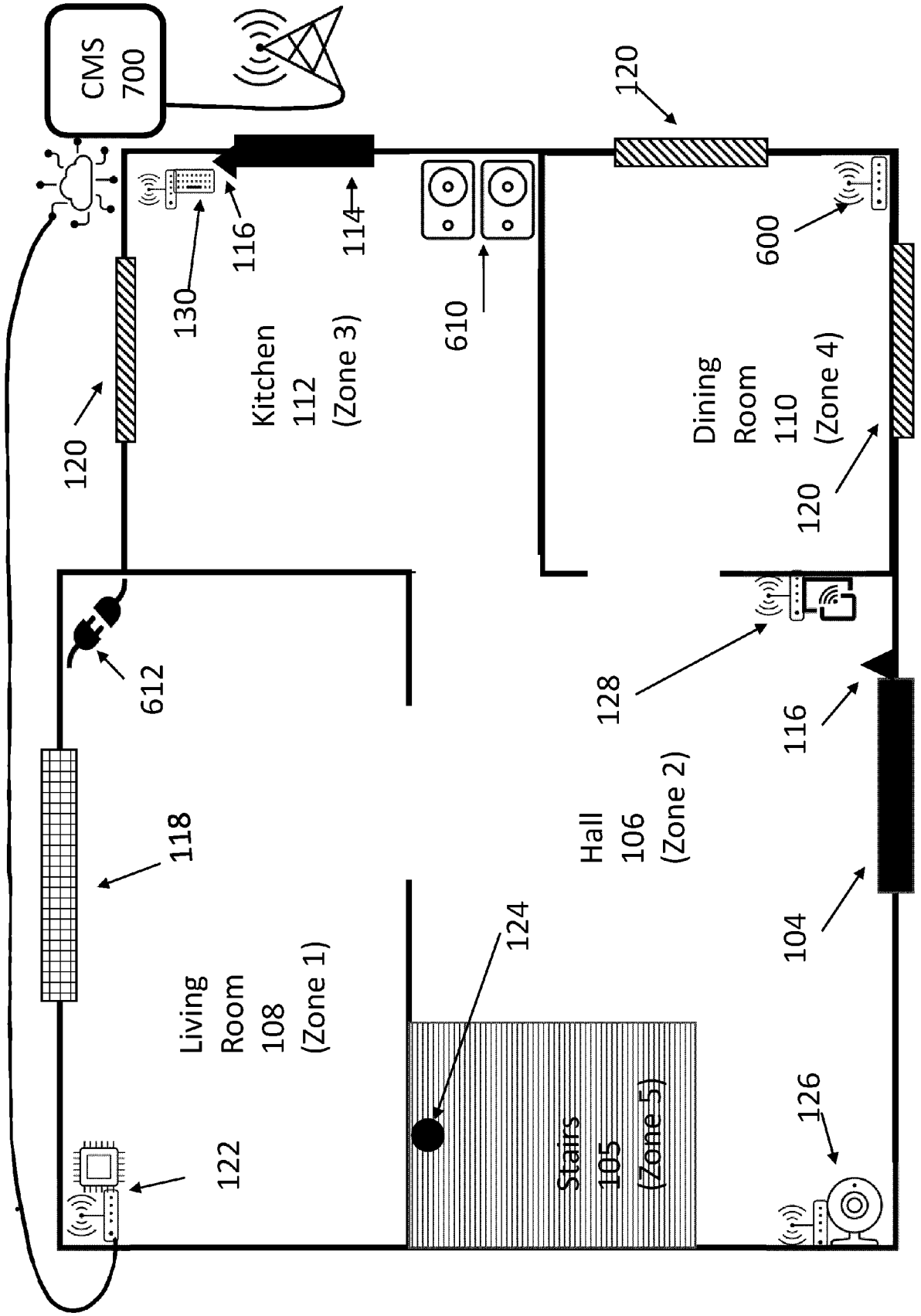
CMS
700
120
130
116
114
Kitchen
112
(Zone 3)
610
600
Dining
Room
110
(Zone 4)
120
120
612
128
116
118
Hall
106
(Zone 2)
Living
Room
108
(Zone 1)
124
104
122
Stairs
105
(Zone 5)
126

Figure 1

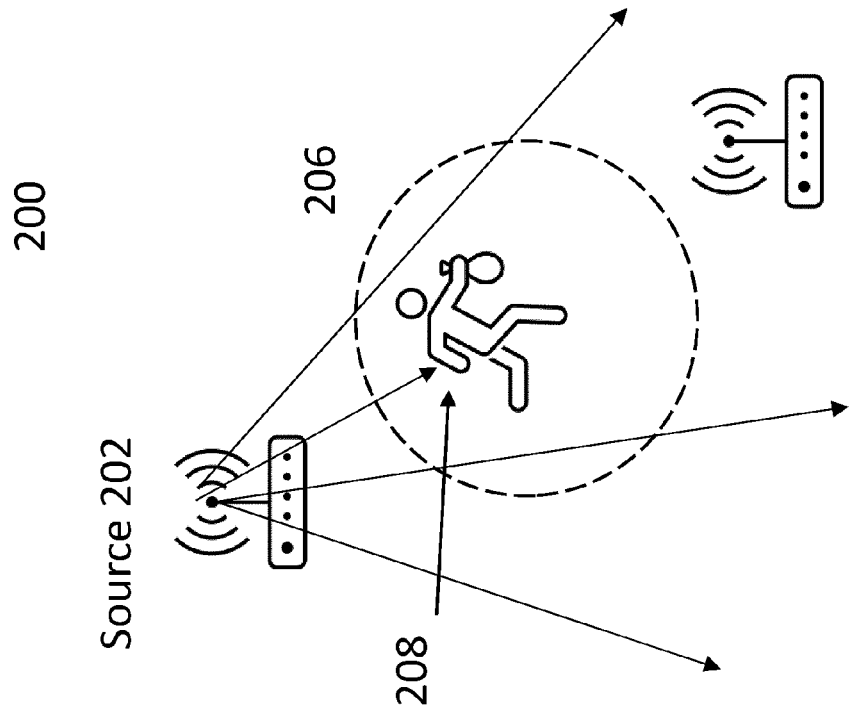

Figure 2B

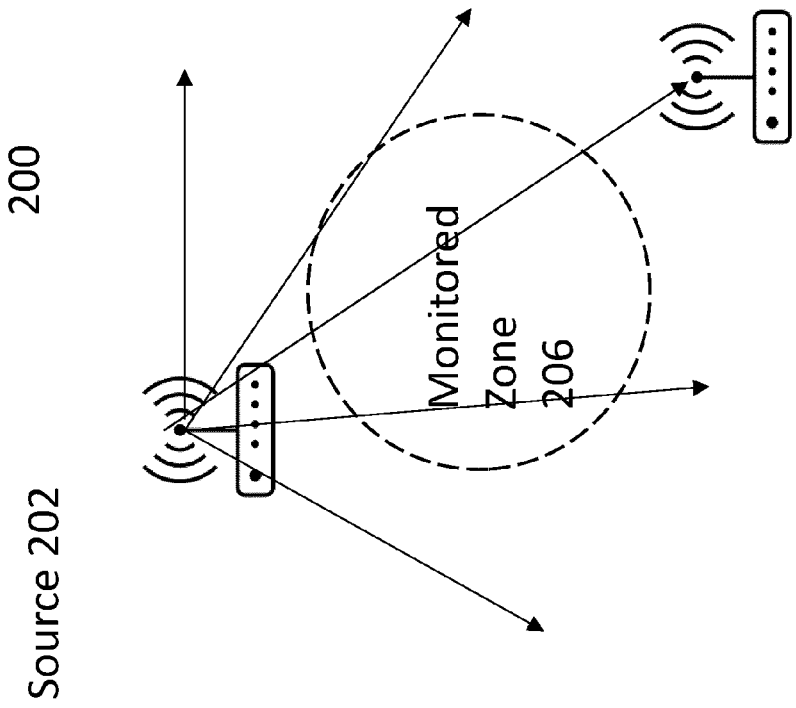

Figure 2A

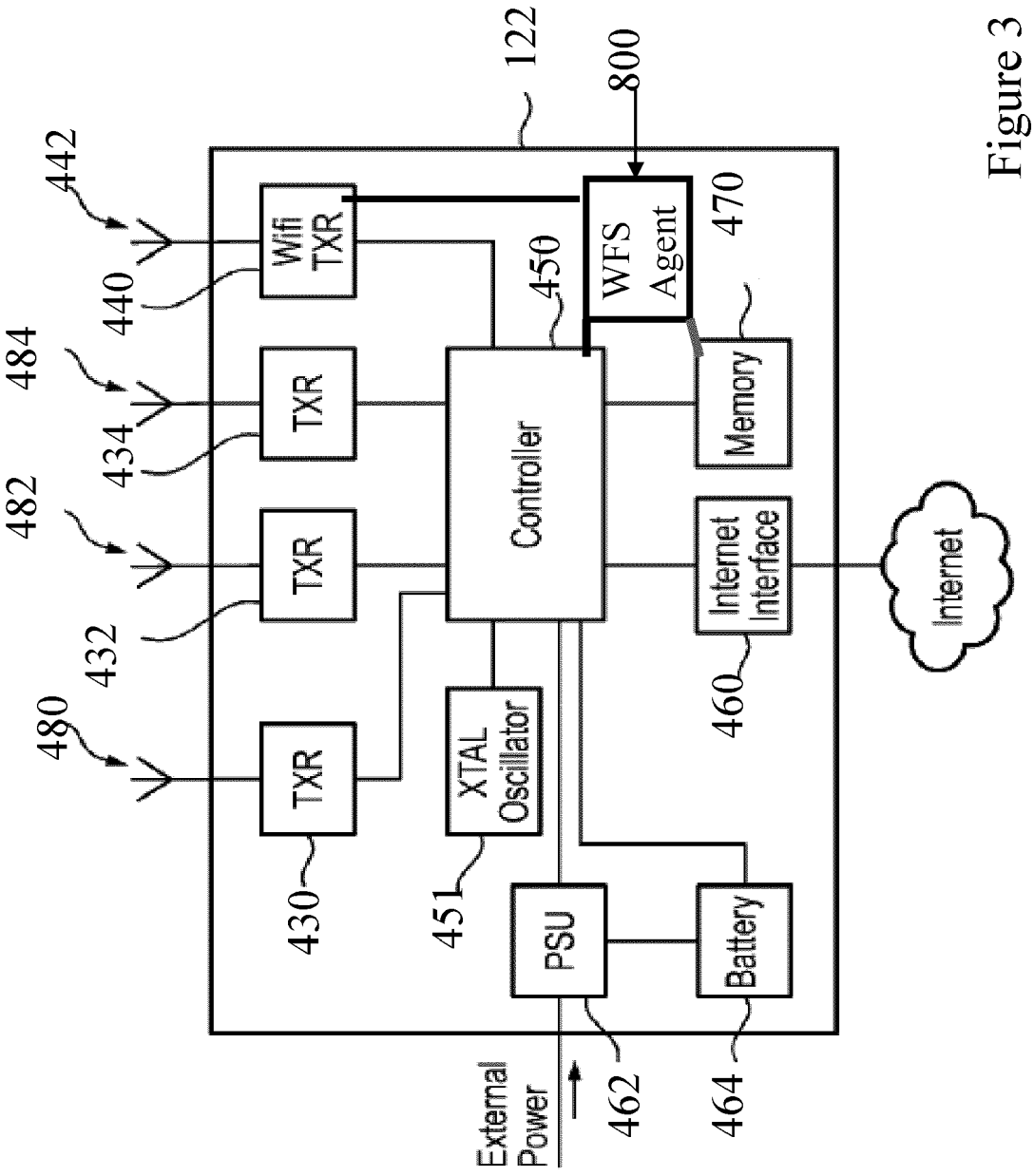
122
800
442
440
484
434
482
432
480
430
Wifi TXR
TXR
TXR
TXR
450
WFS Agent
470
Memory
Controller
Internet Interface
460
Internet
XTAL Oscillator
451
PSU
Battery
External Power
462
464

Figure 3

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 21 21 8141

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 A	US 2007/247302 A1 (MARTIN CHRISTOPHER D [US]) 25 October 2007 (2007-10-25) * figure 1 * * paragraph [0002] * * paragraph [0004] * * paragraph [0005] * * paragraph [0006] * * paragraph [0007] * * paragraph [0020] * * paragraph [0028] * * paragraph [0029] * * paragraph [0039] *	1-8,11, 19,20 9,12-18, 21 10	INV. G08B25/00
Y,D	US 2020/302187 A1 (WANG FENGYU [US] ET AL) 24 September 2020 (2020-09-24) * paragraph [0031] * * paragraph [0067] * * paragraphs [0069] - [0071] *	9,12-18, 21	
A	EP 2 698 773 A1 (SECURITAS DIRECT AB [SE]) 19 February 2014 (2014-02-19) * figure 1 * * paragraph [0006] * * paragraph [0023] *	1-21	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	30 May 2022	Plathner, B

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 21 8141

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.

30-05-2022

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007247302 A1	25-10-2007	NONE	
US 2020302187 A1	24-09-2020	NONE	
EP 2698773 A1	19-02-2014	NONE	

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

REFERENCES CITED IN THE DESCRIPTION

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

Patent documents cited in the description

- US 20200302187 A1 **[0063]**