

(19)



(11)

EP 4 207 117 B1

(12)

EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention
of the grant of the patent:

28.05.2025 Bulletin 2025/22

(51) International Patent Classification (IPC):

G08B 13/04 (2006.01) **G08B 25/14** (2006.01)

G08B 25/00 (2006.01) **G08B 13/16** (2006.01)

G08B 13/24 (2006.01)

(21) Application number: **21218148.1**

(52) Cooperative Patent Classification (CPC):

G08B 25/002; G08B 17/10; G08B 13/1654;

G08B 13/1672; G08B 13/2491

(54) **SENSOR NODE FOR SECURITY MONITORING SYSTEMS**

SENSORKNOTEN FÜR SICHERHEITSÜBERWACHUNGSSYSTEME

NOEUD DE CAPTEUR POUR SYSTÈMES DE SURVEILLANCE DE SÉCURITÉ

(84) Designated Contracting States:

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

(43) Date of publication of application:

05.07.2023 Bulletin 2023/27

(73) Proprietor: **Verisure Sàrl**

1290 Versoix (CH)

(72) Inventors:

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

(74) Representative: **Dennemeyer & Associates S.A.**

**Postfach 70 04 25
81304 München (DE)**

(56) References cited:

EP-A1- 3 065 117 EP-A2- 1 437 701
CN-A- 104 700 580 US-A1- 2016 189 533

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

Description

Field

[0001] The present invention relates generally to sensor nodes for security monitoring systems, and in particular to alarm event sensors that have more than two output states, premises security monitoring systems and installations including such sensors, 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] Sensor nodes or alarm event sensors (sometimes just referred to as "sensors") for security monitoring systems essentially fall into two classes. In a first class are those sensors that have just two output states - e.g. magnetic and other contact switches are either electrically open or electrically closed, indicating either a continuance of a condition or state, or a change in that condition or state. The sensors in this class may be considered to be "binary" in nature - in effect providing a signal that is a zero or a one (or a signal or no signal): just two output states are possible. In the second class are sensors such as microphones, motion detectors (e.g. PIR sensors), and sensors based on magnetometers or accelerometers (e.g. shock sensors for doors or windows), and cameras that provide, or can provide more nuanced outputs and in particular more than two output states and more than two output levels. Their outputs may be analogue or digital, but they provide outputs of many levels.

[0005] Some sensor nodes in this second class have internal processing capability that is used to process the output of a sensing sub-system, so that the output of the sensor node may be a processed representation of the output of the sensing sub-system rather than the "raw" output data - although the processing may just involve thresholding.

[0006] Some sensor nodes in this second class, for example shock sensors have internal processing capability that is used to process the output of a sensing sub-system (e.g. magnetometers or accelerometers) and to discriminate between low level output signals, indicative of a gentle impact, and high level output signals, indicative of a significant impact - in effect thresholding the input signals and reporting, for example to a local management device of a security monitoring system, only those events which produce an above-threshold response from the sensing sub-system. The idea behind the use of thresholding is to avoid burdening the local management unit with incident reports that could safely be ignored - for example which result from the impact of a football accidentally stroking a window or door during a children's game of football, while reporting all incidents that are likely to be the result of a deliberate attack - either of vandalism or an attempt at breaking in to the premises secured by the security monitoring system. The problem is, at what level to set the threshold. Some such sensor nodes have provision for the threshold to be adjusted, so that the sensor node can be "tuned" for its particular application and situation: adjustment may be possible via the security monitoring system or via a suitably programmed freestanding terminal (such as a smartphone

or laptop). This kind of adjustment typically involves one or more site visits by an engineer, which can be inconvenient or expensive to arrange, particularly if multiple visits are needed. As an alternative, the local management device of the security monitoring system may be reconfigured to ignore all notifications received from any "troublesome" nodes - creating a potential gap in an otherwise secure perimeter: indeed some villains will deliberately target a particular window or door that the think or know to be equipped with a shock sensor - striking the door or window, not hard enough to break anything, but hopefully hard enough to trigger an incident report on repeated occasions in the hope that eventually either the shock sensor will be cut out of the system (i.e. ignored) or that its threshold will be raised significantly, so that at some later date the would-be intruder can effect a break-in without triggering the sensor. There therefore exists a need to address this problem.

[0007] The present invention seeks to provide at least a partial solution to the problem of sensor threshold setting, and to the problem of deliberate interference intended to have the sensor node taken out of service and hence ignored by the local management device.

[0008] CN104,700,580A concerns a portable device for monitoring carbon monoxide levels in a vehicle, and providing warnings in the event that the detected concentration of carbon monoxide is too high. Because the danger posed by carbon monoxide increases with increasing concentration, the device determines carbon monoxide levels with respect to various threshold levels. At concentrations up to 50ppm the alarm device is inactive. If the level rises to between 50ppm and 100ppm, the device sounds a buzzer intermittently and an alarm light flashes "call the police". If the level is between 100ppm and 300ppm the buzzer sounds long and the alarm light stays on. If the level exceeds 300ppm the device also activates the car's horn, activates a camera to capture the scene and sends three instructions to a GSM module. The first instruction controls the GSM module to send a text message including information such as the concentration of harmful gases, the temperature of the scene, and the location of the incident to a mobile phone whose number is stored. The second command controls the GSM module to automatically make a call to the mobile phone with the predetermined number, and if the call is picked up the scene sound can be monitored. The third command controls the GSM module to send the scene image in the form of MMS to the mobile phone whose number is stored so that the contact can clearly see the scene and take corresponding action in a timely manner.

[0009] EP1,437,701 provides a detection system for detecting at least one hazardous condition in an enclosure including a ventilation system, where the ventilation system is capable of operating in either an on or off mode. The system includes at least one detector capable of detecting at least one level (such as concentration of carbon monoxide, or aerosol/particulate concentration)

representative of the severity of the hazardous conditions within the enclosure, where each level (e.g. carbon monoxide or smoke concentration) is associated with a pre-alarm threshold and an alarm threshold that is higher than the pre-alarm threshold. The detection system also includes a controller capable of operating the ventilation system in the off or on mode when at least one level detected by the detectors is above or below the respective pre-alarm threshold, respectively. The controller is also capable of reporting the hazardous condition when the at least one level is above or below the respective alarm threshold, respectively. The idea is to shut off the ventilation system when a pre-alarm threshold is met - thereby preventing the ventilation system from suppressing the detected level of the hazardous component so that the concentration(s) will rise more rapidly and hence trigger an alarm condition more quickly.

[0010] US2016/189,533A provides a system including a plurality of inter-connected premises management devices, each including one or more sensors that generate data about an environment, and a control device to control one or more operations of the premises management system, the control device including a movement detector. The premises management system detects an attempt by an intruder to damage the control device based on data from the movement detector indicating an abnormal movement applied to the control device, historical data obtained from the sensors, and current data obtained from the sensors. The sensor(s) may be an environmental sensor, such as a temperature sensor, smoke sensor, carbon monoxide sensor, motion sensor, accelerometer, proximity sensor, passive infrared (PIR) sensor, magnetic field sensor, radio frequency (RF) sensor, light sensor, humidity sensor, pressure sensor, microphone, compass or any other suitable environmental sensor, that obtains or provides a corresponding type of information about the environment in which the premises management device is located. The system may use a score model and define threshold scores of response. Different responses may be appropriate for different ranges of scores. For example, if the score falls below a first threshold value, the system will ignore the event. If the score is between the first threshold value and a second threshold value, the system will further investigate the event. If the score is above the second threshold value, the system will immediately initiate an alarm sequence and notify the monitoring service and/or law enforcement agency.

[0011] EP 3,065,117A1 provides a hazardous condition detection system for an enclosure includes at least three detectors and a controller. Each detector is mounted within the enclosure. Each detector is configured to output a signal representing a first lower level of severity (a pre-alarm threshold) and a signal representing a second higher level of severity (an alarm threshold). The controller monitors the operational status of each of the detectors. In a first mode when all the detectors are operational, the controller generates an alarm signal

when at least two detectors output a signal at the alarm threshold level. In a second mode when at least one of the at least three detectors are inoperative and at least two of the at least three detectors are operational, the controller generates an alarm signal when one detector outputs a signal at the alarm threshold level and another detector outputs a signal at the pre-alarm threshold level.

Summary

[0012] According to a first aspect of the invention, there is provided an alarm event sensor according to the wording of claim 1. Such an alarm event sensor can help to reduce the incidence of false alarms while also improving the detection of real alarm incidents, with appropriate choice of the two thresholds, because the local management device effectively makes a collaborative decision about reporting incidents to the remote monitoring centre based on data from multiple sensors and preferably multiple sensor types. In effect, events that produce outputs above the second threshold are considered genuine, while those with outputs below or not exceeding the first threshold are ignored. Those events with outputs between the two thresholds are considered "potential" events to be checked by the local management device (central unit) using data from other sensors.

Sensor sub-system outputs having a magnitude not exceeding the first threshold may be stored and periodically reported to the local management device, optionally on demand. These data may be useful in determining an appropriate first threshold level, and also in revealing patterns of behaviour or environmental changes that may have significance.

[0013] The sensing sub-system may include a magnetometer or an accelerometer, and optionally the alarm event sensor may be configured as a shock sensor - for example for mounting on or in a door or window, or in or on the frame of a window or door, or as a sensor to provide positional information on the status of a window or door

[0014] Alternatively, the sensing sub-system may include an optical sensor or a passive infrared sensor.

[0015] According to a second aspect there is provided a premises security monitoring system having a local management device, and operatively coupled to the local management device an alarm event sensor according to the first aspect and a plurality of other alarm event sensors, the local management device being configured: on receiving an alert of the first type from the alarm event sensor according to the first aspect, to report the alert as an alarm event to a remote monitoring station; on receiving an alert of the second type from the alarm event sensor according to the first aspect, to determine, based on information from the plurality of other alarm event sensors, whether the alert of the second type should be treated as an alert of the first type, and only if it should be so treated to report the alert of the second type as an alarm event to the remote monitoring station.

[0016] In premises security monitoring system accord-

ing to the second aspect, the local management device may be configured to determine that the alert of the second type should be treated as an alert of the first type if the information from the plurality of other alarm event sensors indicates that a break in has occurred at the premises.

[0017] In premises security monitoring system according to the second aspect, the local management device may be configured to determine that the alert of the second type should not be treated as an alert of the first type if the information from the plurality of other alarm event sensors indicates that the premises has not been the subject of a break in.

[0018] According to a third aspect there is provided a premises security monitoring system having a local management device, and operatively coupled to the local management device an alarm event sensor according to the first aspect and a radio-based location sensing arrangement to detect human presence and location within the premises that is configured to sense presence and location based on detecting perturbations of radio signals;

the local management device being configured: on receiving an alert of the first type from the alarm event sensor according to the first aspect, to report the alert as an alarm event to a remote monitoring station; on receiving an alert of the second type from the alarm event sensor according to the first aspect, to determine, based on information from the radio-based location sensing arrangement and or from one or more other alarm event sensors of the system, whether the alert of the second type should be treated as an alert of the first type, and only if it should be so treated to report the alert of the second type as an alarm event to the remote monitoring station.

[0019] According to a fourth aspect there is provided a local management device for a premises security monitoring system, the local management device being configured to be coupled to an alarm event sensor according to the first aspect and a plurality of other alarm event sensors, the local management device being configured: on receiving an alert of the first type from the alarm event sensor according to the first aspect, to report the alert as an alarm event to a remote monitoring station; on receiving an alert of the second type from the alarm event sensor according to the first aspect, to determine, based on information from the plurality of other alarm event sensors, whether the alert of the second type should be treated as an alert of the first type, and only if it should be so treated to report the alert of the second type as an alarm event to the remote monitoring station.

[0020] According to a fifth aspect there is provided a local management device for a premises security monitoring system, the local management device configured to be coupled to an alarm event sensor according to the first aspect and a radio-based location sensing arrangement to detect human presence and location within the premises that is configured to sense presence and location based on detecting perturbations of radio signals; the

local management device being configured: on receiving an alert of the first type from the alarm event sensor according to the first aspect, to report the alert as an alarm event to a remote monitoring station; on receiving an alert of the second type from the alarm event sensor according to the first aspect, to determine, based on information from the radio-based location sensing arrangement and or from one or more other alarm event sensors of the system, whether the alert of the second type should be treated as an alert of the first type, and only if it should be so treated to report the alert of the second type as an alarm event to the remote monitoring station. Optionally, the local management device is configured to run the radio-based location sensing arrangement.

[0021] In a sixth aspect of the invention there is provided a method according to claim 11.

[0022] In a seventh aspect of the invention there is provided a method according to claim 12.

Brief description of the drawings

[0023] Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 illustrates schematically the construction and operation of a non-binary sensing node;
 Figure 2 illustrates schematically the behaviour of a non-binary sensing node that applies a single threshold;
 Figure 3 corresponds generally to Figure 2, but illustrates schematically the behaviour of a non-binary sensing node that applies two thresholds;
 Figure 4 is a schematic plan of a single floor of premises in which a first security monitoring system has been installed, the system optionally including a radio-based presence and location sensing system;
 Figure 5 illustrates schematically the principles of radio-based presence and location sensing; and
 Figure 6 illustrates schematically features of a local management device of the system of Figure 4.

Specific description

[0024] Figure 1 shows schematically the behaviour of a non-binary sensor node, in this case a shock sensor 100. In figure 1A the main components of the non-binary sensing node are shown schematically. These include a sensing sub-system 102, which in the case of a shock sensor may be based on an accelerometer, typically a multi-axis accelerometer, or a magnetometer. The output 104 of the sensing sub-system is fed to a processing subsystem 106 which is in turn coupled to a memory 108 and a transceiver 110 by means of which the sensing node can receive control signals from a local management device (also called a central unit) of a security monitoring system, as well as transmit event notifications and data to the local management device. The sensing

node 100 also preferably includes an internal power supply 112. When the sensing node is powered, a mechanical input 114 in the form of an impact stimulates the sensing subsystem 102, generating output 104, which is processed by the processing subsystem 106 which may apply one or more algorithms to determine whether to ignore the output - in effect sending it to discard bin 116, or to produce an incident report which is transmitted, using transceiver 110, to the local management device of the security monitoring system.

[0025] Figure 1B shows schematically what happens when the sensor node receives a small impact, such as might occur in the event that a window or door to which the sensor node is

attached is struck by a football from an informal game taking place in the garden of the house. The blow from the football 118 causes the sensing subsystem 102 to generate output 124 which, when processed by the processing subsystem is seen to be of small amplitude and is hence discarded with no alert being provided to the transceiver or sent to the central unit of the security monitoring system.

[0026] Conversely, figure 1C represents the window or door to which the sensor node is attached being struck violently with a sledgehammer, for example by a villain trying to break into the premises. The sensing subsystem 102 again produces an output 134 which, when processed by the processing subsystem 106 is found to be of large amplitude and consequently an event report is prepared and supplied to the transceiver 110 and hence to the central unit, potentially leading to the central unit reporting an alarm event to a remote monitoring station.

[0027] The difference in the behaviour of the shock sensor between figure 1B and figure 1C can be understood by reference to figure 2. Here we see that the low magnitude impact caused by the football 118 gave rise, when processed by the processing subsystem 106, to a low-level output 124. Conversely the blow struck by the sledgehammer 128 gave rise to a large magnitude output 134, and the processing subsystem applied a threshold 140 - illustrated in the plot of sensing subsystem output magnitude against time, to discriminate between the two signals. As mentioned previously, deciding what threshold level to set is not easy, as it is a balance between two conflicting requirements: make it low enough not to miss any serious intrusion attempts, while keeping it high enough to avoid too many false alarms. This dilemma about choosing the optimum threshold value is not restricted to shock sensors, nor to the use of accelerometers or magnetometers, but rather applies generally to many non-binary sensor nodes.

[0028] Figure 3 illustrates schematically an approach to dealing with this problem according to embodiments of the invention. The figure corresponds generally to figure 2 but now we see that in the plot of sensing subsystem output magnitude against time two new thresholds, T1 and T2, in addition to the original threshold T0. The

processing subsystem 106 now applies two thresholds, rather than one, to the output of the sensing subsystem. A first (low) threshold T1 is set at a magnitude beneath which sensing subsystem outputs can reliably be ignored without risk of missing an intrusion attempt. Conversely, a second (high) threshold T2 is set at a magnitude above which sensing subsystem outputs can reliably be recognised as intrusion attempts without significant risk of reporting accidental impacts. It will be seen that the low threshold T1 is significantly lower than the previous threshold T0, while the second threshold T2 is significantly higher than the previous threshold T0. (Although shown in figure 3, the original threshold T0 is not applied by the processing subsystem 106, merely be included here for reference.)

[0029] The processing subsystem 106 is configured to ignore output signals from the sensing subsystem which do not exceed the first threshold T1, and to report to the central unit events in which the output signals from the sensing subsystem exceed the second threshold T2. However, in addition the processing subsystem 106 also reports to the central unit events in which the output signals from the sensing subsystem is between the first and second threshold, but in this case the reports include a flag or marker to indicate that they are "qualified" reports which in effect need to be confirmed or denied based on other data. The central unit of the security monitoring system can then use these "qualified" reports to confirm an indication of a potential intruder or a potential event which is apparent from data received from other sensors or other sources - in effect the data from other sensors or other sources confirming the qualified report, which may then form the basis of an incident report to the external monitoring station. Or, data from other sensors or other sources either disproves or doesn't support the suggestion that there is a reportable incident, in which case the central unit of the security monitoring system will not report an incident to the remote monitoring station. For example, if the non-binary sensor is a window or door shock sensor node, the central unit of the security monitoring system could confirm a "qualified" report from the node based on receiving indications of movement inside the protected premises at a location in the vicinity of the shock sensor node (e.g. in the same room or space, or leading away from the same room or space) when previously there was no motion inside the premises.

[0030] One particularly favoured source of data to confirm or deny such "qualified" reports from a non-binary sensor node is a radio-based location sensing based on detecting perturbations of radio signals.

[0031] We will now describe, with reference to Figure 4, an example of a security monitoring installation that could (and preferably does) use a radio-based location sensing arrangement to detect human presence and location in the premises based on detecting perturbations of radio signals and in which a local management device may use the radio-based location sensing arrangement to validate "qualified" reports from non-binary sensor nodes such as

shock sensor nodes coupled to doors or windows.

[0032] Figure 4 shows schematically a security monitoring system installation in a dwelling, having a perimeter. In this example, the dwelling is a multi-storey house. A front door 404 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 405. The living space includes an entrance hall 406, onto which the front door 404 opens, off which are a rear living room 408, a front dining room 410, and a rear kitchen 412.

[0033] The kitchen 412 includes the back door 414 of the premises. The front 404 and back 414 doors are each provided with a sensor arrangement 416, a proximity sensor that is triggered by the opening of the relevant door - for example, a sensor arrangement 416 including a magnetically triggered sensor such as a reed relay or a magnetometer.

[0034] The living room 408 is provided with glazed doors 418, 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 418 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. In this case they are provided with a shock sensor 419 that uses a magnetometer to sense the magnetic field from one or more magnets. Similarly, windows 220 to the kitchen 212 and dining room 210 may also not be provided with any sensing arrangement to detect their opening, again as a means of reducing the cost of installing the security monitoring system. In the example shown, however, each of the doors and windows includes a shock sensor node 419 that uses an accelerometer or a magnetometer in a sensing sub-system

[0035] The security monitoring system includes a controller or central unit (which may also be referred to as a local management device) 422 which is operatively coupled to the door opening sensors 416, the shock sensors 419, 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 422 is operatively connected, for example via a wired and/or wireless Internet connection, to a remote monitoring station 490 to which alarm events are communicated for review and for appropriate intervention or other action to be taken. The remote monitoring station 490 (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).

[0036] The security monitoring system also includes one or more motion sensors, typically line-of-sight motion sensors such as PIR sensors. Preferably, at least if the system is to be used without radio-based sensing, a motion sensor is provided in each of the rooms and common areas, so that patterns of movement between the different rooms can be revealed - as this may facilitate determination of whether "qualified" reports received by the central unit 422 from shock sensor nodes 419 should be reported to the remote monitoring station or not. In the illustrated example, a motion sensor 424 is shown as being installed at the head of the stairs 405 that lead to the upper floor(s), as well as in the hall and each of the rooms. Similarly, although not shown, the installation may also include a motion sensor 424 for some or all of the rooms (with the possible exception of bathrooms and toilets) and landings on the upper floors. 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 422 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 490.

[0037] The upper floor(s) of the premises may also be provided with a further motion-triggered video camera, typically at the head of the stairs. Depending upon the proximity of climbable features externally, such as rain-water 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).

[0038] The security monitoring system also includes a user interface or control panel 428 in the hall 406 fairly close to the front door 404. This control panel 428 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 228 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 428 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

430, 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 430 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 230 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 416, 419, and 424, the control panel 428 and disarm node 430 are preferably provided with at least one radio transceiver for communication with the control unit 422, 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 422, 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.

[0039] 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 416 on the front 404 and back 414 doors, but typically also including one or more sensors to detect the opening of windows 420) and internal movement or presence sensors, 424 typically result in the central unit 422 determining an alarm event which may then be reported to the central monitoring station 490. 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 416 (or window sensors if present) count as potential alarm events to be reported by the central unit 222 to the remote monitoring station 490 - 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 422 will routinely be arranged not to request any internal (video) camera to share images with the central unit 422 - so that user privacy is maintained.

[0040] 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 residents 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 490 (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.

[0041] The installation shown in Figure 4 may also be provided with 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), and that is configured to sense presence and location based on detecting perturbations of radio signals. Figure 4 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.

[0042] The radio-based presence sensing, which here is conveniently 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 422 which operates as a Wi-Fi Access Point (AP) and which serves as a Wi-Fi sensing receiver. Figure 4 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.

[0043] 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 422 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.

[0044] 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 426, and a

battery powered control unit may be replaced by a mains powered equivalent 428 that is Wi-Fi capable (although the control unit 428 will typically still use something other than a Wi-Fi transceiver (e.g. a low power ISM transceiver) to communicate with the central unit 422).

[0045] 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 422 will be an AP of that network.

[0046] The central unit AP 422 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 422 - such as broadband router 600, to provide an Extended Service Set (ESS).

[0047] For ease of explanation, we will assume initially that the central unit AP 422 provides just a BSS and not an ESS, and that only the central unit AP 422 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 428 and a Wi-Fi-enabled camera 426 in the hall, and optionally the disarm node 430 in the kitchen. Preferably, because of the power consumption concerns, both the Wi-Fi enabled camera and the disarm node 430 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 430 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.

[0048] With the arrangement shown in Figure 4 the control unit 422 (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.

[0049] Although Figure 4 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.

[0050] 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 non-telecommunications or Industrial, Scientific and Medical (ISM) spectral regions without departing from the scope of the invention, as defined in the appended claims.

[0051] 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 (pre-installed 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.

[0052] The idea is illustrated very schematically in Figure 5, here with an installation 500 including just a single source (or illuminator) 502 and just a single receiver 504, for simplicity, although in practice there will typically be multiple sources (illuminators) and sometimes plural receivers. The installation 500 has been established to monitor a monitored zone 506. In Figure 5A we see that in steady state, and in the absence of a person, radio signals are transmitted from the source 502, spread through the monitored zone 506, and are received by the receiver 504. 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 504. 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 508, as shown in Figure 5B. From Figure 5B 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 504. 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 502 to the receiver 504 is likely to change as the intruder 508 enters, passes through, and leaves the monitored area 506, 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".

[0053] 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.

[0054] 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.

[0055] 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.

[0056] Although the Figure 5 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.

[0057] Now, considering once again the installation of Figure 4, 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, the location(s) of any humans present, and the actions/activities of any people present. This capability means that the central unit of such a security monitoring system should in effect have more sensor data to work with (the combination of WFS data and alarm event sensor data) than would typically be available from a system just using line-of-sight based motion/presence detection and may be capable of discriminating more reliably between "qualified" reports from non-binary nodes that should be treated as threats and hence reported to the remote monitoring station and those that can safely be ignored.

[0058] In an aspect there is provided an alarm event sensor for a security monitoring system, the alarm event sensor configured to generate alerts for the security monitoring system, the alarm event sensor comprising: a sensing sub-system; a transceiver for communicating with a controller of the security monitoring system; and a processing arrangement operatively coupled to the sensing sub-system and the transceiver, the sensing sub-system being configured to provide an output having a magnitude that can have more than two values and that varies in response to changes in a sensed input, the processing arrangement configured to: process outputs

of the sensing subsystem in accordance with a first threshold and a second threshold higher than the first; generate alerts of a first type in respect of outputs having a magnitude greater than the second threshold; not to generate alerts in respect of outputs having a magnitude not exceeding the first threshold; generate alerts of a second type in respect of outputs having a magnitude between the first and second thresholds; and to cause the transceiver to transmit the alerts of the first and second types to the controller of the security monitoring system.

[0059] Such an alarm event sensor can help to reduce the incidence of false alarms while also improving the detection of real alarm incidents, with appropriate choice of the two thresholds, because the local management device effectively makes a collaborative decision about reporting incidents to the remote monitoring centre based on data from multiple sensors and preferably multiple sensor types.

[0060] Sensor sub-system outputs having a magnitude not exceeding the first threshold may be stored and periodically reported to the local management device, optionally on demand. These data may be useful in determining an appropriate first threshold level, and also in revealing patterns of behaviour or environmental changes that may have significance.

[0061] Optionally, the sensing sub-system includes a magnetometer or an accelerometer. It can be difficult to define an appropriate threshold with such sensors. This problem is rendered more tractable by the use of two thresholds that can be chosen independently of each other, and with the local management device making decisions about reporting to the remote monitoring centre based in effect on information from multiple sensors - and preferable of more than one type. Such an alarm event sensor may be configured as a shock sensor, for example for use on or in windows or doors, or their frames.

[0062] Alternatively, the sensing sub-system may include an optical sensor or a passive infra-red sensor.

[0063] In a second aspect there is provided a premises security monitoring system having a local management device, and operatively coupled to the local management device an alarm event sensor according to the first aspect and a plurality of other alarm event sensors, the local management device being configured: on receiving an alert of the first type from the alarm event sensor according to the first aspect, to report the alert as an alarm event to a remote monitoring station; on receiving an alert of the second type from the alarm event sensor according to the first aspect, to determine, based on information from the plurality of other alarm event sensors, whether the alert of the second type should be treated as an alert of the first type, and only if it should be so treated to report the alert of the second type as an alarm event to the remote monitoring station.

[0064] In premises security monitoring system according to the second aspect the local management device may be configured to determine that the alert of the second type should be treated as an alert of the first type

if the information from the plurality of other alarm event sensors indicates that a break in has occurred at the premises.

[0065] In premises security monitoring system according to the second aspect the local management device may be configured to determine that the alert of the second type should not be treated as an alert of the first type if the information from the plurality of other alarm event sensors indicates that the premises has not been the subject of a break in.

[0066] In a third aspect there is provided a premises security monitoring system having a local management device, and operatively coupled to the local management device an alarm event sensor according to the first aspect and a radio-based location sensing arrangement to detect human presence and location within the premises that is configured to sense presence and location based on detecting perturbations of radio signals; the local management device being configured: on receiving an alert of the first type from the alarm event sensor according to the first aspect, to report the alert as an alarm event to a remote monitoring station; on receiving an alert of the second type from the alarm event sensor according to the first aspect, to determine, based on information from the radio-based location sensing arrangement and or from one or more other alarm event sensors of the system, whether the alert of the second type should be treated as an alert of the first type, and only if it should be so treated to report the alert of the second type as an alarm event to the remote monitoring station.

[0067] In a fourth aspect there is provided a local management device for a premises security monitoring system, the local management device configured to be coupled to an alarm event sensor according to the first aspect and a plurality of other alarm event sensors, the local management device being configured: on receiving an alert of the first type from the alarm event sensor according to the first aspect, to report the alert as an alarm event to a remote monitoring station; on receiving an alert of the second type from the alarm event sensor according to the first aspect, to determine, based on information from the plurality of other alarm event sensors, whether the alert of the second type should be treated as an alert of the first type, and only if it should be so treated to report the alert of the second type as an alarm event to the remote monitoring station.

[0068] In a fifth aspect there is provided a local management device for a premises security monitoring system, the local management device configured to be coupled to an alarm event sensor according to the first aspect and a radio-based location sensing arrangement to detect human presence and location within the premises that is configured to sense presence and location based on detecting perturbations of radio signals; the local management device being configured: on receiving an alert of the first type from the alarm event sensor according to the first aspect, to report the alert as an alarm event to a remote monitoring station;

[0069] on receiving an alert of the second type from the alarm event sensor according to the first aspect, to determine, based on information from the radio-based location sensing arrangement and or from one or more other alarm event sensors of the system, whether the alert of the second type should be treated as an alert of the first type, and only if it should be so treated to report the alert of the second type as an alarm event to the remote monitoring station.

[0070] A local management device according to the fifth aspect may be configured to run the radio-based location sensing arrangement

[0071] Preferably the radio-based sensing arrangement in any of the third, fifth, and seventh aspects 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.

[0072] Preferably for the radio-based sensing arrangement in any of the third, fifth, and seventh aspects 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.

[0073] Preferably for the radio-based sensing arrangement in any of the third, fifth, and seventh aspects uses changes in channel state information or received signal strength in determining presence.

[0074] Preferably for the radio-based sensing arrangement in any of the third, fifth, and seventh aspects the local management device 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. Optionally, 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.

[0075] Preferably for the radio-based sensing arrangement in any of the third, fifth, and seventh aspects the local management device is further configured to perform processing of signals as part of the radio-based location sensing arrangement.

[0076] Preferably for the radio-based sensing arrangement in any of the third, fifth, and seventh aspects 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 deter-

mine the presence of one or more intruders based on a detected change in the people count when the system is in a disarmed mode.

[0077] In a sixth aspect there is provided a method performed by a local management device of a premises security monitoring system installation, the local management device being coupled to an alarm event sensor according to the first aspect and a plurality of other alarm event sensors, the method comprising: on receiving an alert of the first type from the alarm event sensor according to the first aspect, reporting the alert as an alarm event to a remote monitoring station; on receiving an alert of the second type from the alarm event sensor according to the first aspect, determining based on information from the plurality of other alarm event sensors, whether the alert of the second type should be treated as an alert of the first type, and only if it should be so treated reporting the alert of the second type as an alarm event to the remote monitoring station.

[0078] In a seventh aspect there is provided a method performed by a local management device for a premises security monitoring system, the local management device configured to be coupled to an alarm event sensor according to the first aspect and a radio-based location sensing arrangement to detect human presence and location within the premises that is configured to sense presence and location based on detecting perturbations of radio signals; the method comprising: on receiving an alert of the first type from the alarm event sensor according to the first aspect, reporting the alert as an alarm event to a remote monitoring station; on receiving an alert of the second type from the alarm event sensor according to the first aspect, determining, based on information from the radio-based location sensing arrangement and or from one or more other alarm event sensors of the system, whether the alert of the second type should be treated as an alert of the first type, and only if it should be so treated reporting the alert of the second type as an alarm event to the remote monitoring station.

[0079] 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 compared to an expected person count (based on usual occupancy for the time of day and day of the week - e.g., taking account of stored information on "normal" or "usual" behaviour for the relevant day and time).

[0080] 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.

[0081] 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 transmit-

ters that are in a common wireless network with the local management device.

[0082] 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.

[0083] Preferably, the sensing arrangement to detect human presence uses changes in channel state information or received signal strength in determining presence.

[0084] 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.

[0085] 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.

[0086] Preferably, the local management device is further configured to perform processing of signals as part of the radio-based location sensing arrangement.

[0087] Figure 6 is a schematic drawing showing in more detail features of the gateway or central unit 422 of Figure 4. The gateway 422 includes a first transceiver 630 coupled to the first antenna 680, and optionally a second transceiver 632 coupled to a second antenna 682. The transceivers 630 and 632 can each both transmit and receive, but a transceiver cannot both transmit and receive at the same time. Thus, the transceivers 630, 632 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 630, 632 may be arranged such that one transceiver 630 uses a first frequency for transmit and receive and the second transceiver 632 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 630 and 632 are coupled to a controller 650 by a bus. The controller 650 is also connected to a network interface 660 by means of which the controller 650 may be provided with a wired connection to the Internet and hence to the monitoring centre 490. The controller 650 is also coupled to a memory 670 which may store data received from the various nodes of the installation for example event data, sounds, images and video data. The central unit 422 also includes a crystal oscillator 651, 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 422 includes a power supply 662 which is coupled to a domestic mains supply, from which the gateway 422 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 422 also includes a Wi-Fi transceiver 640, and associated antenna arrangement 642, 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 428 or disarm node 430) to enable the occupier to arm or disarm the system from near the main entrance, or it may for example be an image-capture device such as a video camera. Similarly, an interface enabling bidirectional communication over a Public Land Mobile Network (PLMN), such as GSM or LTE, may optionally be provided. Optionally, a third antenna 684 and associated ISM transceiver 634 may be provided, for example for communication with the monitoring centre 490 over, for example, the European 863MHz to 870MHz frequency band. Optionally, the third transceiver 634 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.

[0088] The first 630 and second 632 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 subbands 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.

[0089] The controller 650 is configured to run a sensing application using a WFS software agent 800, which may be stored in memory 670. The WFS software agent 800 uses WFS radio APIs in the Wi-Fi transceiver 640 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.

[0090] 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 600, of the premises, with the AP configured to report the result of presence detection to the central unit 422. 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 422 which would be the overall master in terms of reporting the "alarm".

[0091] 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.

[0092] 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.

[0093] 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.

[0094] 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.

[0095] 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.

[0096] 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).

[0097] Invoked measurement involves utilizing a packet transmission that is in response to a packet received from the Wi-Fi Sensing receiver device.

[0098] 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.

[0099] 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.

[0100] A WFS system can be built based on existing Wi-Fi standards, hardware, software and infrastructure.

[0101] 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.

[0102] 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.

[0103] 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.

[0104] 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.

[0105] 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.

[0106] 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.

[0107] 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).

[0108] The application layer can potentially reside on any networked device: in some embodiments of the present invention, it will reside in the central unit 222 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.

[0109] 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.

[0110] 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.

[0111] 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.

[0112] 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.

[0113] 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. How-

ever, 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.

[0114] 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.

[0115] 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.

[0116] 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.

[0117] 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.

[0118] 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-Wi-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. Sec-

ondly 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.

[0119] 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.

[0120] 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.

[0121] The IEEE 802.11a 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. 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.

[0122] The IEEE 802.11ad amendment defines a Di-

rectional-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 802.11ad (and is also part of the subsequent 802.11ay 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.

[0123] 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.

[0124] 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.

[0125] 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.

[0126] 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 802.11n 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.

[0127] 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.

[0128] 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 receivers 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.

[0129] 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 devel-

opers 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.

[0130] 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.

[0131] 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.

[0132] 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. An alarm event sensor (100, 419) for a premises security monitoring system, the alarm event sensor being configured to generate alerts for the premises security monitoring system, the alarm event sensor (100, 419) comprising:
 - a sensing sub-system (102);
 - a transceiver (110) or output interface for communicating with a controller (422) of the premises security monitoring system; and
 - a processing arrangement (106) operatively coupled to the sensing sub-system (102) and the transceiver (110) or output interface, the sensing subsystem (102) being configured to provide an output having a magnitude that can

have more than two values and that varies in response to changes in a sensed input, the alarm event sensor (100, 419) being **characterised in that** the processing arrangement (106) is configured to:

process outputs of the sensing subsystem (102) in accordance with a first threshold and a second threshold higher than the first; generate alerts of a first type in respect of outputs having a magnitude greater than the second threshold; not to generate alerts in respect of outputs having a magnitude not exceeding the first threshold; generate alerts of a second type in respect of outputs having a magnitude between the first and second thresholds; and to cause the transceiver (110) to transmit the alerts of the first and second types to the controller (422) of the premises security monitoring system.

2. The alarm event sensor of claim 1, wherein the sensing sub-system (102) includes a magnetometer or an accelerometer.
3. The alarm event sensor of claim 1, wherein the alarm event sensor (100, 419) is configured as a shock sensor.
4. The alarm event sensor of claim 1, wherein the sensing sub-system (102) includes an optical sensor or a passive infra-red sensor.
5. A premises security monitoring system having a local management device (422), and operatively coupled to the local management device (422) an alarm event sensor (100, 419) as claimed in any one of claims 1 to 4 and a plurality of other alarm event sensors (416, 424), the local management device (422) being configured:

on receiving an alert of the first type from the alarm event sensor (100, 419) as claimed in any one of claims 1 to 4, to report the alert as an alarm event to a remote monitoring station (490);

on receiving an alert of the second type from the alarm event sensor (100, 419) as claimed in any one of claims 1 to 4, to determine, based on information from the plurality of other alarm event sensors (416, 424), whether the alert of the second type should be treated as an alert of the first type, and only if it should be so treated to report the alert of the second type as an alarm event to the remote monitoring station (490).

6. The premises security monitoring system of claim 5, wherein the local management device (422) is configured to determine that the alert of the second type should be treated as an alert of the first type if the information from the plurality of other alarm event sensors (416, 424) indicates that a break in has occurred at the premises. 5
7. The premises security monitoring system of claim 5 or claim 6, wherein the local management device (422) is configured to determine that the alert of the second type should not be treated as an alert of the first type if the information from the plurality of other alarm event sensors (416, 424) indicates that the premises has not been the subject of a break in. 10 15
8. A premises security monitoring system having a local management device (422), and operatively coupled to the local management device (422) an alarm event sensor (100, 419) as claimed in any one of claims 1 to 4 and a radio-based location sensing arrangement to detect human presence and location within the premises that is configured to sense presence and location based on detecting perturbations of radio signals; 20 25
the local management device (422) being configured:
- on receiving an alert of the first type from the alarm event sensor (100, 419) as claimed in any one of claims 1 to 4, to report the alert as an alarm event to a remote monitoring station (490); 30
on receiving an alert of the second type from the alarm event sensor (100, 419) as claimed in any one of claims 1 to 4, to determine, based on information from the radio-based location sensing arrangement and or from one or more other alarm event sensors (416, 424) of the system, whether the alert of the second type should be treated as an alert of the first type, and only if it should be so treated to report the alert of the second type as an alarm event to the remote monitoring station (490). 35 40
9. A local management device (422) for a premises security monitoring system, the local management device (422) being configured to be coupled to an alarm event sensor (100, 419) as claimed in any one of claims 1 to 4 and a plurality of other alarm event sensors (416, 424), the local management device (422) being configured: 45 50
on receiving an alert of the first type from the alarm event sensor (100, 419) as claimed in any one of claims 1 to 4, to report the alert as an alarm event to a remote monitoring station (490); 55

on receiving an alert of the second type from the alarm event sensor (100, 419) as claimed in any one of claims 1 to 4, to determine, based on information from the plurality of other alarm event sensors (416, 424), whether the alert of the second type should be treated as an alert of the first type, and only if it should be so treated to report the alert of the second type as an alarm event to the remote monitoring station (490).

10. A local management device (422) for a premises security monitoring system, the local management device (422) being configured to be coupled to an alarm event sensor (100, 419) as claimed in any one of claims 1 to 4 and a radio-based location sensing arrangement to detect human presence and location within the premises that is configured to sense presence and location based on detecting perturbations of radio signals; the local management device (422) being configured:

on receiving an alert of the first type from the alarm event sensor (100, 419) as claimed in any one of claims 1 to 4, to report the alert as an alarm event to a remote monitoring station (490);

on receiving an alert of the second type from the alarm event sensor (100, 419) as claimed in any one of claims 1 to 4, to determine, based on information from the radio-based location sensing arrangement and or from one or more other alarm event sensors (416, 424) of the system, whether the alert of the second type should be treated as an alert of the first type, and only if it should be so treated to report the alert of the second type as an alarm event to the remote monitoring station (490).

11. A method performed by a local management device (422) of a premises security monitoring system, the local management device (422) being coupled to an alarm event sensor (100, 419) as claimed in any one of claims 1 to 4 and a plurality of other alarm event sensors (416, 424), the method comprising:

on receiving an alert of the first type from the alarm event sensor (100, 419) as claimed in any one of claims 1 to 4, reporting the alert as an alarm event to a remote monitoring station (419);

on receiving an alert of the second type from the alarm event sensor (100, 419) as claimed in any one of claims 1 to 4, determining based on information from the plurality of other alarm event sensors (416, 424), whether the alert of the second type should be treated as an alert of the first type, and only if it should be so treated

reporting the alert of the second type as an alarm event to the remote monitoring station (490).

12. A method performed by a local management device (422) of a premises security monitoring system installation, the local management device (422) being coupled to an alarm event sensor (100, 419) as claimed in any one of claims 1 to 4 and to a radio-based location sensing arrangement to detect human presence and location within the premises that is configured to sense presence and location based on detecting perturbations of radio signals; the method comprising:

on receiving an alert of the first type from the alarm event sensor (100, 419) as claimed in any one of claims 1 to 4, reporting the alert as an alarm event to a remote monitoring station (490);

on receiving an alert of the second type from the alarm event sensor (100, 419) as claimed in any one of claims 1 to 4, determining, based on information from the radio-based location sensing arrangement and/or from one or more other alarm event sensors (416, 424) of the system, whether the alert of the second type should be treated as an alert of the first type, and only if it should be so treated reporting the alert of the second type as an alarm event to the remote monitoring station (424).

Patentansprüche

1. Alarmereignissensor (100, 419) für ein Geländesicherheitsüberwachungssystem, wobei der Alarmereignissensor dazu konfiguriert ist, Alarmer für das Geländesicherheitsüberwachungssystem zu erzeugen, der Alarmereignissensor (100, 419) umfassend:

ein Erfassungsteilsystem (102);
einen Sender-Empfänger (110) oder eine Ausgabeschnittstelle zum Kommunizieren mit einer Steuerung (422) des Geländesicherheitsüberwachungssystems; und
eine Verarbeitungsanordnung (106), die betriebsfähig mit dem Erfassungsteilsystem (102) und dem Sender-Empfänger (110) oder der Ausgabeschnittstelle gekoppelt ist, wobei das Erfassungsteilsystem (102) dazu konfiguriert ist, eine Ausgabe mit einer Magnitude bereitzustellen, die mehr als zwei Werte aufweisen kann und die als Antwort auf Veränderungen einer erfassten Eingabe variiert, wobei der Alarmereignissensor (100, 419) **dadurch gekennzeichnet ist, dass** die Verarbeitungsanordnung (106) dazu konfiguriert ist:

Ausgaben des Erfassungsteilsystems (102) gemäß einem ersten Grenzwert und einem zweiten Grenzwert, der höher ist als der erste, zu verarbeiten;

Alarmer eines ersten Typs in Bezug auf Ausgaben mit einer Magnitude, die größer als der zweite Grenzwert ist, zu erzeugen;

keine Alarmer in Bezug auf Ausgaben mit einer Magnitude die den ersten Grenzwert nicht überschreitet, zu erzeugen;

Alarmer eines zweiten Typs in Bezug auf Ausgaben mit einer Magnitude, die zwischen dem ersten und dem zweiten Grenzwert liegt, zu erzeugen; und

zu veranlassen, dass der Sender-Empfänger (110) die Alarmer des ersten und des zweiten Typs an die Steuerung (422) des Geländesicherheitsüberwachungssystems sendet.

2. Alarmereignissensor nach Anspruch 1, wobei das Erfassungsteilsystem (102) ein Magnetometer oder einen Beschleunigungsmesser beinhaltet.

3. Alarmereignissensor nach Anspruch 1, wobei der Alarmereignissensor (100, 419) als Schocksensor konfiguriert ist.

4. Alarmereignissensor nach Anspruch 1, wobei das Erfassungsteilsystem (102) einen optischen Sensor oder einen passiven Infrarotsensor beinhaltet.

5. Geländesicherheitsüberwachungssystem mit einer lokalen Managementvorrichtung (422) und, betriebsfähig mit der lokalen Managementvorrichtung (422) gekoppelt, einem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, und einer Vielzahl anderer Alarmereignissensoren (416, 424), wobei die lokale Managementvorrichtung (422) dazu konfiguriert ist:

bei Empfangen eines Alarms des ersten Typs von dem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, den Alarm als ein Alarmereignis an eine entfernte Überwachungsstation (490) zu melden;

bei Empfangen eines Alarms des zweiten Typs von dem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, auf Basis von Informationen von der Vielzahl anderer Alarmereignissensoren (416, 424) zu bestimmen, ob der Alarm des zweiten Typs als ein Alarm des ersten Typs behandelt werden sollte, und nur wenn er als solcher behandelt werden sollte, den Alarm des zweiten Typs als ein Alarmereignis an die entfernte Überwachungsstation (490) zu melden.

6. Geländesicherheitsüberwachungssystem nach Anspruch 5, wobei die lokale Managementvorrichtung (422) dazu konfiguriert ist, zu bestimmen, dass der Alarm des zweiten Typs als ein Alarm des ersten Typs behandelt werden sollte, wenn die Informationen von der Vielzahl anderer Alarmereignissensoren (416, 424) angeben, dass auf dem Gelände ein Einbruch aufgetreten ist. 5
7. Geländesicherheitsüberwachungssystem nach Anspruch 5 oder 6, wobei die lokale Managementvorrichtung (422) dazu konfiguriert ist, zu bestimmen, dass der Alarm des zweiten Typs nicht als ein Alarm des ersten Typs behandelt werden sollte, wenn die Informationen von der Vielzahl anderer Alarmereignissensoren (416, 424) angeben, dass das Gelände nicht Ziel eines Einbruchs war. 10 15
8. Geländesicherheitsüberwachungssystem mit einer lokalen Managementvorrichtung (422) und, betriebsfähig mit der lokalen Managementvorrichtung (422) gekoppelt, einem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, und einer funkbasierten Standorterfassungsanordnung zum Erkennen einer Anwesenheit und eines Standorts von Menschen innerhalb des Geländes, die dazu konfiguriert ist, eine Anwesenheit und einen Standort auf Basis des Erkennens von Störungen von Radiosignalen zu erfassen; wobei die lokale Managementvorrichtung (422) dazu konfiguriert ist: 20 25 30
- bei Empfangen eines Alarms des ersten Typs von dem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, den Alarm als ein Alarmereignis an eine entfernte Überwachungsstation (490) zu melden; 35
- bei Empfangen eines Alarms des zweiten Typs von dem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, auf Basis von Informationen von der funkbasierten Standorterfassungsanordnung oder von einem oder mehreren Alarmereignissensoren (416, 424) des Systems zu bestimmen, ob der Alarm des zweiten Typs als ein Alarm des ersten Typs behandelt werden sollte, und nur wenn er als solcher behandelt werden sollte, den Alarm des zweiten Typs als ein Alarmereignis an die entfernte Überwachungsstation (490) zu melden. 40 45
9. Lokale Managementvorrichtung (422) für ein Geländesicherheitsüberwachungssystem, wobei die lokale Managementvorrichtung (422) dazu konfiguriert ist, mit einem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, und einer Vielzahl anderer Alarmereignissensoren (416, 424) gekoppelt zu sein, wobei die lokale Managementvorrichtung (422) dazu konfiguriert ist: 50 55

bei Empfangen eines Alarms des ersten Typs von dem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, den Alarm als ein Alarmereignis an eine entfernte Überwachungsstation (490) zu melden;

bei Empfangen eines Alarms des zweiten Typs von dem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, auf Basis von Informationen von der Vielzahl anderer Alarmereignissensoren (416, 424) zu bestimmen, ob der Alarm des zweiten Typs als ein Alarm des ersten Typs behandelt werden sollte, und nur wenn er als solcher behandelt werden sollte, den Alarm des zweiten Typs als ein Alarmereignis an die entfernte Überwachungsstation (490) zu melden.

10. Lokale Managementvorrichtung (422) für ein Geländesicherheitsüberwachungssystem, wobei die lokale Managementvorrichtung (422) dazu konfiguriert ist, mit einem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, und einer funkbasierten Standorterfassungsanordnung zum Erkennen einer Anwesenheit und eines Standorts von Menschen innerhalb des Geländes gekoppelt zu sein, die dazu konfiguriert ist, eine Anwesenheit und einen Standort auf Basis des Erkennens von Störungen von Radiosignalen zu erfassen; wobei die lokale Managementvorrichtung (422) dazu konfiguriert ist: 50

bei Empfangen eines Alarms des ersten Typs von dem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, den Alarm als ein Alarmereignis an eine entfernte Überwachungsstation (490) zu melden;

bei Empfangen eines Alarms des zweiten Typs von dem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, auf Basis von Informationen von der funkbasierten Standorterfassungsanordnung oder von einem oder mehreren Alarmereignissensoren (416, 424) des Systems zu bestimmen, ob der Alarm des zweiten Typs als ein Alarm des ersten Typs behandelt werden sollte, und nur wenn er als solcher behandelt werden sollte, den Alarm des zweiten Typs als ein Alarmereignis an die entfernte Überwachungsstation (490) zu melden.

11. Verfahren, das von einer lokalen Managementvorrichtung (422) eines Geländesicherheitsüberwachungssystems durchgeführt wird, wobei die lokale Managementvorrichtung (422) mit einem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, und einer Vielzahl anderer Alarmereignissensoren (416, 424) gekoppelt ist, das Verfahren umfassend: 50 55

bei Empfangen eines Alarms des ersten Typs von dem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, Melden des Alarms als ein Alarmereignis an eine entfernte Überwachungsstation (419); 5

bei Empfangen eines Alarms des zweiten Typs von dem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, auf Basis von Informationen von der Vielzahl anderer Alarmereignissensoren (416, 424) Bestimmen, ob der Alarm des zweiten Typs als ein Alarm des ersten Typs behandelt werden sollte, und nur wenn er als solcher behandelt werden sollte, den Alarm des zweiten Typs als ein Alarmereignis an die entfernte Überwachungsstation (490) zu melden. 10 15

12. Verfahren, das durch eine lokale Managementvorrichtung (422) einer Geländesicherheitsüberwachungssystem-Anlage durchgeführt wird, wobei die lokale Managementvorrichtung (422) mit einem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, und einer funkbasierten Standorterfassungsanordnung zum Erkennen einer Anwesenheit und eines Standorts von Menschen innerhalb des Geländes gekoppelt ist, die dazu konfiguriert ist, eine Anwesenheit und einen Standort auf Basis des Erkennens von Störungen von Radiosignalen zu erfassen; das Verfahren umfassend: 20 25 30

bei Empfangen eines Alarms des ersten Typs von dem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, Melden des Alarms als ein Alarmereignis an eine entfernte Überwachungsstation (490); 35

bei Empfangen eines Alarms des zweiten Typs von dem Alarmereignissensor (100, 419), wie in einem der Ansprüche 1 bis 4 beansprucht, auf Basis von Informationen von der funkbasierten Standorterfassungsanordnung oder von einem oder mehreren Alarmereignissensoren (416, 424) des Systems Bestimmen, ob der Alarm des zweiten Typs als ein Alarm des ersten Typs behandelt werden sollte, und nur wenn er als solcher behandelt werden sollte, den Alarm des zweiten Typs als ein Alarmereignis an die entfernte Überwachungsstation (424) zu melden. 40 45 50

Revendications

1. Capteur d'événements d'alarme (100, 419) pour un système de surveillance de sécurité de locaux, le capteur d'événements d'alarme étant configuré pour générer des alertes pour le système de surveillance de sécurité de locaux, le capteur d'événements d'alarme (100, 419) comprenant : 55

un sous-système de détection (102) ;
un émetteur-récepteur (110) ou une interface de sortie pour communiquer avec un contrôleur (422) du système de surveillance de sécurité de locaux ; et
un dispositif de traitement (106) couplé de manière fonctionnelle au sous-système de détection (102) et à l'émetteur-récepteur (110) ou l'interface de sortie, le sous-système de détection (102) étant configuré pour fournir une sortie ayant une amplitude qui peut avoir plus de deux valeurs et qui varie en réponse à des changements dans une entrée détectée, le capteur d'événements d'alarme (100, 419) étant **caractérisé en ce que** le dispositif de traitement (106) est configuré pour :

traiter les signaux de sortie du sous-système de détection (102) conformément à un premier seuil et à un deuxième seuil supérieur au premier ;
générer des alertes d'un premier type concernant des signaux de sortie ayant une amplitude supérieure au deuxième seuil ;
ne pas générer d'alertes concernant des signaux de sortie ayant une amplitude ne dépassant pas le premier seuil ;
générer des alertes d'un deuxième type concernant des signaux de sortie ayant une amplitude comprise entre les premier et deuxième seuils ; et
amener l'émetteur-récepteur (110) à transmettre les alertes des premier et deuxième types au contrôleur (422) du système de surveillance de sécurité de locaux.

2. Capteur d'événements d'alarme selon la revendication 1, dans lequel le sous-système de détection (102) inclut un magnétomètre ou un accéléromètre.
3. Capteur d'événements d'alarme selon la revendication 1, dans lequel le capteur d'événements d'alarme (100, 419) est configuré comme un capteur de choc.
4. Capteur d'événements d'alarme selon la revendication 1, dans lequel le sous-système de détection (102) inclut un capteur optique ou un capteur infrarouge passif.
5. Système de surveillance de sécurité de locaux ayant un dispositif de gestion local (422), et couplé de manière fonctionnelle au dispositif de gestion local (422), un capteur d'événements d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4 et une pluralité d'autres capteurs d'événements d'alarme (416, 424), le dispositif de gestion local (422) étant configuré :

- lors de la réception d'une alerte du premier type provenant du capteur d'événements d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4, pour transmettre l'alerte comme un événement d'alarme à une station de surveillance à distance (490) ;
- lors de la réception d'une alerte du deuxième type provenant du capteur d'événements d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4, pour déterminer, en fonction d'informations provenant de la pluralité d'autres capteurs d'événements d'alarme (416, 424), si l'alerte du deuxième type doit être traitée comme une alerte du premier type et, seulement si elle doit être traitée de la sorte, pour transmettre l'alerte du deuxième type comme un événement d'alarme à la station de surveillance à distance (490).
6. Système de surveillance de sécurité de locaux selon la revendication 5, dans lequel le dispositif de gestion local (422) est configuré pour déterminer que l'alerte du deuxième type doit être traitée comme une alerte du premier type si les informations provenant de la pluralité d'autres capteurs d'événements d'alarme (416, 424) indiquent qu'une effraction s'est produite au niveau des locaux.
7. Système de surveillance de sécurité de locaux selon la revendication 5 ou la revendication 6, dans lequel le dispositif de gestion local (422) est configuré pour déterminer que l'alerte du deuxième type ne doit pas être traitée comme une alerte du premier type si les informations provenant de la pluralité d'autres capteurs d'événements d'alarme (416, 424) indiquent que les locaux n'ont pas fait l'objet d'une effraction.
8. Système de surveillance de sécurité de locaux ayant un dispositif de gestion local (422), et couplé de manière fonctionnelle au dispositif de gestion local (422), un capteur d'événements d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4 et un dispositif de détection de localisation par radio pour détecter une présence humaine et sa localisation à l'intérieur des locaux qui est configuré pour détecter une présence et une localisation en fonction de la détection de perturbations de signaux radio ; le dispositif de gestion local (422) étant configuré :
- lors de la réception d'une alerte du premier type provenant du capteur d'événements d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4, pour transmettre l'alerte comme un événement d'alarme à une station de surveillance à distance (490) ;
- lors de la réception d'une alerte du deuxième type provenant du capteur d'événement d'alarme (100, 419) selon l'une quelconque des

revendications 1 à 4, pour déterminer, en fonction d'informations provenant du dispositif de détection de localisation par radio et/ou d'un ou plusieurs autres capteurs d'événements d'alarme (416, 424) du système, si l'alerte du deuxième type doit être traitée comme une alerte du premier type et, seulement si elle doit être traitée de la sorte, pour transmettre l'alerte du deuxième type comme un événement d'alarme à la station de surveillance à distance (490).

9. Dispositif de gestion local (422) pour un système de surveillance de sécurité de locaux, le dispositif de gestion local (422) étant configuré pour être couplé à un capteur d'événements d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4 et à une pluralité d'autres capteurs d'événements d'alarme (416, 424), le dispositif de gestion local (422) étant configuré :

lors de la réception d'une alerte du premier type provenant du capteur d'événements d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4, pour transmettre l'alerte comme un événement d'alarme à une station de surveillance à distance (490) ;

lors de la réception d'une alerte du deuxième type provenant du capteur d'événements d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4, pour déterminer, en fonction d'informations provenant de la pluralité d'autres capteurs d'événements d'alarme (416, 424), si l'alerte du deuxième type doit être traitée comme une alerte du premier type et, seulement si elle doit être traitée de la sorte, pour transmettre l'alerte du deuxième type comme un événement d'alarme à la station de surveillance à distance (490).

10. Dispositif de gestion local (422) pour un système de surveillance de sécurité de locaux, le dispositif de gestion local (422) étant configuré pour être couplé à un capteur d'événements d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4 et à un dispositif de détection de localisation par radio pour détecter une présence humaine et sa localisation à l'intérieur des locaux qui est configuré pour détecter la présence et la localisation en fonction d'une détection de perturbations de signaux radio ; le dispositif de gestion local (422) étant configuré :

lors de la réception d'une alerte du premier type provenant du capteur d'événements d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4, pour transmettre l'alerte comme un événement d'alarme à une station de surveillance à distance (490) ;

lors de la réception d'une alerte du deuxième

type provenant du capteur d'événement d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4, pour déterminer, en fonction d'informations provenant du dispositif de détection de localisation par radio et/ou d'un ou plusieurs autres capteurs d'événements d'alarme (416, 424) du système, si l'alerte du deuxième type doit être traitée comme une alerte du premier type et, seulement si elle doit être traitée de la sorte, pour transmettre l'alerte du deuxième type comme un événement d'alarme à la station de surveillance à distance (490).

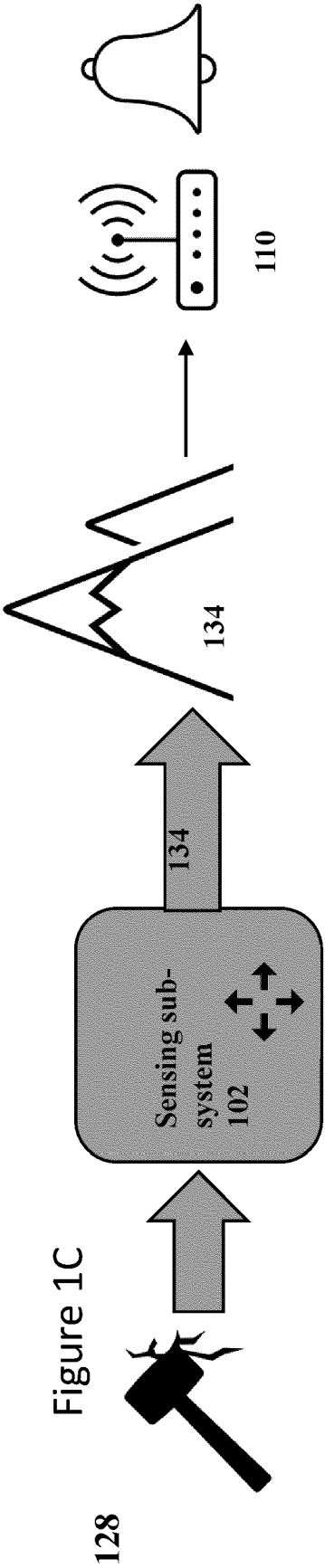
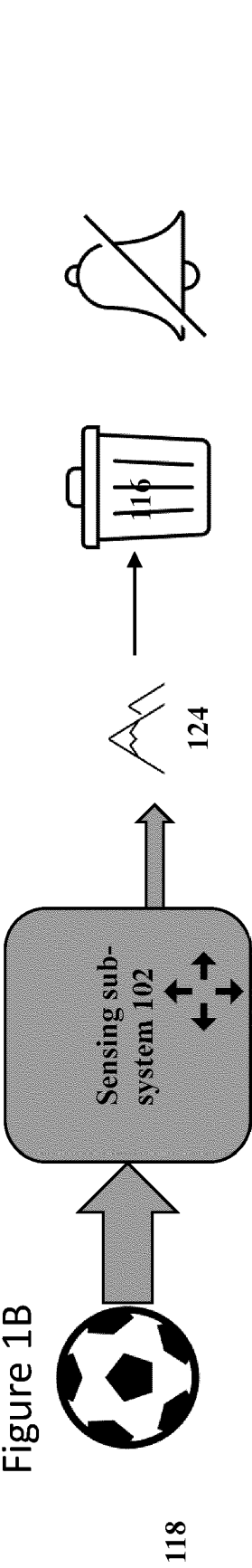
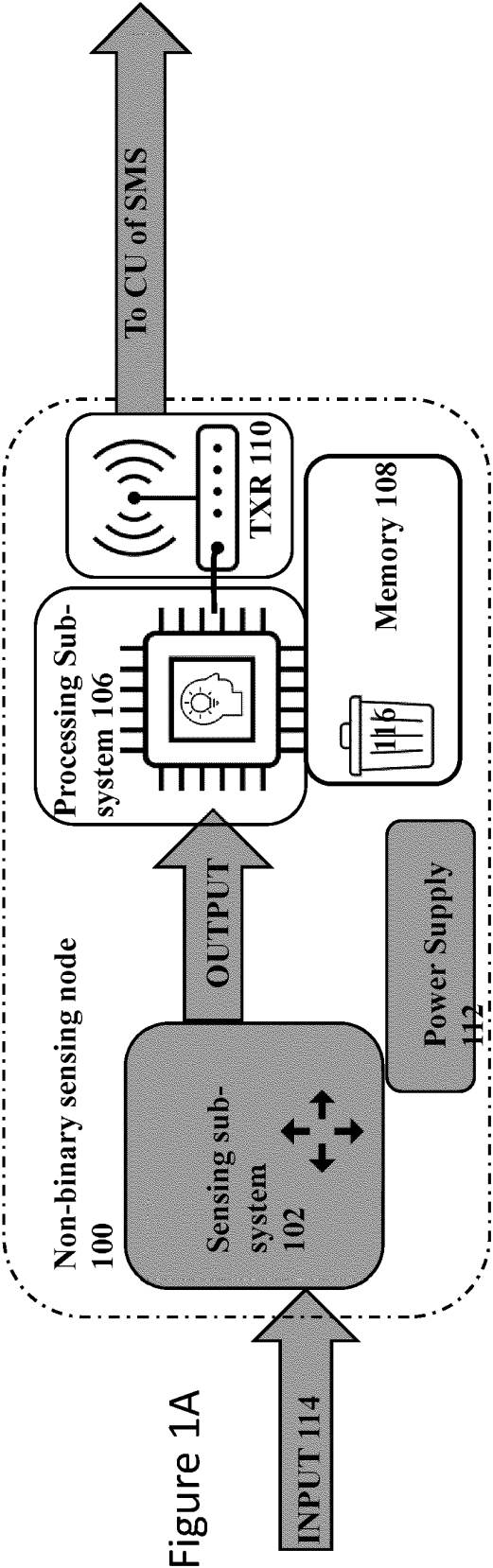
11. Procédé réalisé par un dispositif de gestion local (422) d'un système de surveillance de sécurité de locaux, le dispositif de gestion local (422) étant couplé à un capteur d'événements d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4 et à une pluralité d'autres capteurs d'événements d'alarme (416, 424), le procédé comprenant :

lors de la réception d'une alerte du premier type provenant du capteur d'événements d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4, la transmission de l'alerte comme un événement d'alarme à une station de surveillance à distance (490) ;
lors de la réception d'une alerte du deuxième type provenant du capteur d'événements d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4, le fait de déterminer, en fonction des informations provenant de la pluralité d'autres capteurs d'événement d'alarme (416, 424), si l'alerte du deuxième type doit être traitée comme une alerte du premier type et, seulement si elle doit être traitée de la sorte, la transmission de l'alerte du deuxième type comme un événement d'alarme à la station de surveillance à distance (490).

12. Procédé réalisé par un dispositif de gestion local (422) d'un système de surveillance de sécurité de locaux, le dispositif de gestion local (422) étant couplé à un capteur d'événements d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4 et à un dispositif de détection de localisation par radio pour détecter une présence humaine et sa localisation à l'intérieur des locaux qui est configuré pour détecter la présence et la localisation en fonction d'une détection de perturbations de signaux radio, le procédé comprenant :

lors de la réception d'une alerte du premier type provenant du capteur d'événements d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4, la transmission de l'alerte comme un événement d'alarme à une station de surveillance à distance (490) ;

lors de la réception d'une alerte du deuxième type provenant du capteur d'événement d'alarme (100, 419) selon l'une quelconque des revendications 1 à 4, le fait de déterminer, en fonction d'informations provenant du dispositif de détection de localisation par radio et/ou d'un ou plusieurs autres capteurs d'événements d'alarme (416, 424) du système, si l'alerte du deuxième type doit être traitée comme une alerte du premier type et, seulement si elle doit être traitée de la sorte, la transmission de l'alerte du deuxième type comme un événement d'alarme à la station de surveillance à distance (424).



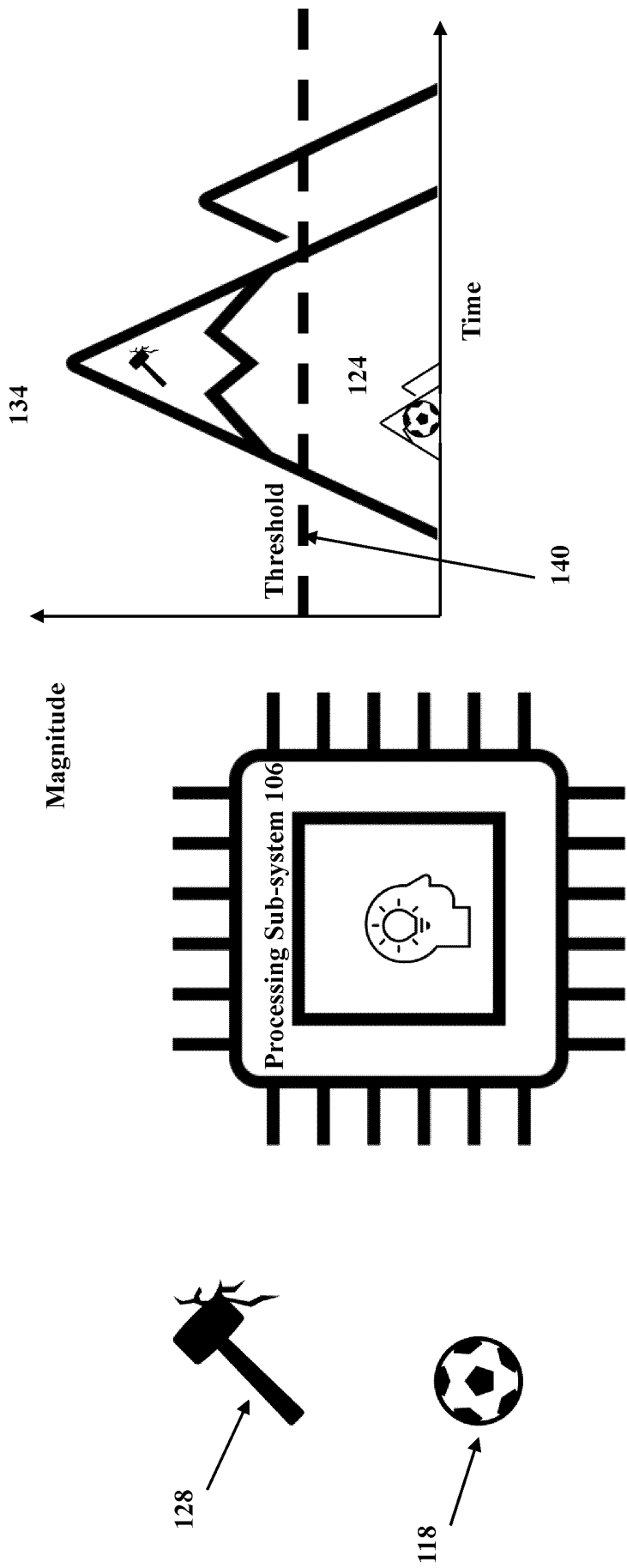


Figure 2

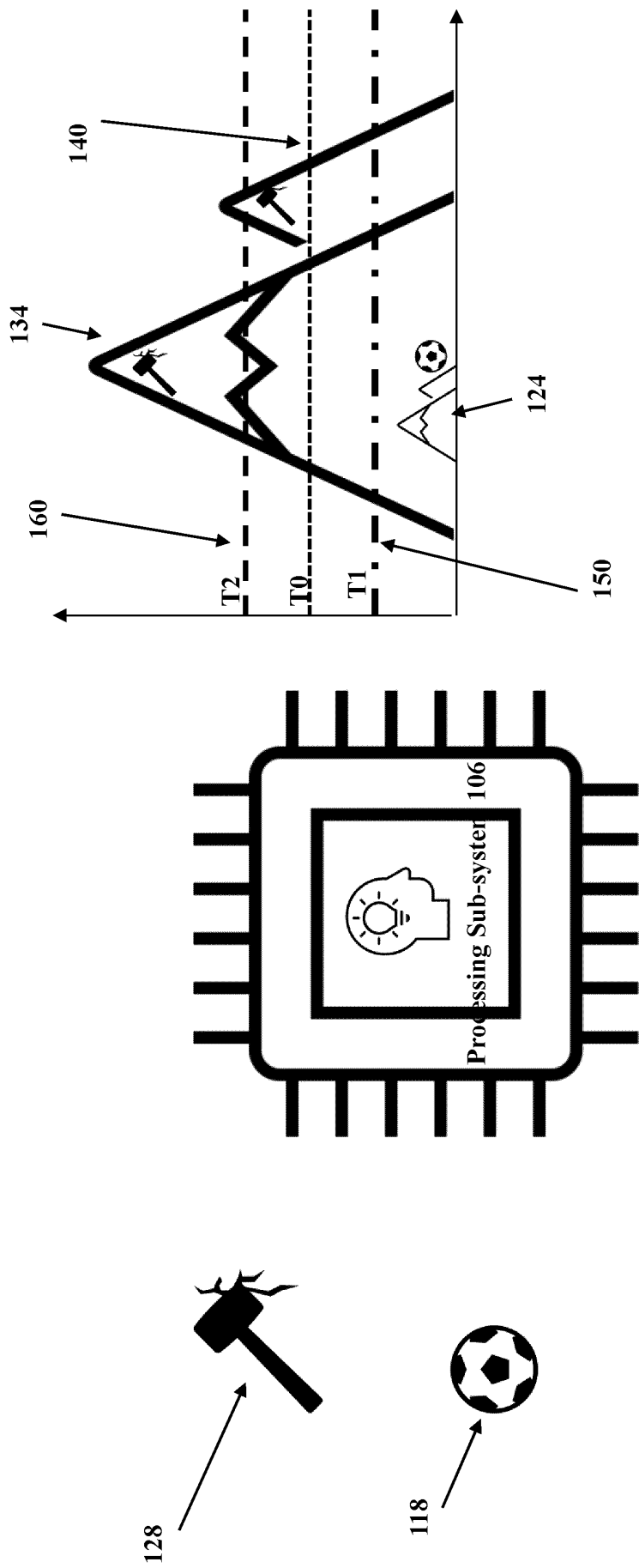


Figure 3

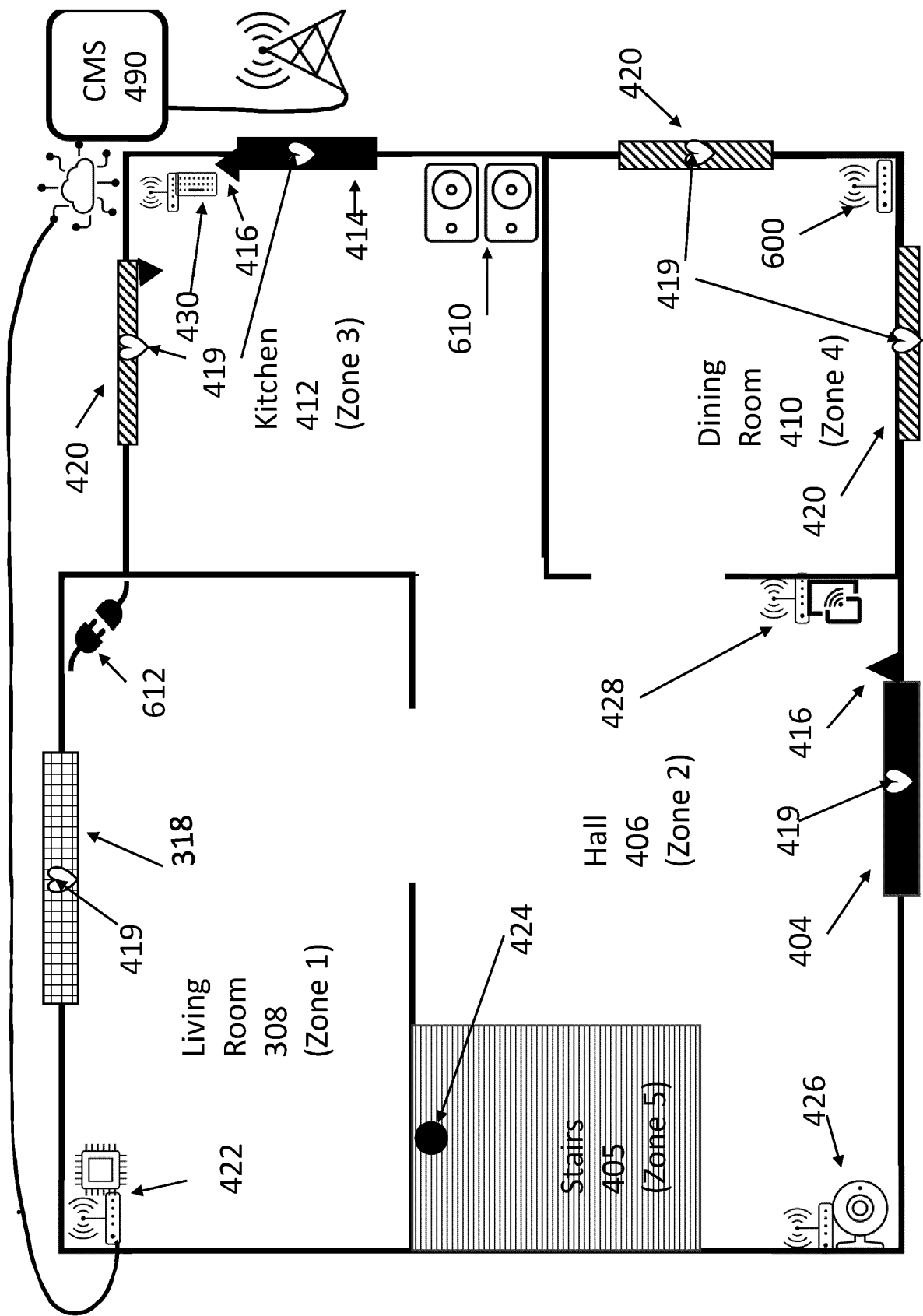


Figure 4

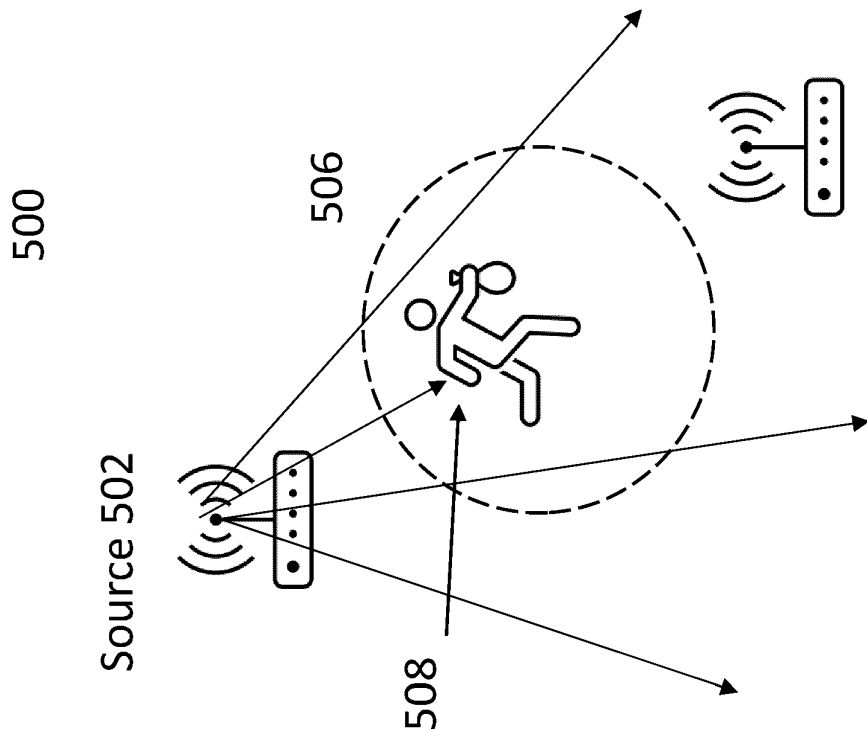


Figure 5B

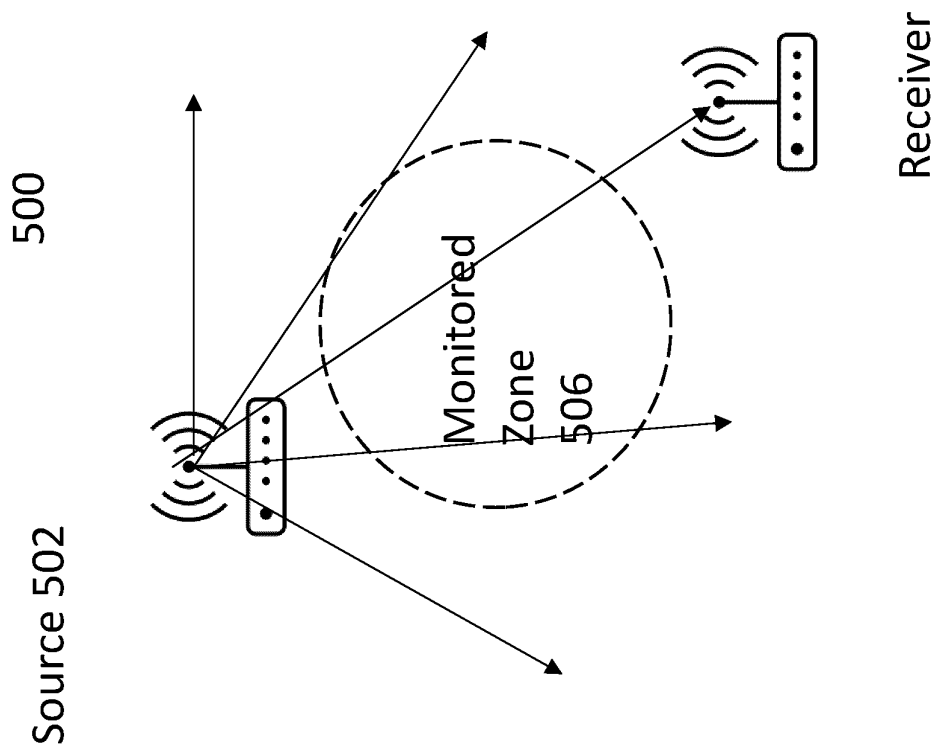


Figure 5A

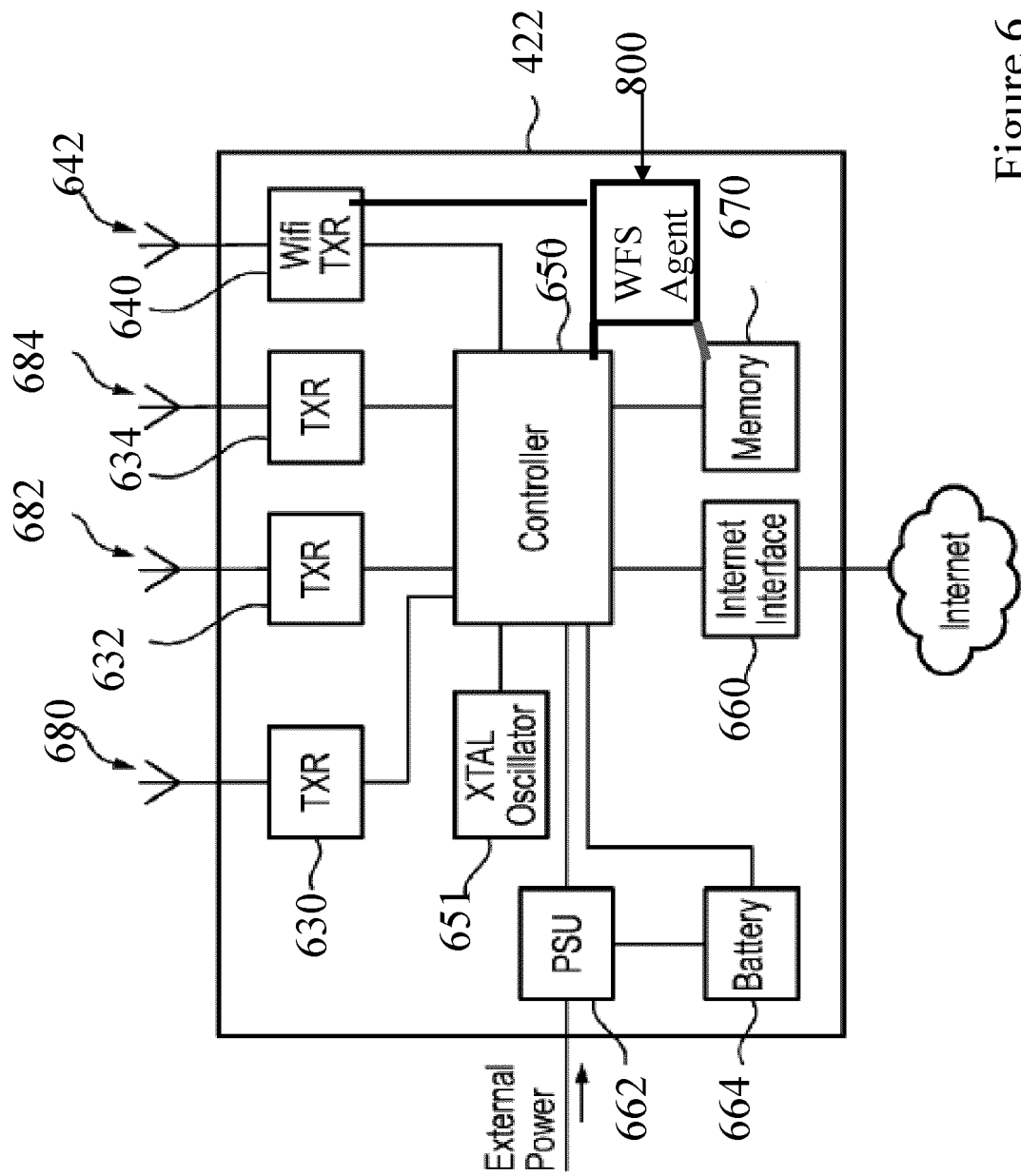


Figure 6

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

- CN 104700580 A [0008]
- EP 1437701 A [0009]
- US 2016189533 A [0010]
- EP 3065117 A1 [0011]
- US 20200302187 A1 [0080]