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

(11) **EP 4 207 124 A1**

(12) **EUROPEAN PATENT APPLICATION**

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

(21) Application number: **21218147.3**

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

(51) International Patent Classification (IPC):
G08B 25/00 *(2006.01)* ***G08B 13/24*** *(2006.01)*
G08B 13/19 *(2006.01)* ***G08B 13/196*** *(2006.01)*

(52) Cooperative Patent Classification (CPC):
G08B 25/008; G08B 13/196; G08B 13/2491

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

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

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

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

(54) SECURITY MONITORING SYSTEMS

(57) A security monitoring system installation in a location, the location having a perimeter, and the system including a sensing arrangement to detect human presence within a monitored area within the perimeter, the monitored area comprising a plurality of monitored zones, at least one pair of the monitored zones being remote from each other, each remote pair consisting of a first and a second of the monitored zones, human passage between the first and second zones of a pair that are remote from each other only being possible, within the premises, via at least one intermediate zone that is adjacent the second zone of the pair, and the system having an armed at home state in which it is so configured that, in the event that:
at a first instant human presence is detected in the first remote zone of the pair but not in any of the second or intermediate zones of the pair; and
subsequently, at a second instant, human presence is detected in the second zone of the pair without presence having been detected in any of the one or more intermediate zones of the pair in the interval between the first and second instants; an alert is raised.

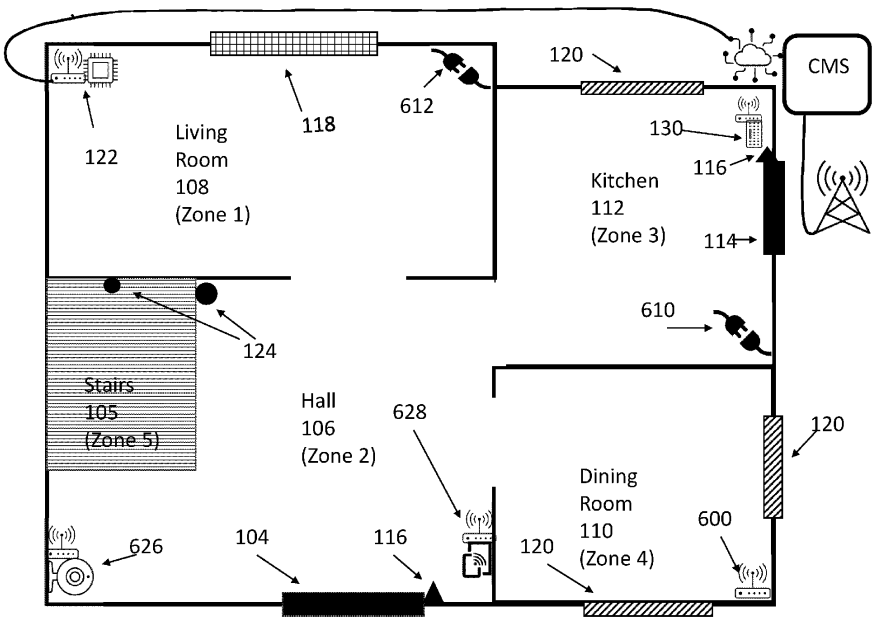


Figure 6

EP 4 207 124 A1

Description

Technical field

[0001] The present invention relates generally to security monitoring systems for premises.

Background

[0002] Security monitoring systems for premises (hereinafter referred to simply as security monitoring systems), often referred to as "burglar alarms", are typically arranged, when armed, to provide some kind of alarm signal if a "break-in" is detected at the premises protected by the system. Detection of a "break-in" may be through the triggering of a sensor at a perimeter of the premises, for example a sensor arranged to detect the opening of a door or window, or by the triggering of a sensor within the premises that implies human presence within the premises. The triggering of a sensor signifying a "break-in" is referred to as an alarm event.

[0003] The cost of installing a security monitoring system generally increases with the number of sensors used in the installation - so it is not uncommon for systems to be installed with sensors provided to only some of the external doors or windows that define the premises' perimeter. For example, with only sensors on the main entrance door, or the main entrance door and the (principal) back door, but with no or few window sensors. Likewise, when it comes to internal sensing arrangements it is common for sensing to be limited to the provision of motion sensors (typically in the form of PIR sensors) in one or more transit areas - such as entrance halls, and possibly in a subset of rooms to which a burglar might effect access from outside the premises. Motion sensing is an example of presence detection, and this may be supplemented or replaced by other forms of presence detection - such as detection of door opening, detection of switches - such as light switches, being operated, sound detection, etc.

[0004] Although a key function of security monitoring systems is to protect premises when they are unoccupied - using an armed state that is commonly referred to as "armed away", security monitoring systems are also used to provide a feeling of comfort and security to occupants of the premises when they are at home - by providing an armed state that is commonly referred to as "armed at home" or "secure perimeter". The idea behind the armed at home state is that by monitoring the protected perimeter of the premises, occupants can be warned in the event that an attempt is made to enter the premises while they are inside - often the scariest prospect for many homeowners. There may be more than one armed at home status, for example a daytime setting in which occupants are expected to move around the living spaces or zones of the home, and possibly also move between the living spaces and the sleeping spaces. There may also be a nighttime or "sleep" armed at home status which occupants select when they retire to bed - and in which movement or presence within the living zone leads to an alarm event being reported, while presence in the sleeping zone(s) is expected and hence does not lead to an alarm event.

[0005] Conventionally, it is unusual to provide motion or presence sensing in every room, or even every principal room, of a house or dwelling - indeed, seldom does every room in the living accommodation of a home or dwelling have its own motion or presence sensor. It is generally considered that a satisfactory level of security can be achieved by providing motion sensing only in a subset of rooms or spaces - for example, by providing motion sensing in a space that links several rooms (typically "important" rooms that contain valuables, or which are likely otherwise to be attractive to burglars). This, coupled with a limited deployment of door and window sensors, is conventionally assumed to provide a satisfactory level of security while helping to limit the complexity and hence cost of an installed security monitoring system.

[0006] It is also conventionally accepted that, for a daytime armed at home setting, monitoring is limited to the monitoring of the protected perimeter of the premises, although in some instances motion detection may still be turned on for rooms or zones of the house which are generally not visited by legitimate occupants of the premises when the armed at home setting is used.

[0007] In recent years various new approaches to presence detection has been proposed that infer presence based on detecting perturbations in radio signals. Prominent among these approaches is what has become known as Wi-Fi Sensing, and which is based on detection of changes in channel state information (CSI) of Wi-Fi signals. Wi-Fi sensing is the subject of a standardisation program led by the Wireless Broadband Alliance (WBA). In 2019, the WBA produced a paper on Wi-Fi Sensing entitled "Wi-Fi Sensing A New Technology Emerges" which includes the following explanation of the technology's background:

"In Wi-Fi Sensing, radio information obtained during signal processing is used to detect environmental changes caused by motion of objects, pets and people. In many cases, the primary information extracted from the radio for Wi-Fi Sensing is the channel frequency response and/or the received signal strength. Computing this quantity is a typical function of any Wi-Fi receiver, as it enables a mechanism to compensate for the distortion introduced by the wireless channel. Wi-Fi Sensing builds upon these mechanisms, allowing any Wi-Fi device perform sensing and learn about changes in the environment.

[0008] Using one or multiple collaborating Wi-Fi devices to sense the environment and detect motion has many benefits and enables many new business opportunities. Network providers can utilize information made available through sensing to provide a new set of services to customers. Hardware original equipment manufacturers (OEMs) and chipset vendors can add Wi-Fi sensing as

a feature to differentiate products. Advances in signal processing and feature extraction algorithms produce even more detailed information. As Wi-Fi sensing technology matures, new and more complex use cases are enabled.". The paper also provides quite a detailed overview of how the technology works and how it may be deployed, and the reader is directed to this paper as useful background for understanding the present invention.

[0009] The WBA's standardisation program arose from developments made by several companies who realised that radio transmissions of many kinds, not just Wi-Fi, could potentially be used to detect presence - and even gestures, biometrics, and possibly even be used for identification of individuals.

[0010] Among the companies most active in this area are Origin Wireless, who have patents and applications on wireless motion monitoring and object tracking using broadcasting (not just based on Wi-Fi signals), with priority dates as early as December 2012 - e.g. see US10,374, 863 "event recognition based on a wireless signal" and US10, 742, 475 "object tracking and sensing using broadcasting"; Aerial Technologies, who have patents and applications with priority dates as early as May 2015 - e.g. see WO2020/240,526 "proximity based model for indoor localization using wireless signals", US2020/296556 "Sensing Changes in an Environment Using Wireless Communication Signals", US11,082,109 "Self-learning based on Wi-Fi-based monitoring and augmentation", US11,043,094 "smart intrusion detection using wireless signals and artificial intelligence", and WO2021/081,365 "Using MIMO training fields for motion detection"; Tandem Launch Inc. who have patents and applications with priority dates as early as December 2015, e.g. see WO2017/106976 "Sensing Changes in an Environment Using Wireless Communication Signals"; and Cognitive Systems (Corp.) who have patents and applications with priority dates as early as May 2016, e.g. see US9,524,628 "Detecting signal modulation for motion detection", EP3796037 "Detecting signal modulation for motion detection", and WO2021/062,522 "Using MIMO training fields for motion detection". The reader is directed to these patents and applications (the contents of which are hereby incorporated by reference), along with others from these companies, as they variously explore different approaches to what may generally be referred to as radio-based sensing, and also explain how radio signals other than those from Wi-Fi networks can be used for movement (and hence presence) sensing. Generally, these methods involve the use of plural devices operating according to a common wireless standard, metrics being extracted from wireless signals transmitted and received by the devices. The characteristics of the communication channels experienced by the various wireless signals are first determined for a steady state condition (for example for an unoccupied space), and this background state will be disturbed by the presence and movement of any sizeable object within the monitored space due to changes in the reflection, scattering, and diffraction experienced by the wireless signals. These perturbations result in detectable changes in the wireless signals received by one or more of the wireless devices. Some of the approaches are closely allied with RADAR, but many propose the use of Channel State Information (CSI) or some variant thereof, RSSI measurement, etc.

[0011] Although various of these companies' patents and applications mention the possible application of some of these detection techniques to intruder detection, such technologies have largely yet to be deployed, at least in domestic and small-business security monitoring systems. Thus, currently, security monitoring systems that are commercially available predominantly continue to detect presence using line of sight detectors such as PIR sensors.

[0012] Embodiments of the present invention derive from the inventors' insight that enhanced security can be provided by a security monitoring system in an armed at home state through a different approach to using presence sensing - largely irrespective of the type of presence sensing used.

Summary

[0013] According to a first aspect there is provided a security monitoring system installation in a location, the location having a perimeter, the perimeter enclosing a first zone and a second zone distinct from the first zone, and one or more third zones adjacent the second zone and intermediate along a possible human route between the first and second zones, the second zone being accessible on a possible human route within the perimeter only via at least one of the one or more third zones; the security monitoring system including a sensing arrangement to detect human presence within the perimeter and the system having an armed at home state in which it is so configured that, in the event that: at a first instant human presence is detected in the first zone but not in any of the second or third zones; and subsequently, at a second instant, human presence is detected in the second zone without presence having been detected in any of the one or more third zones in the interval between the first and second instants; an alert is raised.

[0014] A zone is adjacent the second zone only if a person can pass from the zone into the second zone without needing to pass through a further zone.

[0015] According to a second aspect there is provided a security monitoring system installation in a location, the location having a perimeter, and the system including a sensing arrangement to detect human presence within a monitored area within the perimeter, the monitored area comprising a plurality of monitored zones, at least one pair of the monitored zones being remote from each other, each remote pair consisting of a first and a second of the monitored zones, human passage between the first and second zones of a pair that are remote from each other only being possible, within the premises, via at least

one intermediate zone that is adjacent the second zone of the pair, and the system having an armed at home state in which it is so configured that, in the event that: at a first instant human presence is detected in the first remote zone of the pair but not in any of the second or intermediate zones of the pair; and subsequently, at a second instant, human presence is detected in the second zone of the pair without presence having been detected in any of the one or more intermediate zones of the pair in the interval between the first and second instants; an alert is raised.

[0016] A PIR detector or other optical or line-of-sight sensor may be used to detect (or infer) presence in the third zone (e.g. a mix of line of sight and radio-based sensing), rather than requiring radio-based sensing in all three zones (first, second, and intermediate).

[0017] Also, sensing in the first and second zones may be done by different systems, even if these are both radio-based.

[0018] In installations according to the second aspect, the sensing arrangement to detect human presence within the perimeter may comprise a plurality of line-of-sight detectors, for example PIR detectors or other optical detectors.

[0019] In installations according to the second aspect, the monitored area may include a monitored zone that comprises multiple rooms, some at least of the rooms being linked by means of a hall, landing or walkway, at least one line-of-sight detector of the sensing arrangement being provided to monitor the hall, landing or walkway, and optionally some at least of the multiple rooms do not contain line-of-sight detectors.

[0020] In installations according to the second aspect, the sensing arrangement to detect human presence within the perimeter may comprise a radio-based system that is configured to sense presence and location based on detecting perturbations of radio signals. Optionally, the radio-based system may be configured to process communication signals received from one or more radio transmitters operating according to one or more communication standards or protocols.

[0021] Installations according to the second aspect may further comprise a control unit wherein the control unit includes a radio receiver of the radio-based presence and location sensing system. Optionally, the control unit is configured to process radio signals to derive location and presence data in respect of monitored zones.

[0022] In installations according to the second aspect, optionally the sensing arrangement to detect human presence uses changes in channel state information or received signal strength in determining presence.

[0023] In installations according to the second aspect, the control unit may function as an access point of a radio network whose signals are used by the radio-based presence and location sensing system, and optionally the radio network is a Wi-Fi network.

[0024] In installations according to the second aspect, the sensing arrangement to detect human presence within the perimeter may further comprise one or more line of sight detectors, for example PIR detectors.

[0025] According to a third aspect there is provided a control unit for a security monitoring system for premises, the control unit comprising a processor, a memory communicatively coupled to the processor and a set of instructions stored in the memory which when executed by the processor cause the control unit to: determine an alert condition after entering an armed at home single occupancy mode, by determining the location of an occupant within the premises; storing the determined location as a current location of the occupant; receiving sensing data; determining a new location based on the sensing data comparing the new location with the stored current location; if the new location is neither the same as the stored current location nor a location adjacent the stored current location, raising an alert; if the new location is the same as the stored current location or is a location adjacent the stored current location, setting the new location as the current location of the occupant.

[0026] A control unit according to the third aspect may further comprise a radio transceiver communicatively coupled to the processor, wherein the processor is configured to derive the received sensing data from radio signals received by the transceiver.

[0027] In a control unit according to the third aspect the processor may be configured to determine location based on signals received from one or remote nodes of the security monitoring system, the one or more remote nodes including at least one line-of-sight presence detector.

[0028] In a control unit according to the third aspect the processor may be configured to raise an alert in the event that received sensing data reveal human presence at more than one location, and hence the presence of more than one person, within the premises

[0029] The real time, always on nature of the systems and methods according to embodiments of the invention allows for an always on armed home experience that follows you around (especially for solo occupants). As you move multiple rooms away, the central unit can have sensors automatically swap in and out of alarm triggering. The sensors will always report events (like motion), but the central unit will fuse these data together with real time presence to determine if it should act on it or not.

[0030] According to a fourth aspect there is provided a method of detecting an intrusion in premises protected by a security monitoring system installation, the premises having a perimeter, the perimeter enclosing a first zone and a second zone, and one or more third zones adjacent the second zone and intermediate along a possible human route between the first and second zones, the second zone being accessible on a possible human route within the perimeter only via at least one of the one or more third zones;

the method comprising at a first instant detecting human presence in the first zone but not in any of the

second or third zones;
at a second instant, after a time interval
detecting human presence in the second zone; and
determining an alert condition if presence was detected in none of the one or more third zones in the time interval between the first and second instants.

[0031] According to a fifth aspect there is provided a method of detecting an intrusion in premises protected by a security monitoring system installation, the premises having a perimeter and a monitored area within the perimeter, the monitored area comprising a plurality of monitored zones, at least one pair of the monitored zones being remote from each other, each remote pair consisting of a first and a second of the monitored zones, human passage between the first and second zones of a pair that are remote from each other only being possible, within the premises, via at least one intermediate zone that is adjacent the second zone of the pair: the method comprising monitoring the monitored area to detect human presence; at a first instant detecting human presence in the first remote zone of the pair but not in any of the second or intermediate zones of the pair; and at a second instant, after a time interval detecting human presence in the second zone of the pair; and determining an alert condition if presence was detected in none of the one or more intermediate zones of the pair in the time interval between the first and second instants.

[0032] According to a sixth aspect there is provided a method of detecting an intrusion in premises protected by a security monitoring system installation, the method comprising: entering an armed at home single occupancy mode; determining the location of an occupant within the premises; storing the determined location as a current location of the occupant; receiving sensing data; determining a new location based on the sensing data comparing the new location with the stored current location; if the new location is neither the same as the stored current location nor a location adjacent the stored current location, raising an alert; if the new location is the same as the stored current location or is a location adjacent the stored current location, setting the new location as the current location of the occupant.

[0033] According to a seventh aspect there is provided a method of detecting an intrusion in premises protected by a security monitoring system installation the method comprising: entering an armed at home single occupancy mode; determining the location of an occupant within the premises based on received *sensing* data; storing the determined location as a current location of the occupant; receiving new sensing data relating to the location of an occupant; determining a new location based on the new sensing data comparing the new location with the stored current location; if the new location is neither the same as the stored current location nor a location adjacent the stored current location, raising an alert; if the new location is the same as the stored current location or is a location adjacent the stored current location, setting the new location as the current location of the occupant.

[0034] The invention has particular, but not exclusive application to security monitoring systems for domestic premises.

Brief description of the drawings

[0035] Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a schematic plan of a single floor of premises in which a security monitoring system has been installed;
Figure 2 is another schematic plan which illustrates limitations of line of sight sensing;
Figure 3A-3C illustrate schematically an arrangement of motion sensors in multi-storey premises;
Figure 4 illustrates schematically features of the local management device of a security monitoring system of Figures 1 and 2;
Figure 5 illustrates schematically the principles of radio-based presence and location sensing;
Figure 6 corresponds to Figure 1 but additionally showing multiple sources of radio signals for use in a radio-based presence and location sensing system based on detecting perturbations of radio signals;
Figure 7 corresponds to Figure 2 but additionally showing multiple sources of radio signals for use in a radio-based presence and location sensing system based on detecting perturbations of radio signals;
Figure 8 illustrates schematically features of the local management device of the system of
Figure 6; and
Figure 9 is a flow chart of a method according to an embodiment of the invention.

Specific description

[0036] Figure 1 shows schematically a security monitoring system installation 100 in a location, in this case a dwelling, having a perimeter. In this example, the dwelling is a semi-detached or terraced house with a shared (party) wall to the left of the figure, a front wall or façade 102 including a front door 104 that serves as the main entrance to the premises, a side wall and a rear wall (here shown as staggered). The figure shows just one floor of the dwelling, in this instance a ground floor, which accommodates what may be termed the living space - as opposed to the sleeping space which is provided on one or more other (upper) floors accessed via stairway 105. The living space includes an entrance hall 106, onto which the front door 104 opens, off which are a rear living room 108, a front dining room 110, and a rear kitchen 112.

[0037] The kitchen 112 includes the back door 114 of the premises. The front 104 and back 114 doors are each provided with a sensor arrangement 116 that is triggered by the opening of the relevant door - for example, a sensor

arrangement 116 including a magnetically triggered sensor such as a reed relay or a magnetometer.

[0038] The living room 108 is provided with glazed doors 118, which may be in the style of "French Windows" or the like, which permit access to a rear garden, but which are not intended, or used, for regular access to the interior of the premises. Consequently, these glazed doors 118 are preferably provided with bolts or similar security fasteners on their inner side - so that they cannot readily be opened from outside when the bolts are secured. These doors 118 may not be provided with any sensing arrangement to detect their opening (to reduce the cost of installing the security monitoring system). Similarly, windows 120 to the kitchen 112 and dining room 110 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.

[0039] The security monitoring system includes a controller or central unit 122 which is operatively coupled to the door opening sensors 116 and any other sensors of the system preferably wirelessly using radio frequency (RF) communication rather than via a wired connection. In addition, the central unit 122 is operatively connected, for example via a wired and/or wireless Internet connection, to a remote monitoring station 200 to which alarm events are communicated for review and for appropriate intervention or other action to be taken - and preferably the remote monitoring station 200 (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).

[0040] The security monitoring system also includes one or more motion sensors, such as a PIR sensor. In the illustrated example, motion sensors 124 are shown as being installed in each of the rooms (108, 110, 112), and in the hall 106, with another motion sensor optionally being provided to monitor the stairs 105 that lead to the upper floor(s).

[0041] Preferably, as shown, the security monitoring system includes at least one camera 126, preferably a video camera with an associated (integral or separate) motion sensor, activation of which may cause the camera (or the motion sensor) to report an event to the central unit. In response, the central unit 122 may or may not instruct the camera 126 to transmit images (still or video) to the central unit for onward reporting to the CMS 200.

[0042] The security monitoring system also includes a user interface or control panel 128 in the hall 106 fairly close to the front door 104. This control panel 128 is provided so that a user can arm and disarm the security monitoring system using either a code or PIN (e.g. a 4 or 6 digit PIN) or a token (using e.g. RFID, NFC, BTLE, technology or the like). The control panel may also be used to set the security monitoring system to an armed at home state, optionally directly from an armed away state. The control panel 128 preferably includes a visual display, such as a screen (optionally a touch sensitive display) to provide users with system information, status updates, event reports, and even possibly face to face communication with personnel in the central monitoring station (for which purpose the control panel 128 may have a built in video camera and optionally lighting). Although the same type of user interface may also be provided adjacent the back door (within the premises), typically a rather simpler device - known as a disarm node 130, may be provided to enable a user to disarm or arm the system, again optionally using a PIN, code, or dongle/device. Such a disarm node 130 may include one or more indicator lights, featuring e.g. RGB LEDs, to provide visual feedback on arming status (armed away, armed at home (and possibly other armed states), alarm event status, as well as at least an audio source to provide warning and advisory tones or messages. Preferably the disarm node includes both an audio source (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 needs be. Like the sensors 116 and 124, the control panel 128 and disarm node 130 are preferably provided with at least one radio transceiver for communication with the control unit 122, as well as having at least built in autonomous power supplies (e.g. each having a battery power supply). The various nodes of the security monitoring system, other than the central unit 122, are preferably battery powered and communicate using RF transceivers that consume little power (hence, not relying on Wi-Fi, 802.11... protocols, as these tend to be very power hungry) and that typically rely on radio frequencies in approved ISM frequency bands - such as between 860 and 900 MHZ

[0043] Conventionally, when such a security monitoring system is in the disarmed state, opening of the front or back doors, or triggering any of the motion sensors 124 doesn't constitute an alarm event. The relevant sensor 116, 124 may be configured to report a sensed event to the central unit 122 irrespective of the arm state of the security monitoring system, but the central unit 122 will disregard such reported events when the system is disarmed. In the fully armed state, which may be termed the "armed away" state, event notifications from perimeter sensors (in the illustrated example the door opening sensors 116 on the front 104 and back 114 doors, but typically also including one or more sensors to detect the opening of a window 120) and internal movement or presence sensors, typically result in the central unit 122 determining an alarm event which may be reported to the central monitoring station.

[0044] Typically, the security monitoring system also

has a second armed state in which only the security of the perimeter is monitored - so that only events reported by one or other of the door sensors 116 (or window sensors if present) count as potential alarm events to be reported by the central unit 122 to the central monitoring station - and this may be termed the "armed at home" state. The armed at home state is intended to be used when the premises are occupied. In the armed at home state the central unit 122 will routinely be arranged not to request any internal (video) camera to share images with the central unit 122 - so that user privacy is maintained.

[0045] There may be more than one variant of the armed at home state - so that, for example during the daytime only the perimeter may be monitored, but at night (or upon the occupants retiring to bed) the system may be set to an armed at home (night) state in which movement within the living accommodation can also give rise to an alarm event potentially to be reported to the CMS 200 (including images from any camera within the monitored zone)- but the triggering of any movement sensors for the sleeping accommodation will not give rise to alarm events.

[0046] As previously mentioned, embodiments of the present invention derive from the inventors' insight that enhanced security can be provided in an armed at home state through a different approach to presence sensing.

[0047] Looking again at Figure 1 it can be observed that for someone within the perimeter to pass between any of the rooms (living room 108, kitchen 112, dining room 110 but which may also be referred to as zones 1, 3, and 4 respectively) it is necessary to pass through the hall 106 (or zone 2). In an installation in which it is possible to determine presence in multiple (preferably each) of the zones it may be possible to generate a useful alarm event based on a sequence of events in which (human) presence is detected at a first instant in one of the zones but not in any of the other zones and subsequently, at a second instant, human presence is detected in the second zone without presence having been detected in the third zone in the interval between the first and second instants.

[0048] So, for example, suppose that someone comes home to an empty house, and disarms the security monitoring system from an armed away state and then sets the security monitoring system to a (daytime) armed at home setting, for example using the control panel 128 (which may be powered just by an internal power supply, such as a battery power supply, but may be mains powered with battery back up) by the front door 104. The system may be configured to provide the user with the option to go straight into the armed at home state from the armed away state, or may require the user first to disarm the system, and then to select the (or one of two or more) armed at home state.

[0049] The user then starts work in the kitchen (zone 3) preparing a meal. The presence of the person preparing the meal in the kitchen is detected by the zone 3 presence detector (in this case the PIR sensor 124 in the kitchen). As the person moves around the kitchen, his or her presence continues to be detected by the relevant PIR sensor.

[0050] Meanwhile, the rest of the home is empty. Thus, the central unit is aware of presence in Zone 3 and also, due to the lack of signals from the presence sensors in zones 1, 2, and 4, the absence of presence in those other zones.

[0051] Now suppose that an intruder enters the house through the French windows 118 in the living room 108 (zone 1) - the French windows 118 having unintentionally been left unlocked or locked but not bolted. The presence of the intruder in zone 1, the living room 108, is detected, for example by means of a PIR sensor 124 in the living room 108, and the central unit 122 is informed of this development. The central unit 122 is aware of the (previous and continuing) presence in zone 3 but is also aware that between the last presence update (e.g. as the result of movement being detected in the kitchen) in respect of zone 3 and the new presence report in zone 1 there has been no presence reported for zone 2. The only entrance to the living room 108, other than via the hall, is through the French windows 118 which are normally locked and bolted - and which are therefore not an accepted point of entrance. The central unit 122 can therefore deduce that an intruder is present and raise an alarm with the CMS - and optionally with one or more local alarm indicator (alarm sounder, flashing lights, etc.) to warn the person who is already legitimately present.

[0052] Conversely, if entrance is effected through the front door 104 (or even through the back door 114 if this is an accepted entrance point), the relevant door sensor 116 will be triggered before a new presence is detected. The central unit 122 will therefore cause a challenge or warning to be issued - for example, by means of the control unit 128 (if entrance is via the front door) or by means of the disarm node 130 (if entrance is via the back door) to the person entering that the system is armed and will need to be disarmed (by entering a code at a user interface 128 or 130, or by presenting a dongle or token to a reader 128 or 130) within a predetermined disarm period in order to avoid an alarm event being raised with the CMS 200. If the person entering through the accepted entrance point is authorised, they will be able to disarm the system, but otherwise an alarm event will be raised - as is conventional.

[0053] If the person preparing a meal in the kitchen leaves the kitchen to go into the living room (zone 1), the dining room (zone 4), or to go upstairs (via zone 5), they must first enter the hall (zone 2) where their presence will be detected by the relevant presence sensor 124. The central unit will therefore receive a presence update from zone 2 before receiving a presence update from any of the other zones (1, 4, or 5), but having previously been aware of presence in zone 3, a new report of presence in zone 2 does not constitute an alarm event, and therefore the central unit does not report the change to

the CMS 200.

[0054] The central unit 122 of the security monitoring system is preferably configured by an engineer when the system is first installed so that the various zones within the premises are defined, each typically based on the relevant presence detector, and the possible zone sequences are also defined. The installation engineer can be provided with an appropriate app on a smart phone or other device which can communicate with the central unit, typically via a supplier back-end server, the app preferably having a graphical interface which allows the engineer either to couple the various zones into allowable sequences or to specify any sequences that are not allowed. With the security monitoring system installation illustrated in Figure 1 every allowable sequence moves from a zone other than zone 2 into zone 2. But it will be recognised that other room arrangements, especially those in which some rooms have multiple entry/exit points, may make possible numerous alternative routes between different zones or different rooms.

[0055] The central unit 122 is preferably configured in an armed at home state to maintain a presence state for each monitored zone of the premises, so that presence state information is available for each zone. The system does not need to be able to "see" an occupant in a zone to be aware of their presence, as long as the system is so configured that it is impossible for a person to move from one zone to another undetected. The system also copes with multiple "authorised" occupants being present simultaneously without needing to count the occupants and without needing to be told the number of occupants. So, for example, suppose that a parent and child come home and enter through the front door. If the security monitoring system is armed it will need to be disarmed, and then set to armed at home (or if allowed, transitioned directly from armed away to armed at home). If the armed at home setting is chosen from the control panel 128 in the hall, presence can be inferred from the disarming/arming activity at the control panel, as well as established by activation of the hall motion/presence sensor. If the parent and child both go into the kitchen, their arrival in the kitchen will be detected by the kitchen presence sensor. But suppose that the child wants to go to their bedroom while the parent remains in the kitchen, then the kitchen presence sensor will continue to be triggered by the presence of the parent while first the hall motion sensor and then the stair motion sensor are triggered. Even in the absence of presence sensors on the upper floor(s) the system can infer that someone has gone upstairs - and is no longer on the stairs, because the stair presence sensor is no longer being triggered and also because the sensed presence sequence was hall - stairs-absent, rather than hall-stairs-hall (as it would have been if, for example, the child had mounted the stairs to retrieve something left on the stairs. The system can store an "upstairs" status in the event of such a hall-stairs-absent sequence. Then, if subsequently the system detects a new presence on the stairs followed by the detection of presence in the hall, no alarm may be triggered. But, the system may still be configured to trigger an alarm in the event of a new presence on the stairs that doesn't follow on from detection of presence in the hall if no hall-stairs-absent sequence has been detected since the system was put into the armed at home status.

[0056] Also, the system may be configured to operate on the basis that if the system was in the armed away status shortly before being put into the armed at home status, it may be considered safe to assume that no intruder is lurking on an upper floor.

[0057] Depending on the layout of the premises, and the likelihood of an intruder gaining unlawful access to the premises via an upper floor, it may be considered that the likelihood is so low that an alarm event is not triggered in the event that presence is detected on the stairs when no presence has been detected in the hall. If the threat of a break in on an upper floor is significant, then preferably at least one motion/presence detector is provided on the relevant upper floor.

[0058] A single zone may also include more than one room or may include part where presence can be monitored and part where presence cannot be monitored. Examples of such a situation is illustrated in Figure 2. Figure 2 corresponds very closely with Figure 1, but includes architectural features that mean that some zones have parts where presence cannot be monitored by the presence sensor allocated to the relevant zone. For example, the kitchen, zone 3, now includes a walk-in pantry 212 (for the storage of food, wine, kitchen equipment, etc.) which can only be entered via a door that opens into the kitchen. If someone enters the pantry, they must do so from the kitchen, and the presence sensor 124 for the kitchen will detect their presence until they enter the pantry. Once inside the pantry 212, the person is no longer visible to the kitchen presence sensor 124. In the armed at home state previously described, where the occupant has been working in the kitchen, the central unit 122 is aware of presence in the kitchen up until the point that the user enters the pantry. The kitchen presence sensor will then stop sending "presence detected" signals to the central unit, but the central unit will also not receive any signal from the back door sensor 116, nor from the hall presence sensor. Eventually, the person will emerge from the pantry, once again triggering the kitchen presence sensor. No alarm condition exists because the central unit 122 has a record (i.e. the central unit 122 "knows") of the last detected presence having been in zone 3 (the kitchen). But if, while the cook is in the pantry, an intruder enters the living room , zone 1,via the French windows 118 as before, the central unit 122 will trigger an alarm because the zone presence sequence Zone 3- Zone 1 is not permitted.

[0059] A similar situation may arise with the user entering the cloakroom 222 illustrated as being installed under the stairs 105, and accessible only from the hall 106 (zone 2). The hall presence sensor 124 is capable of detecting human presence of anyone in the hall itself,

the understairs cloakroom is not "seen" by the sensor, so that when someone enters the cloakroom from the hall, the central unit is aware of presence in zone 2 but then ceases to receive updated "presence detected" reports from the hall presence sensor. But as long as no presence is detected in any of the other zones, and as long as the sensor 116 for the front door doesn't report a door opening event, the central unit still has a record of "last reported presence" as being zone 2. Thus, when the person emerges into the hall 106 from the cloakroom, the central unit sees no change in presence location, and no alarm is raised.

[0060] In this case, the central unit may be programmed to take account of the fact that the pantry represents an "invisible" portion of zone 2 - in that if the central unit receives a report of presence in zone 2 and then, without receiving a door open event report from front door sensor 116, receives no presence report from any of zones 1, 3, 4, or 5, within a predetermined interval, the central unit assumes unseen user presence in zone 2. If the hall presence sensing arrangement is such that when the user leaves the cloakroom they will trigger the hall presence sensor before they can enter any other zone, the central unit can be arranged to trigger an alarm event if an intruder enters the living room while someone is in the cloakroom (assuming that the system is in the relevant "armed at home" setting) because in effect we have an unallowable zone transition. Clearly such a situation may require more careful positioning and targeting of presence detectors, as well as appropriate extra programming of the central unit, but it may avoid the need to provide an extra presence sensor in or for the cloakroom (which would be a possible alternative) to make the cloakroom a further zone. It will also be appreciated that in this cloakroom example the turning on of a light within the cloakroom may be taken as an indication of presence in the cloakroom, although in practice that may only work reliably as an indication of the cloakroom being entered - as the light may inadvertently be left on - although again, as anyone leaving the cloakroom should be detected by the hall presence detector, the person will again be seen by the central unit as having emerged into zone 2.

[0061] Complications may arise if there are zone areas (such as the pantry or cloakroom) or zones (e.g. upstairs) where presence cannot be detected, and we have multiple "authorised" occupants, because one of multiple occupants in a given zone may enter a hidden area of the zone (e.g. enter the pantry from the kitchen) while the other occupant leaves the kitchen for the living room, via the hall. When the person leaves the pantry they will once again be seen as present in the kitchen - which may trigger an alarm if the other occupant is by now in the living room. To avoid this situation, we can configure the system to count the number of people (possibly just categorising a count as "one" or "many") entering or within each monitored zone, and then use these data to determine if someone has stayed behind in a zone while someone else has moved to another zone. We may also configure the system so that a user arming the system to armed at home has the option of selecting "single occupant" or "multiple occupants", so that the system can provide an appropriate response more rapidly particularly in the case that there is only a single (authorised) occupant - as this may be the situation that most worries many occupiers. If the system knows that there are multiple legitimate occupiers, it can configure itself to keep track of multiple occupants, hopefully avoiding false alarms. Whereas, if the system knows that there is only a single legitimate occupant any unexpected presence may be treated as an alarm or alert condition.

[0062] The central unit may be further configured to use data from the radio-based location sensing arrangement to perform people counting, and optionally to use determine the presence of one or more intruders based on a detected change in the people count when the system is in the nocturnal armed mode. For example, the techniques and methods described in US2020/0302187A1, assigned to Origin Wireless, can be used to count occupants and determine their locations in installations, systems and methods according to embodiments of the invention

[0063] It will be appreciated that premises or dwellings with fewer zones and/or fewer rooms may be protected in the same way but with fewer presence sensors - generally just one such sensor per zone.

[0064] Because we are primarily interested in detecting human presence, rather than simply detecting movement, steps are preferably taken in situations where animals (e.g. pets) or machines (automated fans, robot vacuum cleaners, or other machines that may trigger a kind of motion sensor used in the installation) can be expected to move within or between monitored zones. So called "smart" PIRs exist which can distinguish between pets and humans, and these may also distinguish between humans and things like robot vacuum cleaners. Machine learning or other AI-assisted systems may also be used to discriminate between pets and humans, and between humans and non-humanoid robots (and currently the incidence of humanoid robots in the domestic setting is extremely rare).

[0065] It can be seen that configuring a security monitoring system to trigger alarm events, in an armed at home setting, based on impermissible zone sequences may provide enhanced security without necessarily needing to install additional perimeter sensors. Conventionally, security monitoring systems rely exclusively or almost exclusively on perimeter sensors (typically just for doors, windows and the like) to detect alarm events. Whereas security monitoring systems according to embodiments of the present invention are capable of detecting further alarm conditions based on presence detection rather than relying on detecting breaches in a secured perimeter.

[0066] Figures 3A and 3B show schematically a three-storey building or dwelling (which may be a subset of a larger building) which illustrates an application of embod-

iments of the invention. Figure 3A is a schematic floor plan of one floor (here the ground floor, for example), showing an arrangement of rooms 301 - 306 that are linked by a common access corridor or hallway 307. It can be assumed that each of the rooms 301-306 has a door, but these are omitted for clarity. The hallway has a line-of-sight movement (presence) sensor 308, which may conveniently be ceiling mounted so that the sensor can detect any human presence in the hallway 307. The hallway 307 leads to stairs 105 that lead to the first floor 310. Above the stairs 105 is mounted another presence sensor 309 which is arranged to detect any human presence on the stairs 105. The layout of each of the other floors may be assumed to be the same, although clearly a different disposition of rooms around the common hallway can be provided.

[0067] The ground floor has front and back doors 104 and 114, together with a control unit 128 adjacent the front door, and a disarm node 116 in the kitchen 304 adjacent the back door 114. A central unit 122 of a security monitoring system according to an embodiment of the invention, which may correspond generally to the system described with reference to Figure 1, is provided in one of the rooms 306.

[0068] It will be noted that none of the rooms 301 to 306 is shown to include a movement sensor. Instead, the idea is that the motion (presence) sensor 308 in the hall 307 will detect the presence and movement of anyone in the hall 307, including anyone emerging from any of the rooms 301-306. In effect, the ground floor hallway constitutes a monitored zone of which the rooms 301-306 are concealed areas. Anyone using the stairs 105 to access the first floor 310 will enter a second zone, monitored by the stair movement/presence sensor 309. Anyone who comes up the stairs 105 must enter a third monitoring zone overseen by the movement/presence sensor 319 of the first-floor hallway before they can enter any room on the first floor, or before they can reach the second set of stairs 205 that leads from the first floor 310 to the second floor 320. The second set of stairs 205 is within a fourth monitoring zone overseen by the presence/movement sensor 329, and on the second floor the hall constitutes a fifth monitoring zone overseen by the second-floor hall presence/motion sensor 339. Later we will describe radio-based sensing that can be used as an alternative (or complement) to line-of-sight sensing such as PIRS, and such an approach may have the benefit of enabling presence sensing in all or most of the rooms on any given floor without the need to provide a line-of-sight sensor in each room in respect of which presence sensing is required. But the arrangement illustrated here can still provide usefully enhanced security in armed at home states, particularly for armed at home sole occupancy, while using a low device count and hence reduced installation costs.

[0069] Figure 3C is a schematic floorplan showing premises having another kind of room/zone arrangement in which there are two independent, non-overlapping, routes between a pair of zones (here, zones 1 and 4). A room 1 has two doors, 350, 351, the latter of which opens onto a second room, room 2, which has a further door 352 which opens into a third room, room 3, which has a further door that opens into a further room, room 6. The other door, 350, in the first room, opens onto a corridor off which are two rooms, rooms 4 and 5. The corridor has a door 357 that opens into room 6, which itself has an external door 356 which provides external access into the premises. Each of the rooms has a window 120, and room 1 also includes a French window 118. The premises has a central unit 122 which provides a security monitoring system for the premises, and to which several line-of-sight presence/movement sensors 370, 372, 373, 376, and 377, in zones 1, 2, 3, 4, and 5 are wirelessly coupled along with the door sensor 116, and control unit 128, which are both associated with the external entrance door 356. It can be seen that there are two exits from zone 1, one which opens into the corridor that leads to zone 4, and the other of which leads into zone 2 which in turn leads into zone 3 and thence into zone 4. Thus, each of zones is adjacent two other zones and there are two exits from every zone.

[0070] If the security monitoring system is set into an armed at home state, the central unit 122 can track the movement of the occupant(s) through the various zones provided by the presence/movement sensors. If someone passes from zone 5 into room 4 or room 5, the central unit will continue to record their presence in zone 5 until their presence is detected by either sensor 370 or sensor 374 after once again having been detected by sensor 375. In an armed at home state, if the security monitoring system holds a single current location, e.g. in zone 1, there are two adjacent zones - in this case zone 2 and zone 5, and two remote zones, in this case zones 3 and 6. If the next presence report received is for one of the adjacent zones no alert is raised unless the system is in armed at home single occupancy and presence continues to be detected in zone 1 - which would indicate presence of at least two people. But if the next presence report received is for a remote zone, the system will raise an alert - for example reporting an event to the central monitoring station and optionally providing an alert (local and/or pushed) to warn the existing occupants of the premises of the detection of a suspected intruder in a named zone or room.

[0071] Figure 4 is a schematic drawing showing in more detail features of the gateway or central unit 122 of Figures 1 and 2. The gateway 122 includes a first transceiver 430 coupled to the first antenna 480, and optionally a second transceiver 432 coupled to a second antenna 482. The transceivers 430 and 432 can each both transmit and receive, but a transceiver cannot both transmit and receive at the same time. Thus, the transceivers 430, 432 each operate in half duplex. Preferably a transceiver will use the same frequency to transmit and receive (although of course if the two transceivers are to operate simultaneously but in opposite modes, they will operate

on different frequencies). The transceivers 430, 432 may be arranged such that one transceiver 430 uses a first frequency for transmit and receive and the second transceiver 432 uses the same first frequency for transmit and receive, i.e. the transceivers are arranged to operate in a diversity-like arrangement. Alternative, the second transceiver may, depending on configuration, be arranged to use a second frequency for transmit and/or receive. The transceivers 430 and 432 are coupled to a controller 450 by a bus. The controller 450 is also connected to a network interface 460 by means of which the controller 450 may be provided with a wired connection to the Internet and hence to the monitoring centre 200. The controller 450 is also coupled to a memory 470 which may store data received from the various nodes of the installation for example event data, sounds, images and video data. The central unit 122 also includes a crystal oscillator 451, which is preferably a temperature controlled or oven-controlled crystal oscillator. This is used for system clocking and also frequency control of the transceivers. The gateway 122includes a power supply 362 which is coupled to a domestic mains supply, from which the gateway 122 generally derives power, and a backup battery pack 464 which provides power to the gateway in the event of failure of the mains power supply. Preferably, as shown, the central unit 122 also includes a Wi-Fi transceiver 440, and associated antenna arrangement 442, which may be used for communication with any of the nodes that is Wi-Fi enabled. The Wi-Fi enabled node may be a remote control or control panel that may for example be located close to the main entrance to the building (e.g., control panel 128 or disarm node 130) to enable the occupier to arm or disarm the system from near the main entrance, or it may for example be an image-capture device such as a video camera (e.g. camera 126). Similarly, an interface enabling bidirectional communication over a Public Land Mobile Network (PLMN), such as GSM or L TE, may optionally be provided. Optionally, a third antenna 484 and associated ISM transceiver 434 may be provided, for example for communication with the monitoring centre 200 over, for example, the European 863MHz to 870MHz frequency band. Optionally, the third transceiver 434 may be a Sigfox transceiver configured to use the Sigfox network to contact the central monitoring station especially in the event that jamming of other radio channels is detected.

[0072] The first 430 and second 432 transceivers may both be tuneable ISM devices, operating for example in the European 863MHz to 870MHz frequency band or in the 915MHz band (which may span 902-928MHz or 915-928MHZ depending upon the country). In particular, both of these devices may be tuned, i.e. may be tuneable, to the frequencies within the regulatorily agreed 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.

[0073] We will now provide a brief introduction to radio-based presence detection, for example 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 may operate in non-telecommunications or Industrial, Scientific and Medical (ISM) spectral regions without departing from the scope of the invention.

[0074] Essentially the idea is to use radio signals to probe the zone or zones of interest, and to analyse and extract statistics from these signals, in particular looking at the physical layer and/or data link layer such as MAC address measurements that expose the frequency response of a radio channel (e.g., CSI or RSSI measurements). These measurements are processed to detect anomalies and variations over time, and in particular to detect changes signifying the entrance of a person and/or movement of a person within a monitored zone. The zone(s) to be monitored need to be covered sufficiently by radio signals, but the sources of the radio signals may either already be present before a monitoring system is established - for example from the plurality of Wi-Fi or Bluetooth capable devices that are now dotted around the typical home or office, or the sources may be added specifically to establish a monitoring system. Often some established (i.e., already located or installed) radio devices are supplemented by some extra devices added as part of establishing a radio-based presence detection system. Among the types of devices (preinstalled or specifically added) that may be used as part of such a detection system are Wi-Fi access points, Wi-Fi routers, smart speakers, Wi-Fi repeaters, as well as video cameras and video doorbells, smart bulbs, etc. Because presence (or intrusion) is detected by detecting a change in the properties or character of radio signals compared to some previous reference signal(s), it is preferred to establish what might be termed the monitoring network between radio devices that are essentially static (i.e., that remain in the same position for extended periods) rather than relying on devices that are repeatedly moved - such as smart phones, headphones, laptops, and tablet devices. It is not strictly speaking essential for all the devices whose signals are used by the monitoring system to be part of the same network - for example, signals from Wi-Fi access points of neighbouring premises could be used as part of a monitoring system in different premises. Again, a primary consideration is the stability of the signals from the signal sources that are used. Wi-Fi access points provided by broadband routers are seldom moved

and rarely turned off, consequently they can generally be relied upon as a stable signal source - even if they are in properties neighbouring the property containing the zone or zones to be monitored.

[0075] 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.

[0076] 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 is 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.

[0077] 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.

[0078] The system may need to be retrained for the base setting if bulky furniture (or if a large metal objects) is 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 is 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.

[0079] Although the Figure 5 example uses just a single source (illuminator) and a single receiver, as already mentioned often 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 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.

[0080] Figure 6 corresponds closely to Figure 1 but in this embodiment radio-based presence detection is used instead of relying on zone-specific presence detection

as described with reference to Figures 1 and 2. The radio-based presence sensing, which may conveniently be based on the monitoring of Wi-Fi signals, and which for convenience we will refer to as WFS, is here performed by the central unit 122 which operates as a Wi-Fi Access Point (AP) and which serves as a Wi-Fi sensing receiver. The Figure shows the presence of various radio transceivers that are used to provide radio-based presence detection in place of the conventional presence/movement detectors 124 that were used in each of the interior zones of the premises of the Figure 1 embodiment.

[0081] To ensure that the WFS effectively covers the whole area of interest (for example, the whole ground floor of the premises) we need to provide a sufficient number of suitable located Wi-Fi stations (STAs) as WFS illuminators so that Wi-Fi signals received at the central unit AP 122 traverse the whole area of interest. 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 with mains powered equivalents - so, for example, a battery powered (video) camera such as 126 might be replaced by a mains powered equivalent 626, and battery powered control unit 128 may be replaced by a mains powered equivalent 628 that is Wi-Fi capable (although the control unit may still use something other than Wi-Fi to communicate with the central unit).

[0082] 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.

[0083] The central unit AP 122 preferably works in infrastructure mode in conjunction with the various other Wi-Fi stations (STAs) to form either an infrastructure Basic Service Set (BSS) or, in conjunction with another AP connected to the same Local Area Network as the central unit 122 - such as broadband router 600, to provide an Extended Service Set (ESS).

[0084] For ease of explanation, we will assume initially that the central unit AP 122 provides just a BSS and not an ESS, and that only the central unit AP 122 serves as a Wi-Fi sensing receiver. Some or all of the STAs in the BSS act as illuminators to provide signals which the CU 122 analyses in order to perform WFS. As shown, these other STAs include the broadband router 600 in the dining room, the control unit 628 and a Wi-Fi-enabled camera 626 in the hall, and optionally the disarm node 130 in the kitchen. Preferably, because of the power consumption concerns, both the Wi-Fi enabled camera and the disarm node 130 are fed with power from a mains electricity supply as well as having an autonomous internal power supply. In addition, both the kitchen and the living room are provided with an STA in the form of for example a "smart plug" 610, 612. If the disarm node 130 only has an internal power supply, and is not mains fed, it may not be configured as a Wi-Fi STA but instead some other Wi-Fi STA device 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.

[0085] With the arrangement shown in Figure 6 the control unit 122 (or more generally the security monitoring system, given that some entity other than the central unit may be responsible for determining presence and location of presence) is configured, when in an armed at home state, to use the radio-based presence sensing to detect and locate presence within the monitored area(s). So, as described with reference to Figures 1 and 2, when an occupant comes home to the premises and puts the system into an armed at home state, the central unit starts to sense presence and the location of presence. As a first step, the system may infer presence in the hall, zone 2, if the occupant used the control panel 128 to put the system into the armed at home state. Similarly, if the system is put into the armed at home state using the disarm node 130 in the kitchen, the system may infer presence in the kitchen.

[0086] The system (typically the central unit) 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) will start to receive 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. Suppose that once again our newly arrived occupant goes first to the kitchen from the hall, with the intention of preparing a meal. The system will detect the arrival of the person in the kitchen as well as detecting their exit from the hall. These data, and their timings, are recorded in the database. At this point, the system (e.g the central unit) is aware that there is presence in the monitored area, and that this presence is of one person in zone 3 (the kitchen). Now suppose that, while the meal is being prepared in the kitchen, an intruder gains access to the living room (zone 1). The arrival of the intruder in the monitored area will be detected by the radio-based sensing arrangement and the system (e.g. central unit) will now be aware that there is human presence in zone 1, but that this presence has been detected without any presence having been detected in zone 2 since presence was last detected in zone 1. The system is therefore able to determine that the person present in zone 1 is not the person who was previously known to be in zone 3. The system (e.g central unit) can therefore raise an alarm - either by signalling the remote central monitoring station, or by pushing a notification to the authorised user(s) of the system e.g. by sending a message to a back end server of the security monitoring system, or by triggering an audible alarm at the premises (optionally via a voiced

announcement from one or both of the control panel 128 or the disarm node 130), or some combination of these. The message pushed to the (devices of the) authorised and/or that sent to the remote monitoring station 200 may specify that the alert has been triggered by an unexplained presence in zone 1 (the living room) while presence had been/was detected in zone 3, without any presence having been detected in zone 2 before the detected presence in zone 1.

[0087] Figure 6 only illustrates a single floor of premises, but it will be appreciated that if it is desired to provide a WFS capability for other floors of the premises it will be necessary to ensure suitable Wi-Fi network coverage those floors, typically by providing a corresponding access point and a plurality of Wi-Fi STAs 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 a WFS system.

[0088] Figure 7 corresponds generally to Figure 2, and includes a pantry 712 in zone 3, and a cloakroom 722 in zone 2, but this time the installation is configured, like the installation of Figure 6, to use radio-based sensing such as Wi-Fi sensing. A Wi-Fi extender 700 is here shown as present in the pantry, but is primarily provided to improve the radio signal coverage of the monitored area. Instead of providing a radio-sensing component such as the Wi-Fi extender in the pantry 712, the component may be located in the adjacent corner of the dining room or adjacently in the kitchen. It is desirable, when installing a security monitoring system that uses radio based sensing for presence/position determination, to adjust the number and position of the radio components of the system to ensure, through trial and error, that the disposition of the radio components provides sufficient radio coverage of the monitored area for reliable detection of presence and location.

[0089] Although one line of sight presence detector, 124, is shown as included in the system of Figure 7 - in this case to detect anyone ascending or descending the stairs 105, and hence to detect transitions between stairs (zone 5) and upstairs (and vice versa), installations according to the invention may instead rely solely upon radio-based presence and location sensing, or may use line of sight (e.g. PIR) sensing only in conjunction with, or as part of, a camera (e.g. a video camera) . As previously mentioned, radio-based presence sensing coverage for the upper floor(s) of the premises may require the installation of another WFS receiver on (each of) the upper floor(s), possibly together with one or more illuminator device per floor. But this will depend upon the dimensions, materials, and construction of the premises. In lightly built structures which are wholly or largely timber built, the spread of radio signals between floors may make presence detection on one floor possible from an adjacent floor. Whereas structures built of masonry, with for example reinforced concrete floors, will almost always require sensing components, including illuminators, installed on each floor for which presence detection is required.

[0090] Figure 8 corresponds generally to Figure 4 but shows schematically details of a central unit 122 configured to perform radio-channel based sensing, in this example WFS. The controller 350 is configured to run a WFS software agent 800, which may be stored in memory 370. The WFS software agent 800 uses WFS radio APIs in the Wi-Fi transceiver 340 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, and thus to provide alarm indications based on unacceptable presence sequences - i.e. presence detected in a zone without presence first having been detected in an adjacent zone. Two zones are considered to be adjacent only if a person can pass between them without needing to pass through a distinct third zone. That is, two zones are adjacent if a person can pass directly between them without needing to pass through a third, intermediate, zone.

[0091] We can also look at this another way, and consider as remote from a first zone any zone which cannot be reached directly from the first zone - the system being configured to flag an alarm or alert condition if, subsequent to presence being detected in a first zone, presence is detected in a remote zone without presence having been detected in an intermediate zone between the detection of presence in the first zone and the detection of presence in the remote zone.

[0092] Thus, there is provided a security monitoring system installation in a location, the location having a perimeter, the perimeter enclosing a first zone and a second zone distinct from the first zone, the second zone being accessible from within the perimeter only via one or more third zones intermediate the first and second zones; the security monitoring system including a sensing arrangement to detect human presence within the perimeter and the system having an armed at home state in which it is so configured that, in the event that: at a first instant human presence is detected in the first zone but not in any of the second or third zones; and

subsequently, at a second instant, human presence is detected in the second zone without presence having been detected in the third zone in the interval between the first and second instants; an alert is raised.

[0093] As an alternative to incorporating the radio sensing application into the central unit, this functionality

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

[0094] A brief explanation will now be given of how WFS works, and how WFS 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.

[0095] 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.

[0096] 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.

[0097] 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.

[0098] 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.

[0099] 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).

[0100] Invoked measurement involves utilizing a packet transmission that is in response to a packet received from the Wi-Fi Sensing receiver device.

[0101] 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.

[0102] 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.

[0103] 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.

[0104] A WFS system can be built based on existing Wi-Fi standards, hardware, software and infrastructure.

[0105] 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.

[0106] 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.

[0107] 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.

[0108] 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.

[0109] 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.

[0110] 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.

[0111] 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).

[0112] The application layer can potentially reside on any networked device: in some embodiments of the present invention it will reside in the central unit 122 along with the WFS agent, but in other embodiments the application layer may exist in an external server or even in the central monitoring station. We prefer, however, to provide the application layer on the central unit to avoid potential problems with signalling delays (for example due to accidental or deliberate network interruption) between the central unit (or other WFS receiver) and a remotely located entity. The application layer receives input from one or multiple Wi-Fi sensing software agents. It combines the information and delivers it to the security management system which may then in turn provide it to the CMS and/or to a cloud service by means of which push notifications may be sent to a registered user device such as a smartphone - allowing users to receive real-time notifications and the ability to view historic data.

[0113] 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.

[0114] 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.

[0115] 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.

[0116] 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.

[0117] 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.

[0118] 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.

[0119] 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.

[0120] 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.

[0121] 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.

[0122] One of the parameters that impacts the quality of the received signal in a wireless network is the amount of interference present. Interference can be caused by other Wi-Fi devices operating in the same band, which causes cochannel interference, or in an adjacent channel, which causes adjacent channel interference. It can also be caused by non-W-Fi devices, which can be other communication systems or unintentional transmissions that create electromagnetic noise in the band. Interference can impact Wi-Fi Sensing performance in two ways. Firstly, it may interfere with the sensing transmissions and thereby reduce the number of measurements made in a given time interval. As such, it introduces jitter in time instants during which the measurements are made. Secondly channel-state measurements may capture the impact of transient interference, such as for a non-Wi-Fi device, as opposed to motion in the environment.

[0123] 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.

[0124] 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.

[0125] 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.

[0126] 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.

[0127] The IEEE 802.11ad amendment defines a Directional-Multi-Gigabit (DMG) PHY for operation in the 60GHz band. While there are three different modulation schemes (Control, Single-Carrier and OFDM) defined, Control and the Single Carrier PHY are the primary PHY used in 802.11ad (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.

[0128] 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.

[0129] 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.

[0130] 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.

[0131] 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.

[0132] 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.

[0133] 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.

[0134] 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. Definition of a standard interface/API enables radio firmware and driver developers to ensure compliance and enables reuse of components or common codes, which may be placed into a

library. Most Wi-Fi drivers are based on either the wireless-extensions framework or the more recent and actively developed cfg80211 / nl80211 framework. As the system integration components are largely provided, these frameworks enable Wi-Fi driver developers to focus on the hardware aspects of the driver. These frameworks also offer significant potential as a location for defining a WFS API. The WFS interface should provide the WFS agent with STA identification and enable the WFS agent to track the physical device in the network (i.e., the AP to which it is connected), as well as the device's capability and availability to participate in the measurements.

[0135] 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.

[0136] 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.

[0137] 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.

[0138] We will now consider some ideas about sequencing that are applicable irrespective of the type of presence location employed in the security monitoring system.

[0139] When someone enters the premises legitimately (i.e., they enter through an approved entrance and are in possession of a disarm code or a disarm token) while the security monitoring system is in the armed away state, the system may be configured to define a location based on the location of a terminal used to transition the security monitoring system from the armed away state to an armed at home state. For example, consider the arrangement of Figures 1, 2, 6 and 7, depending upon whether the control panel in the hall or the disarm node in the kitchen is used, the system may store the hall (zone two) or the kitchen (zone three) as a first location which we store as the current location until the position location system associated with the security monitoring system provides a new location report. If the system doesn't derive a location from the place where the system was put into the armed at home state, then it may determine a current location based on a first report from the position location system.

[0140] If the armed at home state supports multiple occupants, for example is a specific armed at home multiple occupants setting, then the system is preferably configured to try to locate and, in effect, track the various occupants of the premises. If the system was put into the armed at home state from an armed away state, or with little delay (e.g. a minute or less) from the detected entering of the premises, then the system may assume that the premises are empty except for the zone or zones around the point of entry - whose location the system can derive from the identity and hence location of the sensor that detected the opening of an external entrance door. This can be used to provide a single initial or current presence location which is then updated and/or supplemented based on presence reports in respect of other zones. Thereafter different occupants may in effect be tracked based on the zones in respect of which presence is detected, given that the system knows which zones are adjacent the zones in respect of which current locations are stored. The system is also aware of the identities of zones where for example line of sight presence sensing may not always provide a presence signal in respect of an occupant, for example as is the case in respect of the pantry and cloakroom of Figures 2 and 7. The system may be configured to maintain a current presence for the relevant zone at least until a presence report is received from an adjacent zone. And if the system considers it possible that there are multiple occupants in a zone where line of sight detection has blind spots, then that zone may be retained as a current zone at least until the relevant number of occupants have been detected in or passing through adjacent zones. The system may also be configured to learn typical durations for how long people spend in the different zones, optionally correlated with time-of-day, day of week, holidays, and even occupant's calendars. Based on the zones in respect of which current locations are stored, the arrival of a new presence indication is checked against all stored current locations, and if the new presence indication is in respect of a zone which is neither a stored current location nor a location adjacent such a stored current location, this suggests the arrival of an intruder and hence the system may treat this as an alert condition. For example, reporting the alert, and the relevant conditions, to the central monitoring station and optionally providing a warning (e.g. a voiced warning of the presence of an apparent intruder in a specified zone or room) to occupants of the premises through for example the control panel in the hall and the disarm node in the kitchen, as well as for example, through any smart speakers or the like to which the central unit of the security monitoring system has access through an appropriate radio channel.

[0141] With a single-occupancy armed at home state, we may be able to ignore the disarming of the system from a fully armed state, instead paying attention to the entering of the alarmed at home state (single occupancy).

If we can determine a location based on the act of entering the alarmed at home state - i.e. because we know the location of the terminal that was used to enter the state, we can capture that location as our first location. The first location is now our current location. On the other hand, if we can't determine the location based on the arming of the system, instead we look for the first location information from the presence sensing arrangement, and we make that our current location. When we receive another presence/location signal or message we check to see whether that equals our current location. If it does, our current location remains the same, and no alert is raised. Conversely, if the new location does not equal the current location, we check whether the new location is an adjacent location (that is, adjacent to the location that is stored as the current location). If it is an adjacent location, the new location becomes the current location, and no alert is raised. But if the new location is neither the current location nor an adjacent location, it is a remote location, and an alert is raised. Although the system, e.g. the central unit 122, knows that there should only be a single occupant, then the detection of a second presence through for example the triggering of motion or presence sensing in two zones simultaneously or almost simultaneously signifies the arrival of a second occupant, and that should itself result in an alert being raised. But we also need to remember that even if we only see presence or occupancy information for a single zone there may in fact be two or more occupants because this situation can arise when we have hidden zones, such as the pantry or cloakroom examples or in the later drawings where we have rooms without sensors which lead off a corridor which does have a sensor. So, in a system which provides a setting for armed at home single-occupant, the system can raise an alert when two or more people are detected based, for example, of the simultaneous detection of presence in two or more remote zones (care needs to be taken, or system adjustments made if for example line of sight presence detection in two or more adjacent zones can be triggered simultaneously or quasi simultaneously, e.g., a matter of a few seconds apart, by a single occupant: if the sensing arrangement is such that this situation cannot occur, then an alert may sensibly be raised in the event that simultaneous presence or quasi simultaneous presence is detected in adjacent zones.

[0142] Another way of looking at this is that when we have the alarm system set to sole occupant armed at home we track the current location of the known occupant. If we sense occupancy in more than one place, i.e. more than one zone, then we should raise an alert. But we should also raise an alert if we see a new presence in a zone which is remote from the last current location - the assumption is that the authorised occupant may be in a hidden part of the current location, which explains why we don't see present signals for two zone simultaneously.

[0143] Now consider what happens when a monitored door (e.g. an external door with a door opening sensor, such as a magnetic sensor) in the periphery is opened while the security monitoring system is in the armed at home state single-occupant. The door may have been opened from outside or from inside. First of all, we need to decide which of these events has happened. We can determine, with reasonable certainty, that the door has been opened from inside if we have tracked presence to the zone within the perimeter that is served by the door. If the occupant has opened the door, the occupant should be reminded to enter a code or present a token or dongle at a control panel or disarm node to prevent an alarm being raised. But if the system is in the armed at home single occupant state, we don't really want the system to be fully disarmed just because the occupant has opened, say, the back door to pick some herbs from the garden. Rather, we want the system to continue to monitor the perimeter and to continue to check for presence within the monitored area, so we may just in effect flag signals from the relevant door sensor (in the central unit, for example) to the effect that these can currently be ignored. Then we have a choice, to re-arm the system automatically in respect of that door once the door is being closed, or to remind the occupant - for example by voiced announcement from the disarm node, to confirm that they want to re-arm the door. Automated rearming may be performed within say one or two minutes of the door being closed again. We might also take account of information from a lock (e.g. an electronically controlled lock) of the door, so that the door is automatically re-armed if the occupant locks the door again after closing it.

[0144] But suppose, instead, that the known occupant wasn't in the relevant location to open the door from the inside -, i.e., current location equals neither the monitored zone served by the door nor an adjacent location, then the system can assume that a new entrant has arrived. The control panel or disarm node will provide the audible and/or visual reminder of the need to check in (e.g., enter an appropriate code or present an appropriate token) to prevent an alarm event being reported to the central monitoring station. If the security monitoring system allows an armed at home state to be entered directly from the armed away state, the new entrant may try to effect such a change, not noticing that the current state is already an armed at home state. The system is preferably configured to provide an audible warning, e.g. by means of a voiced announcement, that the system is currently in the armed at home single-occupant status. Or, in other words, the someone else is already present. Under these circumstances, the system may also be configured to invite the new entrant to enter an armed at home multiple-occupant state. If the new entrant declines (e.g. doesn't perform the action(s) required to enter the armed at home multiple-occupant state), the system may be completely disarmed or, more preferably is put into an armed at home state which continues to monitor the perimeter by which no longer monitors presence within the perimeter. Of course, the new entrant should be given the option to select an appropriate armed state, other than the armed

at home single occupant state. Similarly, even if the security monitoring system doesn't permit the system to be switch directly from the armed away to an armed at home state, the new entrant needs to be warned against setting the armed at home single-occupant status - on the basis that someone is already home. This warning, again preferably provided at least audibly, may only be provided in the event that the new entrant tries to select this option, or the warning may be provided upon the new entrant entering their code (or a common system code) or presenting a dongle. For example, "thank you for identifying yourself, the system was in the armed at home sole occupant state, would you like to switch to armed at home perimeter only state (which may be the only alternative armed at home state) or would you like to disarm the system fully?", although if the system supports a further armed at home state, for multiple occupants, the new entrant may be asked whether they want to enter this state. The entering of a new armed at home state may be conditional upon the further presentation of a dongle or the entering the code, or one or other of these conditions may need to be met only in the event that there has been a significant delay (e.g. one or two minutes or more) between the arrival of the new entrant and the attempt to change the arm state.

[0145] Of course, a person entering through an allowed entry point may be somebody other than an authorised person, in which case they will presumably be unable to provide either a disarm code or a disarm dongle. The security monitoring system is thus preferably configured in the armed at home single-occupant state (just as it is from the armed away state) to contact the central monitoring station with a report of an alarm condition. But if such an entry occurs when the system is in an armed at home state, then preferably the system is configured also to provide a warning to existing occupant(s) of the premises that an entrance has been effected via, for example, the front door or the back door, so that they may themselves exit the premises for safety. Such warnings may be provided audibly via a disarm node or control panel remote from the door that was used to effect entrance, and the system may also be configured to push notifications to user devices, such as smart phones, etc. of authorised occupants warning them of the intrusion. Pushing such warnings to all authorised users of the system (which may mean those having a unique disarm code, and or a dongle or tag associated with their identity, or may mean everyone on a list of authorised users or occupants - for each of whom contact details such as mobile phone numbers, WhatsApp, or other messenger identifies, are stored) means that there is a good likelihood of warning the authorised occupant currently in the premises, as well as providing warnings to other family members, etc. so that they may take appropriate action. In addition, of course, the central unit of the security monitoring system will also send an alarm indication to the central monitoring station where a human operator may become involved, for example viewing video footage from the premises, and possibly involving security personnel or the local police, et cetera.

[0146] When the system is armed at home for multiple occupants, we are interested in identifying any new presence reports that relate to a location that is remote from all current locations. This presupposes that we can track, and store or log, the locations of everyone legitimately within the premises. If our presence/location sensing system makes this possible, we can simply compare each new presence report with our log of current locations, and if the new presence report is for a location that is neither current nor adjacent any current location, then an alert should be raised - because the new location is a remote location.

[0147] The idea of providing an armed at home single-occupant state can usefully be considered an example of enabling a user to arm the security monitoring system appropriately, while providing enhanced security - since it means that the system is armed to respond to the threat signified by the detection of more than one person. For a single-occupancy household, or for a household where someone is often "home alone", the option, which might be presented as the default or first-choice option, of an armed at home single-occupant state provides not only greater security - by triggering an alarm event if two or occupants are detected, even though no perimeter breach has been detected. Although the "normal" condition may be "home alone", the system is preferably configured to provide a user arming the system with an easy option to increase the number of occupants in the armed at home mode, to take account of the presence of friends, family members, etc. So, for example, the system may be configured to provide a, preferably, voiced prompt such as "You've chosen the single-occupant mode. Is that correct, or do you need to adjust the number of people?", with the further option to enable the user to use a dedicated button (physical or virtual - such as on a touchscreen), keypad or touchscreen (or even a voice interface to allow the user to voice a command - such as "increase the people count to two") to increase the number of occupants to match the number present. This approach is also applicable to occupant counts other than one. For example, instead of defaulting to a "home alone" option, the system could be configured to default to "family" or "gang" with the count appropriate to the size of the family (e. g three or four) or the number of flatmates or whatever. Again, the system would preferably be configured to provide a, preferably, voiced prompt such as "You've chosen the family- mode with three occupants. Is that correct, or do you need to adjust the number of people?", with the further option to enable the user to use a dedicated button (physical or virtual - such as on a touchscreen), keypad or touchscreen (or even a voice interface to allow the user to voice a command - such as "decrease the people count to two") to decrease the number of occupants to match the number present.

[0148] If the security monitoring system includes perimeter sensors for windows or for doors that are not prin-

cipal entrances, it will typically be configured to raise an alert or alarm in the event that one of these sensors is triggered while the perimeter is being monitored (armed away or armed at home). But with knowledge of the location of a single occupant, or possibly of all occupants, we can consider whether such a perimeter sensor is triggered in a current or adjacent location - and if so possibly label any alert sent to the central monitoring station that the breaching of the monitored perimeter is likely to be occupant activity - and also to provide some sort of warning to the occupant, so they need to check-in at the control unit or at a disarm node to confirm that they opened the relevant door or window. The system could tailor the interval for the occupant to provide at disarm code or a disarm dongle, based on the relative location (i.e. walking distance) between the location of the opened window and the nearest control panel or disarm node. If no code or token is provided, the opening of the door or window is treated as an alarm event.

[0149] Conversely, if the location of the detected perimeter breach is in a remote location (zone), rather than in a current or adjacent location, the security monitoring system can immediately treat the breach as an alarm event and report it as such to the central monitoring station, as well as preferably also providing a warning, such as a local voiced alert to the premises occupant.

[0150] Figure 9 is a flowchart that illustrates the possible operation of a security monitoring system, and in particular the operation of a central unit of such a system, in an armed at home single occupancy mode. The process starts at 1000, and the first step at 1010 involves setting the security monitoring system in an armed at home single occupancy mode. This operation may be performed at a control unit, such as 128 or 628, or at a disarm node 130, or even at the central unit 122.

[0151] If a fixed node of the system, e.g. 128, 628 or 130, is used to put the system into the armed at home mode, the system may, at 1020, use the known location of the relevant node to determine the current location of the occupant (e.g zone 2 for 128 or 628, or zone 3 for 130). This location is stored 1030 as the user's current location. But if the system cannot establish a location based on the arming of the system then a current location is not determined until, at step 1040, the system receives a location report from the presence location system. At 1050 the system checks to see whether a current location is already stored. If no current location was previously stored, then this new location report is used to determine a current location and this is stored as the current location at 1060.

[0152] If a current location was already stored, at 1070 the system compares the newly reported location with the current location: if the newly reported location matches the current location or is a location adjacent the current location, the newly reported location is stored as the current location. Optionally, if the new location matches the previous current location then the current location is not updated, but a time stamp associated with the current location may be updated based on the time stamp of the newly reported location. As a general rule, it is preferable for the system (e.g. the central unit 122) to associate a time stamp with the stored current location, and it can be useful to store not only a timestamp in respect of the most recent location update but also, when a new location report is for the stored current location, it may be useful to track (record) the duration of the stay in that location (e.g. the location pendency). Stored location pendencies can, for example, be compared with past pendency durations for the relevant zone - and may for example be used to trigger an alert if the pendency significantly exceeds regular pendency durations. So for example, the normal pendency in a cloakroom or toilet may be 3 to 9 minutes, so that a pendency of more than 12 or 15 minutes may indicate that the person in the cloakroom has collapsed or is in difficulty. The system could flag an alert to the central monitoring station and/or to a list of users/contacts stored by the system (e.g. in the memory of the central unit) and push notifications could be sent to these contacts. This same monitored pendency idea is also applicable to the multiple occupancy armed at home mode - and in that case the system is preferable configured to trigger a voiced announcement to the effect that someone may be in difficulty in an identified zone (e.g. the downstairs cloakroom).

[0153] However, if the newly reported location neither matches the current location nor a location adjacent the current location, the suspicion arises that there has been an intrusion and an alert is (or may be) raised at 1090. If this situation arises with the first location report from the location sensing system, shortly after the system was armed, it suggests that the occupant may have selected the wrong arming mode - as perhaps someone was already in the premises, or perhaps they arrived home with a child or children who have dispersed in the premises before the system was set into the armed at home single occupancy status. The likelihood of these various possibilities depends to some extent on whether the system was in the armed away state shortly before the system was put into the armed at home state, and if so how long an interval there was between the system being fully armed and the system entering the new state. Clearly, if the system was fully armed until shortly before being put into the armed at home state, there is very little likelihood that another authorised user was already present. Again, if the interval was very short then the distance that accompanying children may have gone into the premises is limited - so that detection of presence remote from both the point of entry to the house and from the arming point, if know, is probably more likely to be an intruder than not. Preferably, on installation the system is supplied with transit times between the permitted points of entry and the remote zones, and between the various arming points and their remote zones (clearly, the concept of remote zones is based on a point of reference, and hence what constitutes a remote zone depends upon the reference zone or starting point). The system may also be config-

ured to learn and store route sequences and timings, based on the behaviours of the usual occupants - since young children and the elderly are likely to move through premises, and between zones, at very different. These data may be used by the security monitoring system (e.g. the controller 122) to categorise detected movement patterns and hence behaviours as more or less likely to indicate an event or condition that should be reported to the central monitoring station or trigger an alert or an alarm.

[0154] Whether or not the process of step 1070 results in the reporting of an alert or not, the process preferably continues 1110 with a return to step 1040. The system continues to receive and assess new location reports to look for intrusion events. This continuing monitoring is useful in the event of an intrusion since it enables the movements, and hence current location, of the intruder to be tracked and reported to the central monitoring station. Personnel in the central monitoring station can hence use this information to guide the police or other security personnel who may be sent to attend the premises in response to the detected intrusion.

Claims

1. A security monitoring system installation in a location, the location having a perimeter, and the system including a sensing arrangement to detect human presence within a monitored area within the perimeter, the monitored area comprising a plurality of monitored zones, at least one pair of the monitored zones being remote from each other, each remote pair consisting of a first and a second of the monitored zones, human passage between the first and second zones of a pair that are remote from each other only being possible, within the premises, via at least one intermediate zone that is adjacent the second zone of the pair, and the system having an armed at home state in which it is so configured that, in the event that:

   at a first instant human presence is detected in the first remote zone of the pair but not in any of the second or intermediate zones of the pair; and
   subsequently, at a second instant, human presence is detected in the second zone of the pair without presence having been detected in any of the one or more intermediate zones of the pair in the interval between the first and second instants; an alert is raised.

2. The security monitoring system of claim 1, wherein the sensing arrangement to detect human presence within the perimeter comprises a plurality of line-of-sight detectors, for example PIR detectors or other optical detectors.

3. The security monitoring system of claim 2, wherein the monitored area includes a monitored zone that comprises multiple rooms, some at least of the rooms being linked by means of a hall, landing or walkway, at least one line-of-sight detector of the sensing arrangement being provided to monitor the hall, landing or walkway, and optionally some at least of the multiple rooms do not contain line-of-sight detectors.

4. The security monitoring system of claim 1, wherein the sensing arrangement to detect human presence within the perimeter comprises a radio-based system that is configured to sense presence and location based on detecting perturbations of radio signals.

5. The security monitoring system of claim 4, wherein the radio-based system is configured to process communication signals received from one or more radio transmitters operating according to one or more communication standards or protocols.

6. The security monitoring system as claimed in claim 4 or claim 5, further comprising a control unit wherein the control unit includes a radio receiver of the radio-based presence and location sensing system.

7. The security monitoring system as claimed in claim 6, wherein the control unit is configured to process radio signals to derive location and presence data in respect of monitored zones.

8. The security monitoring system as claimed in any one of claims 4 to 7, wherein the sensing arrangement to detect human presence uses changes in channel state information or received signal strength in determining presence.

9. The security monitoring system as claimed in claim 6 or claim 7, as dependent on claim 5, wherein the control unit functions as an access point of a radio network whose signals are used by the radio-based presence and location sensing system.

10. The security monitoring system of claim 8, wherein the radio network is a Wi-Fi network.

11. The security monitoring system as claimed in any one of claims 4 to 10, wherein the sensing arrangement to detect human presence within the perimeter further comprises one or more line of sight detectors, for example PIR detectors.

12. A control unit for a security monitoring system for premises, the control unit comprising a processor, a memory communicatively coupled to the processor and a set of instructions stored in the memory which

when executed by the processor cause the control unit, after entering an armed at home single occupancy mode, to monitor the premises against intrusion by:

determining the location of an occupant within the premises;
storing the determined location as a current location of the occupant;
receiving sensing data relating to the location of an occupant;
determining a new occupant location based on the sensing data
comparing the new location with the stored current location;
if the new location is neither the same as the stored current location nor a location adjacent the stored current location, raising an alert;
if the new location is the same as the stored current location or is a location adjacent the stored current location, setting the new location as the current location of the occupant.

13. A control unit as claimed in claim 12, further comprising a radio transceiver communicatively coupled to the processor, wherein the processor is configured to derive the received sensing data from radio signals received by the transceiver.

14. A control unit as claimed in claim 12 or 13, wherein the processor is configured to determine location based on signals received from one or more nodes of the security monitoring system remote from the control unit, the one or more remote nodes including at least one line-of-sight presence detector.

15. A control unit in any one of claims 12 to 14, wherein the processor is configured to raise an alert in the event that received sensing data reveal human presence at more than one location, and hence the presence of more than one person, within the premises

16. A method of detecting an intrusion in premises protected by a security monitoring system installation for, the premises having a perimeter and a monitored area within the perimeter, the monitored area comprising a plurality of monitored zones, at least one pair of the monitored zones being remote from each other, each remote pair consisting of a first and a second of the monitored zones, human passage between the first and second zones of a pair that are remote from each other only being possible, within the premises, via at least one intermediate zone that is adjacent the second zone of the pair:

the method comprising monitoring the monitored area to detect human presence;
at a first instant detecting human presence in the first remote zone of the pair but not in any of the second or intermediate zones of the pair; and
at a second instant, after a time interval
detecting human presence in the second zone of the pair; and
determining an alert condition if presence was detected in none of the one or more intermediate zones of the pair in the time interval between the first and second instants.

17. A security monitoring system installation in a location, the location having a perimeter, the perimeter enclosing a first zone and a second zone, and one or more third zones adjacent the second zone and intermediate along a possible human route between the first and second zones, the second zone being accessible on a possible human route within the perimeter only via at least one of the one or more third zones;
the security monitoring system including a sensing arrangement to detect human presence within the perimeter and the system having an armed at home state in which it is so configured that, in the event that:

at a first instant human presence is detected in the first zone but not in any of the second or third zones; and
subsequently, at a second instant, human presence is detected in the second zone without presence having been detected in any of the one or more third zones in the interval between the first and second instants; an alert is raised.

18. A method of detecting an intrusion in premises protected by a security monitoring system installation, the premises having a perimeter, the perimeter enclosing a first zone and a second zone, and one or more third zones adjacent the second zone and intermediate along a possible human route between the first and second zones, the second zone being accessible on a possible human route within the perimeter only via at least one of the one or more third zones;

the method comprising at a first instant detecting human presence in the first zone but not in any of the second or third zones;
at a second instant, after a time interval
detecting human presence in the second zone; and
determining an alert condition if presence was detected in none of the one or more third zones in the time interval between the first and second instants.

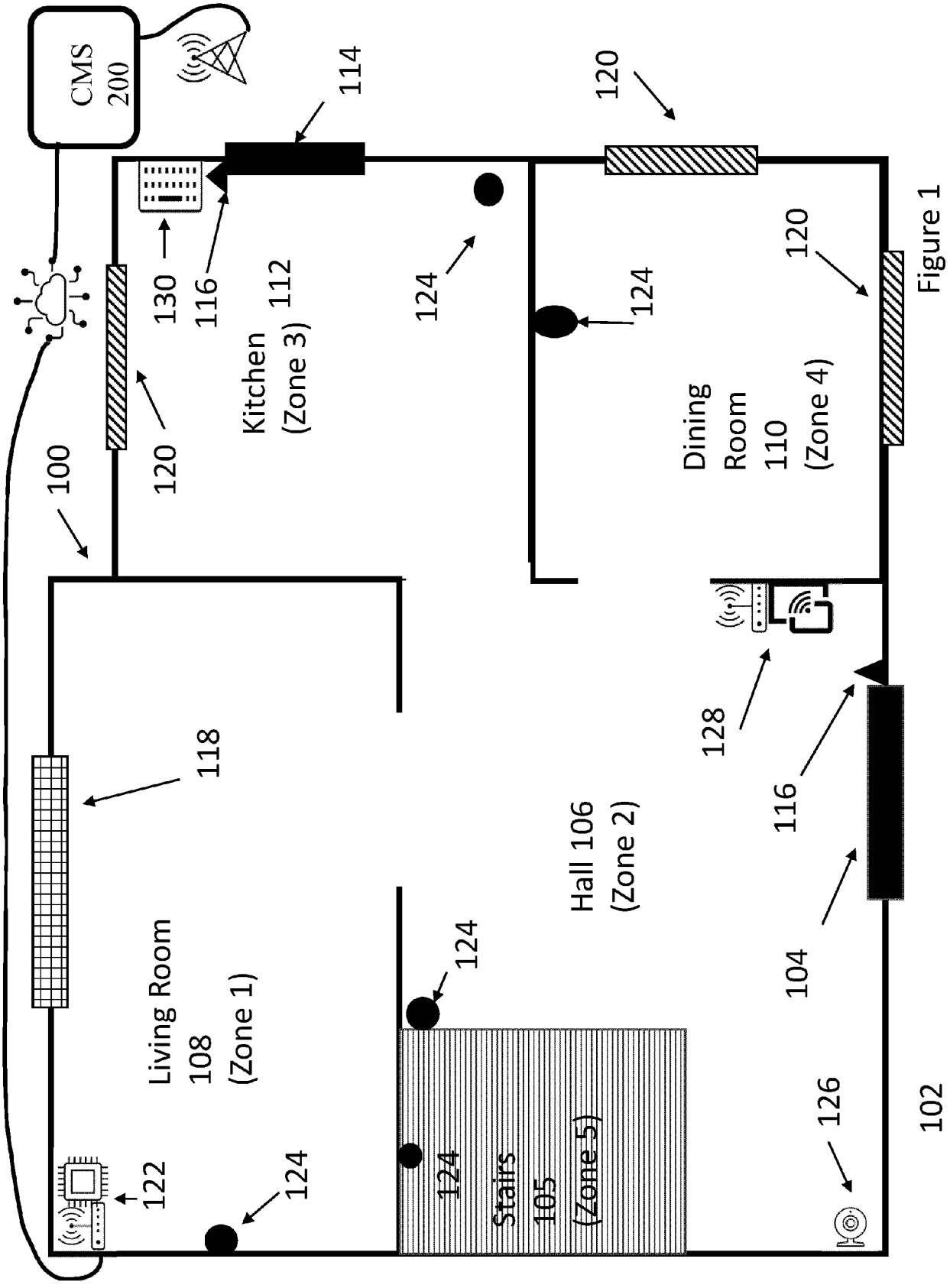

CMS
200
114
120
130
116
Kitchen
(Zone 3)
112
124
124
120
Dining
Room
110
(Zone 4)
120
100
118
128
116
Hall 106
(Zone 2)
Living Room
108
(Zone 1)
124
104
124
Stairs
105
(Zone 5)
122
124
126
102

Figure 1

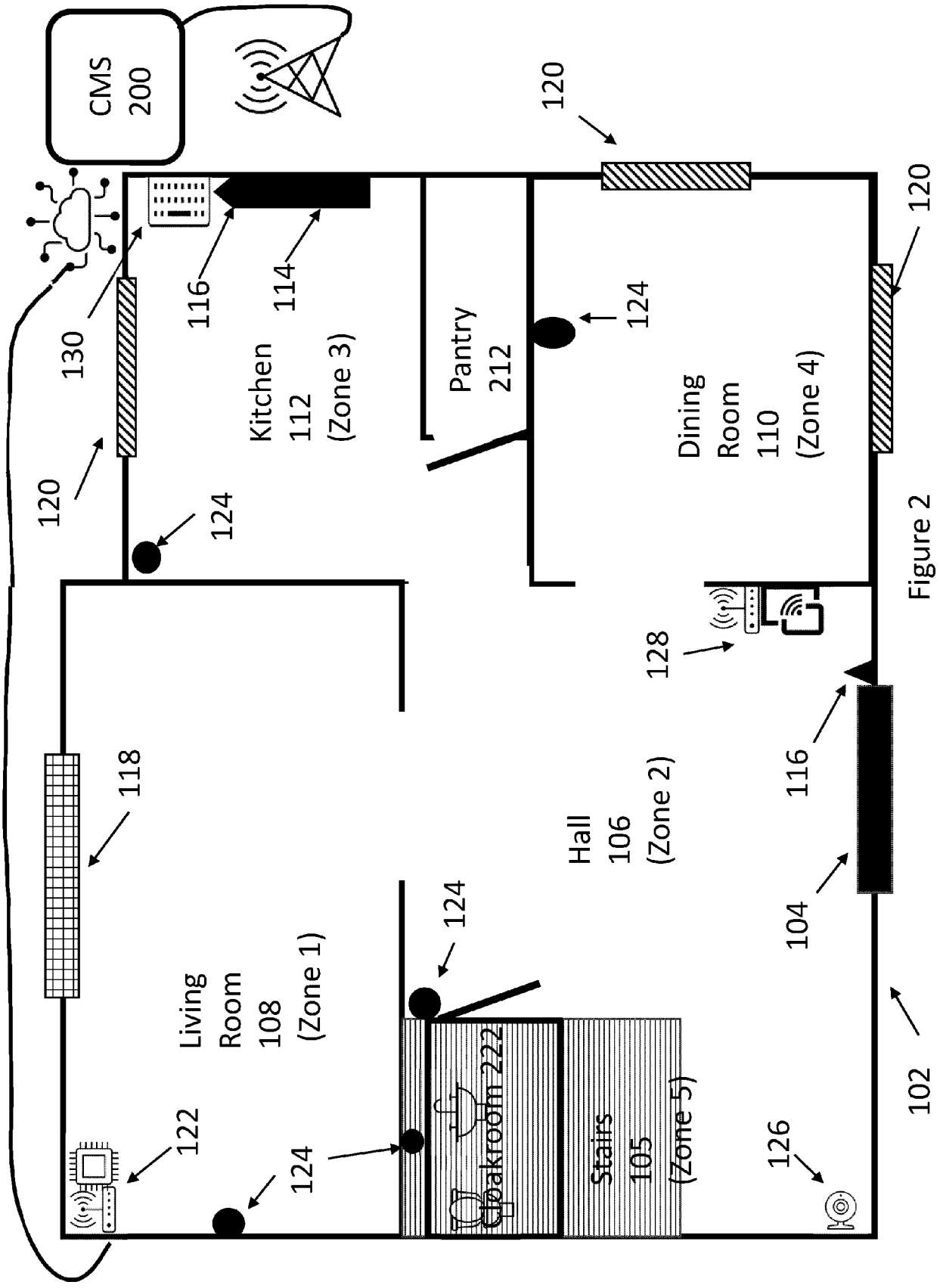

CMS
200
120
130
116
114
Kitchen
112
(Zone 3)
Pantry
212
124
Dining
Room
110
(Zone 4)
120
120
124
128
118
Hall
106
(Zone 2)
116
Living
Room
108
(Zone 1)
124
104
Cloakroom 222
Stairs
105
(Zone 5)
122
124
126
102

Figure 2

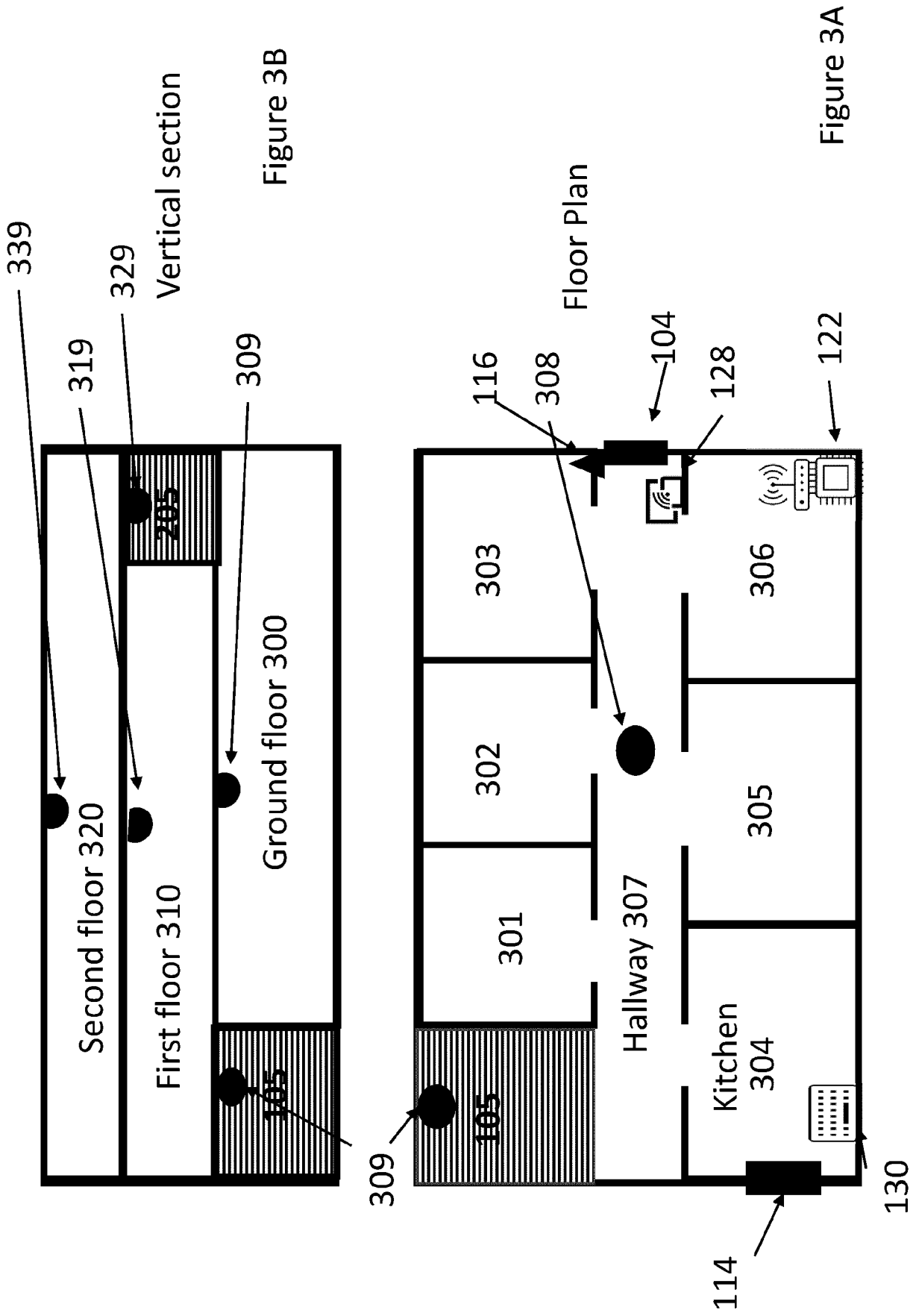


Figure 3A

Figure 3B

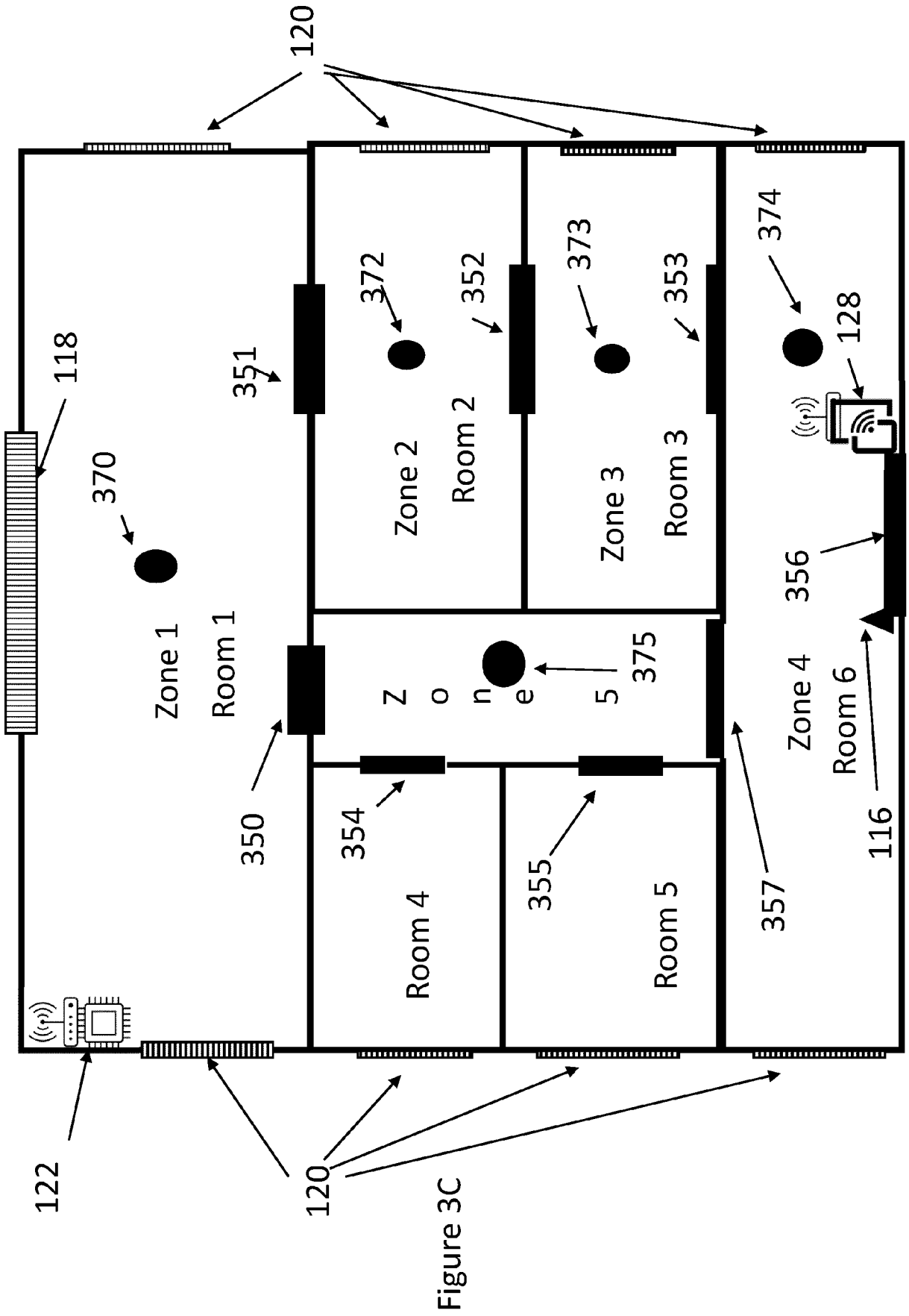

120
118
370
Zone 1
Room 1
351
372
352
Zone 2
Room 2
373
353
Zone 3
Room 3
374
128
356
Zone 4
Room 6
116
375
Zone 5
350
354
Room 4
355
Room 5
357
122
120

Figure 3C

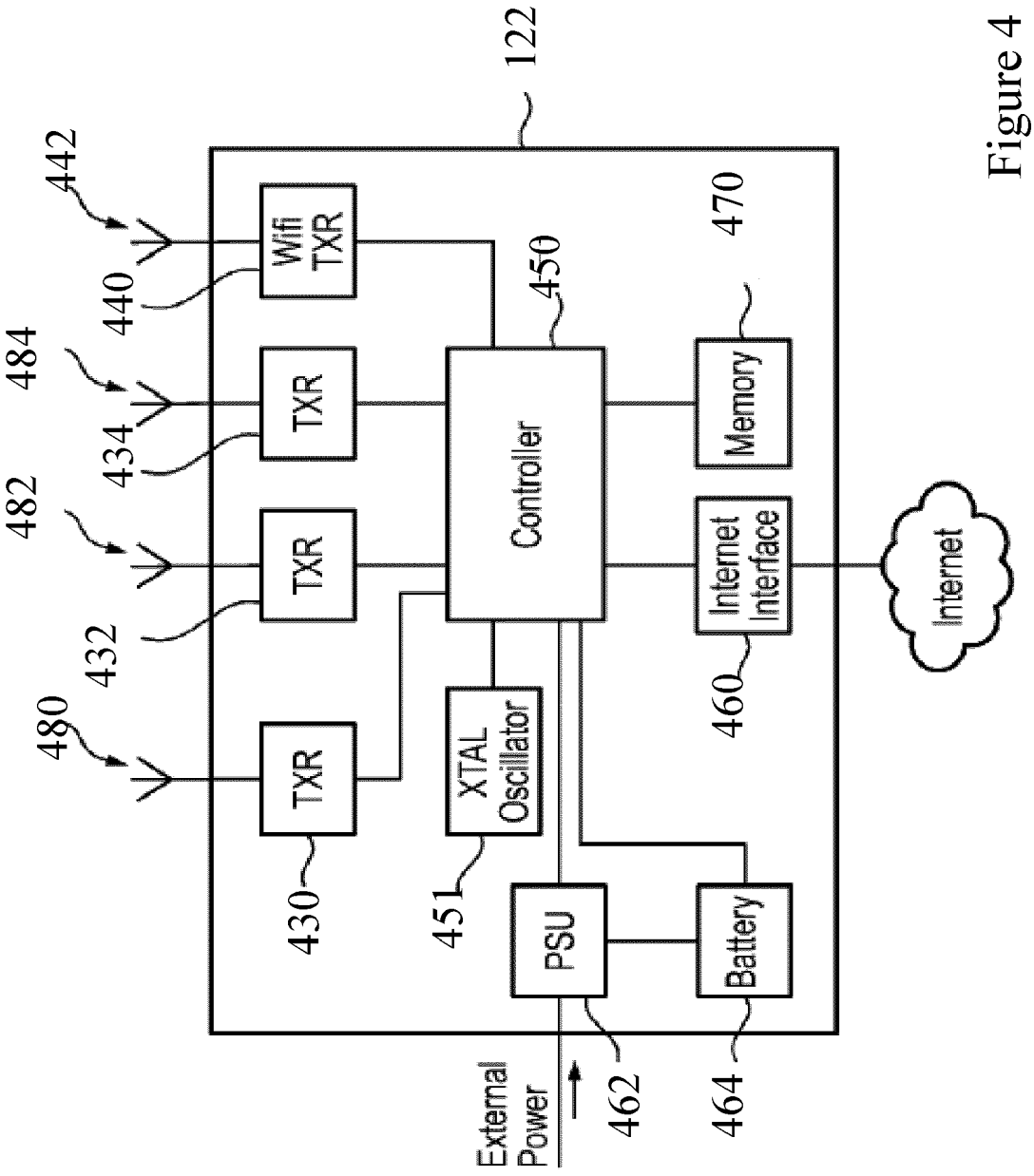

122
442
440
Wifi TXR
450
470
484
434
TXR
Controller
Memory
482
TXR
Internet Interface
Internet
432
480
TXR
XTAL Oscillator
460
430
451
PSU
Battery
External Power
462
464

Figure 4

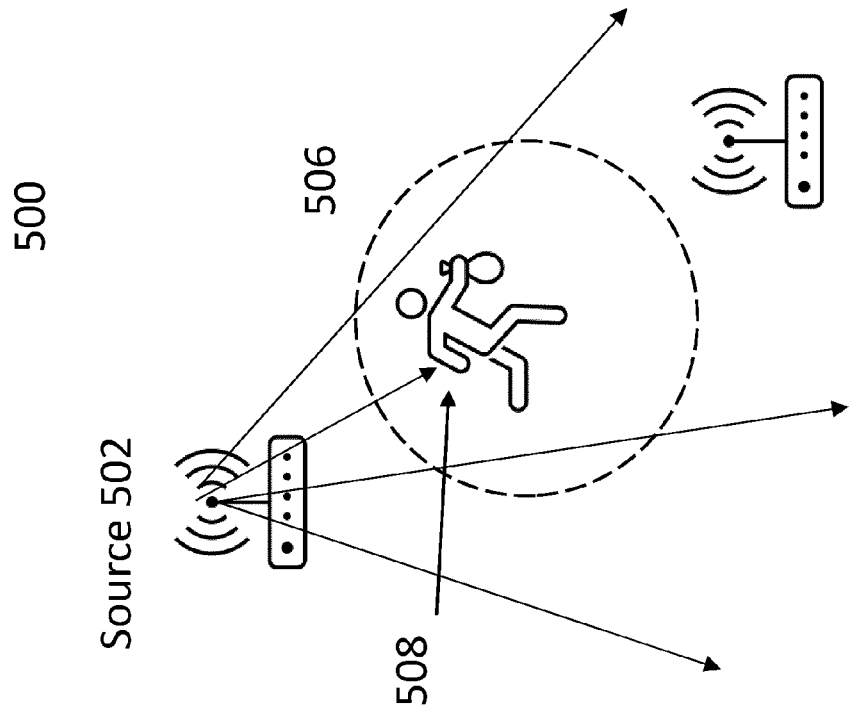


Figure 5B

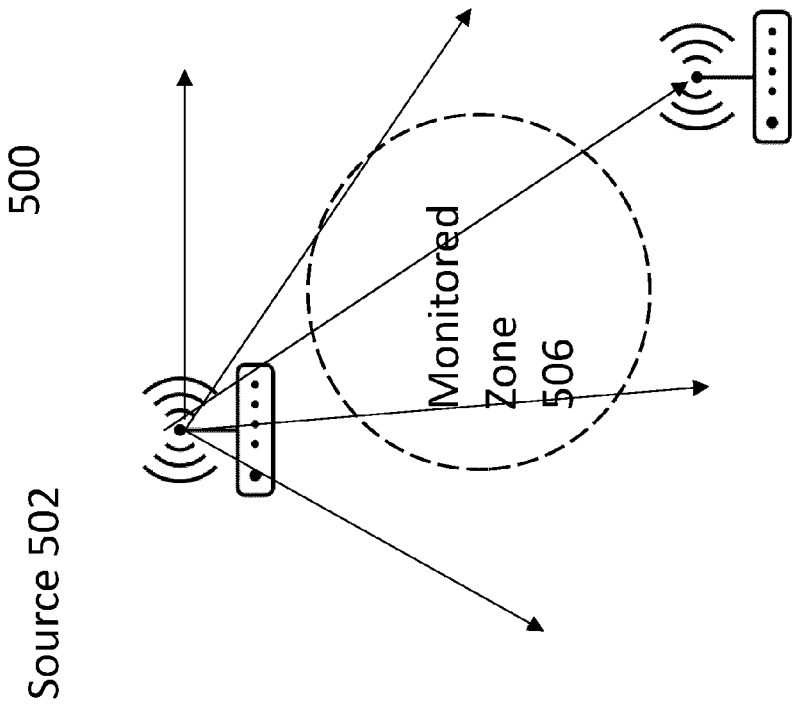


Figure 5A

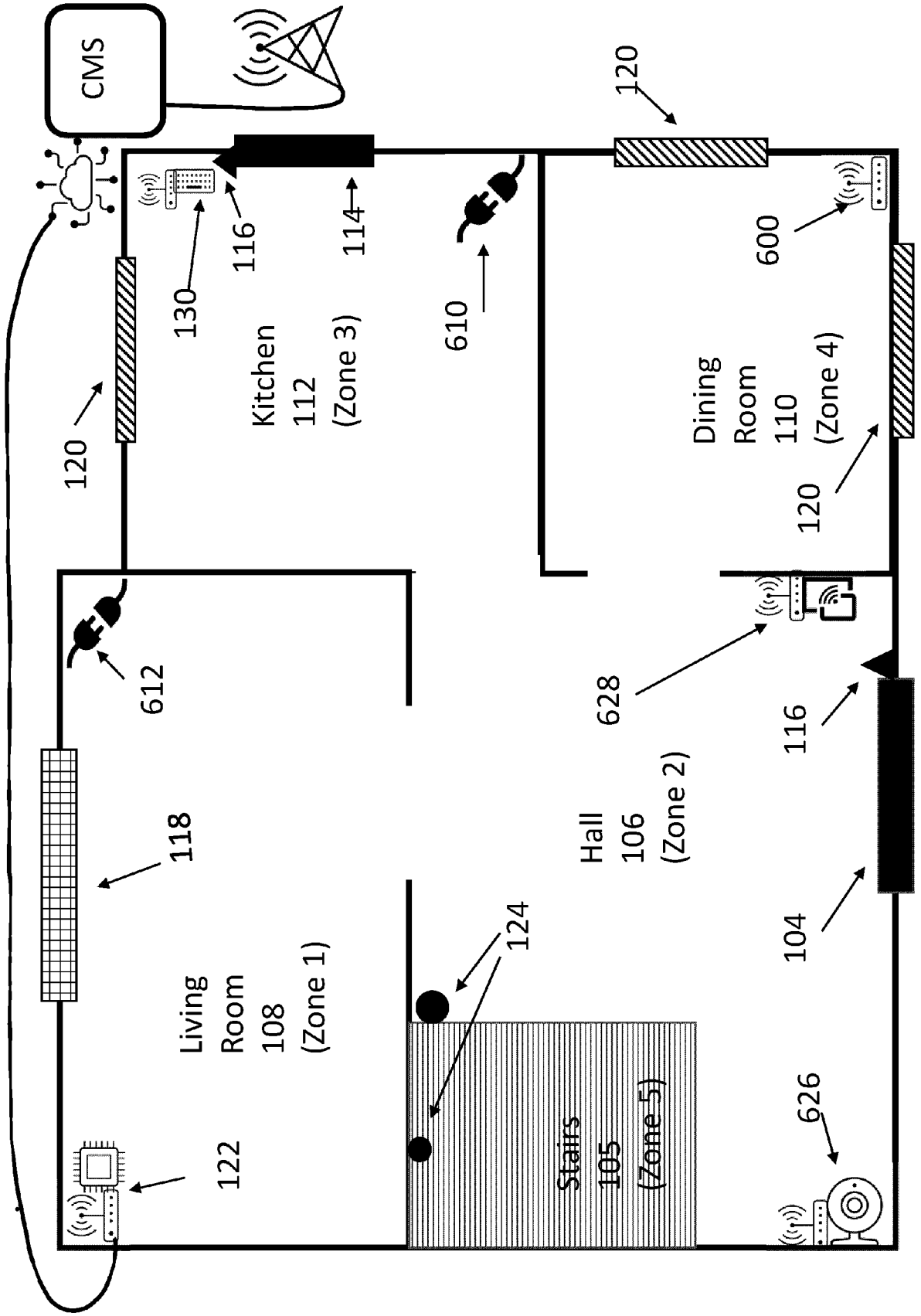

CMS
120
130
116
114
Kitchen
112
(Zone 3)
610
600
Dining
Room
110
(Zone 4)
120
120
612
628
116
118
Hall
106
(Zone 2)
124
104
Living
Room
108
(Zone 1)
Stairs
105
(Zone 5)
122
626

Figure 6

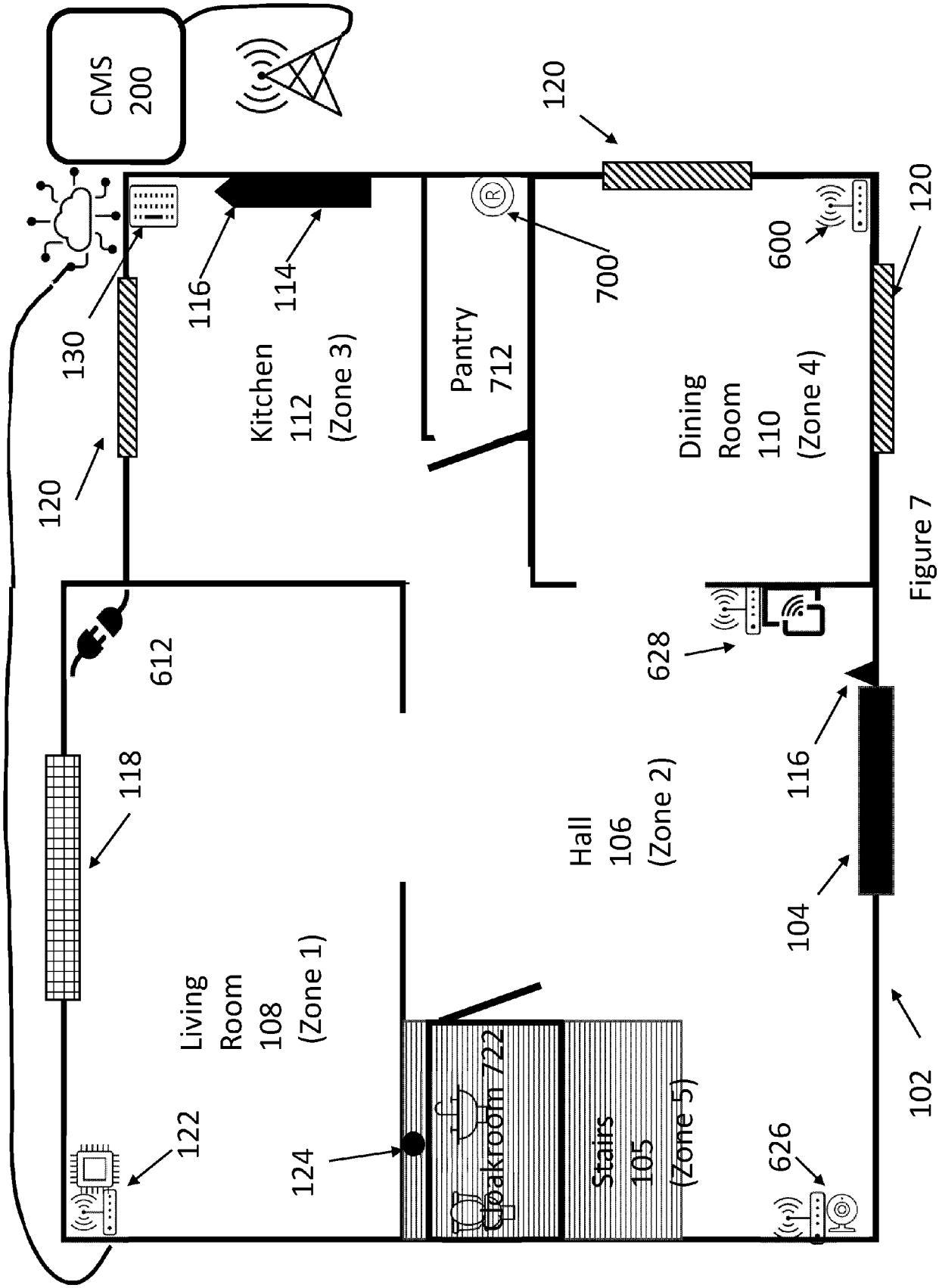

CMS
200
120
130
116
114
Kitchen
112
(Zone 3)
Pantry
712
700
600
Dining
Room
110
(Zone 4)
120
612
628
118
Hall
106
(Zone 2)
116
Living
Room
108
(Zone 1)
104
122
124
Cloakroom 722
Stairs
105
(Zone 5)
626
102

Figure 7

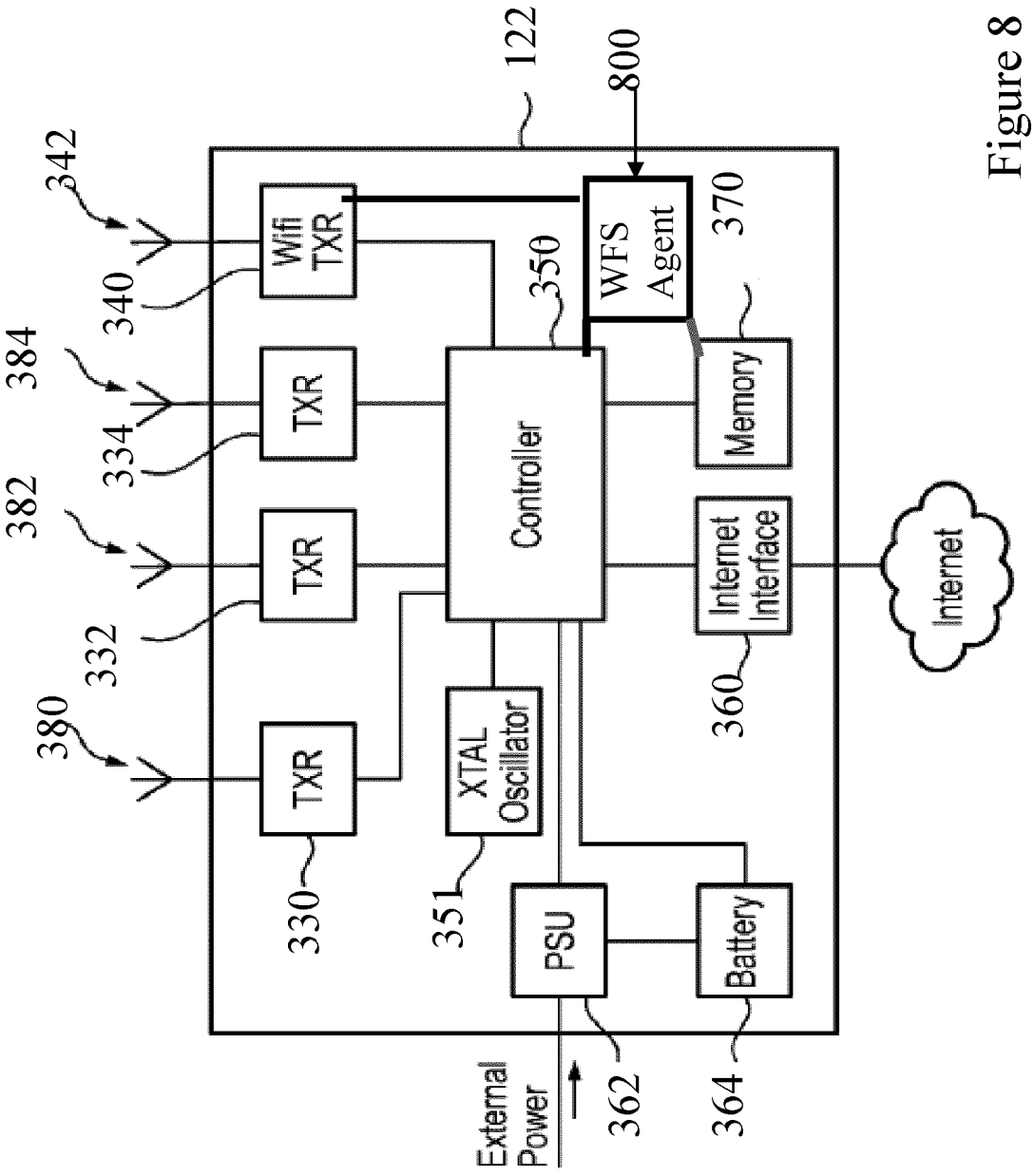
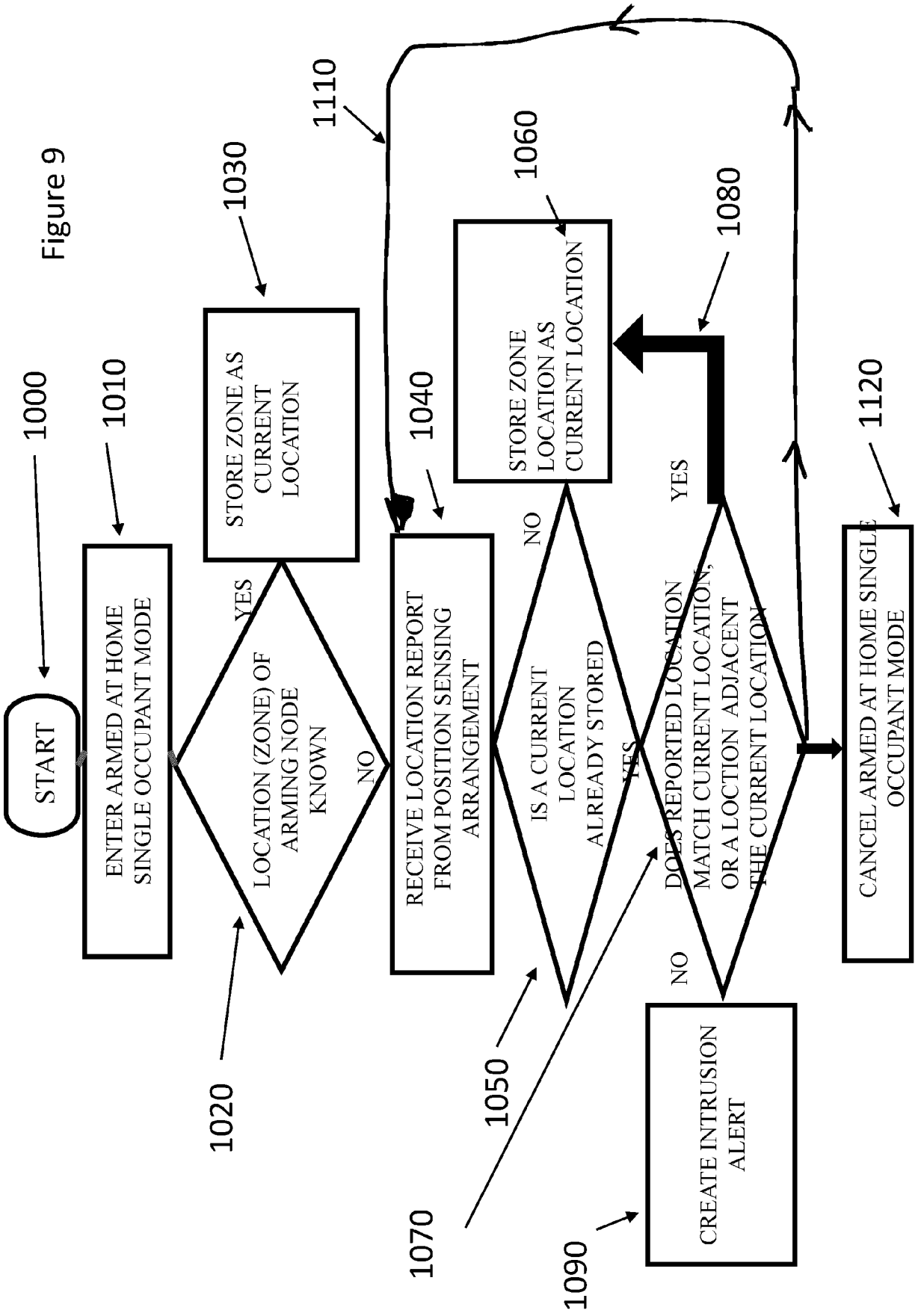

122
800
342
340
384
334
382
332
380
330
Wifi TXR
TXR
TXR
TXR
Controller
WFS Agent
370
350
Memory
Internet Interface
360
Internet
XTAL Oscillator
351
PSU
Battery
External Power
362
364

Figure 8

Figure 9


START
1000
ENTER ARMED AT HOME SINGLE OCCUPANT MODE
1010
LOCATION (ZONE) OF ARMING NODE KNOWN
YES
NO
1020
STORE ZONE AS CURRENT LOCATION
1030
RECEIVE LOCATION REPORT FROM POSITION SENSING ARRANGEMENT
1040
IS A CURRENT LOCATION ALREADY STORED
NO
YES
1050
STORE ZONE LOCATION AS CURRENT LOCATION
1060
DOES REPORTED LOCATION MATCH CURRENT LOCATION, OR A LOCTION ADJACENT THE CURRENT LOCATION
YES
NO
1070
1080
CREATE INTRUSION ALERT
1090
CANCEL ARMED AT HOME SINGLE OCCUPANT MODE
1120
1110

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 21 21 8147

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X Y	US 2012/019353 A1 (KNASEL DONALD LEE [US]) 26 January 2012 (2012-01-26) * paragraph [0011] - paragraph [0019] * * paragraph [0041] - paragraph [0050] * * paragraph [0053] - paragraph [0054] * * figures *	1-3,11, 12,14-18 4-10,13	INV. G08B25/00 G08B13/24 G08B13/19 G08B13/196
Y	US 11 006 245 B2 (COGNITIVE SYSTEMS CORP [CA]) 11 May 2021 (2021-05-11) * page 4, line 35 - page 9, line 29 *	4-10,13	
A	DE 10 2019 111345 A1 (VERISURE SARL [CH]) 5 November 2020 (2020-11-05) * paragraph [0005] - paragraph [0007] * * paragraph [0026] - paragraph [0033] * * figures *	1-18	

TECHNICAL FIELDS SEARCHED (IPC)

G08B

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	31 May 2022	Köniğer, Axel

CATEGORY OF CITED DOCUMENTS

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

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

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 21 21 8147

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

31-05-2022

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012019353 A1	26-01-2012	NONE	
US 11006245 B2	11-05-2021	CA 3151444 A1	08-04-2021
		US 10924889 B1	16-02-2021
		US 10952181 B1	16-03-2021
		US 2021099835 A1	01-04-2021
		US 2021099836 A1	01-04-2021
		US 2021281974 A1	09-09-2021
		WO 2021062522 A1	08-04-2021
DE 102019111345 A1	05-11-2020	AU 2020265397 A1	18-11-2021
		DE 102019111345 A1	05-11-2020
		EP 3963555 A1	09-03-2022
		PE 20220651 A1	29-04-2022
		WO 2020221844 A1	05-11-2020

EPO FORM P0459

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

REFERENCES CITED IN THE DESCRIPTION

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

Patent documents cited in the description

- US 10374863 A **[0010]**
- US 10742475 B **[0010]**
- WO 2020240526 A **[0010]**
- US 2020296556 A **[0010]**
- US 11082109 B **[0010]**
- US 11043094 B **[0010]**
- WO 2021081365 A **[0010]**
- WO 2017106976 A **[0010]**
- US 9524628 B **[0010]**
- EP 3796037 A **[0010]**
- WO 2021062522 A **[0010]**
- US 20200302187 A1 **[0062]**