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

(11) **EP 4 207 122 A1**

(12) **EUROPEAN PATENT APPLICATION**

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

(21) Application number: **21218149.9**

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

(51) International Patent Classification (IPC):
G08B 13/24 *(2006.01)* ***G08B 15/02*** *(2006.01)*

(52) Cooperative Patent Classification (CPC):
G08B 15/02; 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) INTRUDER LOCALISATION

(57) There is provided a premises security monitoring installation having a plurality of alarm event sensors and a plurality of intervention devices, e.g. visibility impairment devices, a location sensing arrangement to detect human presence and location within the premises and comprising a radio-based system that is configured to sense presence and location based on detecting perturbations of radio signals; a local management device to report alarm events to a remote monitoring station, "CMS", the local management device being configured to:
notify the CMS on receiving notification of an alarm event and to supply to the CMS location data from the location sensing arrangement, receive from the CMS a request to trigger a particular one of the plurality of intervention devices based on the supplied location data; and signal to activate the requested intervention device.

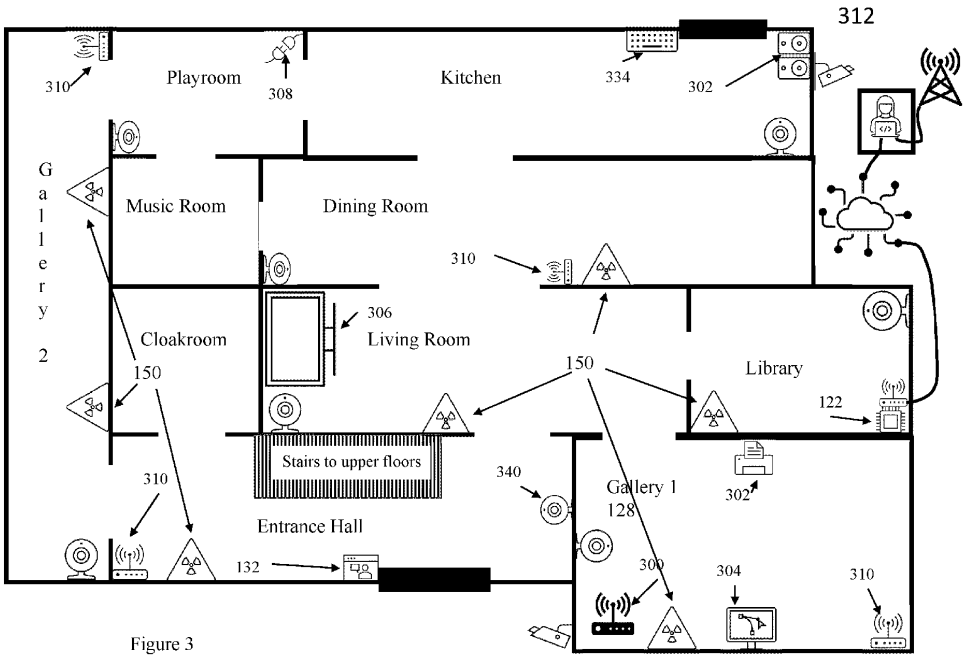

Figure 3

EP 4 207 122 A1

Description

Field

[0001] The present invention relates generally to security monitoring systems for premises, and in particular to such installations including one or more intervention devices.

Background

[0002] Security monitoring systems for monitoring premises, often referred to as alarm systems, typically provide a means for detecting the presence and/or actions of people at the premises and reacting to detected events. Commonly such systems include sensors to detect the opening and closing of doors and windows, movement detectors to monitor spaces (both within and outside buildings) for signs of movement, microphones to detect sounds such as breaking glass, and image sensors to capture still or moving images of monitored zones. Such systems may be self-contained, with alarm indicators such as sirens and flashing lights that may be activated in the event of an alarm condition being detected. Such installations typically include a control unit (which may also be termed a central unit or local management device), generally mains powered, that is coupled to the sensors, detectors, cameras, etc. ("nodes"), and which processes received notifications and determines a response. The local management device or central unit may be linked to the various nodes by wires, but increasingly is instead linked wirelessly, rather than by wires, since this facilitates installation and may also provide some safeguards against sensors/detectors effectively being disabled by disconnecting them from the central unit. Similarly, for ease of installation and to improve security, the nodes of such systems typically include an autonomous power source, such as a battery power supply, rather than being mains powered.

[0003] As an alternative to self-contained systems, a security monitoring system may include an installation at a premises, domestic or commercial, that is linked to a remotely located monitoring station where, typically, human operators manage the responses required by different alarm and notification types. These monitoring stations are often referred to as Central Monitoring Station (CMS) because they may be used to monitor a large number of security monitoring systems distributed around the monitoring station, the CMS located rather like a spider in a web. In such centrally monitored systems, the local management device or central unit at the premises installation typically processes notifications received from the nodes in the installation, and notifies the Central Monitoring Station of only some of these, depending upon the settings of the system - in particular whether it is fully or only partially armed, and the nature of the detected events. In such a configuration, the central unit at the installation is effectively acting as a gateway between the nodes and the Central Monitoring Station. Again, in such installations the central unit may be linked by wires, or wirelessly, to the various nodes of the installation, and these nodes will typically be battery rather than mains powered.

[0004] Security monitoring systems particularly externally monitored systems may also include what may be termed "intervention devices" that are intended to cause an intruder to withdraw from the protected premises or at least to withdraw from or refrain from entering a particular room or zone of the premises. The most common form of intervention device is one which restricts an intruder's ability to see - typically by filling the relevant room or zone with smoke or a smoke-like substance (an opaque gas, a cloud of fine particles or droplets. Sonic intervention devices are also known and may either involve the generation of painfully high sound levels (e.g., 110dB or 120dB or more), or the generation of sounds that are psychologically disturbing or otherwise debilitating.

[0005] Intervention devices that restrict an intruder's ability to see can typically only be discharged once before needing to be refilled - in effect, they are single-use items (albeit that their housings and electronics may be reusable). Such devices may also leave a residue on surfaces in their vicinity or otherwise disrupt normal usage of the room or zone where the device is housed. These factors mean that it is very desirable to avoid triggering these devices as the result of a false alarm. Most false alarms are caused by occupants forgetting that the system is armed and then triggering an alarm event by opening a protected door or window, or by triggering a movement sensor in an armed zone. If an occupant does one of these things and fails to disarm the alarm in time, an alarm event will be reported to the remote monitoring station and/or a local alarm event warning device (e.g., a klaxon, siren and/or flashing lights).

[0006] Because of the single-use nature of vision-limiting intervention devices, and the potential disruption that their use may cause, such devices tend only to be deployed in conjunction with a suitably positioned video camera and with a remote monitoring arrangement in which a human operator can use the video camera to check that it is appropriate to operate the intervention device. For example, the operator in the remote monitoring centre will check to see that image from the video camera, and possibly from other video cameras at the security monitoring system installation, show that there has actually been an intrusion rather than the alarm having been triggered by a pet, children, or some other recognisably false alarm trigger. Only if the operator has a high confidence that the event is not a false alarm, will the operator send a signal to the control unit of the security monitoring system to trigger the intervention device.

[0007] Sometimes however villains use a multi-stage approach to prevent deployment of intervention devices. As a first step, a villain or an accomplice either disturbs

the video camera that monitors the zone containing the intervention device, obscures the lens or the motion sensor associated with the video camera, or otherwise prevents correct operation of the camera. Then later, when they want access to whatever is protected by the intervention device, they break in or otherwise enter the premises and are safe in the knowledge that even though they may trigger an alarm the intervention device will not operate - simply because the monitoring centre operative cannot determine that the event is not a false alarm and that it is safe to trigger the device. By interfering with one or more video cameras or their associated motion sensors, a villain may in effect be able to render useless multiple intervention devices.

[0008] Embodiments of the present invention seek to address this problem.

Summary

[0009] According to a first aspect there is provided a premises security monitoring installation having a plurality of alarm event sensors and one or more (e.g. a plurality) intervention devices (e.g. smoke generating devices);

a location sensing arrangement that uses channel state information analysis to detect human presence and location within the premises;
a local management device to report alarm events to a central monitoring station, "CMS",
the local management device being configured to:

notify the CMS on receiving notification of an alarm event and to supply to the CMS location data from the location sensing arrangement,
receive from the CMS a request to trigger a particular one of the one or more intervention devices based on the supplied location data;
and signalling to activate the requested intervention device.

[0010] Thus, even if the CMS operator cannot see the intruder, the right intervention device can be triggered - or of course a decision may be made not to fire an intervention device because WFS shows that the intruder has already left.

[0011] According to a second aspect there is provided a control unit for a security monitoring system for premises, the system including one or more (e.g. a plurality of) intervention devices, e.g. visibility impairment devices, and 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: perform location sensing to detect human presence and location within the premises based on detecting perturbations of radio signals; notify the CMS on receiving notification of an alarm event and to supply to the CMS location data derived from detected perturbations of radio signals; receive from the CMS a request to trigger a particular one of the plurality of intervention devices based on the supplied location data; and signal to activate the requested intervention device.

[0012] According to a third aspect there is provided a local management device for a premises security monitoring installation, the management device configured to be coupled to: one or more (e.g. a plurality of) intervention devices, e.g. visibility impairment devices, of the installation; a plurality of alarm event sensors; and to a remote monitoring station, "CMS", for the reporting of alarm events; and further configured to: perform location sensing to detect human presence and location within the premises based on detecting perturbations of radio signals; notify the CMS on receiving notification of an alarm event and to supply to the CMS location data derived from detected perturbations of radio signals;
receive from the CMS a request to trigger a particular one of the one or more intervention devices based on the supplied location data; and signal to activate the requested intervention device.

[0013] According to a fourth aspect there is provided a method performed by a local management device of a premises security monitoring installation, the installation including one or more intervention devices, e.g. visibility impairment devices, a location sensing arrangement to detect human presence and location within the premises and comprising a radio-based system that is configured to sense presence and location based on detecting perturbations of radio signals, the method comprising: receiving notification of an alarm event;

notifying a remote monitoring station, "CMS", of the alarm event; supplying the CMS with location data from the location sensing arrangement; receiving from the CMS a request to trigger a particular one of the plurality of intervention devices based on the supplied location data;
and signal to activate the requested intervention device.

Brief description of the drawings

[0014] Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a schematic plan of a single floor of premises in which a first security monitoring system has been installed, the system including a plurality of intervention devices;
Figure 2 illustrates schematically the principles of radio-based presence and location sensing;
Figure 3 is a schematic floor plan corresponding generally to Figure 1 but additionally showing multiple sources of radio signals for use in a radio-based presence and location sensing system based on de-

tecting perturbations of radio signals; and
Figure 4 illustrates schematically features of the local management device of the system of Figure 3.

Specific description

[0015] Figure 1 shows schematically a security monitoring system installation 100 in premises comprising a dwelling standing in grounds, not shown. In this example the premises are in the form of a multi-story house, of which only the ground floor is shown. The house has a front door 104, that serves as the main entrance, and which leads into an entrance hall 106. For simplicity and ease of description the various rooms are shown as linked by doorways, but with doors omitted. In practice, of course, most of the doorways would typically be fitted with doors, and some or all of these doors may be fitted with door opening sensors such as that shown on the front door as sensor 107. Typically, these door opening sensors will be battery powered, using a magnet and a sensing element such as a magnetometer or reed switch, and include a radio transceiver for communicating with the local management device, or central unit, 122 of the security monitoring system. The entrance hall leads through to the living room 108, a dining room 110, and thence into a kitchen 112. The kitchen 112 includes the house's back door 114. Like the front door 104, the back door 114 is also provided with the door opening sensor 107. From the kitchen 112 there is an entry to a playroom 118. The playroom leads into a music room 120, and a first gallery 124 which in turn leads back into the entrance hall 106 which in turn leads to a cloakroom 125. Leading off the living room 108 is a library 126, and a second gallery 128. Stairs 130 in the hall lead up to the upper floors of the house.

[0016] Adjacent the front door 104, in the entrance hall, is a control panel 132 by means of which a user may arm and disarm the security monitoring system 100. In particular, when entering the house through the front door 104 when the system is armed, a user may use the control panel 132 to disarm the monitoring system 100, or to change the armed state from "armed away" - in which the security monitoring system both secures the perimeter of the house, and also monitors the interior of the house with the possibility of an alarm event being triggered upon motion been detected within the house; to "armed at home" state, in which the perimeter is monitored but movement within the house does not give rise to the central unit 122 raising an alarm event.

[0017] Another similar control panel, including a display, may also be provided adjacent the back door, but in this example a disarm node 134 is provided instead. The disarm node permits arming and disarming of the security monitoring system using a dongle, a suitably programmed smart phone, or the like, and possibly arming and disarming by the entry of a PIN using a physical keypad or touchscreen.

[0018] The central unit 122 of the security monitoring system 100, here located in the library 126, is coupled to an external monitoring station 700 by means of a wired (broadband) connection the Internet 710 and also by at least one radio network, e.g. a public land mobile network (PLMN). When the security monitoring system 100 is in the armed state, the triggering of an alarm event will cause the central unit 122 to report the alarm event to the external monitoring station 700, where typically a human operator will intervene, involving police and other security personnel as necessary.

[0019] The house shown in Figure 1 is provided with a plurality of intervention devices 150. Here the intervention devices include a canister of pyrotechnics that can be electrically fired to produce smoke, but they could alternatively contain a heating arrangement and a volatile substance which when heated by the heating arrangement produces a gas, vapour or smoke, or any equivalent which can produce the result of obscuring vision in the vicinity of the device for several minutes upon being triggered. Preferably the intervention device or devices in a room should be able to provide almost complete obscuration of sight throughout the rom in less than 30 seconds - and ideally anyone in the room when the obscuring substance has been released should not be able to see more than 150 mm. Intervention devices 150 are located in the two galleries 124 and 128, the entrance hall 106. the living room 108, the dining room 110, and the library 126. Because of its size and volume, the first gallery 124 is provided with two intervention devices.

[0020] Each room with an intervention device preferably has a video camera 140, and video cameras are also provided in two rooms that do not have intervention devices: the kitchen and the playroom. In addition, external video cameras 142 are provided to the front and rear of the premises. All or some of these video cameras may be connected to a mains power supply, but more commonly only the external video cameras are powered in this way (with a battery power supply backup). The internal video cameras may rely on autonomous power supplies, such as internal battery power supplies. The cameras relying on autonomous power supplies will typically include a first transceiver, with low-power consumption and low bandwidth, for receiving control signals from, and for reporting events to the central unit 122, along with a larger bandwidth and more power-hungry second transceiver, such as a Wi-Fi transceiver, for the transmission of images and video signals to the central unit (typically only done on command from the central unit, often as a result of an intervention from the remote monitoring station 700).

[0021] The house is shown without any windows, but of course in practice there would be windows and typically some at least of these windows would be provided with sensors to detect opening or attempted opening the windows, again battery-powered and typically coupled to the central unit by means of an internal low bandwidth and low power transceiver.

[0022] If an intruder breaks into the house when the

security monitoring system is in the armed away state, typically a window or door sensor node will be triggered, resulting in an alarm event signal being sent by the node central unit 122. Upon receiving the alarm event signal, the central unit 122 will typically report this to the remote monitoring station 700. As the intruder moves around the house, there are likely to trigger motion sensors, for example integrated into or associated with one or more of the internal video cameras 140. The relevant motion sensor or camera will then likewise report an alarm event to the central unit 122, which will typically again be forwarded to the remote monitoring station 700. As soon as the central unit determines that there is an alarm event it will typically send a request to each camera, as soon as the camera is triggered, to transmit its video to the central unit 122. The central unit is typically not configured to store the videos received from the video cameras but instead forwards them to the remote monitoring station immediately upon receipt. At the central monitoring station 700 received videos are stored for review by an operative of the CMS.

[0023] As the intruder moves from room to room, different ones of the internal video cameras, or their associated motion sensors, will be triggered, causing further alarm event notifications to the central unit. The internal video cameras 140 may be configured to start to capture images, and possibly video sequences, starting from the triggering of the respective motion sensor, and typically these images and video sequences are initially stored on internal memory of the cameras 140 until they have been sent to the central unit 122, upon its request. Because the internal cameras 140 are typically battery-powered, and because the large bandwidth transceivers (e.g. Wi-Fi transceiver is used to transmitting video from the cameras to the central unit 122 tend to be power hungry, it is often the case that the battery-powered cameras are configured only to transmit video (more generally, images) on request from the central unit 122.

[0024] At the remote monitoring station, when the human operator picks up the alarm event notification from the central unit, the operator needs to assess whether the alarm indications suggest that there is a real incident, or whether it is a false alarm. This can be difficult without seeing images, and in particular high resolution video images. So the operator will review the video files or image files from the cameras that have been triggered and which have been received by the remote monitoring station. The operator will be aware that the security monitoring system installation includes several intervention devices 150 but will also be aware of the need to review relevant video/images showing the regions about the various intervention devices before deciding to trigger one or more of the intervention devices.

[0025] But if the villain or an accomplice has interfered with the relevant video cameras or their associated motion sensors (e.g., internal or external PIR device), the relevant cameras will not provide any usable video even if they are triggered. Consequently, with the operator unable to determine whether it is appropriate to trigger any of the intervention devices, none of the devices will be triggered and the villain/intruder will be free to explore the premises and able to see valuables and navigate through the various rooms without any problem - the intervention devices having been rendered ineffective.

[0026] There therefore exists a need to solve the problem of intervention devices having been rendered ineffective by interruption of relevant video feeds.

[0027] This is the main problem addressed by the present invention.

[0028] The underlying idea is to introduce to the premises a radio-based location sensing arrangement to detect human presence and that is configured to sense presence and location based on detecting perturbations of radio signals, and for the local management device to report alarm events to the remote monitoring station, on receiving notification of an alarm event and to supply location data from the location sensing arrangement. The remote monitoring station can then use the supplied location data, and knowledge of the location of the intervention device(s) in the premises, to determine which intervention devices it wants to trigger, if any, based on analysis of the supplied location data. The monitoring station can then send to the central unit of the security monitoring system a request to trigger an identified one of the plurality of intervention devices selected based on the supplied location data, and the central unit can then signal to activate the requested intervention device. The volume of data that needs to be transferred to the remote monitoring station to enable the current location of an intruder is relatively small and can therefore generally be transferred quite quickly. This means that the remote monitoring station, typically a human operative, is able rapidly to determine where an intruder is with respect to the intervention device(s) in the house, without requiring confirmation from video/images from the relevant video cameras of the installation. And if the presence/location information shows that there is no longer anyone present, the operator can safely make the decision not to trigger any intervention device and inform the police or other security personnel that there is no longer an imminent threat.

[0029] Consequently, the remote monitoring centre can make decisions and interventions based on what is happening in the premises. In effect embodiments of the invention enable intruder localisation, and the use of intruder localisation in speeding up decision making and interventions when relevant images/videos are unavailable.

[0030] We will now provide a brief introduction to radio-based presence detection, which may for example be based on analysing the signal dynamics and signal statistics of radio signals and/or detecting changes in channel state information (CSI). A radio (or wireless) signal as used herein refers to a signal transmitted from a radio transmitter and received by a radio receiver, wherein the radio transmitter and radio receiver operate according to

a standard or protocol. Such standards include, but are not limited to, IEEE 802.11. (which includes the Wi-Fi standards), IEEE 802.15 (which includes Zigbee), Bluetooth SIG, IEEE 802.16, IEEE 802.20, UMTS, GSM 850, GSM 900, GSM 180, GSM 19011, GPM ITU-R 5.13, GPM ITU-R 5.150, ITU-R 5.280, 3GPP 4G (including LTE), 3GPP 5G, 3GPP NR, AND IMT-2000. However, the radio transmitters and receivers may operate in non-telecommunications or Industrial, Scientific and Medical (ISM) spectral regions without departing from the scope of the invention.

[0031] Essentially the idea is to use radio signals to probe a zone or zones of interest, and to analyse and extract statistics from these signals, in particular looking at the physical layer and/or data link layer such as MAC address measurements that expose the frequency response of a radio channel (e.g., CSI or RSSI measurements). These measurements are processed to detect anomalies and variations over time, and in particular to detect changes signifying the entrance of a person and/or movement of a person within a monitored zone. The zone(s) to be monitored need to be covered sufficiently by radio signals, but the sources of the radio signals may either already be present before a monitoring system is established - for example from the plurality of Wi-Fi or Bluetooth capable devices that are now dotted around the typical home or office, or the sources may be added specifically to establish a monitoring system. Often some established (i.e., already located or installed) radio devices are supplemented by some extra devices added as part of establishing a radio-based presence detection system. Among the types of devices (preinstalled or specifically added) that may be used as part of such a detection system are Wi-Fi access points, Wi-Fi routers, smart speakers, Wi-Fi repeaters, as well as video cameras and video doorbells, smart bulbs, etc. Because presence (or intrusion) is detected by detecting a change in the properties or character of radio signals compared to some previous reference signal(s), it is preferred to establish what might be termed the monitoring network between radio devices that are essentially static (i.e., that remain in the same position for extended periods) rather than relying on devices that are repeatedly moved - such as smart phones, headphones, laptops, and tablet devices. It is not strictly speaking essential for all the devices whose signals are used by the monitoring system to be part of the same network - for example, signals from Wi-Fi access points of neighbouring premises could be used as part of a monitoring system in different premises. Again, a primary consideration is the stability of the signals from the signal sources that are used. Wi-Fi access points provided by broadband routers are seldom moved and rarely turned off, consequently they can generally be relied upon as a stable signal source - even if they are in properties neighbouring the property containing the zone or zones to be monitored.

[0032] The idea is illustrated very schematically in Figure 2, here with an installation 200 including just a single source (or illuminator) 202 and just a single receiver 204, for simplicity, although in practice there will typically be multiple sources (illuminators) and sometimes plural receivers. The installation 200 has been established to monitor a monitored zone 206. In Figure 2A we see that in steady state, and in the absence of a person, radio signals are transmitted from the source 202, spread through the monitored zone 206, and are received by the receiver 204. Of course, in most installations there will be walls, ceilings, floors, and other structures that will tend to reflect, at least in part, signals from the source. Furniture and other objects may block and attenuate the signals, the reflected signals will give rise to multiple paths, and the signals may interfere with each other, and there may be scattering and other behaviours, such as phase shifts, frequency shifts, all leading to complexity in the channels experienced by the radio signals that arrive at the receiver 204. But while the environment is static and unchanging, the receiver will tend to see a consistent pattern of radio signals. And this is true whether or not the source transmits continuously or transmits periodically. But this consistent pattern of received signals is changed by the arrival of an intruder 208, as shown in Figure 2B. From Figure 2B we see that, at the very least, the presence of a person in the monitored zone blocks at least some of the signals from the source, and that affects the pattern of radio signals received by the receiver 204. The changed pattern of signals received by the receiver enables the presence of the intruder to be detected by a presence monitoring algorithm that is supplied with information derived from the received signals. It will be appreciated that the nature and extent of the perturbation of the signals passing from the source 202 to the receiver 204 is likely to change as the intruder 208 enters, passes through, and leaves the monitored area 206, and that this applies also to reflected, refracted, and attenuated signals. These changes may enable the location of a person within the zone, and their speed of movement, to be determined.

[0033] It will be realised that signals that are received from an illuminator device (or from more than one illuminator device) after having passed through a monitored space (or volume), have in effect been filtered by the environment to which they have been exposed. We can therefore imagine the monitored volume as a filter having a transfer coefficient, and we can see that a received signal is at least in part defined by the properties, or channel response, of the wireless channel through which it 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.

[0034] 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.

[0035] 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.

[0036] Although the Figure 2 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 multiple zones may have a dedicate receiver that does not serve other zones. Likewise, a radio signal source (illuminator) may provide illuminating signals for a single monitored zone or for multiple monitored zones. Also, a presence monitoring system (and a security monitoring system including such a presence monitoring system) may use mesh network arrangement, for example a Wi-Fi mesh network, in which multiple devices act as receivers for illuminating signals - either for a single monitored zone or for multiple monitored zones.

[0037] Figure 3 is based on Figure 1 but illustrates the presence of multiple sources of radio signals that may be used in a radio-based system that senses presence and location based on detecting perturbations of radio signals. For clarity, elements already labelled in Figure 1 should be considered to carry the same reference numerals, although in the interests of clarity these have largely been omitted. Newly introduced elements are indicated by new reference numerals. As explained with reference to Figure 2, ideally we want to ensure that the whole area of interest is adequately covered by radio signals (from relevant sources, of course) so that there are no blind spots.

[0038] The radio-based presence sensing, which may conveniently be based on the monitoring of Wi-Fi signals, and to which for convenience we will refer hereafter 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.

[0039] 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 140 might be replaced by a mains powered equivalent 340, and battery powered disarm node 134 may be replaced by a mains powered equivalent 334 that is Wi-Fi capable (although the control unit may still use something other than Wi-Fi to communicate with the central unit).

[0040] Alternatively (or additionally) we may simply add new mains powered Wi-Fi capable devices such as smart plugs, smart bulbs, Wi-Fi range extenders (for example of the type that simply plug in to a socket of the mains electricity supply), to provide a Wi-Fi network that covers the whole of the area of interest.

[0041] The central unit AP 122 preferably works in infrastructure mode in conjunction with the various other Wi-Fi stations (STAs) to form either an infrastructure Basic Service Set (BSS) or, in conjunction with another AP connected to the same Local Area Network as the central unit 122 - such as broadband router 300, to provide an Extended Service Set (ESS).

[0042] For ease of explanation, we will assume initially that the central unit AP 122 provides just a BSS and not an ESS, and that only the central unit AP 122 serves as a Wi-Fi sensing receiver. Some or all of the STAs in the BSS act as illuminators to provide signals which the CU 122 analyses in order to perform WFS. As shown, these other STAs include the broadband router 300, in the second gallery, a smart TV 306 in the living room, a smart plug 308 in the play room, Wi-Fi range extenders 310 in various rooms, the control unit 130 and a Wi-Fi-enabled camera 340 in the hall, and optionally the disarm node 334 in the kitchen. Preferably, because of the power consumption concerns, both the Wi-Fi enabled camera and the disarm node 334 are fed with power from a mains electricity supply as well as having an autonomous internal power supply. In addition, the kitchen is provided with

an STA in the form of for example a "smart speaker" 312. If the disarm node 334 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.

[0043] It will be appreciated that by combining a radio-based location sensing arrangement with a security monitoring system that includes one or more intervention devices it is possible to use the location sensing arrangement as a guide as to which if any intervention device is likely to be best located to thwart the activities of an intruder. And we can even use this information predictively, so that for example the monitoring station may instruct the central unit 122 to activate an intervention device based on a prediction that the intruder will imminently enter the space in which the intervention device is deployed. Depending upon the layout of the premises, the locations of the intervention devices it may even be possible to guide the intruder out of the premises by selectively blocking certain routes by selective triggering of intervention devices - on the basis that it may be preferable to eject the intruder than to prevent his/her escape.

[0044] Thus the problem is solved by providing a premises security monitoring installation having a plurality of alarm event sensors and one or more intervention devices, e.g. visibility impairment devices, a location sensing arrangement to detect human presence and location within the premises and comprising a radio-based system that is configured to sense presence and location based on detecting perturbations of radio signals; a local management device to report alarm events to a remote monitoring station, "CMS", the local management device being configured to: notify the CMS on receiving notification of an alarm event and to supply to the CMS location data from the location sensing arrangement, receive from the CMS a request to trigger a particular one of the one or more intervention devices based on the supplied location data; and signal to activate the requested intervention device.

[0045] Optionally, the one or more intervention devices comprise visibility impairment devices, optionally smoke generating devices, and preferably electrically triggered pyrotechnic smoke devices.

[0046] In security monitoring installation according to embodiments of the invention the radio-based system is preferably configured to process communication signals received from one or more radio transmitters operating according to one or more communication standards or protocols, as distinct for example from merely processing RF carrier waves or other unmodulated signals. It will be appreciated that the ubiquity of sources of communication signals in the domestic (and commercial) environment mean that by using such sources the cost of deployment, and the time involved in deploying, a radio-based presence and location system are much reduced. Moreover, communication signals according to communication standards or protocols typically have structures and features that can readily be exploited in the provision of radio-based presence and location systems. The one or more radio transmitters may be in a common wireless network with the local management device, as this facilitates integration of the radio-based presence and location system into the security monitoring system - which is likely to reduce both the cost and the installation time required to deploy such a security monitoring system.

[0047] The local management device of security monitoring installations according to embodiments of the invention preferably includes a radio receiver of the radio-based presence and location sensing system, rather than for example receiving presence and location data or signals from another device which is part of the radio-based presence and location sensing system. This helps to reduce complexity and hence also reduce both cost and speed of deployment. Importantly, in the cases that the radio-based system is configured to process communication signals according to one or more communication standards or protocols, it also enables the local management device to benefit directly from recovery protocols and mechanisms integrated into the relevant communication standards or protocols.

[0048] Preferably, the local management device includes a processor and a memory holding software instructions that when run on the processor cause the local management device to process radio signals to derive location and presence data. This helps to reduce complexity and hence also reduce both cost and speed of deployment.

[0049] Optionally, in security monitoring installations according to embodiments of the invention the sensing arrangement to detect human presence uses changes in channel state information or received signal strength in determining presence.

[0050] Optionally, in security monitoring installations according to embodiments of the invention the local management device functions as an access point of a radio network, such as a Wi-Fi network, whose signals are used by the radio-based presence and location sensing system. This may have the benefits of reducing installation complexity and enabling quicker setup. In such security monitoring installations, the radio network for which the local management device functions as an access point may include at least one further access point. For example, in a Wi-Fi deployment the Wi-Fi network may be based on an Extended Service Set model, with two or more interconnected APs.

[0051] Optionally, in security monitoring installations according to embodiments of the invention the one or more radio transmitters may include one or more of the following: a Wi-Fi access point, a Wi-Fi extender, a smart plug or smart socket, a smart speaker, a smart bulb, a control panel of the security monitoring system, a Wi-Fi-enabled video camera.

[0052] In an embodiment there is provided a control

unit for a security monitoring system for premises, the system including one or more intervention devices, e.g. visibility impairment devices, and 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: perform location sensing to detect human presence and location within the premises based on detecting perturbations of radio signals; notify the CMS on receiving notification of an alarm event and to supply to the CMS location data derived from detected perturbations of radio signals; receive from the CMS a request to trigger a particular one of the one or more intervention devices based on the supplied location data; and signal to activate the requested intervention device.

[0053] The control unit may further comprise a radio transceiver communicatively coupled to the processor, wherein the processor is configured to perform location sensing by detecting perturbations in radio signals received by the transceiver.

[0054] In a further embodiment there is provided a local management device for a premises security monitoring installation, the management device configured to be coupled to:

> one or more intervention devices, e.g. visibility impairment devices, of the installation;
> a plurality of alarm event sensors; and to a remote monitoring station, "CMS", for the reporting of alarm events; and further configured to: perform location sensing to detect human presence and location within the premises based on detecting perturbations of radio signals; notify the CMS on receiving notification of an alarm event and to supply to the CMS location data derived from detected perturbations of radio signals; receive from the CMS a request to trigger a particular one of the one or more intervention devices based on the supplied location data; and signal to activate the requested intervention device.

[0055] Preferably the local management device is configured to perform location sensing by processing communication signals received from one or more radio transmitters operating according to one or more communication standards or protocols. In an alternative, something else such as Wi-Fi extender, or another AP, may perform the location and presence sensing and provide the results to a local management device or central unit.

[0056] Preferably the local management device further comprises a radio transceiver that the local management device uses as a radio receiver of a radio-based presence and location sensing system. The local management device may be a controller of a security monitoring system in which the intervention device(s), video cameras and other sensors are coupled to the local management device using wires rather than wirelessly. But, in general, the local management device will include one or more transceivers for wireless exchange of control and housekeeping signals with video cameras and other nodes and sensors of the system, but these will typically support the use of low bandwidth transmissions that can be supported by low power, low bandwidth transceivers in the nodes and sensors of the system - permitting the use of internal battery power supplies in the nodes and sensors, while still achieving reasonable battery life. The local management device may include a further transceiver, such as a Wi-Fi transceiver, that is used as a radio receiver of the radio-based presence and location sensing system - and optionally also for the transfer of video data from video cameras of the security monitoring system.

[0057] Preferably, the local management device further comprises a processor and a memory holding software instructions, the software instructions when run on the processor causing the local management device to process radio signals to derive location and presence data.

[0058] Preferably, the local management device is configured to detect human presence and location using changes in channel state information or received signal strength.

[0059] In an embodiment there is provided a method performed by a local management device of a premises security monitoring installation, the installation including one or more *intervention* devices, e.g. visibility impairment devices, a location sensing arrangement to detect human presence and location within the premises and comprising a radio-based system that is configured to sense presence and location based on detecting perturbations of radio signals, the method comprising: receiving notification of an alarm event; notifying a remote monitoring station, "CMS", of the alarm event; supplying the CMS with location data from the location sensing arrangement; receiving from the CMS a request to trigger a particular one of the one or more intervention devices based on the supplied location data; and signal to activate the requested intervention device.

[0060] Preferably the method further comprises determining a location of human presence within the premises before the step of supplying the CMS with location data from the location sensing arrangement.

[0061] Figure 4 is a schematic drawing showing in more detail features of the gateway or central unit 122 of Figures 1. The gateway 122 includes a first transceiver 430 coupled to the first antenna 480, and optionally a second transceiver 432 coupled to a second antenna 482. The transceivers 430 and 432 can each both transmit and receive, but a transceiver cannot both transmit and receive at the same time. Thus, the transceivers 430, 432 each operate in half duplex. Preferably a transceiver will use the same frequency to transmit and receive (although of course if the two transceivers are to operate simultaneously but in opposite modes, they will operate on different frequencies). The transceivers 430, 432 may be arranged such that one transceiver 430 uses a first frequency for transmit and receive and the second transceiver 432 uses the same first frequency for transmit and

receive, i.e. the transceivers are arranged to operate in a diversity-like arrangement. Alternative, the second transceiver may, depending on configuration, be arranged to use a second frequency for transmit and/or receive. The transceivers 430 and 432 are coupled to a controller 450 by a bus. The controller 450 is also connected to a network interface 460 by means of which the controller 450 may be provided with a wired connection to the Internet and hence to the monitoring centre 700. The controller 450 is also coupled to a memory 470 which may store data received from the various nodes of the installation for example event data, sounds, images and video data. The central unit 122 also includes a crystal oscillator 451, which is preferably a temperature controlled or oven-controlled crystal oscillator. This is used for system clocking and also frequency control of the transceivers. The gateway 122includes a power supply 362 which is coupled to a domestic mains supply, from which the gateway 122 generally derives power, and a backup battery pack 464 which provides power to the gateway in the event of failure of the mains power supply. Preferably, as shown, the central unit 122 also includes a Wi-Fi transceiver 440, and associated antenna arrangement 442, which may be used for communication with any of the nodes that is Wi-Fi enabled. The Wi-Fi enabled node may be a remote control or control panel that may for example be located close to the main entrance to the building (e.g., control panel 128 or disarm node 130) to enable the occupier to arm or disarm the system from near the main entrance, or it may for example be an image-capture device such as a video camera (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 700 over, for example, the European 863MHz to 870MHz frequency band. Optionally, the third transceiver 434 may be a Sigfox transceiver configured to use the Sigfox network to contact the central monitoring station especially in the event that jamming of other radio channels is detected.

[0062] The first 430 and second 432 transceivers may both be tuneable ISM devices, operating for example in the European 863MHz to 870MHz frequency band or in the 915MHz band (which may span 902-928MHz or 915-928MHZ depending upon the country). In particular, both of these devices may be tuned, i.e. may be tuneable, to the frequencies within the regulatorily agreed sub-bands within this defined frequency band. Alternatively, the first transceiver and the second transceiver, if present, may have different tuning ranges and optionally there is some overlap between these ranges.

[0063] The controller 450 is configured to run a sensing application using a WFS software agent 800, which may be stored in memory 470. The WFS software agent 400 uses WFS radio APIs in the Wi-Fi transceiver 440 to interact with the Wi-Fi radio, the APIs enabling extraction of desired channel environment measurement information and provides the ability to assert any related controls to configure WFS features. This behaviour will be described in more detail shortly. The sensing application on the CU will report a presence state change when the appropriate thresholds are triggered, along with the address of the device whose received data triggered the algorithm. The WFS agent provides a monitoring system which enables the security monitoring system to detect presence and movement in a monitored space, without the necessity to use line of sight motion detectors.

[0064] 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".

[0065] 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.

[0066] 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.

[0067] 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.

[0068] Different modes of Wi-Fi Sensing measurements are recognised - Passive, Triggered, Invoked, and Pushed, and these depend upon what triggers the illu-

minator device to transmit a Wi-Fi signal. Preferably the agent improves the usefulness of the standard beacon interval by using optimised timings.

[0069] 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.

[0070] 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).

[0071] Invoked measurement involves utilizing a packet transmission that is in response to a packet received from the Wi-Fi Sensing receiver device.

[0072] 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.

[0073] 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.

[0074] 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.

[0075] A WFS system can be built based on existing Wi-Fi standards, hardware, software and infrastructure.

[0076] 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.

[0077] 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.

[0078] 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.

[0079] 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.

[0080] 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.

[0081] 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.

[0082] 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).

[0083] 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.

[0084] 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.

[0085] 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.

[0086] 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.

[0087] 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.

[0088] The nature of Wi-Fi networks is such that it should be possible able to add additional Wi-Fi sensing capable devices to the network to enhance accuracy, coverage and/or localization. These additional devices do not necessarily need to be Wi-Fi Sensing capable or dedicated Wi-Fi sensing devices to participate; however, optionally they may also identify their Wi-Fi sensing capabilities and supported features to the AP. Internet of Things (IoT) devices for home deployment can typically also be used as part of a WFS installation supporting a WFS-enabled security monitoring system: example include Wi-Fi controllable plugs and sockets, light bulbs, thermostats, smart speakers, and video door bells. However, even when a device connects to the AP and reports that it is Wi-Fi sensing capable, the Wi-Fi Sensing agent may elect not to make use of that device.

[0089] 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.

[0090] 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.

[0091] 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.

[0092] 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.

[0093] 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.

[0094] 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.

[0095] 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.

[0096] The IEEE 802.1 1a preamble is useful for Wi-Fi Sensing. The preamble contains a short training field (STF), a guard interval and a long training field (LTF). The STF is used for signal detection, automatic gain control (AGC), coarse frequency adjustment and timing synchronization. The LTF is used for fine frequency adjustment and channel estimation. Since only 52 subcarriers are present, the channel estimation will consist of 52 frequency points. Newer OFDM PHY versions (HT/VHT/HE) maintain the IEEE 802.11a preamble for backward compatibility and refer to it as the legacy preamble. The legacy preamble spans a 20MHz bandwidth and consists of a legacy STF (L-STF) and legacy LTF (L-LTF). As more recently defined OFDM PHY versions (HT/VHT/HE) introduce wider channel bandwidths (up to 160MHz) for backward compatibility, the legacy preamble is duplicated on each 20MHz channel. This allows the receiver to compute 52, 104, 208 or 416 valid L-LTF frequency points, which represent the channel estimation between the two devices.

[0097] 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.

[0098] 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 802.1 1ad (and is also part of the subsequent 802.1 1ay amendment). Regardless of the modulation scheme, every packet starts with a preamble that consists of a short training field (STF) and a channel estimation field (CEF). The STF is used for timing estimation and AGC adjustment. CEF is used for channel estimation. Similar to the OFDM-based PHYs, the necessary channel estimation for Wi-Fi Sensing is available following successful reception and processing of the preamble of a packet and can be provided to the higher layers. The wide channel bandwidth available in 802.11ad/ay can significantly improve the performance of Wi-Fi Sensing in terms of the resolution; however, the limited communication range in 60GHz band restricts the sensing range and coverage. As such, in many situations the central unit of a security monitoring system may relay instead on frequency bands with longer range, sufficient to cover the majority of households. However, for smaller-scale installations the use of the 60GHz band may be attractive and therefore embodiments of the invention may use this band for WFS.

[0099] 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.

[0100] 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.

[0101] 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.

[0102] As already noted, there are different types of transmissions that can be used for illumination of the Wi-Fi channel and obtaining measurements between two devices. Passive transmissions rely on existing Wi-Fi traffic and do not introduce any new MAC layer requirements. Triggered transmissions, however, rely on additional transmissions. Depending on whether existing packet exchange procedures are used for triggered transmissions or new exchanges are defined, the requirements on the MAC layer will be different. An example of one existing packet exchange that can be used for triggering invoked transmissions is null data packet (NDP) and ACK exchange. NDP transmission by the Wi-Fi Sensing receiver can be used to invoke a Wi-Fi Sensing transmitter to respond with an ACK, which may then be used to compute a channel estimation. The disadvantage of using ACK packets for channel estimation, in 2.4/5GHz bands, is that the ACKs are only transmitted in legacy mode. Another example of how an invoked measurement can be triggered is by use of the implicit unidirectional beamforming procedure, first defined in the IEEE 802.1 In standard. In this procedure, an STA requests beamforming training by sending a MAC frame with the training request (TRQ) bit set to 1. This triggers the receiving device to send an NDP announcement, followed by an NDP to illuminate the channel. The benefit of this invoked measurement is that it is not limited to the legacy preamble for channel measurements and uses the MIMO training fields, as well.

[0103] 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.

[0104] 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.

[0105] To interact with the MAC and PHY, the WFS agent has an interface to pass the WFS control information to the radio and extract the measurement data. The interface should be PHY agnostic and is, therefore, defined in a generic manner and extendable to cover different radio driver implementations, including drivers from different chipset vendors. The interface definition should allow for potential additional features or capabilities provided by a specific PHY or a chipset, as well as a path for growing the technology. Definition of a standard interface/API enables radio firmware and driver developers to ensure compliance and enables reuse of components or common codes, which may be placed into a library. Most Wi-Fi drivers are based on either the wireless-extensions framework or the more recent and actively developed cfg80211 / nl80211 framework. As the system integration components are largely provided, these frameworks enable Wi-Fi driver developers to focus on the hardware aspects of the driver. These frameworks also offer significant potential as a location for defining a WFS API. The WFS interface should provide the WFS agent with STA identification and enable the WFS agent to track the physical device in the network (i.e., the AP to which it is connected), as well as the device's capability and availability to participate in the measurements.

[0106] 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.

[0107] 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.

[0108] The WFS interface should be flexible enough for the radio to specify whether the data payload is in time-domain or frequency-domain, the numerical format, etc. By having this knowledge, the Wi-Fi Sensing agent can correctly interpret the data.

Claims

1. A premises security monitoring installation having a

plurality of alarm event sensors and a plurality of intervention devices, e.g. visibility impairment devices, a location sensing arrangement to detect human presence and location within the premises and comprising a radio-based system that is configured to sense presence and location based on detecting perturbations of radio signals;

a local management device to report alarm events to a remote monitoring station, "CMS", the local management device being configured to:

notify the CMS on receiving notification of an alarm event and to supply to the CMS location data from the location sensing arrangement,
receive from the CMS a request to trigger a particular one of the plurality of intervention devices based on the supplied location data;
and signal to activate the requested intervention device.

2. The security monitoring installation of claim 1, wherein the plurality of intervention devices comprises visibility impairment devices, optionally smoke generating devices, and preferably electrically triggered pyrotechnic smoke devices.

3. The security monitoring installation of claim 1 or claim 2, 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, and optionally wherein the one or more radio transmitters that are in a common wireless network with the local management device.

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

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

6. The security monitoring installation as claimed in any one of the preceding claims, wherein the local management device functions 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 for which the local management device functions as an access point includes at least one further access point, and optionally
the radio network is a Wi-Fi network.

7. The security monitoring installation of claim 6 as dependent on claim 3, wherein the one or more radio transmitters include one or more of the following: a Wi-Fi access point, a Wi-Fi extender, a smart plug or smart socket, a smart speaker, a smart bulb, a control panel of the security monitoring system, a Wi-Fi-enabled video camera.

8. A control unit for a security monitoring system for premises, the system including one or more intervention devices, e.g. visibility impairment devices, and 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:

perform location sensing to detect human presence and location within the premises based on detecting perturbations of radio signals;
notify the CMS on receiving notification of an alarm event and to supply to the CMS location data derived from detected perturbations of radio signals;
receive from the CMS a request to trigger a particular one of the plurality of intervention devices based on the supplied location data;
and signal to activate the requested intervention device.

9. A control unit as claimed in claim 8, further comprising a radio transceiver communicatively coupled to the processor, wherein the processor is configured to perform location sensing by detecting perturbations in radio signals received by the transceiver.

10. The control unit of claim 9, wherein the control unit is configured to perform location sensing by processing communication signals received from one or more radio transmitters operating according to one or more communication standards or protocols.

11. The control unit as claimed in claim 10, further comprising a radio transceiver, the control unit being configured to use the transceiver as a radio receiver of a radio-based presence and location sensing system.

12. The control unit as claimed in any one of claims 8 to 11, wherein the control unit is configured to detect human presence and location using changes in

channel state information or received signal strength.

13. A method performed by a local management device of a premises security monitoring installation, the installation including one or more intervention devices, e.g. visibility impairment devices, a location sensing arrangement to detect human presence and location within the premises and comprising a radio-based system that is configured to sense presence and location based on detecting perturbations of radio signals, the method comprising:

receiving notification of an alarm event;
notifying a remote monitoring station, "CMS", of the alarm event;
supplying the CMS with location data from the location sensing arrangement;
receiving from the CMS a request to trigger a particular one of the plurality of intervention devices based on the supplied location data;
and signal to activate the requested intervention device.

14. The method of claim 13, further comprising determining a location of human presence within the premises before the step of supplying the CMS with location data from the location sensing arrangement.

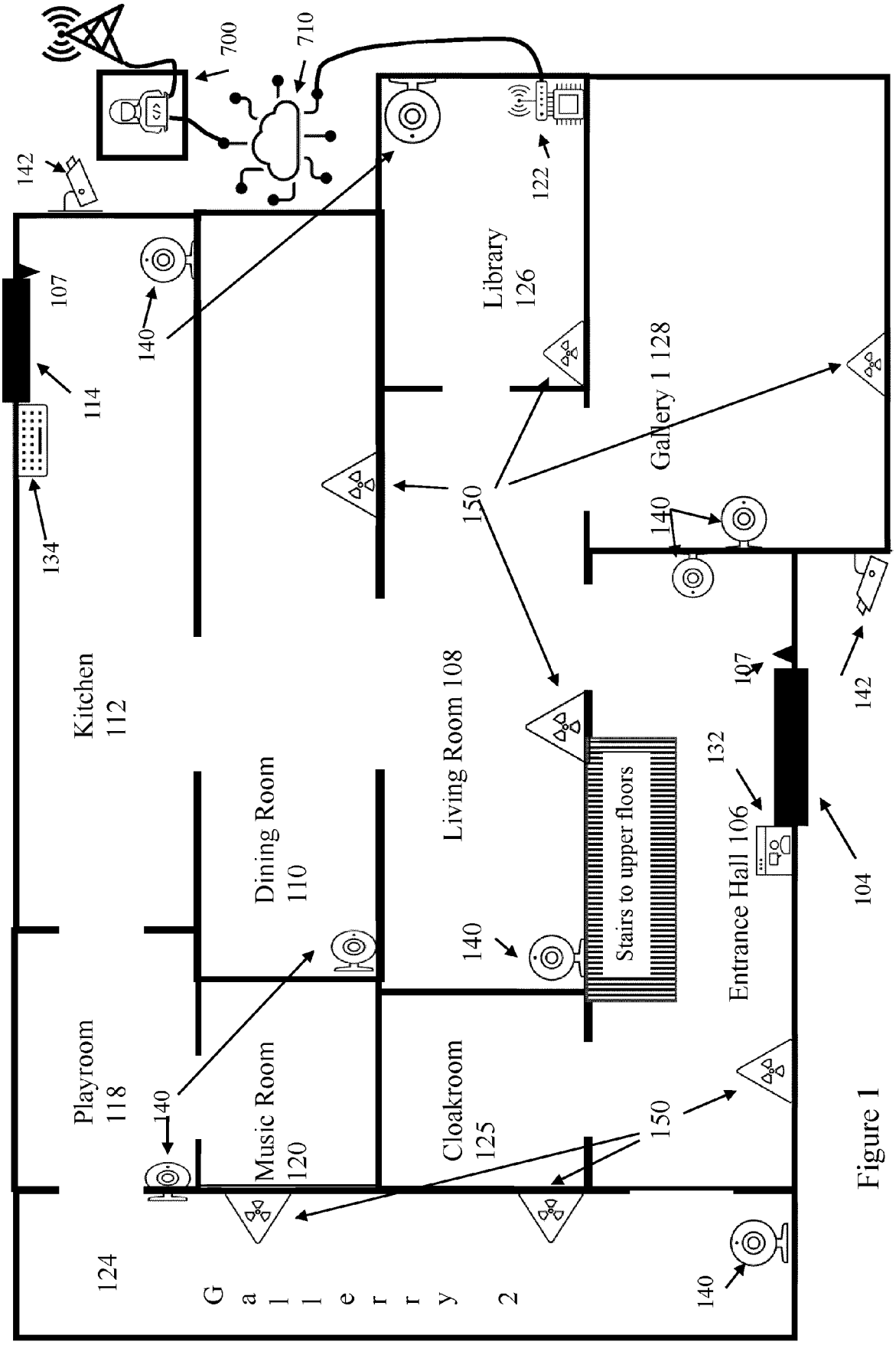
700
710
142
107
114
134
140
122
Library
126
Gallery 1 128
150
Kitchen
112
Living Room 108
Dining Room
110
Stairs to upper floors
132
Entrance Hall 106
104
Playroom
118
Music Room
120
Cloakroom
125
124
Gallery 2

Figure 1

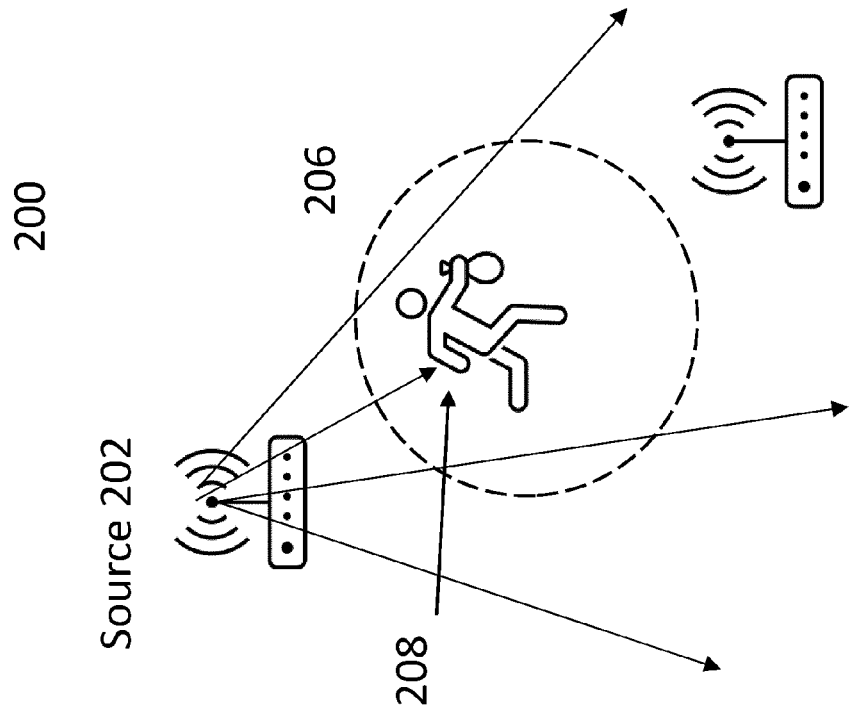

Figure 2B

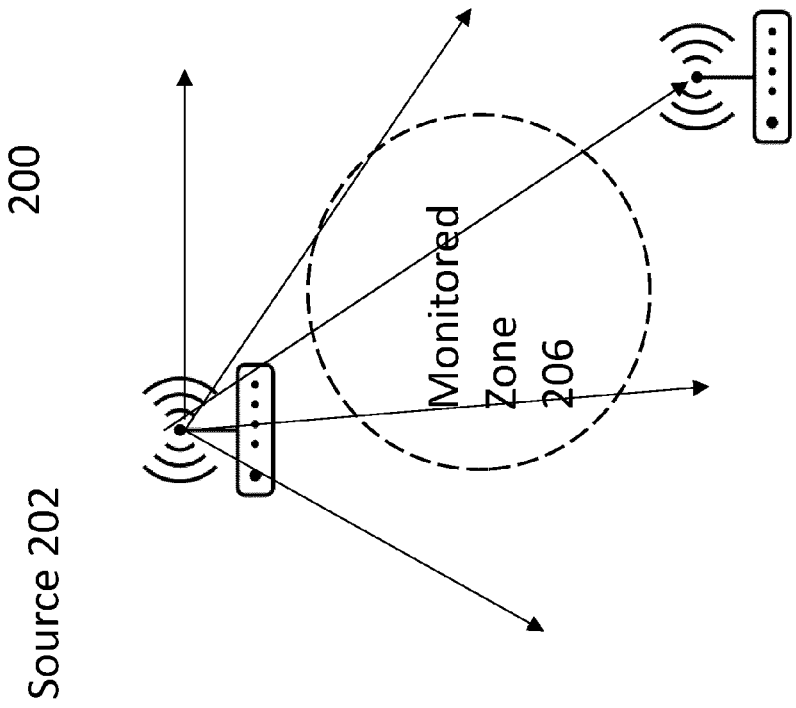

Figure 2A

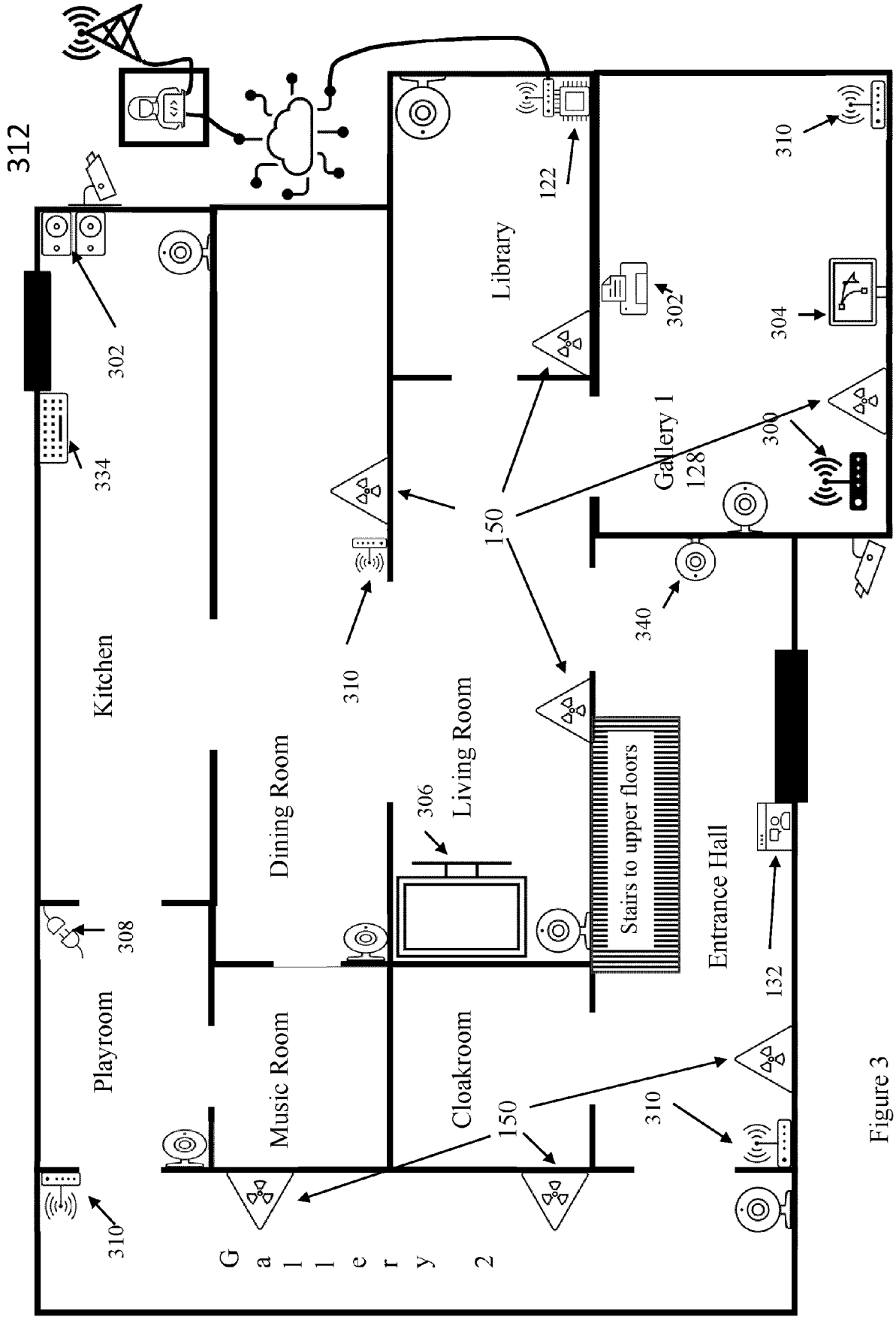
312
Gallery 2
Kitchen
Dining Room
Library
Gallery 1
128
Living Room
Stairs to upper floors
Entrance Hall
Playroom
Music Room
Cloakroom
302
334
310
150
306
308
122
304
340
132

Figure 3

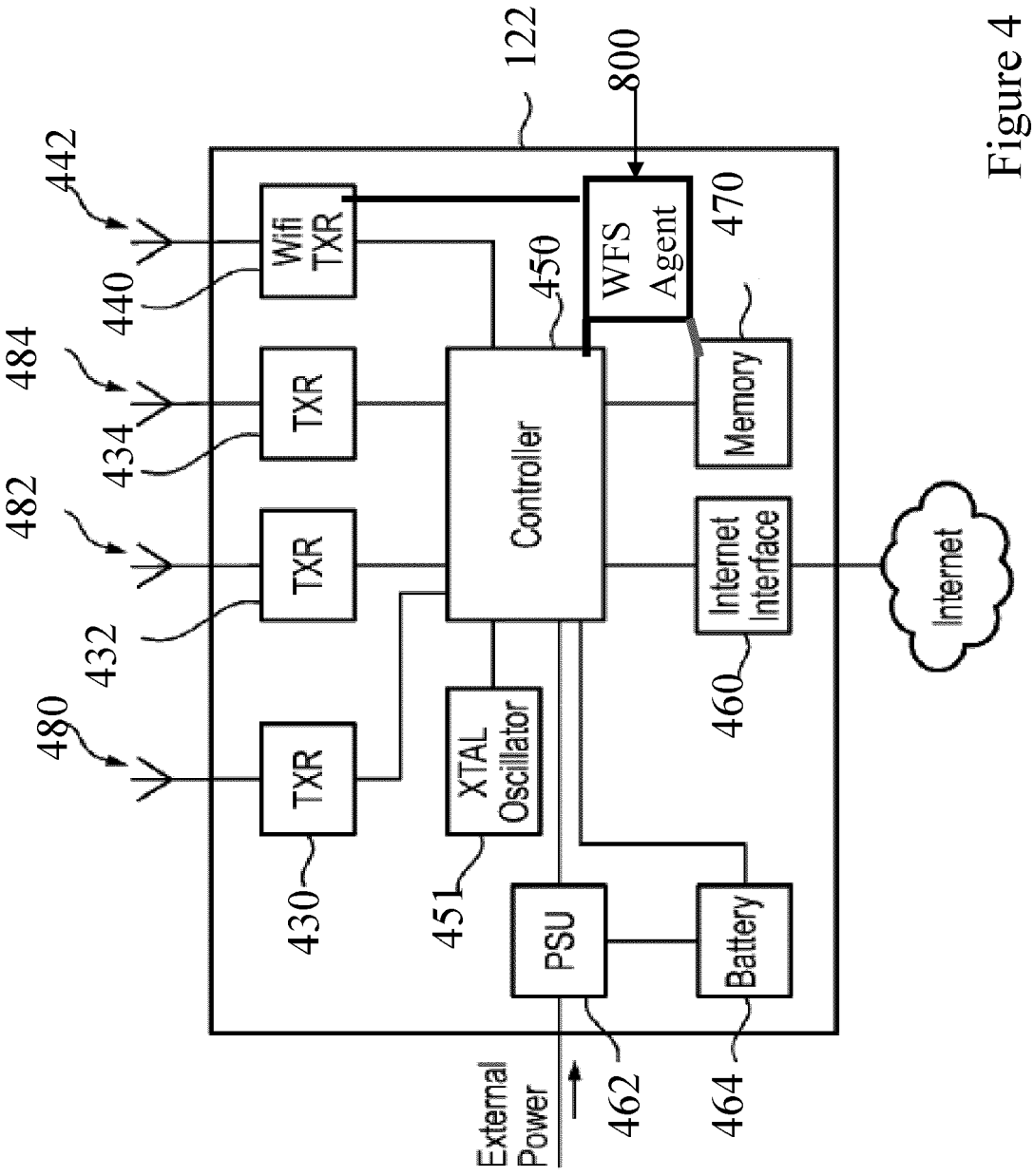
122
800
442
440
484
434
482
432
480
430
Wifi TXR
TXR
TXR
TXR
450
WFS Agent
470
Memory
Controller
Internet Interface
460
Internet
XTAL Oscillator
451
PSU
Battery
External Power
462
464

Figure 4

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 21 21 8149

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
Y	US 2010/128123 A1 (DIPOALA WILLIAM [US]) 27 May 2010 (2010-05-27) * paragraph [0011] - paragraph [0013] * * paragraph [0043] * * paragraph [0060] * * paragraph [0083] - paragraph [0090] * * paragraph [0095] - paragraph [0099] * * figures *	1-14	INV. G08B13/24 G08B15/02
Y	LIU YANG ET AL: "Harvesting Ambient RF for Presence Detection Through Deep Learning", IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, IEEE, USA, vol. 33, no. 4, 23 December 2020 (2020-12-23), pages 1571-1583, XP011905453, ISSN: 2162-237X, DOI: 10.1109/TNNLS.2020.3042908 [retrieved on 2020-12-23] * the whole document *	1-14	TECHNICAL FIELDS SEARCHED (IPC)
Y	US 11 098 984 B2 (VERISURE SARL [CH]) 24 August 2021 (2021-08-24) * column 1, line 48 - column 2, line 6 * * column 2, line 38 - column 5, line 55 *	1-14	G08B
Y	US 2016/373909 A1 (RASMUSSEN CHAD [US] ET AL) 22 December 2016 (2016-12-22) * paragraph [0084] - paragraph [0107] * * figures *	1-14	
A	US 2021/103045 A1 (KRAVETS OLEKSIY [CA] ET AL) 8 April 2021 (2021-04-08) * the whole document *	1-14	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	3 June 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 8149

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.

03-06-2022

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010128123 A1	27-05-2010	NONE	
US 11098984 B2	24-08-2021	AU 2017353293 A1	23-05-2019
		BR 112019009056 A2	16-07-2019
		CA 3042574 A1	11-05-2018
		CL 2019001223 A1	06-09-2019
		CO 2019004564 A2	18-09-2019
		EP 3319055 A1	09-05-2018
		EP 3535740 A1	11-09-2019
		ES 2829334 T3	31-05-2021
		PE 20191285 A1	20-09-2019
		US 2020333115 A1	22-10-2020
		WO 2018083091 A1	11-05-2018
		ZA 201902853 B	29-01-2020
US 2016373909 A1	22-12-2016	NONE	
US 2021103045 A1	08-04-2021	CA 3081537 A1	13-06-2019
		CN 111417864 A	14-07-2020
		EP 3721250 A1	14-10-2020
		JP 2021505856 A	18-02-2021
		KR 20200096505 A	12-08-2020
		US 2019170869 A1	06-06-2019
		US 2021103045 A1	08-04-2021
		WO 2019109174 A1	13-06-2019

EPO FORM P0459

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