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

(11) **EP 4 207 127 A1**

(12) **EUROPEAN PATENT APPLICATION**

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

(21) Application number: **21218150.7**

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

(51) International Patent Classification (IPC):
G08B 25/14 *(2006.01)* ***G08B 29/18*** *(2006.01)*
G08B 13/08 *(2006.01)* *G08B 13/196* *(2006.01)*
G08B 13/24 *(2006.01)* *G08B 25/00* *(2006.01)*

(52) Cooperative Patent Classification (CPC):
G08B 29/188; G08B 13/08; G08B 25/14;
G08B 13/196; G08B 13/2491; G08B 25/008

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

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

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

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

(54) DISTRACTION BURGLARY DETECTION

(57) There is provided a method, performed by a local management device of a security monitoring installation of a dwelling, of detecting a distraction burglary at the dwelling, the method comprising, in response to the local management device becoming aware of the presence of someone outside the dwelling at a main entrance of the dwelling, the main entrance having a door, the steps of: (i) monitoring for the presence of a person inside the dwelling at or approaching the main entrance; (ii) monitoring for the opening of the door of the main entrance; (iii) monitoring for the presence of someone outside the dwelling approaching or proximate the perimeter of the dwelling, remote from the main entrance, and/or detecting the opening of a door or window remote from the main entrance; and in the event that the three steps are satisfied, determining an alarm condition and reporting the alarm condition to a remote monitoring station and/or sounding an alarm at the dwelling. The method may be performed while the security monitoring installation is disarmed.

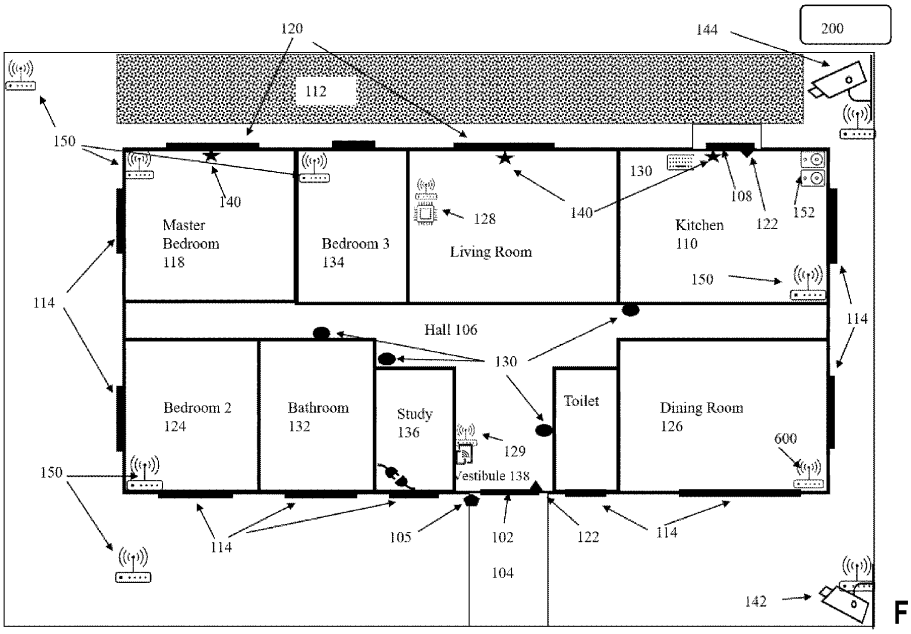

Fig. 1

EP 4 207 127 A1

Description

Field

[0001] The present invention relates generally to security monitoring system installations for premises, and in particular to installations, local management devices, and corresponding methods arranged to detect the possible occurrence of distraction burglaries.

Background

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

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

[0004] It is known for security monitoring systems to include more than one armed mode in addition to a disarmed mode. The ubiquitous armed mode is sometimes referred to as the "armed away" mode - in which the security monitoring system both secures the perimeter of the premises, and also monitors the interior of the premises with the possibility of an alarm event being triggered not only by a detected breach of the secured perimeter (for example upon the opening of a door or window provided typically with a node that senses opening based on a change in a magnetic field) but also upon motion been detected within the premises. A second armed mode, sometimes referred to as "armed at home", secures the perimeter, so that opening of a monitored door or window constitutes an alarm event, but typically movement within the house is not monitored and hence movement does not give rise to an alarm event. But depending upon the arrangement of sensors in the secured premises, there may be a third armed mode, which may be referred to as "night mode", and in which the perimeter is secured and movement within the sleeping accommodation of the premises is not monitored but movement within the living accommodation of the premises is monitored. If the security monitoring system has motion sensors in the living accommodation (e.g. on the ground floor, or "downstairs") but not in the sleeping accommodation (e.g. upstairs) then this night mode may simply be the same as the "armed away" mode.

[0005] The idea behind using the "night mode" (whether it is the armed away mode or a variant of "armed at home") is of course to provide a warning of and to any intruders who break into, or move around within, the living accommodation - which is commonly on the ground floor and hence more readily accessible than the sleeping accommodation that is commonly on an upper floor, while permitting residents occupying the sleeping accommodation to move within and between bedrooms and bathrooms without triggering an alarm. Many burglaries take place at night when there is more likelihood that the living accommodation will be vacant, but the sleeping accommodation occupied - and hence when the sounding of an alarm both to alert the legitimate residents and hopefully deter the intruders has increased value.

[0006] Statistically however, most burglaries take place during the day - probably because, at least historically, residential properties were more likely to be unoccupied during the day, and burglars know that most people hide their valuables, like jewellery, passports, etc. in their bedrooms (apparently, the most popular location is a drawer that also contains underwear). Residents who go to work, leaving their home unoccupied, are very likely to use a security monitoring system if it is available -

arming it to the armed away state as they leave home to go to work.

[0007] In recent years this historic pattern of behaviour has changed, in that many people now work from home, at least some of the time. And of course, Covid-19 has recently made home working more or less the norm for most people whose jobs permit this. Many people working from home do not tend to arm their security monitoring systems during the day, perhaps because they tend to be in and out of the home, possibly into the garden, or to pop to the shops, or to post a letter, etc. This also seems to be true for many people who have dedicated "home offices", whether they are in rooms dedicated to the purpose, or merely as part of some multipurpose space. But the increasing existence and use of the "home office" presents an opportunity to burglars - the perimeter of the property is unlikely to be armed, and the home-worker is likely to be occupied at their desk for a chunk of the morning and possibly a larger chunk of the afternoon, quite probably with the main bedroom (where the valuables are probably hidden) left vacant. Burglars have not been slow to appreciate and exploit this opportunity, and the number of burglaries committed in the occupied homes of home-workers continues to rise, even when the homes have security monitoring systems.

[0008] But another type of daytime burglary, "Distraction Burglary" has existed for many years, and is typically perpetrated against the homes of the elderly and the infirm. In this form of burglary entrance to the home is gained by getting a resident of the home to open a door, typically the front door, to a villain who may try to trick the resident into admitting the villain into the home - the villain typically pretending to be from a utility company such as the supplier of gas, water, telephony/broadband or electricity, or even by pretending to be from the police or some other reputable entity. In a common variant, the villain at the door works with a second villain who attempts to gain access to, typically the rear of, the house while the resident is kept occupied and distracted by the villain at the front door. Because distraction burglary typically involves getting a resident to open the (front) door of the house, even if the house is protected by a security monitoring system that is armed, the resident will need to disarm the system (from armed at home to disarmed) so that their opening of the front door doesn't trigger the system and cause a false alarm. So, while the resident stands at the open front door listening to the first villain's plausible distraction, the villain's accomplice can be safe in the knowledge that opening a door or window at the back of the home (or anywhere else out of sight of the resident at the front door) will not trigger the security monitoring system - a window can be broken, or a window or door forced, open with a low risk of an alarm sounding. The second villain on gaining admittance will quickly grab whatever valuables are to hand. If the first villain is good at his game, the second villain may know that he has time to run to the main bedroom to riffle drawers looking for valuables, as well as to grab any handbags or wallets, etc. that are in sight.

[0009] Residents often feel safe when talking with villains at the front door, provided the door is chained so that it cannot readily be forced open, but with the two-villain distraction burglary the villain at the front door doesn't need to gain admittance in order for a successful burglary - and the first villain's patter may be crafted so as to keep the resident at the front door for 5 minutes or more, without feeling threatened, so that the second villain has more time in which to look for portable valuables. Thus, even though a resident may diligently arm their security monitoring system, they are still at risk from distraction burglaries. With the elderly constituting an increasing proportion of the population of many countries, and with many elderly living alone, the impact of distraction burglaries is likely to increase. And one of the worst things about distraction burglaries is not the loss of heirlooms and items of immense emotional value, sad though this is, but rather the psychological impact and feeling of violation that comes from being a victim of a burglary, and from losing treasured and irreplaceable items. Indeed, it is not uncommon for elderly people who have been the victims of a distraction burglary to go into a decline and die within a few months of being burgled.

[0010] There therefore exists a need to address these problems.

[0011] For the purposes of the present application, "burglary" should be understood in the sense that the offence is defined under English law: entering a building or part of a building as a trespasser intent to commit theft, grievous bodily harm, or criminal damage; or having entered as a trespasser, stealing, or inflicting/attempting to inflict grievous bodily harm. There is no requirement for the entry to involve "breaking in", simply entering through an open or unlocked entrance is sufficient. Throughout the specification we may refer to someone intent on committing burglary as a burglar, intruder, or villain, as distinct from those resident at the property (on a temporary or permanent basis) who do not fit within the definition of burglar - who we will refer to a residents. In terms of detecting presence, movement, and location, both of these classes of people fall within the term "occupant".

[0012] Embodiments of the invention are based on the insight that it may be possible to detect a distraction burglary, possibly even before it has been committed, by checking for the tell-tale signs of such a burglary whenever someone approaches a main entrance of an occupied dwelling or similar building. A range of different technologies may be used to detect the presence of someone at the main entrance, of someone outside approaching or proximate the perimeter of the dwelling remote from the main entrance, and/or to detect the opening of an accessible door or window remote from the main entrance. However, particularly good results may be achieved using a radio-based location sensing arrangement to detect human presence and location based on detecting perturbations of radio signals.

Summary

[0013] According to a first aspect, there is provided a security monitoring system for a dwelling configured to respond to the following set of events:

the detection of someone outside the dwelling at a main entrance of the dwelling, the main entrance having a door;
the detection of a person inside the dwelling at or approaching the main entrance from inside the dwelling; the detection of the opening of the door of the main entrance; the detection of someone outside approaching or proximate the perimeter of the dwelling remote from the main entrance and/or the detection of the opening of an accessible door or window remote from the main entrance; by determining an alarm condition and reporting the alarm condition to a remote monitoring station and/or sounding an alarm at the dwelling.

[0014] According to a second aspect, there is provided a security monitoring system for a building configured to respond to the following sequence of events: the detection of presence outside the building at a main entrance of the building, the main entrance having a door; the detection of a person inside the building at or approaching the main entrance from inside the building; and the detection of the opening of the door of the main entrance; in combination with the detection of someone outside approaching or proximate the perimeter of the building remote from the main entrance and/or the opening of an accessible door or window remote from the main entrance; by determining an alarm condition and reporting the alarm condition to a remote monitoring station and/or sounding an alarm at the building.

[0015] Preferably the building is a dwelling, home, house, or the like rather than a business premises.

[0016] According to a third aspect, there is provided a method, performed by a security monitoring installation of a dwelling, of detecting a distraction burglary at the dwelling, the method comprising, in response to becoming aware of the presence of someone outside the dwelling at a main entrance of the dwelling, the main entrance having a door, the steps of:

(i) monitoring for the presence of a person inside the dwelling at or approaching the main entrance (from inside the dwelling);
(ii) monitoring for the opening of the door of the main entrance;
(iii) monitoring for the presence of someone outside the dwelling approaching or proximate the perimeter of the dwelling, remote from the (main) entrance, and/or detecting the opening of an accessible door or window remote from the (main) entrance;

and in the event that the three steps are satisfied, determining an alarm condition and reporting the alarm condition to a remote monitoring station and/or sounding an alarm at the dwelling. The monitoring steps may be performed by a local management device of the security monitoring installation. Monitoring may involve the local management device of the security monitoring installation waiting to receive a notification.

[0017] According to a fourth aspect, there is provided a local management device for a security monitoring system for a building, the local management device being configured for operative coupling to a plurality of alarm event sensors and to a remote monitoring station, and to respond to the following *sequence* of events:

(i) becoming aware of presence outside the building at a main entrance, the main entrance having a door;
(ii) detection of the presence of a person inside the building at, or approaching, the main entrance from inside the building;

and (iii) detection of the opening of the door of the main entrance;

in combination with (iv) detection of someone outside who is approaching or proximate the perimeter of the building remote from the main entrance and/or (v) detection of the opening of a door or window remote from the main entrance;

by determining an alarm condition and reporting the alarm condition to the remote monitoring station and/or sounding an alarm at the building.

Brief description of the drawings:

[0018] Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

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

Specific description

[0019] Figure 1 is a schematic plan of a single storey dwelling 100 which we will use to illustrate aspects of the invention.

[0020] The dwelling has a front door 102, the dwelling's main entrance, that is accessed externally by a path 104. A doorbell 105 is provided adjacent the front door, preferably in the form of a video doorbell which should preferably be arranged to provide a view of the whole of the

front approach of the house (by means of which the front door can be accessed) including the path 104. The main entrance 102 leads into a hall 106 by means of which all the rooms of the house may be accessed. The dwelling has a rear door 108 that leads out from a kitchen 110 onto a terrace 112. Each of the rooms includes at least one window 114, or in the case of the living room 116 and master bedroom 118 a pair of French Windows 120 that open out onto the terrace 112. The front 102 and back 108 doors are each provided with a sensor arrangement 122 that is triggered by the opening of the relevant door - for example, a sensor arrangement 122 including a magnetically triggered sensor such as a reed relay or a magnetometer.

[0021] The living room's French Windows permit access to the terrace and a rear garden, but are not intended, or used, for regular access to the interior of the premises. These doors 120 may not be provided with any sensing arrangement to detect their opening (to reduce the cost of installing the security monitoring system), but preferably are. Similarly, windows 114 to the kitchen 110, other bedrooms 124,134, and dining room 126 may also not be provided with any sensing arrangement to detect their opening (but preferably are) - again as a means of reducing the cost of installing the security monitoring system.

[0022] The security monitoring system includes a controller or central unit (which may also be referred to as a local management device) 128 which is operatively coupled to the door opening sensors 122 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 128 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).

[0023] The security monitoring system also includes a user interface or control panel 129 in the hall 106 fairly close to the front door 102. This control panel 129 is provided so that a user can arm and disarm the security monitoring system using either a code or PIN (e.g. a 4 or 6 digit PIN) or a token (using a short-range communication technology e.g. RFID, NFC, BTLE). The control panel may also be used to set the security monitoring system to an armed at home state, optionally directly from an armed away state. The control panel 129 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 129 may have a built-in video camera and optionally lighting). Although the same type of user interface may also be provided adjacent the back door (within the premises), typically a rather simpler device - known as a disarm node 130, may be provided to enable a user to disarm or arm the system, again optionally using a PIN, code, or dongle/device. Such a disarm node 130 may include one or more indicator lights, featuring e.g. RGB LEDs, to provide visual feedback on arming status (armed away, armed at home, and possibly other armed states), alarm event status, as well as at least an audio output device to provide warning and advisory tones or messages. Preferably the disarm node 130 includes both an audio output device (e.g. one or more loudspeakers and optionally an alarm sounder) and a microphone so that a user can talk with a CMS operator if necessary. The control panel 129 and disarm node 130, like motion sensors 131, are preferably provided with at least one radio transceiver for communication with the control unit 128, 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 128, are preferably battery powered and communicate using RF transceivers that consume little power (hence, not relying on Wi-Fi, 802.11 protocols, as these tend to be very power hungry) for control signals and for event reporting and that typically rely on radio frequencies in approved ISM frequency bands - such as between 860 and 900 MHZ. As already mentioned, any video cameras will typically include in addition a Wi-Fi transceiver for use in transmitting image and video data, on request, to the central unit.

[0024] The security monitoring system also includes one or more motion sensors, typically line-of-sight motion sensors such as PIR sensors. In the illustrated example, motion sensors 131 are installed at various locations in the hall - one between the kitchen 110 and the dining room 126, another towards the other end of the hall between the bathroom 132 and the first of the bedrooms 134, another outside the study 136 and another in the initial entrance part of the hall, the vestibule 138, close to the front door 102. These hall motion sensors are positioned and configured so that each only "sees" a proximate part of the hall, with the result that a person walking from the kitchen to the front door, for example, triggers first the sensor by the kitchen, then that by the study, and finally that in the vestibule. Conversely, someone coming from the bathroom or one of the bedrooms will trigger first the sensor near the bathroom, then the sensor by the office, and then the sensor in the vestibule 138. Fur-

ther motion sensors may be provided in various of the rooms, and here the presence of the French Windows means that a motion sensor is provided in the master bedroom 118 and in the living room 116. The French Windows 120 are also preferably provided with shock sensors 140, which may be based on an accelerometer or a magnetometer, for example, and which send an alert to the central unit 128 if the window or window frame is struck forcibly (such as during an attempt to break the window or break in through the French window 120. The back door 108 may also be fitted with a shock sensor, particularly if the door is largely glazed - so that access to the interior of the premises could be obtained by breaking or removing the glass. Other large windows that could also potentially provide access to the interior if their glass was broken or removed may also be provided with shock sensors. Because of our interest in knowing about presence at the front door, we may also want to provide a shock sensor at the front door too, as in this way we may detect when someone knocks at the front door rather than ringing the doorbell 105. Of course, if the doorbell 105 is a video doorbell the system can be so configured that presence alerts (e.g., push communications) from the doorbell are received by the central unit 128.

[0025] Other approaches which may be used to detect presence at the main entrance (here front door 102) include a freestanding motion sensor(s) such as a PIR sensor(s), an ultrasonic or optical presence sensing arrangement, or a presence sensing arrangement that uses LIDAR, which scans or monitors a zone in front of the front door, in each case arranged so that the presence sensing arrangement will be triggered by anyone approaching or presenting themselves at the front door, or a pressure pad or pads located where someone presenting themselves at the front door will stand.

[0026] It would also be possible to use a video camera other than a camera in a video doorbell, (e.g. triggered by an internal or external motion sensor) that observes the front door and the approach to the front door (e.g. the path 104 leading up to the front door), but this is a less preferred option because we don't actually need to see images to determine presence - and if we did want frequently to see images we would need to provide a mains power supply to the video camera, because otherwise battery life will tend to be too short. We could in effect use just the motion sensing feature of the video camera, but if that is all we need then it makes more sense to use a freestanding motion sensor - and in fact there are, as we have seen, several alternatives to using a line-of-sight motion sensor such as a PIR. That said, images from a video camera that observes the front of the house, and in particular the front door and its approach may of course be useful in identifying villains perpetrating distraction burglaries, but these may more conveniently be provided by a mains-powered video doorbell that faces out from the façade of the house - and which consequently is likely to be able capture full-face views of people at the front door.

[0027] Preferably, as shown, the security monitoring system includes at least one camera, preferably a video camera with an associated (integral or separate) motion sensor, activation of which may cause the camera (or the motion sensor) to report an event to the central unit. In response, the central unit 128 may or may not instruct the camera to transmit images (still or video), for example using a Wi-Fi transceiver, to the central unit for onward reporting to the CMS 200. In the installation shown in Figure 1 a first external video camera 142 is provided at the front of the premises, with a view over the front garden, the path 104, the front door 102 and the façade of the house (including each of the windows in the front aspect). A second video camera 144 is provided at the rear of the property, with a view of the rear aspect of the house, including the rear door and all the rear windows, and along the terrace 112.

[0028] The operation of the security monitoring system (installation) to detect (and hopefully to thwart) an attempt at a distraction burglary will now be described with reference to Figure 1. Let us assume that the house has only a single occupant, and that the security monitoring system is in in an armed at home mode, in which the perimeter is secured - meaning that if any of the doors or windows that have sensors to detect their opening is opened, the central unit will treat the alert signal received from the relevant sensor as a trigger for an alarm event, to be reported to the remote monitoring station 200 unless this is cancelled by a user providing the relevant PIN, or a disarm dongle, at the control panel 129 or at the disarm node 130.

[0029] Now imagine that a pair of villains want to pull off a distraction burglary. One villain, Fred, goes behind the property but initially doesn't enter the back garden. The other villain, Ginger, is going to approach the front of the house, to ring the bell - or knock at the door, to distract the resident. Ginger has a smartphone and Fred has a Bluetooth earpiece coupled to the smartphone meaning that Fred can hear when Ginger has managed to get the resident to the front door, and also listen to the conversation - so that he knows when he should be free from surveillance, and when he needs to vacate the premises.

[0030] Ginger approaches the front door, and knocks. His knock and/or his approach is/are sensed using one or more of the sensing arrangements provided (e.g. video doorbell, shock sensor, motion sensor, contact pad, etc.) and a corresponding "event" signal is sent to the central unit 128 (e.g. using an internal transceiver for direct communication with the central unit, or possibly indirectly in the form of a push message from a video doorbell).

[0031] The central unit 128 is now alerted and waits to see whether the presence is detected of a person inside the building at, or approaching, the main entrance from inside the building - which may be sensed by the hall-mounted motion sensors 130 (as previously described).

[0032] The resident, believing that it is safe to open the door because it is fitted with a stout chain that should

prevent it readily being forced open, presents her security fob or dongle to the control panel 129 to disarm the security monitoring system from "armed at home" mode to "disarmed", and opens the door. Ginger starts his patter, and this is the cue for Fred to enter the back garden and quickly try to gain access to the house via a window or door at the back of the house. This will require Fred to "try" the back door, French windows, and other windows to see whether one has been left unlocked or can readily be prized open. Fred's manipulation of the doors and windows may be detected by any shock sensors fitted, and thus the central unit will become aware of Fred's presence. Later we will describe the use of a radio-based presence detection technique that can sense Fred's arrival before he even "tries" any of the doors or windows, but the same effect can be achieved using one of the more conventional approaches discussed in the context of detecting presence at the front door, each of which can be applied to detect presence at the rear of the house - even of course a video doorbell.

[0033] Of course, if Fred is to enter the house from the rear, he will need either to open a door or window, or break in, in either case a shock sensor or an "opening" sensor on the relevant door or window should register the event and report it to the central unit. Fred will be aware that any alarm system will have been turned off to enable the front door to be opened without triggering an alarm, so he doesn't care about breaking in - provided he can do it quietly enough not to be heard by the resident or by any neighbours.

[0034] When the central unit 128 detects Fred's presence or his entrance in addition to Ginger's arrival, the resident's approach to the front door, and the opening of the front door, an alarm event notification is sent to the remote monitoring station 200. The central unit 122 will preferably be configured automatically to send any captured video/images to the remote monitoring station in the event of reporting an alarm event - by instructing any triggered video camera to transmit any captured video, typically via Wi-Fi, to the central unit 128 which then forwards these to the remote unit 200.

[0035] An operator at the remote monitoring station will then instruct intervention by security personnel and/or advise the local police of the events unfolding at the premises, taking account of the content of any video provided by the central unit 128.

[0036] Another approach that may be used to detect presence, and determine location, of a resident, villain or intruder is radio-based location sensing based on detecting perturbations of radio signals. This may be used in addition to, or as an alternative to the presence/movement sensing techniques already described.

[0037] We will now provide a brief introduction to radio-based presence detection, which may for example be based on analysing the signal dynamics and signal statistics of radio signals and/or detecting changes in channel state information (CSI). A radio (or wireless) signal as used herein refers to a signal transmitted from a radio transmitter and received by a radio receiver, wherein the radio transmitter and radio receiver operate according to a standard or protocol. Such standards include, but are not limited to, IEEE 802.11. (which includes the Wi-Fi standards), IEEE 802.15 (which includes Zigbee), Bluetooth SIG, IEEE 802.16, IEEE 802.20, UMTS, GSM 850, GSM 900, GSM 180, GSM 19011, GPM ITU-R 5.13, GPM ITU-R 5.150, ITU-R 5.280, 3GPP 4G (including LTE), 3GPP 5G, 3GPP NR, AND IMT-2000. However, the radio transmitters and receivers providing and using radio signals for WFS may operate in non-telecommunications or Industrial, Scientific and Medical (ISM) spectral regions without departing from the scope of the invention.

[0038] Essentially the idea is to use radio signals to probe a zone or zones of interest, and to analyse and extract statistics from these signals, in particular looking at the physical layer and/or data link layer such as MAC address measurements that expose the frequency response of a radio channel (e.g., CSI or RSSI measurements). These measurements are processed to detect anomalies and variations over time, and in particular to detect changes signifying the entrance of a person and/or movement of a person within a monitored zone. The zone(s) to be monitored need to be covered sufficiently by radio signals, but the sources of the radio signals may either already be present before a monitoring system is established-for example from the plurality of Wi-Fi or Bluetooth capable devices that are now dotted around the typical home or office, or the sources may be added specifically to establish a monitoring system. Often some established (i.e., already located or installed) radio devices are supplemented by some extra devices added as part of establishing a radio-based presence detection system. Among the types of devices (pre-installed or specifically added) that may be used as part of such a detection system are Wi-Fi access points, Wi-Fi routers, smart speakers, Wi-Fi repeaters, as well as video cameras and video doorbells, smart bulbs, etc. Because presence (or intrusion) is detected by detecting a change in the properties or character of radio signals compared to some previous reference signal(s), it is preferred to establish what might be termed the monitoring network between radio devices that are essentially static (i.e., that remain in the same position for extended periods) rather than relying on devices that are repeatedly moved - such as smart phones, headphones, laptops, and tablet devices. It is not strictly speaking essential for all the devices whose signals are used by the monitoring system to be part of the same network - for example, signals from Wi-Fi access points of neighbouring premises could be used as part of a monitoring system in different premises. Again, a primary consideration is the stability of the signals from the signal sources that are used. Wi-Fi access points provided by broadband routers are seldom moved and rarely turned off, consequently they can generally be relied upon as a stable signal source - even if they are in properties neighbouring the property containing the zone or zones to be monitored.

[0039] The idea is illustrated very schematically in Figure 2, here with an installation 200 including just a single source (or illuminator) 202 and just a single receiver 204, for simplicity, although in practice there will typically be multiple sources (illuminators) and sometimes plural receivers. The installation 200 has been established to monitor a monitored zone 206. In Figure 2A we see that in steady state, and in the absence of a person, radio signals are transmitted from the source 202, spread through the monitored zone 206, and are received by the receiver 204. Of course, in most installations there will be walls, ceilings, floors, and other structures that will tend to reflect, at least in part, signals from the source. Furniture and other objects may block and attenuate the signals, the reflected signals will give rise to multiple paths, and the signals may interfere with each other, and there may be scattering and other behaviours, such as phase shifts, frequency shifts, all leading to complexity in the channels experienced by the radio signals that arrive at the receiver 204. But while the environment is static and unchanging, the receiver will tend to see a consistent pattern of radio signals. And this is true whether or not the source transmits continuously or transmits periodically. But this consistent pattern of received signals is changed by the arrival of an intruder 208, as shown in Figure 2B. From Figure 2B we see that, at the very least, the presence of a person in the monitored zone blocks at least some of the signals from the source, and that affects the pattern of radio signals received by the receiver 204. The changed pattern of signals received by the receiver enables the presence of the intruder to be detected by a presence monitoring algorithm that is supplied with information derived from the received signals. It will be appreciated that the nature and extent of the perturbation of the signals passing from the source 202 to the receiver 204 is likely to change as the intruder 208 enters, passes through, and leaves the monitored area 206, and that this applies also to reflected, refracted, and attenuated signals. These changes may enable the location of a person within the zone, and their speed of movement, to be determined. Indeed, these techniques have been shown even to be capable of detecting gestures, and patterns of human respiration, as well as enabling "people counting".

[0040] It will be realised that signals that are received from an illuminator device (or from more than one illuminator device) after having passed through a monitored space (or volume), have in effect been filtered by the environment to which they have been exposed. We can therefore imagine the monitored volume as a filter having a transfer coefficient, and we can see that a received signal is at least in part defined by the properties, or channel response, of the wireless channel through which it propagated. If the environment provided by the monitored volume changes, for example by the addition of a person, then the transfer coefficient of the filter, and the channel response or properties, will also change. The changes in the transfer coefficient, and in the channel response, consequent on the change in the environment of the monitored space, can be detected and quantified by analysing radio signals received by the wireless sensing receiver(s). Both the introduction of an object, e.g. a person, into the monitored space, and movement of that object within the monitored space will change the environment and hence change the effective transfer coefficient and the channel response.

[0041] 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.

[0042] The system may need to be retrained for the base setting if bulky furniture or other large objects (particularly if made of metal) are added to or moved within the monitored space, because these can be expected to change the propagation properties of the relevant zone/space. The data for unoccupied states are preferably retained within a database of "unoccupied" states, even when there are changes to the arrangement of furniture etc. It may not be necessary to retrain for the occupied states if the system can determine a delta function between the previous base state and the new one, because the delta function may also be applicable in occupied states. But if not, it may be sufficient to retrain only a subset of the occupied states previously learnt. The system may also be configured to self-learn to accommodate changes in the characteristics of the zones when unoccupied, and to add newly determined unoccupied state data to the database.

[0043] Although the Figure 2 example uses just a single source (illuminator) and a single receiver, as already mentioned generally multiple sources (illuminators) will be used in order to achieve satisfactory coverage of the zone or zones to be monitored. Multiple zones may be monitored by a single receiver through the use of multiple strategically placed sources, but each zone, or some zones of multiples zones may have a dedicate receiver that does not serve other zones. Likewise, a radio signal source (illuminator) may provide illuminating signals for a single monitored zone or for multiple monitored zones. Also, a presence monitoring system (and a security monitoring system including such a presence monitoring system) may use mesh network arrangement, for example a Wi-Fi mesh network, in which multiple devices act as receivers for illuminating signals - either for a single monitored zone or for multiple monitored zones.

[0044] Now, consider once again Figure 1. The observant reader will have noticed that this includes features whose presence has not yet been mentioned, and these

are elements that may play a role in providing WFS. The central unit 128 here functions as an access point for a Wi-Fi network and as the WFS receiver, and various Wi-Fi devices are positioned around the premises both to perform their normal role but also to act as illuminators for WFS. Within the house there are several Wi-Fi extenders 150 which are convenient because they can readily be positioned in any vacant electrical socket, provide good signal strength, and typically have a small form factor. As shown, these may also be used outside - if weatherproof or protected from the weather. The Wi-Fi cameras 142 and 144 can also function as outdoor illuminators to improve the reach of the WFS - which will enable us to detect Fred's approach to the back of the house, before he starts to try the windows and doors. In the kitchen 110 a smart speaker 152 and a Wi-Fi extender 150 are provided as illuminators, while broadband router or gateway 600 provides illumination from within the dining room. In the study 136 a "smart plug" 154 acts as illuminator, while in the hall the motion sensors (e.g. PIR detectors) 130 and control panel 129 act as illuminators. It will be appreciated that this choice of Wi-Fi sources, and their disposition, is given merely to illustrate a suitable approach - the number of illuminators and the positioning required very much depend upon the area of cover required for WFS and on the size and type of construction of the property being monitored. It may not always be necessary to use external Wi-Fi illuminators in order to extend Wi-Fi sensing to beyond the external walls of a building, but by providing some suitably positioned external illuminated, as shown schematically here, it should be possible to extend the range of WFS to achieve the desired results. With the ubiquity and wide penetration of Wi-Fi devices into the lives of a large proportion of the population of the developed world, it may often the case that no, or very few, Wi-Fi devices need to be added to a home in order to provide a satisfactory level of WFS cover - although that may not always be the case with the elderly.

[0045] It will be appreciated that although the invention does not rely on the use of radio-based position and location sensing, the use of such sensing within the scope of the invention can bring significant advantages.

[0046] In a first aspect there is provided a security monitoring system for a building (such as a dwelling or home), the system including a local management device, the local management device being operatively coupled to a plurality of alarm event sensors and configured to respond to the following sequence of events:

(i) becoming aware of presence outside the building at a main entrance, the main entrance having a door; (ii) detection of the presence of a person inside the building at, or approaching, the main entrance from inside the building; and (iii) detection of the opening of the door of the main entrance; in combination with (iv) detection of someone outside who is approaching or proximate the perimeter of the building remote from the main entrance and/or (v) detection of the opening of a door or window remote from the main entrance; by determining an alarm condition and reporting the alarm condition to a remote monitoring station and/or sounding an alarm at the building.

[0047] Although here we refer to a particular sequence of events, it should be recognised that although this sequence of events is particularly significant as a marker of a distraction burglary, other sequences may also occur during a distraction burglary - such as a reversal of steps (i) and (ii), perhaps because the resident has seen, from the hall, the front door man approaching the house before his presence has been detected by any sensor of the system. Consequently, it may be determined that there is a burglary even if (i) happens after or simultaneously with (ii).

[0048] The local management device is optionally configured to become aware of presence outside the main entrance by receiving a notification from one or more of the following:

a doorbell, optionally a video doorbell (for example receiving a push notification from the doorbell, e.g. via the internet, rather than directly);
a shock sensor for the door (which may be mounted on the door itself or on the frame of the door);
an ultrasonic or optical presence sensing arrangement, for example using one or more beams of invisible (e.g infrared) light the disruption or blockage of which indicates presence;
a presence sensing arrangement that uses LIDAR;
a line-of-sight motion sensor (e.g. a PIR sensor); and
a pressure pad, for example integrated into the floor of a porch or hidden under, or built into, a doormat.
Preferably any such notifications are received by the local management device "over the air" directly from the relevant sensing arrangement, but may - as in the case of push notifications from a smart doorbell come via some intermediary. Such notifications may also be received over a wired connection.

[0049] Optionally, the local management device is configured to detect the presence of a person inside the building at, or approaching, the main entrance from inside the building based on one or more signals received from one or more motion sensors within the building.

[0050] Optionally, the local management device is configured to detect someone outside who is approaching or proximate the perimeter of the building remote from the main entrance based on one or more signals received from one or more of the following:

a shock sensor for a door or window;
a video camera;
an ultrasonic or optical presence sensing arrangement;
a presence sensing arrangement that uses LIDAR;

a line-of-sight motion sensor (e.g. a PIR sensor); and a pressure pad. Preferably any such notifications are received by the local management device "over the air" directly from the relevant sensing arrangement, but may - as in the case of push notifications from a smart doorbell come via some intermediary. Such notifications may also be received over a wired connection.

[0051] Preferably the security monitoring installation of any variant of the first aspect further comprises a radio-based location sensing arrangement to detect human presence and location based on detecting perturbations of radio signals, the local management device being configured to detect one or more of:

presence outside the building at the main entrance;
the presence of a person inside the building at, or approaching, the main entrance;
the presence of someone outside approaching or proximate the perimeter of the building remote from the main entrance;
using the radio-based location sensing arrangement.

[0052] Preferably, the local management device is further configured to determine the alarm condition and report the alarm condition to the remote monitoring station and/or sound the alarm at the building when the security monitoring system is in a disarmed state. This means that even though a resident may have disarmed the security monitoring system in order to open the door of the main entrance without triggering an alarm, detection of a distraction burglary can give rise to a local alarm and/or a report to a remote monitoring station - in either case hopefully leading to apprehension of the villains or at least their being scared away before managing to enter the premises.

[0053] Optionally, in making its determination the local management device is configured to take account, when the presence of a person inside the building at the main entrance is detected, of the amount of time that the person is at the main entrance.

[0054] Optionally, in security monitoring installation according to embodiments of the invention, the door of the main entrance includes at least one door status sensor configured to detect whether the door is ajar, and the local management device is configured to take account of information received from the door status sensor, and optionally the door status sensor is configured to provide information on the use of a security restraint such as a chain that restricts further opening of the door once opened.

[0055] Optionally, the local management device is configured also to take account of one or more of the month, the season, the ambient (external) temperature, the temperature inside the dwelling.

[0056] According to a second aspect there is provided a method, performed by a local management device of a security monitoring installation of a dwelling, of detecting a distraction burglary at the dwelling, the method comprising, in response to the local management device becoming aware of the presence of someone outside the dwelling at a main entrance of the dwelling, the main entrance having a door, the steps of:

(i) monitoring for the presence of a person inside the dwelling at or approaching the main entrance;
(ii) monitoring for the opening of the door of the main entrance;
(iii) monitoring for the presence of someone outside the dwelling approaching or proximate the perimeter of the dwelling, remote from the main entrance, and/or detecting the opening of a door or window remote from the main entrance;

and in the event that the three steps are satisfied, determining an alarm condition and reporting the alarm condition to a remote monitoring station and/or sounding an alarm at the dwelling.

[0057] In the method of the second aspect the local management becoming aware may involve the local management device receiving a notification from a sensor or a sensing arrangement. Optionally, the sensing arrangement comprises a radio-based location sensing arrangement to detect human presence based on detecting perturbations of radio signals.

[0058] In the method of the second aspect the monitoring steps are preferably performed by a local management device of the security monitoring installation.

[0059] In the method of the second aspect monitoring optionally involves the local management device of the security monitoring installation waiting to receive a notification from a sensor or a sensing arrangement.

[0060] Optionally, the method is performed by the local management device when the security monitoring installation is disarmed.

[0061] Optionally, in the method of the second aspect involves the local management device taking account of one or more of the following:

how long the door of the main entrance is open before detecting the opening or attempted opening of a door or window remote from the main entrance;
when the presence of a person inside the building at the main entrance is detected, of the amount of time that the person is at the main entrance;
information received from a door status sensor configured to detect whether the door of the main entrance is ajar;
information received from a door status sensor on the use of a security restraint such as a chain that restricts further opening of the door of the main entrance once opened;
the month, the season, the ambient (external) temperature, and the temperature inside the dwelling.

[0062] In a further aspect there is provided a local management device for a security monitoring system for a building, the local management device being configured for operative coupling to a plurality of alarm event sensors and to a remote monitoring station, and to respond to the following sequence of events:

(i) becoming aware of presence outside the building at a main entrance, the main entrance having a door; (ii) detection of the presence of a person inside the building at, or approaching, the main entrance from inside the building;

and (iii) detection of the opening of the door of the main entrance;

in combination with (iv) detection of someone outside who is approaching or proximate the perimeter of the building remote from the main entrance and/or (v) detection of the opening of a door or window remote from the main entrance;

by determining an alarm condition and reporting the alarm condition to the remote monitoring station and/or sounding an alarm at the building.

[0063] In embodiments or methods according to any of the aspects, the radio-based sensing arrangement may be configured to process communication signals received from one or more radio transmitters operating according to one or more communication standards or protocols, and optionally the one or more radio transmitters that are in a common wireless network with the local management device.

[0064] In embodiments or methods according to any of the aspects,, the local management device includes a radio receiver of the radio-based presence and location sensing system, and optionally the local management device includes a processor and a memory holding software instructions that when run on the processor cause the local management device to process radio signals to derive location and presence data.

[0065] In embodiments or methods according to any of the aspects,, optionally there is provided a sensing arrangement to detect human presence uses changes in channel state information or received signal strength in determining presence.

[0066] In installations according to the first aspect or methods according to the second aspect, the local management device may be configured to function as an access point of a radio network whose signals are used by a radio-based presence and location sensing system. Optionally, the radio network for which the local management device functions as an access point includes at least one further access point. Optionally, the radio network is a Wi-Fi network, and optionally the one or more radio transmitters include one or more of the following: a Wi-Fi access point, a Wi-Fi extender, a smart plug or smart socket, a smart speaker, a smart bulb, a control panel of the security monitoring system, a Wi-Fi-enabled video camera. Optionally, the local management device is further configured to perform processing of signals as part of the radio-based location sensing arrangement.

[0067] The local management device may be further configured to use data from the radio-based location sensing arrangement to perform people counting, and optionally to use determine the presence of one or more intruders based on a detected change in the people count when the system is in the nocturnal armed mode. For example, the techniques and methods described in US2020/0302187A1, assigned to Origin Wireless, can be used to count occupants and determine their locations in installations, systems and methods according to embodiments of the invention. The local management device can, for example use people counting to keep track of the number of people in the house - and this may include being aware of the number of people who have, for example, gone into the rear garden or who are on the terrace. If the local management device is aware that one or more people have recently gone out of the house into the rear garden, then the opening of a rear access point (e.g. door or French window) and/or a person entering at the rear of the house is less likely to be a sign of a "rear entry man" like Fred, but rather to be a resident coming back into the house.

[0068] The local management device may also be configured to receive and store a number corresponding to the number of usual residents - something that is particularly useful if the dwelling is the home of someone who lives alone. In such a case, the local management device can have a high degree of confidence that any activity detected at the rear of the house, while someone (presumably the sole resident) is answering the front door, is likely to be part of a distraction burglary. The system could also be programmed to deal with days or periods when more residents than usual are expected - for example the weekly visit of a cleaner, carer, or heath visitor, or the monthly visits of family or friends. Such information could be entered by the resident or an authorised user or installer using, for example an app on a device or online, or via spoken commands or touch screen input at the control panel 128.

[0069] Figure 3 is a schematic drawing showing in more detail features of the gateway or central unit 122 of Figures 1. The gateway 122 includes a first transceiver 430 coupled to the first antenna 480, and optionally a second transceiver 432 coupled to a second antenna 482. The transceivers 430 and 432 can each both transmit and receive, but a transceiver cannot both transmit and receive at the same time. Thus, the transceivers 430, 432 each operate in half duplex. Preferably a transceiver will use the same frequency to transmit and receive (although of course if the two transceivers are to operate simultaneously but in opposite modes, they will operate on different frequencies). The transceivers 430, 432 may be arranged such that one transceiver 430 uses a first

frequency for transmit and receive and the second transceiver 432 uses the same first frequency for transmit and receive, i.e. the transceivers are arranged to operate in a diversity-like arrangement. Alternative, the second transceiver may, depending on configuration, be arranged to use a second frequency for transmit and/or receive. The transceivers 430 and 432 are coupled to a controller 450 by a bus. The controller 450 is also connected to a network interface 460 by means of which the controller 450 may be provided with a wired connection to the Internet and hence to the monitoring centre 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. 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.

[0070] 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.

[0071] 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.

[0072] As an alternative to incorporating the radio sensing application into the central unit, this functionality can be provided on an access point, e.g. a Wi-Fi access point, AP such as router 300, of the premises, with the AP configured to report the result of presence detection to the central unit 122. In another example, a Wi-Fi range extender could instead be used as sensing master for its connected nodes and configured to report to the central unit 122 which would be the overall master in terms of reporting the "alarm".

[0073] Variants

[0074] As we explained earlier, a class of distraction burglaries involves at least two actors (our Fred and Ginger), one of whom (Ginger) keeps a resident occupied at a main entrance of a dwelling, typically the front door, while the other (Fred) enters the dwelling through another door or a window out of sight of the resident, typically at the rear or side of the dwelling. So far, we have described a method of detecting such a distraction burglary using a method in which, in response to a local management device becoming aware of the presence of someone outside the dwelling at a main entrance of the dwelling, the main entrance having a door, performing the steps of:

(i) monitoring for the presence of a person inside the dwelling at or approaching the main entrance;
(ii) monitoring for the opening of the door of the main entrance;
(iii) monitoring for the presence of someone outside the dwelling approaching or proximate the perimeter of the dwelling, remote from the main entrance, and/or detecting the opening of an accessible door or window remote from the main entrance;

and in the event that the three steps are satisfied, determining an alarm condition and reporting the alarm condition to a remote monitoring station and/or sounding an alarm at the dwelling. And we have described using either motion sensors, such as PIR sensors to detect movement of a resident towards the door of the main entrance, and the alternative approach of using Wi-Fi Sensing to detect the resident's progress towards the door of the main entrance. This aspect of the method provides one way for the local management device to distinguish between a distraction burglary and the coincidence of a first

resident opening the back door of the dwelling just as, or just after, another resident unlocks the door of the main entrance on their return home. It is useful therefore to consider this aspect a little further.

[0075] We have described the role of Ginger, the "front door man" of our distraction burglary double act, how this role differs from that of Fred, the "back door man" of the double act, in that it involves keeping the resident engaged in conversation at the door, freeing Fred free from the resident's observation and attention so that Fred is able to enter and roam the dwelling unobserved and without interference. While Ginger's performance at the main entrance is keeping the resident occupied, the resident will stand inside the house, at the entrance - often with the door of the entrance held only slightly ajar rather than wide open. Indeed the elderly and those living alone are frequently urged to fit a security chain to their front door so that the door can safely be opened to permit conversation with a visitor around the open edge of the door, which is held ajar, while preventing the visitor simply pushing the door open to enter the home. The front door men of distraction burglary double acts often try to reassure residents of their bona fides, for example showing fake official identity cards to show that they do indeed represent the water company, gas company, or whatever. Sometimes this is with the intention of persuading the resident to admit the front door man into the house, so that he too can steal valuables while the resident has been distracted by having been persuaded to perform a task such as running water from the bathroom taps. But often the Gingers of the double acts reassure not because they want to enter the dwellings but rather so that the residents will relax enough to feel comfortable talking to Ginger through a door that is not just ajar but is wide open - because it is easier to engage the resident in a much longer dialogue when they have relaxed enough to open the door wide. So, Ginger will often try to persuade the resident to unlatch the security chain, standing back so as to appear less intimidating, and using body language, "patter" and tone of voice chosen to appear friendly, reassuring and non-threatening. Based on these observations we can see conditions that we can use to identify the presence of a "front door man" - and hence either to flag up the likely incidence of a distraction burglary or to distinguish a potentially real distraction burglary from the innocent coincidence of entrances being made at the front and back doors of a house around the same time.

[0076] The first is whether the door has been opened with a security chain in place - which can be detected using a sensor incorporated in the security chain that senses engagement of the free end of the chain with its corresponding socket or other capture element, optionally in combination with a "door open" sensor provided on the door/the door frame. This may happen when a resident opens the door on returning home - the chain having been engaged by another resident who is at home - but the two situations can readily be distinguished because in a distraction burglary the door is likely to be held open on the chain for an extended period whereas that is unlikely to happen when the door has been opened by a returning resident. So we can consider the time for which the door is held open on the chain - if it is more than 15 to 30 seconds, it suggests a distraction burglary, if it is for a minute or more then a distraction burglary is highly likely - and the local management device can be programmed to use an algorithm that takes this factor into account. We also have the fact that Ginger will try to persuade the resident to open the door again without the chain in place - and we can use the occurrence of a first opening with the security chain in place followed by the door being closed and immediately reopened with the chain off as another warning condition for the algorithm.

[0077] If no security chain is fitted a cautious resident may tend, when opening the front door to strangers, to hold the door ajar - at least initially, rather than opening the door wide as is likely when a visitor is known to the resident. We can arrange sensors to detect that the door has been opened and held ajar, as opposed to simply sensing that the door has been opened, by positioning a door opening sensor on the hinge side of the door/frame, or at the upper edge of the door close to the hinge side (between say 50-200mm, from the hinge edge, preferably 70 to 150mm from the hinge edge - although the optimum position depends to some extent on the width of the door: the wider the door, the less it needs to be rotated about the vertical hinge axis for the gap at the open side to be big enough to talk through). Rather than simply detecting whether the door is open or closed, we want to see whether the door is open just a little - so some kind of proximity sensor, for example based on the combination of a magnetometer and one or more magnets, or based on optical sensing, could be suitable. Any such sensing arrangement should of course be operatively connected to the local management device, for example using an internal transceiver, and preferably powered by an internal power supply such as a battery. We may also be able to detect the condition of "front door ajar" using Wi-Fi sensing.

[0078] The second is the fact that during a distraction burglary a resident is likely to remain at the door, inside the house, for a minute or more, and typically much longer - which again doesn't happen when a resident makes an entrance through the front door. So, we can focus on detecting this "resident pendency" at the main entrance - either using a dedicated motion or presence sensor inside the dwelling at the front door - e.g. by providing one or more PIR sensors (or one or more contact pads on the floor, perhaps under the front door mat or entrance rug) in the hall where the sensor(s) will "see" someone positioned to talk with someone just outside the door but where the sensor(s) will not "see" someone further back inside the house - e.g. further back in the entrance hall. Of course, if our installation includes WFS capability, we can use this to detect the presence of a resident at the door. And again the algorithm used by the local manage-

ment device can take into account the length of time for which a resident remains at the door - anything over a minute is highly suggestive of the presence of a "front door man".

[0079] Another marker for a distraction burglary is the fact that a "rear" entrance (by which we mean an entrance remote from the main entrance at which the resident is kept occupied, but which may be a side entrance rather than actually a rear entrance, assuming that the main entrance is the front door) is opened while a main entrance door is open. This coincidence of opening another entrance door while the front (main) door is in an open condition does occasionally occur without a distraction burglary taking place, but it is not common - and is, for example, unlikely to happen in the winter or when ambient temperatures are less than about 25 Celsius - factors (date/month/time of year, weather, external/internal temperature) which the local management unit can be programmed to take into account in determining whether a distraction burglary is being attempted or is in progress). We can also factor in the presence of someone inside the house, at the main entrance door when a "rear" entrance is opened or breached - a coincidence of circumstances which is highly suggestive of a distraction burglary, particularly if that presence extends for more than a minute (and the longer the pendency the more likely it is that a distraction burglary is taking place). A further consideration is whether multiple rear entrances been "tried", as detected for example by shock sensors on the different rear entrances, while the main entrance is open? This is a strong marker for there being a "Fred" on the premises and tends strongly to distinguish from the innocent activities of a resident.

[0080] We can also usefully take account of how long the door of the main entrance been open before the opening or attempted opening of a door or window remote from the main entrance is detected, because Fred is likely to want to act fairly quickly once he knows that Ginger has got the resident engaged, but he may hold back initially until he knows that the resident has been "hooked" and isn't just going to give Ginger the brush off. Typically, the "back door man" may wait about 30 to 45 seconds, unless he can see valuables like a handbag, wallet, mobile phone, tablet computer or laptop within easy reach of a convenient entrance. But, it is unlikely that "Fred" will wait much more than a minute before trying to enter - or at least testing the windows and doors to see whether one can readily be opened (activity which door/window shock sensors, and WFS may be able to detect) - because he'd be wasting precious time. Whereas a resident who has been on the terrace or in the back garden, whose movements may have nothing to do with any activity at the main entrance, may enter the house via the back door or the French windows at any time. Hence, the algorithm of the local management device will tend to discount rear access activity if it only occurs several minutes or more after the opening of the main entrance door.

[0081] The local management unit is therefore preferably programmed to take all these factors into account in determining whether a distraction burglary is taking place, although some factors or combinations of circumstances will quickly enable a positive determination to be made, an initially negative determination may become positive based on prolonged pendency, for example.

[0082] The local management unit may therefore consider some or all of at least the following factors, using a suitably programmed algorithm, in determining whether to raise an alarm with the remote monitoring station based on the existence of a distraction burglary:

a) Is the main entrance door held ajar for more than a brief period (e.g. longer than 30 seconds) or is the main entrance door opened with the security chain engaged?

b) Is the back door (or other potential entrance) opened while the front door is open (an overlap of periods of opening of front and rear entrances)?

c) Is someone standing inside the house, at the front door, during coincidence b)?

d) How long has the person in c) been standing at the front door before the rear entrance is opened?

e) Have multiple rear entrances been "tried" (as detected for example by shock sensors on the different rear entrances)?

f) How long has the door of the main entrance been open before the opening or attempted opening of a door or window remote from the main entrance is detected?

[0083] A brief explanation will now be given of how Wi-Fi Sensing works, and how Wi-Fi Sensing can be integrated into a security monitoring system, and in particular how WFS can be integrated into a central unit of a security monitoring system.

[0084] 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.

[0085] 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 meas-

urement 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.

[0086] 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.

[0087] 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.

[0088] 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).

[0089] Invoked measurement involves utilizing a packet transmission that is in response to a packet received from the Wi-Fi Sensing receiver device.

[0090] In pushed mode, a transmission is initiated by the illuminator device for measurement. A pushed transmission can be either a unicast or a multicast/broadcast message. Multicast/broadcast messages can be used for measurements by multiple WFS receivers simultaneously if the devices are not in power-save mode. Triggered transmissions introduce overhead because additional over-the-air transmissions are required. Pushed transmissions introduce less overhead compared to invoked transmissions, because the exchange is unidirectional rather than bidirectional. Triggered transmissions allow for a system to control both the rate and occurrence of measurements.

[0091] 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.

[0092] A WFS system can be built based on existing Wi-Fi standards, hardware, software and infrastructure.

[0093] 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.

[0094] 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.

[0095] 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.

[0096] 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.

[0097] 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.

[0098] 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.

[0099] 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).

[0100] 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.

[0101] 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.

[0102] 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.

[0103] 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.

[0104] 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.

[0105] 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.

[0106] 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.

[0107] 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.

[0108] 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.

[0109] 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.

[0110] 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.

[0111] 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.

[0112] 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.

[0113] 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.

[0114] 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.

[0115] 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.

[0116] 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.

[0117] 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.

[0118] 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.

[0119] 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.

[0120] 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.

[0121] 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.

[0122] 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

[0123] 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.

[0124] 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.

[0125] 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.

[0126] The WFS interface should be flexible enough for the radio to specify whether the data payload is in time-domain or frequency-domain, the numerical format, etc. By having this knowledge, the Wi-Fi Sensing agent can correctly interpret the data.

Claims

1. A security monitoring system for a building, the system including a local management device, the local management device being operatively coupled to a plurality of alarm event sensors and configured to respond to the following sequence of events:

   (i) becoming aware of presence outside the building at a main entrance, the main entrance having a door;
   (ii) detection of the presence of a person inside the building at, or approaching, the main entrance from inside the building;

   and (iii) detection of the opening of the door of the main entrance;
   in combination with (iv) detection of someone outside who is approaching or proximate the perimeter of the building remote from the main entrance and/or (v) detection of the opening of a door or window remote from the main entrance;
   by determining an alarm condition and reporting the alarm condition to a remote monitoring station and/or sounding an alarm at the building.

2. The security monitoring installation of claim 1, wherein the local management device is configured to become aware of presence outside the main entrance by receiving a notification from one or more of the following:

   a door bell, optionally a video doorbell;
   a shock sensor for the door;
   an ultrasonic or optical presence sensing arrangement;
   a presence sensing arrangement that uses LIDAR;
   a line-of-sight motion sensor (e.g. a PIR sensor); and
   a pressure pad.

3. The security monitoring installation of claim 1 or claim 2, wherein the local management device is configured to detect the presence of a person inside the building at, or approaching, the main entrance from inside the building based on one or more signals received from one or more motion sensors within the building.

4. The security monitoring installation of any one of the preceding claims, wherein the local management device is configured to detect someone outside who is approaching or proximate the perimeter of the building remote from the main entrance based on one or more signals received from one or more of the following:

   a shock sensor for a door or window;
   a video camera;
   an ultrasonic or optical presence sensing arrangement;
   a presence sensing arrangement that uses LIDAR;
   a line-of-sight motion sensor (e.g. a PIR sensor); and
   a pressure pad.

5. The security monitoring installation of any one of the preceding claims, further comprising a radio-based location sensing arrangement to detect human presence and location based on detecting perturbations of radio signals, the local management device being configured to detect one or more of:

   presence outside the building at the main entrance;
   the presence of a person inside the building at, or approaching, the main entrance;
   the presence of someone outside approaching or proximate the perimeter of the building remote from the main entrance;
   using the radio-based location sensing arrangement.

6. The security monitoring installation of any one of the preceding claims, wherein the local management device is further configured to determine the alarm condition and report the alarm condition to the remote monitoring station and/or sound the alarm at the building when the security monitoring system is in a disarmed state.

7. The security monitoring installation of any one of the preceding claims, wherein in making its determination the local management device is configured to take account, when the presence of a person inside the building at the main entrance is detected, of the amount of time that the person is at the main entrance.

8. The security monitoring installation of any one of the preceding claims, wherein the door of the main entrance includes at least one door status sensor configured to detect whether the door is ajar, and the local management device is configured to take account of information received from the door status sensor, and optionally the door status sensor is con-

figured to provide information on the use of a security restraint such as a chain that restricts further opening of the door once opened.

9. The security monitoring installation of any one of the preceding claims, wherein in making its determination the local management device is configured to take account of one or more of the month, the season, the ambient (external) temperature, the temperature inside the dwelling.

10. A method, performed by a local management device of a security monitoring installation of a dwelling, of detecting a distraction burglary at the dwelling, the method comprising, in response to the local management device becoming aware of the presence of someone outside the dwelling at a main entrance of the dwelling, the main entrance having a door, the steps of:

(i) monitoring for the presence of a person inside the dwelling at or approaching the main entrance;
(ii) monitoring for the opening of the door of the main entrance;
(iii) monitoring for the presence of someone outside the dwelling approaching or proximate the perimeter of the dwelling, remote from the main entrance, and/or detecting the opening of a door or window remote from the main entrance;

and in the event that the three steps are satisfied, determining an alarm condition and reporting the alarm condition to a remote monitoring station and/or sounding an alarm at the dwelling.

11. The method of claim 10, wherein the local management becoming aware involves the local management device receiving a notification from a sensor or a sensing arrangement.

12. The method of claim 11, wherein the sensing arrangement comprises a radio-based location sensing arrangement to detect human presence based on detecting perturbations of radio signals.

13. The method of any one of claims 10 to 12, wherein the monitoring steps are performed by a local management device of the security monitoring installation.

14. The method of any one of claims 10 to 13, wherein monitoring involves the local management device of the security monitoring installation waiting to receive a notification from a sensor or a sensing arrangement.

15. The method of any one of claims 10 to 14, wherein the method is performed by the local management device when the security monitoring installation is disarmed.

16. The method of any one of claims 10 to 14, further comprising the local management device taking account of one or more of the following:

how long the door of the main entrance is open before detecting the opening or attempted opening of a door or window remote from the main entrance;
when the presence of a person inside the building at the main entrance is detected, of the amount of time that the person is at the main entrance;
information received from a door status sensor configured to detect whether the door of the main entrance is ajar;
information received from a door status sensor on the use of a security restraint such as a chain that restricts further opening of the door of the main entrance once opened;
the month, the season, the ambient (external) temperature, and the temperature inside the dwelling.

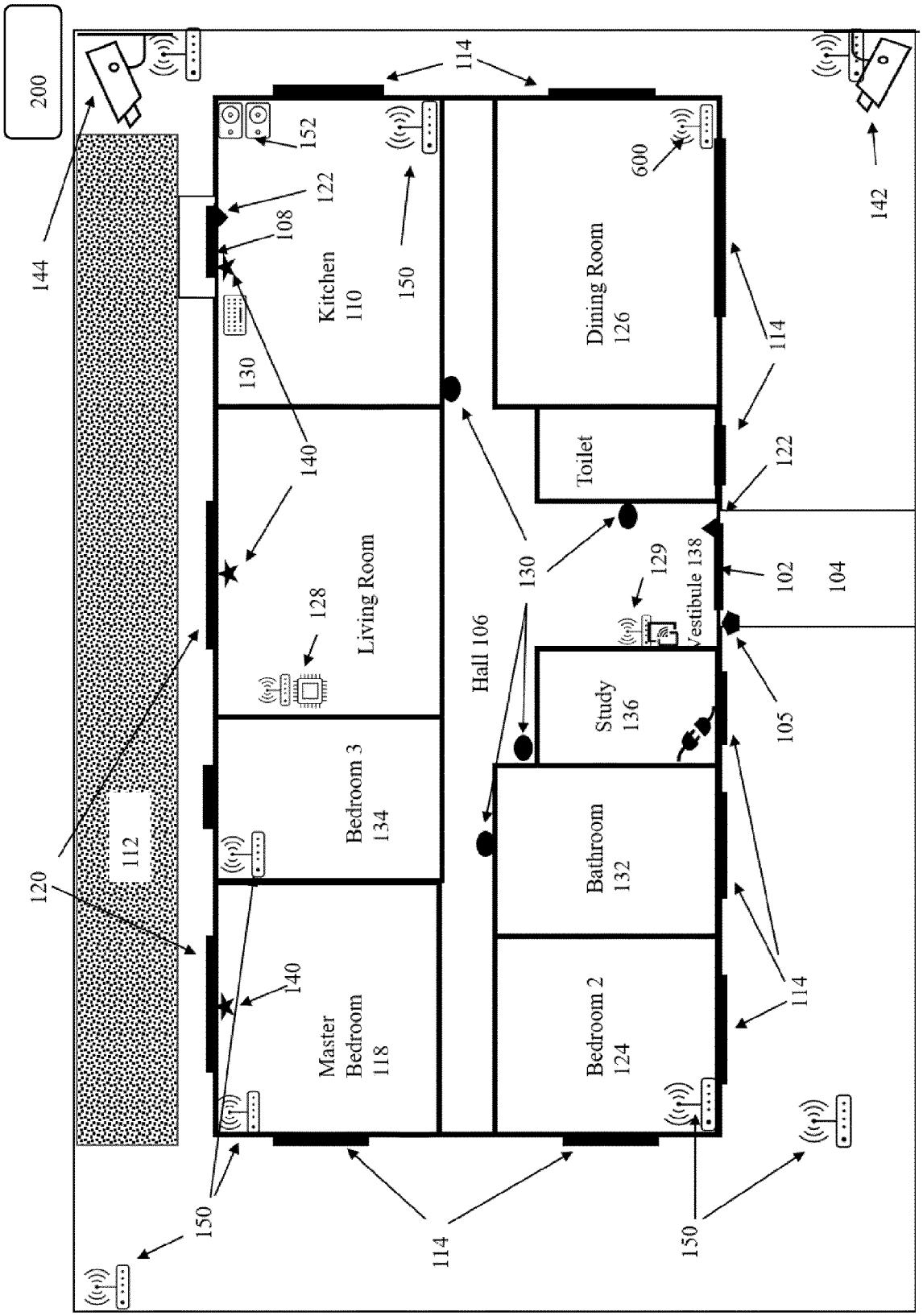
200
144
152
122
108
Kitchen
110
150
130
114
600
Dining Room
126
142
140
Living Room
128
Toilet
122
120
112
Hall 106
130
129
Vestibule 138
102
104
Bedroom 3
134
Study
136
105
Bathroom
132
Master
Bedroom
118
140
Bedroom 2
124
150
114
150
114
150

Fig. 1

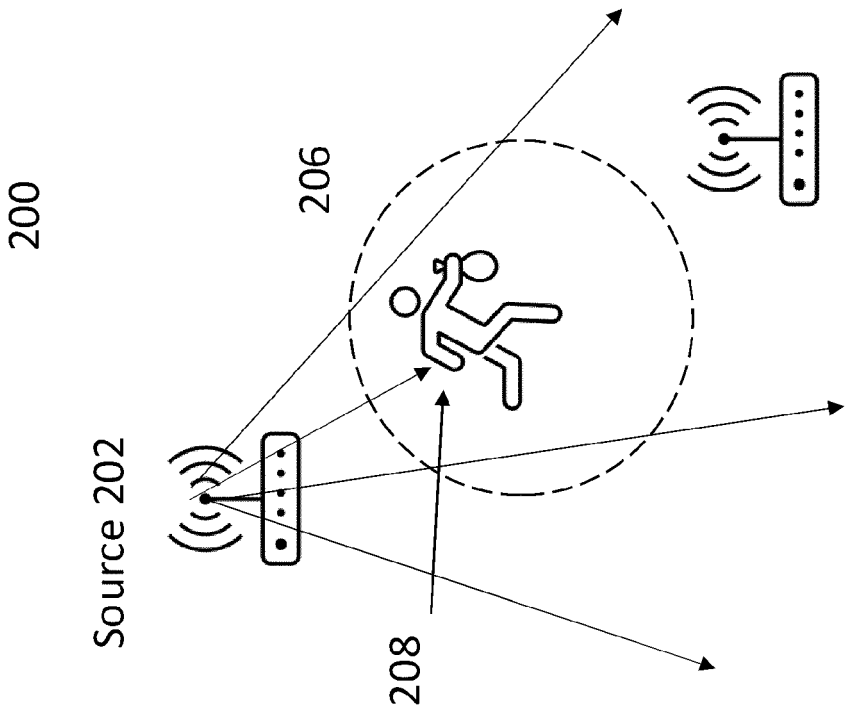
200
Source 202
206
208
Receiver
204

Fig. 2B

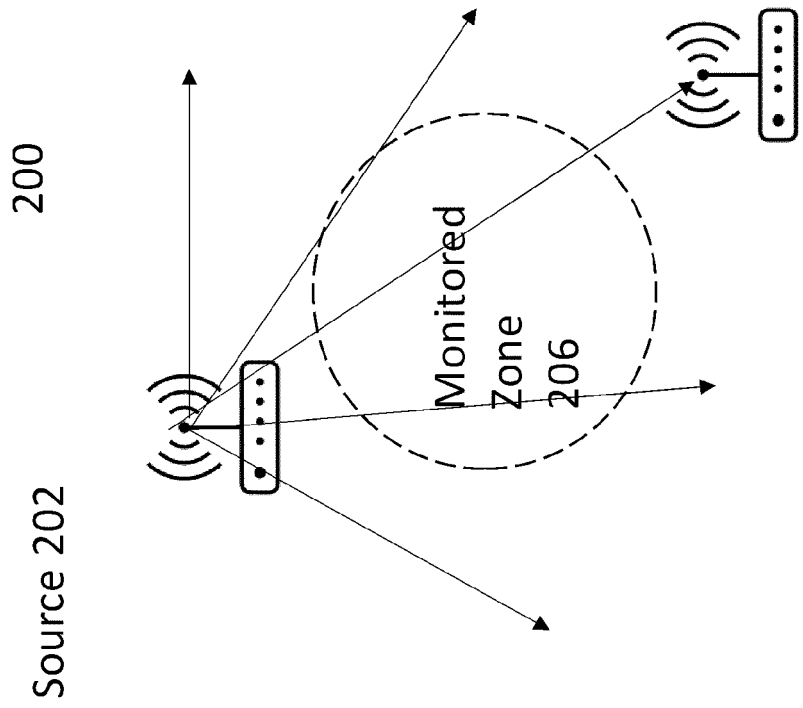
200
Source 202
Monitored
Zone
206
Receiver
204

Fig. 2A

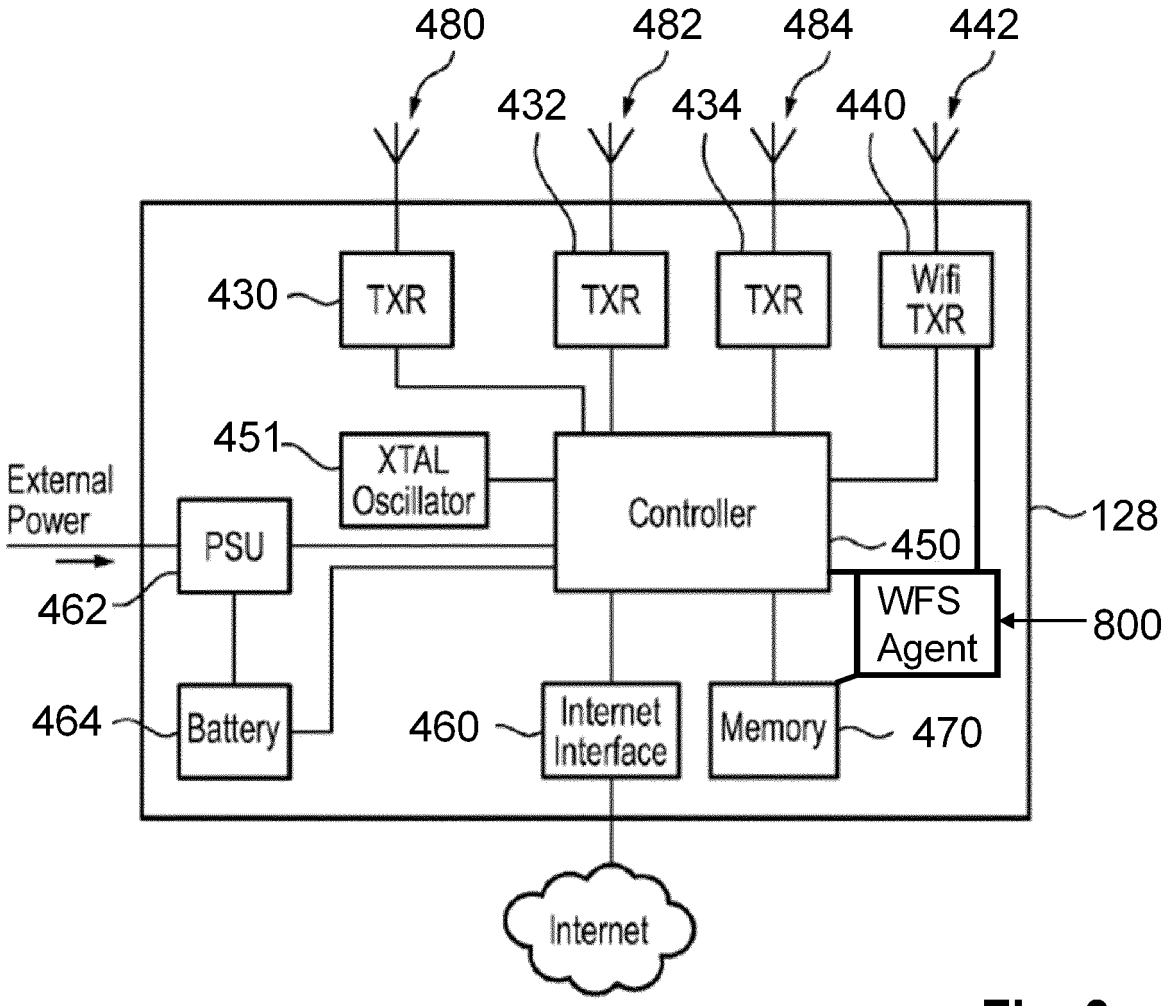
480
482
484
442
432
434
440
430
TXR
TXR
TXR
Wifi TXR
451
XTAL Oscillator
Controller
External Power
PSU
128
450
462
WFS Agent
800
464
Battery
460
Internet Interface
Memory
470
Internet

Fig. 3

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 21 21 8150

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	US 2006/059557 A1 (MARKHAM THOMAS R [US] ET AL) 16 March 2006 (2006-03-16) * paragraphs [0027], [0029], [0079], [0087], [0127] *	1-16	INV. G08B25/14 G08B29/18 ADD. G08B13/08 G08B13/196 G08B13/24 G08B25/00
A	US 2005/134450 A1 (KOVACH JOHN M [US]) 23 June 2005 (2005-06-23) * paragraphs [0028], [0029] *	1-16	
A	US 2019/066464 A1 (WEDIG KURT JOSEPH [US] ET AL) 28 February 2019 (2019-02-28) * paragraphs [0042] - [0048], [0057] - [0060] *	1-16	

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	24 June 2022	Dascalu, Aurel

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 8150

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.

24-06-2022

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006059557 A1	16-03-2006	NONE	
US 2005134450 A1	23-06-2005	NONE	
US 2019066464 A1	28-02-2019	US 2019066464 A1	28-02-2019
		US 2020082682 A1	12-03-2020
		US 2020082683 A1	12-03-2020
		US 2020082684 A1	12-03-2020
		US 2020394880 A1	17-12-2020
		US 2022172585 A1	02-06-2022

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 20200302187 A1 **[0067]**