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

(11) **EP 4 207 125 A1**

(12) **EUROPEAN PATENT APPLICATION**

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

(21) Application number: **21218184.6**

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

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

(52) Cooperative Patent Classification (CPC):
G08B 25/008; G08B 13/19613; G08B 13/2491

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

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

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

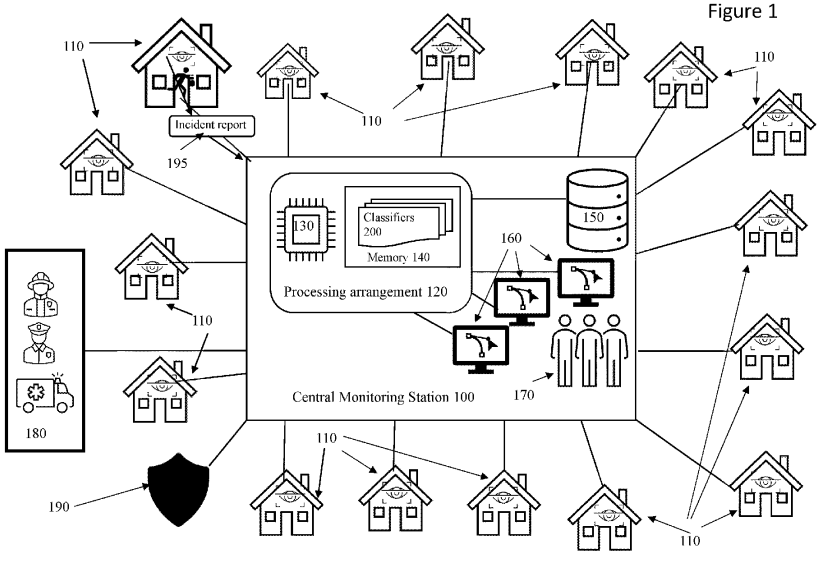
(74) Representative: **Prinz & Partner mbB**
Patent- und Rechtsanwälte
Rundfunkplatz 2
80335 München (DE)

(54) REMOTELY MONITORED PREMISES SECURITY MONITORING SYSTEMS

(57) A method performed by a monitoring centre for remotely monitoring a plurality of premises security monitoring installations, comprises: receiving reports from a local management device of one of the premises security monitoring installations of patterns of sensor data corresponding to movement and behaviour of occupants within the premises; and using a classifier to identify burglaries by processing reported patterns of data received from the local management device, the classifier having been trained to recognise patterns of sensor data that signify burglary events.

A corresponding method is performed by a local management device of a premises security monitoring system installation, the premises used by occupants, and the security monitoring system having an armed state and a disarmed state, the method comprising in the disarmed state: receiving sensor data from a plurality of alarm event sensors of the premises; processing the received data using a classifier trained to discriminate between patterns of sensor data that signify usual behaviour of the occupants and patterns of sensor data that may signify burglary events; and reporting to a remote monitoring centre any patterns of sensor data recognised as signifying a burglary event.

Figure 1



EP 4 207 125 A1

Description

Field

[0001] The present invention relates generally to remotely monitored security monitoring systems for premises, and in particular to remote monitoring stations, installations of such systems, local management devices for such systems, and corresponding methods.

Background

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

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

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

[0005] The idea behind using the "night mode" (whether it is the armed away mode or a variant of "armed at home") is of course to provide a warning of and to any intruders who break into, or move around within, the living accommodation - which is commonly on the ground floor and hence more readily accessible than the sleeping accommodation that is commonly on an upper floor, while permitting 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] There therefore exists a need to address this problem.

[0009] 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".

[0010] Embodiments of the invention are based on the insight that there are patterns of behaviour characteristic of burglary, in particular concerning the patterns of movement characteristic of burglars in action and distinct from the patterns of movement characteristic of people who are just moving around in their own home, that these patterns of movement may be revealed using a suitable sensing arrangement (in particular, but not exclusively, radio-based presence and location sensing, that it is possible to train a classifier to distinguish between these different patterns of behaviour, and that such a classifier supplied with relevant data (for example from radio-based presence and location sensing) could be used to recognise and flag the incidence of patterns characteristic of burglary - and that this could be done irrespective of the armed state of the security monitoring system. In other words, by using a suitably trained classifier it may be possible to provide a security monitoring solution to identifying burglaries whether or not the security monitoring system has been armed.

[0011] Although it is preferred to use radio-based presence and location sensing, based on detecting perturbations of radio signals, as part of the security monitoring systems to which the insight is applied, this is not essential. Systems using only conventional line-of-sight movement/presence detection, e.g based on PIR detectors or the like, could also be used, provided that a sufficient number of rooms/spaces are monitored to enable sufficiently detailed patterns of movement to be provided. Preferably, however, systems will use a combination of conventional movement detectors (e.g. PIRs) together with radio-based presence and location sensing, based on detecting perturbations of radio signals.

[0012] One or more such classifiers, or other suitable AI techniques, could be used by a local management device of a premises security monitoring system to discriminate between "usual" behaviour in the premises and "unusual" behaviour, or to recognise "burglary-like" behaviour that is distinct from usual behaviour at the premises.

[0013] One or more such classifiers, or other suitable AI techniques, could be used in a central monitoring station to process reports received from the local management devices of multiple premises security monitoring system installations.

[0014] Preferably, a local management device of a premises security monitoring system uses at least one classifier, when the security monitoring system is disarmed, at least to discriminate between "usual" behaviour in the premises and "unusual" behaviour, and reports to a remote monitoring station incidents classified as "unusual", and/or those classified as "burglary-like". Preferably, a monitoring station receiving such "unusual" or "burglary-like" reports uses one or more such classifiers to process such reports, received from the local management devices of multiple premises security monitoring system installations, to identify reports classified as highly likely to relate to burglary. Central monitoring stations may in this way use suitably trained classifiers to "triage" received reports, enabling suitable incidents to be prioritized for more immediate attention and possibly for automatic response.

[0015] In the context of the problem of "daytime" burglaries which occur in occupied homes, the insight has application both when the security monitoring system is in an armed at home mode, and when the security monitoring system is disarmed.

[0016] The insight may likewise have application to central monitoring station handling of incident reports received from security monitoring systems that are in an armed away mode, potentially enabling a triage process that discriminates between burglaries and potential false alarms.

Summary

[0017] In a first aspect there is provided a local management device for a premises security monitoring system, the premises used by occupants, and the security monitoring system having an armed state and a disarmed state, the local management device being configured: for coupling to a plurality of alarm event sensors of the premises and to a remote monitoring centre; to use a classifier to process data received from the plurality of alarm event sensors, the classifier having been trained to discriminate between patterns of sensor data that signify usual behaviour of the occupants and patterns of sensor data that may signify burglary events; and when the system is in the disarmed state to report to a remote monitoring centre any patterns of sensor data recognised as signifying a burglary event.

[0018] In a second aspect, there is provided a premises security monitoring system installation including a local management device according to the first aspect, the local management device being operatively coupled to a plurality of alarm event sensors.

[0019] In a third aspect there is provided a monitoring centre for remotely monitoring a plurality of premises security monitoring installations, the monitoring centre being configured to receive, for each security monitoring installation, reports, from a local management device of the security monitoring installation, patterns of sensor data corresponding to movement and behaviour of occupants within the premises; the monitoring centre being further configured to use a classifier to identify burglaries by processing reported patterns of data received from the local management device, the classifier having been trained to recognise patterns of sensor data that signify burglary events.

[0020] In a fourth aspect there is provided a method performed by a local management device of a premises security monitoring system installation, the premises used by occupants, and the security monitoring system having an armed state and a disarmed state, the method comprising in the disarmed state:

receiving sensor data from a plurality of alarm event sensors of the premises;

processing the received data using a classifier trained to discriminate between patterns of sensor data that signify usual behaviour of the occupants and patterns of sensor data that may signify burglary events; and

reporting to a remote monitoring centre any patterns of sensor data recognised as signifying a burglary event.

[0021] The method of the fourth aspect may further comprise using radio-based location sensing presence and location sensing to perform people counting, and optionally determining the presence of one or more intruders based on detecting a change in the people count.

[0022] In a fifth aspect there is provided a method performed by a monitoring centre for remotely monitoring a plurality of premises security monitoring installations, the method comprising: receiving reports from a local management device of one of the premises security monitoring installations of patterns of sensor data corresponding to movement and behaviour of occupants within the premises; and

using a classifier to identify burglaries by processing reported patterns of data received from the local management device, the classifier having been trained to recognise patterns of sensor data that signify burglary events.

[0023] According to another aspect, there is provided in combination a premises security monitoring system and a remote monitoring station, the premises used by occupants, and the security monitoring system having an armed state and a disarmed state, the security monitoring system operatively coupled to the remote monitoring centre, and the installation including a plurality of alarm event sensors, the local management device being configured, when the security monitoring system is in the disarmed state, to report to the remote monitoring centre any patterns of sensor data recognised as differing meaningfully from the stored historic patterns of sensor data,

the remote monitoring centre being configured to use a classifier to identify burglaries by processing reported patterns of data received from the local management device, the classifier having been trained to recognise patterns of sensor data that signify burglary events.

[0024] In another aspect there is provided a local management device for a premises security monitoring system, the premises used by occupants, the local management device being configured for coupling to: a plurality of alarm event sensors of the premises;

a store of historic patterns of sensor data corresponding to movement and behaviour of occupants within the premises; and a remote monitoring centre; the local management device being configured to report to the remote monitoring centre any patterns of sensor data recognised as differing meaningfully from the stored historic patterns of sensor data, for the remote monitoring centre to process using a classifier to identify burglaries, the classifier having been trained to recognise patterns of sensor data that signify burglary events. The local management device may be further configured to compare patterns of received sensor data with stored patterns to identify patterns of received sensor data recognised as differing meaningfully from the stored patterns of sensor data. The local management device may be further configured to use the identification of patterns of received sensor data recognised as differing meaningfully from the stored patterns of sensor data in recognising patterns of sensor data signifying a burglary event.

[0025] The local management device may be further configured to operate a radio-based system to sense presence and location based on detecting perturbations of radio signals, and to use data received from the radio-

based system in identifying patterns of sensor data differing meaningfully from the stored historic patterns of sensor data.

Brief description of the drawings

[0026] Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a schematic drawing of a central monitoring station that supports multiple premises security monitoring systems;

Figure 2 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 3 illustrates schematically the principles of radio-based presence and location sensing; and

Figure 4 illustrates schematically features of a local management device of the system of Figure 2.

Specific description

[0027] As explained above, in a centrally monitored security monitoring system the central unit or local management device of an installation will, when the system is armed, report to the remote monitoring station whenever an alarm event is triggered as a result of input received from one or more alarm event sensors. The task of the central monitoring station, or more specifically of a human operative at the central monitoring station, is to assess the report to determine whether it is a "genuine" incident that requires some kind of response such as the attendance of security personnel, the police, or other services, or whether it is a false alarm - which may require the operative to have a conversation with an occupier for example over an audio (or audio/visual) interface of a control unit used to arm and disarm the system, and/or reset the security monitoring system remotely.

[0028] Figure 1 shows, schematically such a central monitoring station 100 that provides remote monitoring support for security monitoring systems installed in numerous premises 110. The central monitoring station 100 and the local management devices of the installations communicate using "wired" or "wireless" (radio) data links, typically over the Internet. Connections between the central monitoring station 100 and the local management devices are typically on an "as needed" basis, rather than being permanent. The central monitoring station 100 includes a processing arrangement 120 including one or more processors 130 coupled to: a memory 140. The processing arrangement 120 is coupled to a database 150, which will be described later, and preferably to one or more workstations or user interface arrangements 160 for use by one or more human operatives 170 in the viewing and monitoring of any reported incidents. As well as being communicatively coupled to the security monitoring systems installations 110, the central monitoring station 100 is also able to connect to the emergency services 180 so that support can be summoned from one or more of the fire, police, and ambulance services should this be required. Typically, the central monitoring station 100 is also able to call upon security personnel 190 other than the police, for example security guards retained specifically to attend monitored premises in the event of an incident being declared.

[0029] So that an operative 170 is best able to determine the most appropriate response to the reported alarm incident, it is known to supply the remote monitoring station with all the available data from the alarm event sensors (and preferably any other sensors of the system) in the form of an incident report 195 (although this will typically be an ongoing or serial process, rather than a single event). This report will typically include any sensor data from shortly before (typically in the region of 30 seconds before but possibly up to 1 or 2 minutes before or longer) the triggering of the alarm event, and the control unit of the security monitoring system sensor will continue to supply new data as they arrive from sensors until the incident is resolved. For each reported incident (reported alarm event), the remote monitoring station 100 may store not only all the data received from the local management device in respect of the incident, including the time/day/date that the incident occurred, but also a conclusion or finding as to whether the incident was a false alarm or was instead a burglary (there may be other categories of events, and the burglary" and "false-alarm" findings may each be divided into sub-categories). Analysis of these data has been found to reveal the existence of some similarities characteristic of behaviour that is typical to burglaries, and based on this it is possible to use machine learning to train a classifier to process live incident data to determine whether the live incident is a burglary or not (or at least whether it is more likely to be a burglary than not, or vice versa). Figure 1 shows the presence of one or more such classifiers 200 resident in memory 140 of the processing arrangement 120.

[0030] Such a trained classifier 200 can be used to, in effect "triage" incident reports 195 as they arrive at a central monitoring station 100 - so that incident reports deemed likely (or highly likely) to be burglaries can be prioritized. This prioritization may mean being that these incidents go to the front of the queue feeding the human operators, 170 they may be given a flag whose presence is visible to the human operators 170 in the monitoring station 100 and which leads to other kinds of prioritisation - for example in terms of the allocation of visits by security operatives 190 or the involvement of the police 180 (the flag in effect signifying that there's "High Confidence it's a Burglary"). Some providers of monitored security alarms may also consider dispensing with the requirement of human review of all incident reports, and treat highly rated reports as sufficient basis to involve security personnel 190 without initial human review.

[0031] The classifiers 200 may for example be based

on a convolutional neural network, as described for in "Gradient-based learning applied to document recognition", by Y. Lecun, L. Bottou, Y.Bengio, and P. Haffner, published in Proceedings of the IEEE, Vol. 86, no. 11, pp 2278-2324, 1998.

[0032] Additionally, or alternatively, one or more of the classifiers may be based on neural networks and the training of neural networks as described in US10,546,861 (Atomwise), US10,423,861 (Illumina), or US10,417,525 (Samsung).

[0033] The training of the classifier(s) may also use training data derived from "non-events" (i.e. data that does not derive from incident reports 195 but rather is based on monitoring sensor signals ("traffic") seen by local monitoring devices when its security monitoring system is disarmed. Such data would not, of course, routinely be provided by local monitoring devices to the central monitoring station, but could for example be provided shortly after initial installation, and perhaps periodically (e.g. seasonally, given that user behaviour is likely, at least in temperate climates, to change with the seasons) for example every three months, typically being collected routinely by the local management device and being supplied on demand to the central monitoring station.

[0034] The performance of the classifier 200 may be further improved by taking account of premises characteristics on the basis that the characteristic behaviours of burglars differ to some extent according to characteristics of the premises being burgled. The data concerning incident reports are already linked to the identity of the premises to which the reports relate, and the identities of premises are likewise already linked to data (e.g. about premises type: house/apartment etc.) about the premises. These premises data preferably include details about the nature of the premises protected by the monitoring system, as well as about the monitoring system that was installed, and these premises data may be stored in database 150. Salient details about the premises would tend to be:

the type of premises, e.g. apartment, number of floors, the presence of staircases, freestanding or part of a larger building, total floor area, approximate retail or rental value; location - e.g.: rural, urban, village/city, suburban or city centre;
situation - ground level or elevated (accessible/inaccessible), surrounded by a garden, open or closed surrounding spaces, fronting or backing onto a street, exposed on all free sides, etc.; construction type, window construction, number of windows, presence of window locks, presence of window opening sensors, number and type of external doors, details of the door security in use, number of unprotected doors; etc.

[0035] The following data, concerning salient details of the security monitoring system that is linked to the premises identity (for the live incident and for historic incidents) may also be available: details of the perimeter and how it is secured,

number and type (video or other) of cameras installed;
details about the areas protected or not protected by motion sensing;
age and cost (possibly replacement cost) of the system.

[0036] All the foregoing data, or a subset, may be stored in one or more databases 150.

[0037] So, for example, different classifiers 200 may be trained on relevant training data, each classifier being appropriate to different types of premises (e.g., small apartments - possibly on elevated floors, small bungalows, small houses of two floors, large apartments, large houses, etc); likewise different classifiers 200 may be trained taking account of the location/situation of the premises; and different classifiers may be trained taking account of different system installation characteristic. It is likely that once these different classifiers have been trained it will become clear which main variables correlate to certain behaviours - and that some variables seem to have little or no influence on the behaviour of burglars. One or more further rounds of classifier training may then occur taking account of only the variables found to be most significant. Further iterations may be used to optimise a set of classifiers 200 each tuned to a particular characteristic or set of characteristics of the premises/security system. Each live incident will be associated with a premises identifier and the premises identifier possibly linked in a database 150 to one of the characteristics or one of the sets of characteristics to which the various classifiers are linked. This enables the right or best classifier 200 to be selected to process the live incident to determine whether it is a burglary. It will be appreciated that after training the various classifiers, a set of classifiers 200 may be produced, each of which is appropriate for a different "type" or "category" of premises. When this is the case, efficiency can be improved by attributing such a type or category to each of the premises served by a remote monitoring station, i.e. the data record for each premises may be labelled. These labels may be stored in a database 200 that is interrogated by the processing arrangement 120 when an incident report is received, so that the processing arrangement 120 knows which classifier should be used to process that incident report.

[0038] The processing of live incident data in this way also opens up the possibility of revealing more quickly links between reported burglary incidents that may involve the same burglar or same gang of burglars, based on what is in effect detection of linked elements of a modus operandi that may not be immediately evident to a human observer. This may be achieved by identifying common patterns between the data for different incidents reported over the course of a day, a period of a few days, or a period of a week or more, and the geographical range

of incidents whose data are compared may be linked to the duration of the period - so that within a day the range might be 100km or less, a few days 250km or less, etc. A variant on this considers geography (possibly a much smaller range in mountainous terrain for example) or the availability/convenience/speed of transport links: so for example consideration may be given to the local presence of rail links, motorways, etc, as the locations of incidents that at first sight seem remote may actually cluster around a motorway or rail link (i.e. each within a certain distance or time of a station or motorway exit). In this way it may be possible to correlate incidents temporally and possibly geographically - spates of similar burglaries or a burglar or burglary gang hitting a village, town or district - and we may be able to link burglaries that have a similar modus operandi as detected by a "linking" classifier that is exposed to all recent incident reports for a geographical area or a temporal period or some combination of these and which is designed and trained to flag up possible links between incidents. These approaches may require multiple central monitoring stations to share incident data, possibly just of incidents determined by the CMS to be burglaries, but possibly also sharing more or all incident data (because this may flag up as burglaries incidents that were initially determined not to be burglaries, as may happen if the premises are unoccupied and security guard access has not been possible). Optionally multiple central monitoring stations are linked together to form a network to facilitate the sharing of event data, its processing, and the harvesting of intelligence from considering together events that were reported to different CMS.

[0039] Although these methods and approaches can be applied to known central monitoring stations and known conventional security monitoring installations (particularly if the monitored installations have movement/presence sensors, such as PIR sensors, in bedrooms as well as in access spaces - e.g. halls, landings and corridors, so that patterns of movement through the premises can be discerned readily), these techniques are even more powerful if the security monitoring systems use a radio-based location sensing arrangement to detect human presence and location in the premises based on detecting perturbations of radio signals because these techniques of presence and location sensing can cover the entire liveable area of the premises protected by a security monitoring system, without any significant gaps, whereas most conventional security monitoring systems only provide motion (and hence presence) detection at a few locations within the premises (and seldom in many bedrooms), so that most of the premises are not monitored at all for presence or movement. It should also generally be possible to start with historic data gathered from conventional (not using radio-based presence and location sensing based on detecting perturbations of radio signals) installations and to assess live incident reports from installations that do use such radio-based sensing, provided that these live incident reports come from installations with at least some conventional perimeter and movement sensors, so that there is some significant commonality of data. Indeed, initially the classifiers could consider only the comparable sensor data - in effect ignoring the radio-based presence and location data, meanwhile building up a new corpus of data including both conventional and radio-based sensing data. It may quickly become worthwhile to train a new classifier for installations that use radio-based sensing, and that classifier could in turn be used to classify live incidents from installations that perhaps include fewer conventional sensors than would otherwise be desirable.

[0040] The foregoing all has direct application in the event that the incident reports are reported by local management devices when their security management systems are in an armed at home mode, and may also be directly applicable and useful for incident reports received from systems in an armed away mode.

[0041] And although a central monitoring station configured as described above could also handle in the same way "incident reports" received from security management systems that are disarmed, no such reports are currently provided. Typically, therefore some modifications are required before a local management device will provide reports to a central monitoring station of sensor activity (i.e. signals received by the local management device from alarm event sensors and any other sensors in the security management system) when the security management system is disarmed. A convenient approach to such modifications is once again to use some kind of classifier to discriminate between "ordinary patterns" and "unusual patterns" of sensor traffic seen when the security management system is disarmed.

[0042] The local management device may be configured to capture and store data representing the patterns of sensor traffic received while the system is disarmed. Generally, these data will reflect regular patterns of behaviour, for example:

- at the start of the day residents leave their beds, go to the bathroom or toilet, go to the kitchen, maybe back to their bedroom to get dressed for work, some people may leave via a main access door to go off to work, while one or more others may stay behind and maybe do the washing up in the kitchen, do the laundry, watch TV in the lounge, go to the home office,
- or go out into the garden;
- around 10.30 to 11.30, depending upon the timing of breakfast, there may be more traffic centred on the kitchen as morning coffee is prepared;
- later, lunch may give rise to another peak of activity focussed on the kitchen;
- the afternoon may involve more work in the office, daytime TV, afternoon naps, etc; and so on for the rest of the day.

[0043] Similar patterns of behaviour are likely to be ob-

served on similar days - so that, for example, the days of the working week may all be rather similar but differ significantly from both Saturday and Sunday, which also differ from each other. Patterns of behaviour may also repeat across weeks, perhaps reflecting a weekly get together for coffee or tea, or to work on a hobby together. Patterns of behaviour may also repeat across particular days within a week - for example an informal yoga group may meet for an hour or an hour and a half at around 10am each Monday and Thursday. All of these behaviours, and the sensor traffic that accompanies them, will form part of "ordinary patterns" of behaviour.

[0044] The local management device may be configured to use machine learning or the like to extract salient clusters and sequences of sensor activation mapped to time of day, days of the week, national holidays, school holidays (whose dates may be entered into the system by a resident, or which may be derived from calendar access). Residents' diary/schedule information may also be made available to the system, so that the system can adapt to planned changes of timetabling, etc.. In this way, the local management device may generate an activity schedule that maps predicted sensor traffic (representing "ordinary behaviour") to a calendar and time of day - in effect a prediction of the pattern of ordinary behaviours to be expected. This process may start when the security monitoring system is first installed, or when the occupancy or tenancy of the premises changes, for example when the premises are sold.

[0045] The behaviour of an intruder such as a burglar is likely to differ significantly from ordinary behaviour - as generally burglars want to visit quickly as many rooms as possible to identify and grab valuables, and in particular portable valuables - many of which the burglar will expect to find hidden in a bedroom drawer. Hence a burglar is likely to open a lot of doors in quick succession, rapidly go from entering the premises to entering bedrooms, possibly running from room to room and up and down stairs. This general pattern of burglar behaviour, being so distinct from (most) usual patterns of behaviour, should be readily recognisable in sensor traffic data, and it should therefor the possible to train a classifier, or use another suitable AI technique, to process live sensor traffic data (preferably at or supplied by the central unit 222), and to discriminate between these two classes of behaviour. If the classifier identifies in the live sensor traffic feed behaviour corresponding to burglar behaviour, the local management device may be configured to send an "incident report (disarmed)" to the remote monitoring station for review. It may also be useful to have a third category or class of behaviour that is neither "ordinary" nor "burglary", which we might term simply "unusual". Unusual incident reports, suitably flagged, may also be forwarded to the remote monitoring station for review. There, they may be recognised as indicating a burglary, but they may instead be recognised as indicating some other objectionable behaviour - like vandalism, arson, or something like a "rave" or a party - all of which may require intervention by security personnel.

[0046] Thus, preferably a central monitoring station is provided with one or more classifiers to process reports received from security monitoring installations. The reports may be received only from security monitoring installations that are armed, but they may also be received from security monitoring installations that are disarmed. In this latter case, preferably the local management devices of relevant security monitoring installations are configured to use one or more classifiers to discriminate between at least "usual" and "unusual" behaviours, and only to report to the central monitoring station data in respect of unusual behaviours, and optionally only in respect of behaviours classified as burglary behaviour.

[0047] It should also be mentioned that one of the important functions that can be provided by central monitoring stations is to contact individuals associated with a security monitoring installation - which might include the owner(s), relatives of the owner(s) - e.g. children or parents of the owner(s), a specified neighbour. etc. Contact may be made by means of push notifications, especially to the phone/device of the owner/occupier, by calling telephone numbers, using messenger services (such as WhatsApp or Line), etc. Preferably the central monitoring station is also able to make a "call" to the control unit(s) of a security monitoring system so that an operator can speak with, and preferably video-call with, residents of the premises in respect of which a report is received (and at other times, as necessary).

[0048] Preferably incident reports produced when the security monitoring system is disarmed are suitable flagged, so that the central monitoring station can treat them accordingly (possibly employing one or more classifiers specific to this type of report, rather than using the same classifiers irrespective of whether the report comes from an armed system or a disarmed one). That is, the central monitoring station may be configured to treat incident reports differently according to whether they come from a disarmed system, an armed away system, or an armed at home system.

[0049] Thus, according to a first aspect there is provided a local management device for a premises security monitoring system, the premises used by occupants, and the security monitoring system having an armed state and a disarmed state, the local management device being configured: for coupling to a plurality of alarm event sensors of the premises and to a remote monitoring centre;_to use a classifier to process data received from the plurality of alarm event sensors, the classifier having been trained to discriminate between patterns of sensor data that signify usual behaviour of the occupants and patterns of sensor data that may signify burglary events; and when the system is in the disarmed state to report to a remote monitoring centre any patterns of sensor data recognised as signifying a burglary event.

[0050] We will now describe, with reference to Figure 2, an example of a security monitoring installation that could (and preferably does) use a radio-based location

sensing arrangement to detect human presence and location in the premises based on detecting perturbations of radio signals.

[0051] Figure 2 shows schematically a security monitoring system installation 200 in a dwelling, having a perimeter. In this example, the dwelling is a multi-storey house. A front door 204 serves as the main entrance to the premises. The Figure shows just one floor of the dwelling, in this instance a ground floor, which accommodates the living space, while the sleeping space is provided on one or more other (upper) floors accessed via stairway 205. The living space includes an entrance hall 206, onto which the front door 204 opens, off which are a rear living room 208, a front dining room 210, and a rear kitchen 212.

[0052] The kitchen 212 includes the back door 214 of the premises. The front 204 and back 214 doors are each provided with a sensor arrangement 216 that is triggered by the opening of the relevant door - for example, a sensor arrangement 216 including a magnetically triggered sensor such as a reed relay or a magnetometer.

[0053] The living room 208 is provided with glazed doors 218, which may be in the style of "French Windows" or the like, which permit access to a rear garden, but which are not intended, or used, for regular access to the interior of the premises. These doors 218 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 220 to the kitchen 212 and dining room 210 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.

[0054] The security monitoring system includes a controller or central unit (which may also be referred to as a local management device) 222 which is operatively coupled to the door opening sensors 216 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 222 is operatively connected, for example via a wired and/or wireless Internet connection, to a remote monitoring station 290 to which alarm events are communicated for review and for appropriate intervention or other action to be taken. The remote monitoring station 290 (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).

[0055] The security monitoring system also includes one or more motion sensors, typically line-of-sight motion sensors such as PIR sensors. Preferably, at least if the system is to be used without radio-based sensing, a motion sensor is provided in each of the rooms and common areas, so that patterns of movement between the different rooms can be revealed. In the illustrated example, a motion sensor 224 is shown as being installed at the head of the stairs 205 that lead to the upper floor(s), as well as in the hall and each of the rooms. Similarly, although not shown, the installation also preferably includes a motion sensor 224 for each room (with the possible exception of bathrooms and toilets) and landing on the upper floors. Preferably, as shown, the security monitoring system includes at least one camera, preferably a video camera with an associated (integral or separate) motion sensor, activation of which may cause the camera (or the motion sensor) to report an event to the central unit. In response, the central unit 222 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 290.

[0056] The upper floor(s) of the premises may also be provided with a further motion-triggered video camera, typically at the head of the stairs. Depending upon the proximity of climbable features externally, such as rainwater downpipes, soil stacks, trees, outbuildings, some or all of the windows on the upper floors may also be provided with sensors to detect their whether they are opened or closed, and sometimes also to show the degree of their opening if open (e.g. based on one or more magnets and one or more magnetometers or other sensors responsive to a magnetic field).

[0057] The security monitoring system also includes a user interface or control panel 228 in the hall 206 fairly close to the front door 204. This control panel 228 is provided so that a user can arm and disarm the security monitoring system using either a code or PIN (e.g. a 4 or 6 digit PIN) or a token (using a short-range communication technology e.g. RFID, NFC, BTLE). The control panel may also be used to set the security monitoring system to an armed at home state, optionally directly from an armed away state. The control panel 228 preferably includes a visual display, such as a screen (optionally a touch sensitive display) to provide users with system information, status updates, event reports, and even possibly face to face communication with personnel in the central monitoring station (for which purpose the control panel 228 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 230, 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 230 may include one or more indicator lights, featuring e.g. RGB LEDs, to provide visual feedback on arming status (armed away, armed at home, and possibly other armed states), alarm event status, as well as at least an audio

output device to provide warning and advisory tones or messages. Preferably the disarm node 230 includes both an audio output device (e.g. one or more loudspeakers and optionally an alarm sounder) and a microphone so that a user can talk with a CMS operator if necessary. Like the sensors 216 and 224, the control panel 228 and disarm node 230 are preferably provided with at least one radio transceiver for communication with the control unit 222, 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 222, 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.

[0058] Conventionally, when such a security monitoring system is in the disarmed state, opening of the front or back doors, or triggering any of the motion sensors 224 doesn't constitute an alarm event. The relevant sensor 216, 224 will typically be configured to report a sensed event to the central unit 222 irrespective of the arm state of the security monitoring system (since typically the nodes of a security monitoring system are not aware of the arming state of the system), but the central unit 222 will ordinarily disregard such reported events when the system is disarmed. However, as noted above, if the central unit is provided with a classifier or other AI capability enabling the central unit to differentiate between at least "ordinary" patterns of behaviour and "burglary" patterns of behaviour, then the central unit may be configured to generate incident reports in respect of at least suspected "burglary" events, and possibly also in respect of other "unusual" events.

[0059] In the fully armed state, which may be termed the "armed away" state, event notifications from perimeter sensors (in the illustrated example the door opening sensors 216 on the front 204 and back 214 doors, but typically also including one or more sensors to detect the opening of windows 220) and internal movement or presence sensors, 224 typically result in the central unit 222 determining an alarm event which may then be reported to the central monitoring station 290. As previously explained, typically, such security monitoring system also have a second armed state in which only the security of the perimeter is monitored - so that only events reported by one or other of the door sensors 216 (or window sensors if present) count as potential alarm events to be reported by the central unit 222 to the remote monitoring station 290 - and this may be termed the "armed at home" state. The armed at home state is intended to be used when the premises are occupied. In the armed at home state the central unit 222 will routinely be arranged not to request any internal (video) camera to share images with the central unit 222 - so that user privacy is maintained.

[0060] There may be more than one variant of the armed at home state - so that, for example during the daytime only the perimeter may be monitored, but at night (or upon the residents retiring to bed) the system may be set to a nocturnal armed at home state in which movement within the living accommodation (but not the sleeping accommodation) can also give rise to an alarm event potentially to be reported to the CMS 290 (including images from any camera within the monitored zone) - but the triggering of any movement sensors for the area of the sleeping accommodation, e.g. on a landing, will not give rise to alarm events. The illustrated installation provides such a nocturnal armed at home state, as well as a "daytime" armed at home state in which only the perimeter is secured.

[0061] The installation shown in Figure 2 may also be provided with a radio-based location sensing arrangement to detect human presence throughout the premises (both the ground floor "living accommodation" and the "sleeping accommodation" on the upper floor(s), and that is configured to sense presence and location based on detecting perturbations of radio signals. Figure 2 shows various Wi-Fi capable devices which are distributed around the ground floor, signals from which are used by a radio-based location sensing arrangement which is provided as part of the security monitoring system.

[0062] The radio-based presence sensing, which here is conveniently be based on the monitoring of Wi-Fi signals (but which could be based on radio signals from other radio communications standards or protocols), and which for convenience we will refer to as WFS, is here performed by the central unit 222 which operates as a Wi-Fi Access Point (AP) and which serves as a Wi-Fi sensing receiver. Figure 2 shows the presence of various radio transceivers that are used to provide radio-based presence detection in each of the interior spaces of the ground floor of premises. The WFS system may be configured to recognise location "zones" which may map to rooms, or map to floors in premises comprising a plurality of floors, but may also map to regions within rooms, and exterior zones may be identified corresponding to particular sections of the grounds or surroundings of a dwelling or other structure - e.g. terrace, front garden, parking area, etc.

[0063] To ensure that the WFS effectively covers the whole area of interest (for example, the ground of the premises, as shown here) we need to provide a sufficient number of suitable located Wi-Fi stations (STAs) as WFS illuminators so that Wi-Fi signals received at the central unit AP 222 traverse the whole area of interest. If we want to provide WFS cover to multiple floors we may need to provide an appropriate WFS receiver on each floor, together an appropriate number of suitably positioned illuminator devices, although depending on the building's construction signals from illuminators on one floor may

be used by WFS receivers on other floors.

[0064] Because Wi-Fi transceivers are quite power hungry, we will generally want the STAs used as WFS illuminators to be mains powered (but preferably also with some back-up power supply such as an internal battery power source) rather than solely battery powered. That may lead us to replace some battery powered but Wi-Fi capable devices of an existing non-WFS security monitoring system with mains powered equivalents - so, for example, a battery powered video camera might be replaced by a mains powered equivalent 226, and a battery powered control unit may be replaced by a mains powered equivalent 228 that is Wi-Fi capable (although the control unit 228 will typically still use something other than a Wi-Fi transceiver (e.g. a low power ISM transceiver) to communicate with the central unit 222).

[0065] Alternatively (or additionally) we may simply add new mains powered Wi-Fi capable devices such as smart plugs, smart bulbs, Wi-Fi range extenders (for example of the type that simply plug in to a socket of the mains electricity supply), to provide a Wi-Fi network that covers the whole of the area of interest and that is used for WFS. The household may have more than one Wi-Fi network, but generally only one of these will be used for WFS - and conveniently the central unit 222 will be an AP of that network.

[0066] The central unit AP 222 preferably works in infrastructure mode in conjunction with the various other Wi-Fi stations (STAs) to form either an infrastructure Basic Service Set (BSS) or, in conjunction with another AP connected (e.g via ethernet) to the same Local Area Network as the central unit 222 - such as broadband router 600, to provide an Extended Service Set (ESS).

[0067] For ease of explanation, we will assume initially that the central unit AP 222 provides just a BSS and not an ESS, and that only the central unit AP 222 serves as a Wi-Fi sensing receiver. Some or all of the STAs in the BSS act as illuminators to provide signals which the CU 122 analyses in order to perform WFS. As shown, these other STAs include the broadband router 600 in the dining room, the control unit 228 and a Wi-Fi-enabled camera 226 in the hall, and optionally the disarm node 230 in the kitchen. Preferably, because of the power consumption concerns, both the Wi-Fi enabled camera and the disarm node 230 are fed with power from a mains electricity supply as well as having an autonomous internal power supply. In addition, the kitchen is provided with an STA in the form of for example a "smart speaker" 610, and the living room with a "smart plug" 612. If the disarm node 230 only has an internal power supply, and is not mains fed, it is preferably not configured as a Wi-Fi STA but instead some other Wi-Fi STA device (such as the smart speaker 610) may be installed to suitably extend WFS coverage within the kitchen and the living room - for example, a Wi-Fi range extender or smart plug or the like which is plugged into a conveniently located power socket.

[0068] With the arrangement shown in Figure 2 the control unit 222 (or more generally the security monitoring system, given that some entity other than the central unit may be responsible for determining presence and location of presence) may be configured, whatever the arming state of the system, to use the radio-based presence sensing to detect and locate presence within the monitored area(s). The system (typically the central unit) may for example records, e.g. in a database, the location (e.g. the relevant zone identifier) and time of the inferred presence. The system (e.g. central unit) receives information data from the radio-based presence sensing arrangement relating to detected presence and these data will be processed to determine the location(s) (e.g. zone identifier(s)) of any human presence and also preferably information data relating to the person count in each zone determined to be occupied. These data, and their timings, are recorded in the database. The system (e.g., the central unit) is therefore continuously aware when and where there is presence in the monitored areas.

[0069] Although Figure 2 only illustrates a single floor of premises, it will be appreciated that if it is desired to provide a WFS capability for other floors of the premises - as we do here, because the sleeping accommodation is provided on the upper floor(s) while the ground floor is devoted to living accommodation - it is necessary to ensure suitable Wi-Fi network coverage of those floors, typically by providing a corresponding access point, together with a plurality of Wi-Fi STAs as illuminators, for each floor - although sometimes useful WFS capability can be achieved between floors. Understandably, attenuation of signals within a building is critically dependent upon the type of construction and the materials used, and these factors need to be considered when designing and installing any WFS system.

[0070] 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.

[0071] 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 re-

sponse 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.

[0072] The idea is illustrated very schematically in Figure 3, here with an installation 300 including just a single source (or illuminator) 302 and just a single receiver 304, for simplicity, although in practice there will typically be multiple sources (illuminators) and sometimes plural receivers. The installation 300 has been established to monitor a monitored zone 306. In Figure 3A we see that in steady state, and in the absence of a person, radio signals are transmitted from the source 302, spread through the monitored zone 306, and are received by the receiver 304. 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 304. 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 308, as shown in Figure 3B. From Figure 3B 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 304. 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 302 to the receiver 304 is likely to change as the intruder 308 enters, passes through, and leaves the monitored area 306, 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".

[0073] 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.

[0074] 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 super-

vised machine learning approach, but other approaches to training may be used.

[0075] 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.

[0076] Although the Figure 3 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.

[0077] Now, considering once again the installation of Figure 2, and assuming that the location and presence sensing arrangement also covers the sleeping accommodation of the premises, it will be appreciated that by combining a radio-based location sensing arrangement with a premises security monitoring system it is possible for the security monitoring system to be aware of human presence, the location(s) of any humans present, and the actions/activities of any people present. This capability means that a classifier of such a security monitoring system should in effect have more sensor data to work with (the combination of WFS data and alarm event sensor data) than would typically be available from a system just using line-of-sight based motion/presence detection and may be capable of discriminating more reliably between "ordinary" patterns of behaviour and "burglary" patterns of behaviour.

[0078] In an aspect there is provided a local management device for a premises security monitoring system, the premises used by occupants, and the security monitoring system having an armed state and a disarmed state, the local management device being configured: for coupling to a plurality of alarm event sensors of the premises and to a remote monitoring centre;

[0079] to use a classifier to process data received from the plurality of alarm event sensors, the classifier having been trained to discriminate between patterns of sensor data that signify usual behaviour of the occupants and patterns of sensor data that may signify burglary events; and when the system is in the disarmed state to report to a remote monitoring centre any patterns of sensor data recognised as signifying a burglary event; the local management device further configured to operate a radio-based system to sense presence and location within the premises based on detecting perturbations of radio signals.

[0080] Preferably the classifier has been trained using training data comprising patterns of sensor data corresponding to movement and presence data corresponding to usual behaviour of occupants within the premises.

[0081] Preferably the classifier has been trained using training data comprising patterns of sensor data corresponding to movement and presence data corresponding to occupant behaviour during burglaries.

[0082] The local management device is preferably configured to store patterns of sensor data corresponding to movement and behaviour of occupants within the premises.

[0083] The local management device is preferably configured to supply patterns of sensor data from the stored patterns of sensor data to the remote monitoring centre upon receiving a request from the remote monitoring centre.

[0084] In a second aspect there is provided a premises security monitoring system installation including a local management device according to the first aspect, the local management device being operatively coupled to a plurality of alarm event sensors. Optionally, the premises includes living accommodation, sleeping accommodation, and one or more bathrooms and toilets, wherein the plurality of alarm event sensors includes one or more motion sensors to detect movement into rooms providing the sleeping accommodation and one or more motion sensors to detect movement into principal rooms of the living accommodation.

[0085] In a third aspect there is provided a monitoring centre for remotely monitoring a plurality of premises security monitoring installations, the monitoring centre being configured to receive, for each security monitoring installation, reports, from a local management device of the security monitoring installation, patterns of sensor data corresponding to movement and behaviour of occupants within the premises;

[0086] the monitoring centre being further configured to *use* a classifier to identify burglaries by processing reported patterns of data received from the local management device, the classifier having been trained to recognise patterns of sensor data that signify burglary events.

[0087] Preferably the monitoring centre is configured to filter received reports using the classifier, reports recognised as including patterns of sensor data that signify burglary events being supplied to one or more human operators of the monitoring centre for processing.

[0088] Preferably the monitoring centre is further configured, for any received report that includes patterns of sensor data recognised as signifying a burglary event, to send a request for video data to the local management device from which the report was received.

[0089] Preferably the remote monitoring centre is configured to associate each of the premises with one or more identifiers signifying type, size, situation, location, and/or other characteristics of the respective premises.

[0090] Preferably the remote monitoring centre is configured to supply one or more of the associated identifiers to the classifier to improve the classification process of the reported patterns of sensor data for the respective premises. Here, improve means to increase the speed or quality of discrimination.

[0091] Preferably the monitoring centre has been trained using supervised learning based on historic patterns of sensor data for events at multiple premises, some of the events being known burglary events, and others being known not to have been burglary events.

[0092] Preferably the monitoring centre is configured to supply the classifier with updated information based on confirmation of the burglary status of received reports initially recognised as containing patters of sensor data that signify burglary events.

[0093] Preferably the received patterns of sensor data include data in respect of a radio-based system configured to sense presence and location based on detecting perturbations of radio signals.

[0094] Preferably the radio-based sensing arrangement in any of the first through fifth aspects is configured to process communication signals received from one or more radio transmitters operating according to one or more communication standards or protocols, and optionally the one or more radio transmitters that are in a common wireless network with the local management device.

[0095] Preferably for the radio-based sensing arrangement in any of the first through fifth 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.

[0096] Preferably for the radio-based sensing arrangement in any of the first through fifth aspects uses changes in channel state information or received signal strength in determining presence.

[0097] Preferably for the radio-based sensing arrangement in any of the first through fifth aspects the local management device the local management device is configured to function as an access point of a radio network whose signals are used by the radio-based presence and location sensing system. Optionally, the radio network for which the local management device functions as an access point includes at least one further access point. Optionally, the radio network is a Wi-Fi network, and optionally the one or more radio transmitters include one or more of the following: a Wi-Fi access point, a Wi-Fi extender, a smart plug or smart socket, a smart speaker, a smart bulb, a control panel of the security monitoring system, a Wi-Fi-enabled video camera.

[0098] Preferably for the radio-based sensing arrangement in any of the first through fifth aspects the local management device is further configured to perform processing of signals as part of the radio-based location sensing arrangement.

[0099] Preferably for the radio-based sensing arrangement in any of the first through fifth aspects the local management device is further configured to use data from the radio-based location sensing arrangement to perform people counting, and optionally to use determine the presence of one or more intruders based on a detected change in the people count when the system is in a disarmed mode.

[0100] In a fourth aspect there is provided a method performed by a local management device of a premises security monitoring system installation, the premises used by occupants, and the security monitoring system having an armed state and a disarmed state, the method comprising in the disarmed state:

receiving sensor data from a plurality of alarm event sensors of the premises;

processing the received data using a classifier trained to discriminate between patterns of sensor data that signify usual behaviour of the occupants and patterns of sensor data that may signify burglary events; and

reporting to a remote monitoring centre any patterns of sensor data recognised as signifying a burglary event.

[0101] In a fifth aspect there is provided a method performed by a monitoring centre for remotely monitoring a plurality of premises security monitoring installations, the method comprising:

receiving reports from a local management device of one of the premises security monitoring installations of patterns of sensor data corresponding to movement and behaviour of occupants within the premises; and

using a classifier to identify burglaries by processing reported patterns of data received from the local management device, the classifier having been trained to recognise patterns of sensor data that signify burglary events.

[0102] The local management device may be further

configured to use data from the radio-based location sensing arrangement to perform people counting, and optionally to use determine the presence of one or more intruders based on a detected change in the people count compared to an expected person count (based on usual occupancy for the time of day and day of the week - e.g., taking account of stored information on "normal" or "usual" behaviour for the relevant day and time.

[0103] 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.

[0104] The radio-based sensing arrangement is preferably configured to process communication signals received from one or more radio transmitters operating according to one or more communication standards or protocols, and optionally the one or more radio transmitters that are in a common wireless network with the local management device.

[0105] Preferably, the local management device includes a radio receiver of the radio-based presence and location sensing system, and optionally the local management device includes a processor and a memory holding software instructions that when run on the processor cause the local management device to process radio signals to derive location and presence data.

[0106] Preferably, the sensing arrangement to detect human presence uses changes in channel state information or received signal strength in determining presence.

[0107] Preferably, the local management device is configured to function as an access point of a radio network whose signals are used by the radio-based presence and location sensing system. Optionally, the radio network for which the local management device functions as an access point includes at least one further access point.

[0108] Preferably, the radio network is a Wi-Fi network, and optionally the one or more radio transmitters include one or more of the following: a Wi-Fi access point, a Wi-Fi extender, a smart plug or smart socket, a smart speaker, a smart bulb, a control panel of the security monitoring system, a Wi-Fi-enabled video camera.

[0109] Preferably, the local management device is further configured to perform processing of signals as part of the radio-based location sensing arrangement.

[0110] Figure 4 is a schematic drawing showing in more detail features of the gateway or central unit 222 of Figure 2. The gateway 222 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 222 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 222 includes a power supply 362 which is coupled to a domestic mains supply, from which the gateway 222 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 222 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 228 or disarm node 230) 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.

[0111] 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.

[0112] 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.

[0113] As an alternative to incorporating the radio sensing application into the central unit, this functionality can be provided on an access point, e.g. a Wi-Fi access point, AP such as router 600, of the premises, with the AP configured to report the result of presence detection to the central unit 222. 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 222 which would be the overall master in terms of reporting the "alarm".

[0114] 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.

[0115] 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.

[0116] At least one Wi-Fi transmitter and one Wi-Fi receiver are required to perform WFS measurements, and these can be located in the same device (to create a kind of monostatic radar) or in different devices. The measurement is always performed by a Wi-Fi Sensing-enabled receiver on the Wi-Fi signal transmitted by a transmitter, and which may or may not originate from a Wi-Fi sensing-capable device. The device that transmits the signal that is used for measurements is called the "illuminator," as its transmissions enable collection of information about the channel - that is, it illuminates the channel.

[0117] 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.

[0118] 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.

[0119] 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).

[0120] Invoked measurement involves utilizing a packet transmission that is in response to a packet received from the Wi-Fi Sensing receiver device.

[0121] 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.

[0122] 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.

[0123] A WFS system can be built based on existing

Wi-Fi standards, hardware, software and infrastructure.

[0124] 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.

[0125] 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.

[0126] 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.

[0127] 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.

[0128] 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.

[0129] 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.

[0130] 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).

[0131] The application layer can potentially reside on any networked device: in some embodiments of the present invention, it will reside in the central unit 222 along with the WFS agent, but in other embodiments the application layer may exist in an external server or even in the central monitoring station. We prefer, however, to provide the application layer on the central unit to avoid potential problems with signalling delays (for example due to accidental or deliberate network interruption) between the central unit (or other WFS receiver) and a remotely located entity. The application layer receives input from one or multiple Wi-Fi sensing software agents. It combines the information and delivers it to the security management system which may then in turn provide it to the CMS and/or to a cloud service by means of which push notifications may be sent to a registered user device such as a smartphone - allowing users to receive real-time notifications and the ability to view historic data.

[0132] 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.

[0133] 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.

[0134] 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.

[0135] 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.

[0136] 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.

[0137] 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.

[0138] 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.

[0139] The WFS agent needs to have a mechanism to determine which devices are capable and needs to participate in the sensing for each application on a device-specific basis. A WFS agent also needs to be capable of configuring the radio for measurements and triggering transmissions on a periodic basis for sensing measurements, and to enable/disable measurements or adjust configuration parameters for Wi-Fi sensing-capable devices. Optionally, the Wi-Fi Sensing agent is also able to request specific radio resource management operations, such as AP or band steering. The WFS agent is also preferably able to detect and process specific sensing events and communicate the relevant information to the application layer (e.g., the security monitoring system) for specific handling and user presentation.

[0140] 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.

[0141] 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.

[0142] 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.

[0143] The IEEE 802.11a preamble is useful for Wi-Fi Sensing. The preamble contains a short training field (STF), a guard interval and a long training field (LTF). The STF is used for signal detection, automatic gain control (AGC), coarse frequency adjustment and timing synchronization. The LTF is used for fine frequency adjustment and channel estimation. Since only 52 subcarriers are present, the channel estimation will consist of 52 frequency points. Newer OFDM PHY versions (HT/VHT/HE) maintain the IEEE 802.11a preamble for backward compatibility and refer to it as the legacy preamble. The legacy preamble spans a 20MHz bandwidth and consists of a legacy STF (L-STF) and legacy LTF (L-LTF). As more recently defined OFDM PHY versions (HT/VHT/HE) introduce wider channel bandwidths (up to 160MHz) for backward compatibility, the legacy preamble is duplicated on each 20MHz channel. This allows the receiver to compute 52, 104, 208 or 416 valid L-LTF frequency points, which represent the channel estimation

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

[0144] 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.

[0145] 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.

[0146] 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.

[0147] 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.

[0148] 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.

[0149] 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.

[0150] 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.

[0151] To interact with the MAC and PHY, the WFS agent has an interface to pass the WFS control information to the radio and extract the measurement data. The interface should be PHY agnostic and is, therefore, defined in a generic manner and extendable to cover different radio driver implementations, including drivers from different chipset vendors. The interface definition should allow for potential additional features or capabilities provided by a specific PHY or a chipset, as well as a path for growing the technology. Definition of a standard interface/API enables radio firmware and driver developers to ensure compliance and enables reuse of components or common codes, which may be placed into a library. Most Wi-Fi drivers are based on either the wireless-extensions framework or the more recent and actively developed cfg80211 / nl80211 framework. As the system integration components are largely provided, these frameworks enable Wi-Fi driver developers to focus on the hardware aspects of the driver. These frameworks also offer significant potential as a location for defining a WFS API. The WFS interface should provide the WFS agent with STA identification and enable the WFS agent to track the physical device in the network (i.e., the AP to which it is connected), as well as the device's capability and availability to participate in the measurements.

[0152] 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.

[0153] 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.

[0154] 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 local management device for a premises security monitoring system, the premises used by occupants, and the security monitoring system having an armed state and a disarmed state, the local management device being configured:

   for coupling to a plurality of alarm event sensors of the premises and to a remote monitoring centre;
   to use a classifier to process data received from the plurality of alarm event sensors, the classifier having been trained to discriminate between patterns of sensor data that signify usual behaviour of the occupants and patterns of sensor data that may signify burglary events; and when the system is in the disarmed state to report to a remote monitoring centre any patterns of sensor data recognised as signifying a burglary event.

2. The local management device of claim 1, wherein the classifier has been trained using training data comprising patterns of sensor data corresponding to movement and presence data corresponding to usual behaviour of occupants within the premises.

3. The local management device of claim 1 or claim 2, wherein the classifier has been trained using training data comprising patterns of sensor data corresponding to movement and presence data corresponding to occupant behaviour during burglaries.

4. The local management device of any one of the preceding claims, configured to store patterns of sensor data corresponding to movement and behaviour of occupants within the premises.

5. The local management device of claim 1, further configured to supply patterns of sensor data from the stored patterns of sensor data to the remote monitoring centre upon receiving a request from the remote monitoring centre.

6. The local management device of any one of the preceding claims, further configured to operate a radio-based system to sense presence and location within the premises based on detecting perturbations of radio signals.

7. A premises security monitoring system installation including a local management device of any one of the preceding claims, the local management device being operatively coupled to a plurality of alarm event sensors.

8. A monitoring centre for remotely monitoring a plurality of premises security monitoring installations, the

monitoring centre being configured to receive, for each security monitoring installation, reports, from a local management device of the security monitoring installation, patterns of sensor data corresponding to movement and behaviour of occupants within the premises;
the monitoring centre being further configured to use a classifier to identify burglaries by processing reported patterns of data received from the local management device, the classifier having been trained to recognise patterns of sensor data that signify burglary events.

9. The monitoring centre of claim 8, wherein the monitoring centre is configured to filter received reports using the classifier, reports recognised as including patterns of sensor data that signify burglary events being supplied to one or more human operators of the monitoring centre for processing.

10. The monitoring centre of claim 8 or claim 9, wherein the monitoring centre is further configured, for any received report that includes patterns of sensor data recognised as signifying a burglary event, to send a request for video data to the local management device from which the report was received.

11. The monitoring centre as claimed in any one of claims 8 to 10, wherein the remote monitoring centre is configured to associate each of the premises with one or more identifiers signifying type, size, situation, location, and/or other characteristics of the respective premises.

12. The monitoring centre of claim 11, wherein the remote monitoring centre is configured to supply one or more of the associated identifiers to the classifier to improve the classification process of the reported patterns of sensor data for the respective premises.

13. The monitoring centre as claimed in any one of claims 8 to 12, wherein the classifier has been trained using supervised learning based on historic patterns of sensor data for events at multiple premises, some of the events being known burglary events, and others being known not to have been burglary events.

14. The monitoring centre as claimed in any one of claims 8 to 13, wherein the monitoring centre is configured to supply the classifier with updated information based on confirmation of the burglary status of received reports initially recognised as containing patters of sensor data that signify burglary events.

15. The monitoring centre as claimed in any one of claims 8 to 14, wherein the received patterns of sensor data include data in respect of a radio-based system configured to sense presence and location based on detecting perturbations of radio signals.

16. The monitoring centre of claim 15, the local management device of claim 6, or the installation of claim 7 as dependent on claim 6, wherein the radio-based sensing arrangement is configured to process communication signals received from one or more radio transmitters operating according to one or more communication standards or protocols, and optionally the one or more radio transmitters that are in a common wireless network with the local management device.

17. The local management device or installation as claimed in claim 16, wherein the local management device includes a radio receiver of the radio-based presence and location sensing system, and optionally the local management device includes a processor and a memory holding software instructions that when run on the processor cause the local management device to process radio signals to derive location and presence data.

18. The local management device or installation as claimed in claim 16 or claim 17, wherein the sensing arrangement to detect human presence uses changes in channel state information or received signal strength in determining presence.

19. The local management device or installation as claimed in any one of claims 16 to 18, wherein the local management device is configured to function as an access point of a radio network whose signals are used by the radio-based presence and location sensing system.

20. The installation of claim 19, wherein the radio network for which the local management device functions as an access point includes at least one further access point.

21. The installation of claim 19 or claim 20, wherein the radio network is a Wi-Fi network, and optionally the one or more radio transmitters include one or more of the following: a Wi-Fi access point, a Wi-Fi extender, a smart plug or smart socket, a smart speaker, a smart bulb, a control panel of the security monitoring system, a Wi-Fi-enabled video camera.

22. The installation or local management device of any one of claims 16 to 21, wherein the local management device is further configured to perform processing of signals as part of the radio-based location sensing arrangement.

23. A local management device or installation as claimed in any one of claims 16 to 22, wherein the local management device is further configured to use data

from the radio-based location sensing arrangement to perform people counting, and optionally to use determine the presence of one or more intruders based on a detected change in the people count when the system is in a disarmed mode.

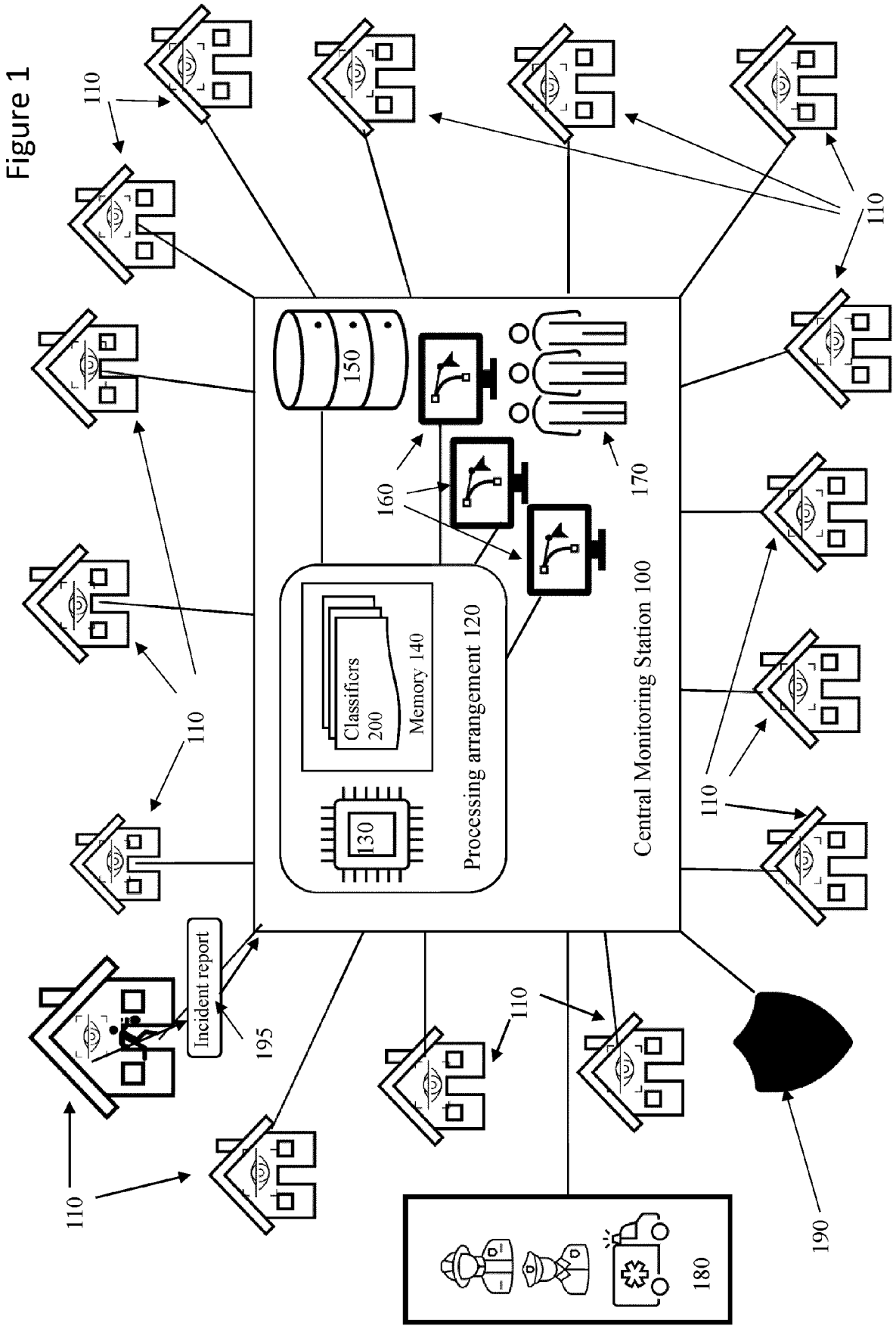
24. A method performed by a local management device of a premises security monitoring system installation, the premises used by occupants, and the security monitoring system having an armed state and a disarmed state, the method comprising in the disarmed state:

receiving sensor data from a plurality of alarm event sensors of the premises;
processing the received data using a classifier trained to discriminate between patterns of sensor data that signify usual behaviour of the occupants and patterns of sensor data that may signify burglary events; and
reporting to a remote monitoring centre any patterns of sensor data recognised as signifying a burglary event.

25. A method performed by a monitoring centre for remotely monitoring a plurality of premises security monitoring installations, the method comprising:

receiving reports from a local management device of one of the premises security monitoring installations of patterns of sensor data corresponding to movement and behaviour of occupants within the premises; and
using a classifier to identify burglaries by processing reported patterns of data received from the local management device, the classifier having been trained to recognise patterns of sensor data that signify burglary events.

Figure 1


110
150
160
170
Classifiers 200
Memory 140
130
Processing arrangement 120
Central Monitoring Station 100
Incident report
195
180
190

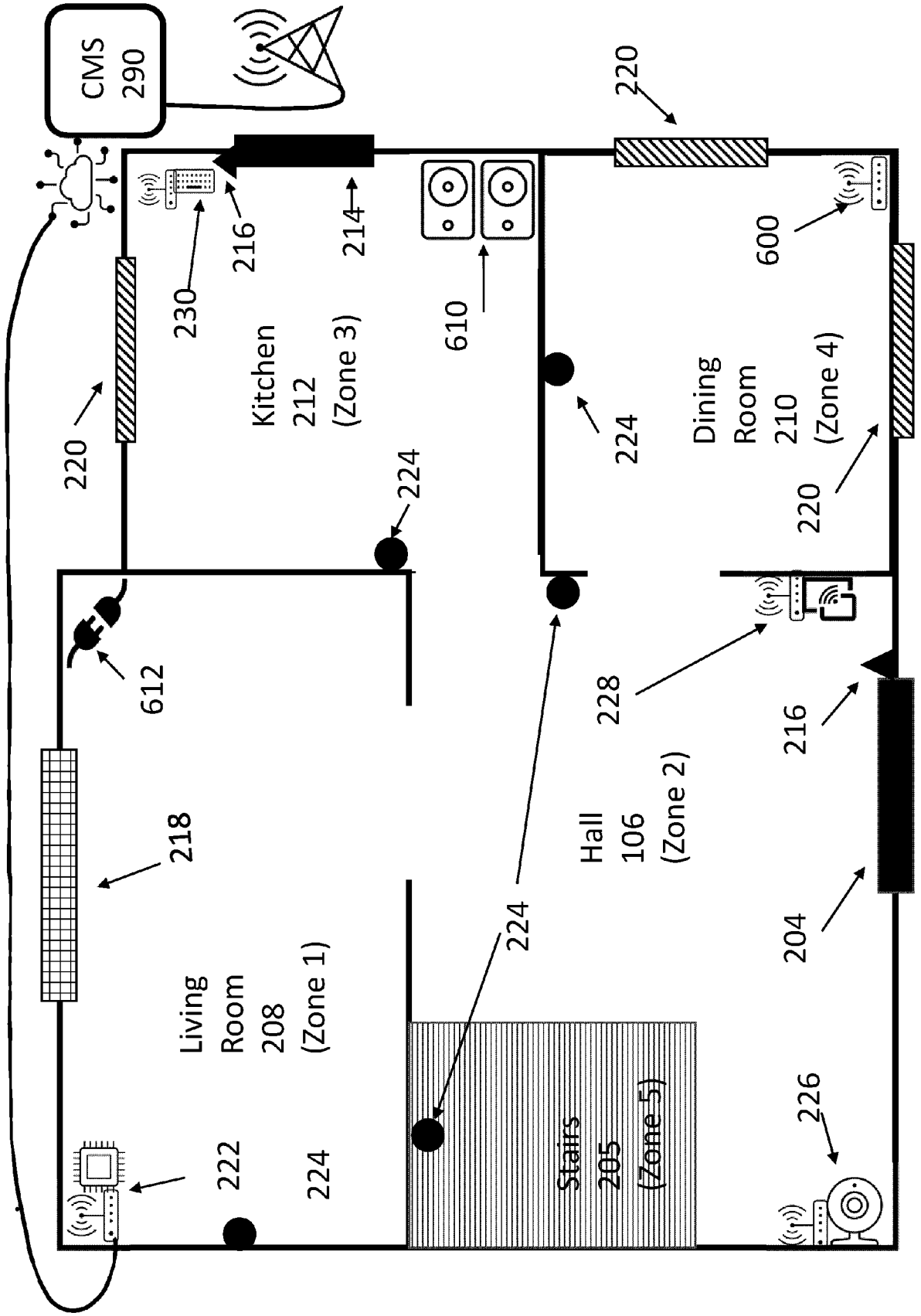

CMS
290
220
600
230
216
214
610
Kitchen
212
(Zone 3)
224
Dining
Room
210
(Zone 4)
220
612
228
216
218
Hall
106
(Zone 2)
224
204
Living
Room
208
(Zone 1)
Stairs
205
(Zone 5)
222
224
226

Figure 2

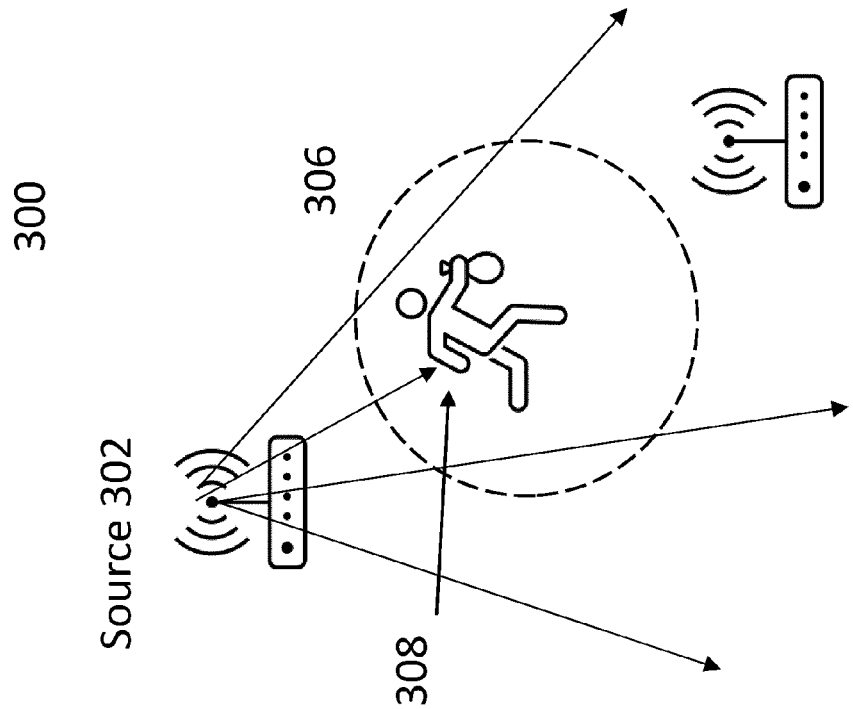


Figure 3B

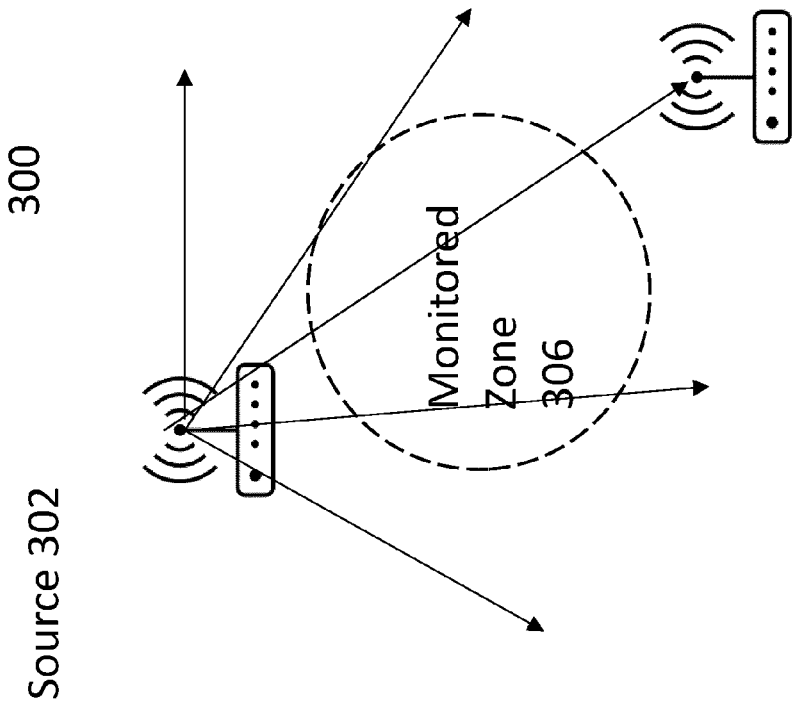


Figure 3A

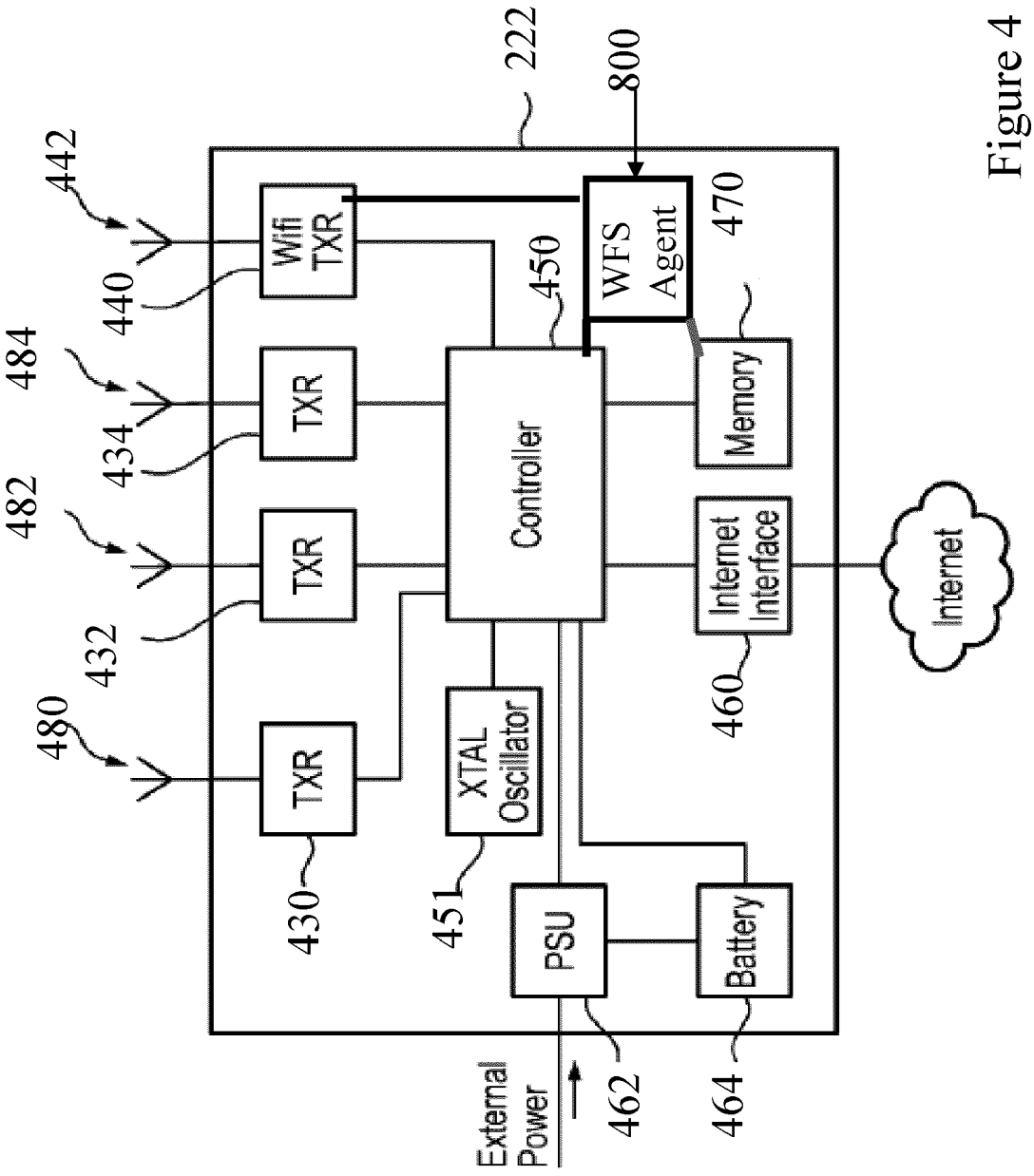

222
800
442
440
484
434
482
432
480
430
Wifi TXR
TXR
TXR
TXR
450
WFS Agent
470
Memory
Controller
Internet Interface
460
Internet
XTAL Oscillator
451
PSU
Battery
External Power
462
464

Figure 4

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 21 21 8184

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 2019/213857 A1 (AERIEL TECH INC) 11 July 2019 (2019-07-11) * paragraph [0034] - paragraph [0038] * * paragraph [0099] - paragraph [0104] * * figures *	1-25	INV. G08B25/00 G08B13/24
X	EP 3 226 220 B1 (GOOGLE LLC [US]) 3 March 2021 (2021-03-03) * paragraph [0018] - paragraph [0029] * * figures *	1-25	
X	US 10 713 928 B1 (GERSTBERGER PETER [US] ET AL) 14 July 2020 (2020-07-14) * the whole document *	1-5, 7-14,24, 25	
X	US 10 755 537 B1 (PALMER KOLTYN CHIARO [US]) 25 August 2020 (2020-08-25) * the whole document *	1-5, 7-14,24, 25	

TECHNICAL FIELDS SEARCHED (IPC)

G08B
G06K

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	10 June 2022	Königer, Axel

CATEGORY OF CITED DOCUMENTS

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

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

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 21 21 8184

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.

10-06-2022

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2019213857 A1	11-07-2019	AU 2017276830 A1	06-12-2018
		CA 3026740 A1	14-12-2017
		CA 3130933 A1	14-12-2017
		EP 3455835 A1	20-03-2019
		US 2019213857 A1	11-07-2019
		US 2021312777 A1	07-10-2021
		WO 2017210770 A1	14-12-2017
EP 3226220 B1	03-03-2021	EP 3226220 A1	04-10-2017
		US 9734697 B1	15-08-2017
US 10713928 B1	14-07-2020	NONE	
US 10755537 B1	25-08-2020	US 10755537 B1	25-08-2020
		US 11341825 B1	24-05-2022

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 10546861 B **[0032]**
- US 10423861 B **[0032]**
- US 10417525 B **[0032]**
- US 20200302187 A1 **[0103]**

Non-patent literature cited in the description

- **Y. LECUN ; L. BOTTOU ; Y.BENGIO ; P. HAFFNER.** Gradient-based learning applied to document recognition. *Proceedings of the IEEE,* 1998, vol. 86 (11), 2278-2324 **[0031]**