(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 June 2015 (04.06.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/079202 A1

(51) International Patent Classification:
H04W 12/12 (2009.01)

(21) International Application Number:
PCT/GB2014/000495

(22) International Filing Date:
28 November 2014 (28.11.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13250116.4 29 November 2013 (29.11.2013) EP

(71) Applicant: **BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY** [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).

(72) Inventor: **MACKENZIE, Richard, Thomas**; PP: C5A, 81 Newgate Street, London EC1A 7AJ (GB).

(74) Agent: **LIDBETTER, Timothy, Guy, Edwin**; BT Legal, Intellectual Property Department, PP: C5A, BT Centre, 81 Newgate Street, London EC1A 7AJ (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: WIRELESS MANAGEMENT

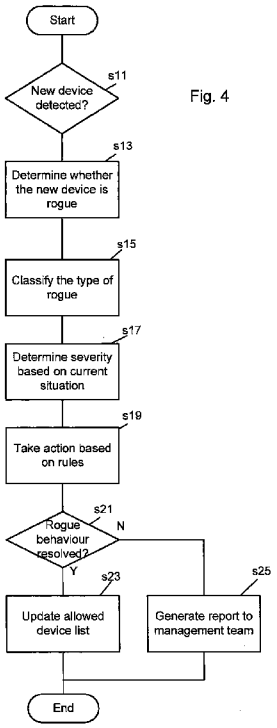

Fig. 4

(57) Abstract: A wireless spectrum management system having a management server and a plurality of sensor nodes detects the presence of non-compliant wireless devices and incorrectly configured wireless devices which may cause interference to other devices in the wireless network environment. The management server receives notifications of devices present on the network from the sensor nodes and uses gathered information about the devices to identify whether the device is rogue, classify the type of interference is may cause and assign a severity based on the current network environment. The management server then attempts to rectify the rogue device or notifies a response team.

WO 2015/079202 A1

Wireless Management

The present invention relates to wireless communication networks and in particular to an apparatus and method for handling interference.

Introduction

In computing networks, wireless communication can provide many advantages in terms of range and ease of deployment compared with traditional wired communication networks.

Typically, wireless networks operate via radio transmissions over an air interface to provide communication between compatible devices. Examples of such wireless protocols are IEEE 802.11 Wi-Fi, Bluetooth, WiMAX, GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telephone System), LTE (Long Term Evolution) and DVB-T (Digital Video Broadcasting - Terrestrial). Each of these protocols operates within certain frequency ranges, for example Wi-Fi typically operates in the 2.4 Ghz and 5 Ghz radio frequency spectrum range.

The number of wireless devices and transmissions has increased greatly in recent times due to the convenience of data communication without wires. As a consequence, the potential for interference between these devices becomes a problem. For a given wireless communication channel, ideally, only one device should transmit at a time to avoid signal corruption at any receivers. Various schemes are known in the art to manage transmissions between the various devices so as to avoid interference as much as possible, for example scheduling, or code division which allows multiple data streams for different devices to be carried at the same time. Unfortunately, such managing schemes are only effective for the same types of networks and devices within networks. External interference cannot be controlled. For example, a microwave oven also operates around the 2.4 Ghz spectrum range and since these types of device do not consider the effect it may have on other devices, when active it will interfere with 2.4Ghz Wi-Fi networks in the same area.

In other cases, devices such as wireless access points are suitable for operation on a wireless network but are misconfigured depending on their location. For example there may be channel restrictions such as use of channel 14 in the 2.4 Ghz in certain countries and or maximum transmission power restrictions.

Clearly, misconfigured or illegitimately operating devices are not desirable in a wireless network environment since they cause interference to legitimate devices and may infringe on commercial agreements.

However, the detection of such "rogue" devices is not trivial. In general, network administrators of a network do not become aware of misconfigured or non-compliant devices causing interference until a fault or complaint regarding deteriorating network performance is logged. Once alerted, typically the complaint must be investigated before any action can be undertaken. This can be a slow process, and in dense usage locations such as an exhibition hall or concert arena, further complicated by the high density of devices which are potential sources of interference.

The present invention aims to address these problems.

Statements of invention

In one aspect, an embodiment of the invention provides a management apparatus for managing wireless devices in a wireless network environment comprising: a network interface for receiving device related characteristic data relating to a device present in the wireless network environment; identifying means for identifying whether said device is a possible source of wireless interference to other devices in the wireless network environment; assessment means for assessing, in the event said device is identified as a possible source of interference, a severity score indicative of the impact said device may cause to the wireless network environment; and resolving means for determining in accordance with said severity score, at least one configuration action for rectifying the source of interference and generating instructions to carry out the at least one configuration action.

In another aspect, an embodiment of the present invention provides a network management system for detecting and correcting wireless interference comprising: an apparatus as set out in any of claims 1 to 4; and a plurality of sensors for detecting devices which may cause interference to other wireless networking devices.

In a further aspect, an embodiment of the present invention provides a method of managing wireless devices in a wireless network environment comprising: receiving device related characteristic data relating to a device present in the wireless network environment; identifying whether said device is a possible source of wireless interference to other devices in the wireless network environment; and in the event said device is identified as a possible source of interference: assessing a severity score indicative of the impact said device may cause to the wireless network environment; and determining in accordance with said severity score, at least one configuration action for rectifying the source of interference and generating instructions to carry out the at least one configuration action.

Figures

Embodiments of the invention will now be described with reference to the accompanying drawings in which:

Figure 1 is an overview of wireless data network being managed by an interference management server in accordance with a first embodiment;

Figure 2 is a schematic showing the functional components of the interference management server illustrated in Figure 1;

Figure 3 is a flowchart showing the operation of reporting nodes connected to the interference management server;

Figure 4 is a flowchart showing the operation of the components within the interference management server when a device is detected by the sensor network; and

Figure 5 is an overview of a geographical area containing a number of wireless data networks and an interference management server in accordance with a second embodiment.

Description

Although the invention is applicable to the detection of many different types of wireless communication network, for ease of explanation, the first embodiment describes a simple exemplary case of a Local Area Network (LAN) of computing devices such as a corporate network where most authorised devices are connected using a wired networking protocol such as Ethernet and only a few wireless access points are present to provide authorised wireless connectivity.

Figure 1 shows a LAN 1 in which the system according to the first embodiment can be deployed. The LAN 1, is comprised of a number of computing devices such as laptops and desktop computers 3 connected via Ethernet to a network backbone 5 so that data can be exchanged between devices 3 across the network. In addition to the Ethernet wired devices 3, the LAN 1 also includes access point devices 7 connected to the network backbone 5 to provide wireless connectivity for some authorised mobile devices 9 to other wired devices 3 and wireless devices 9 on the LAN 1. For the rest of the description, this network having both wired and wireless connectivity will be referred to as a Wireless Local Area Network (WLAN) 1.

In accordance with wireless networking protocols such as the IEEE 802.11 family relating to Wi-Fi, each access point 7 in the WLAN 1 broadcasts data on one of a finite set of available radio channels. To avoid interference, each access point 7 should be on a different channel to its neighbouring access points 7 and ideally the transmissions should be using non-overlapping channels. Under IEEE 802.11n 2.4 Ghz Wi-Fi there are only three non-overlapping channels from a possible thirteen channels namely channels 1, 6 and 11. Whilst in the 5 Ghz Wi-Fi spectrum there are more non-overlapping channels.

In a conventional system, the network administrators for the WLAN 1 will typically specify the wireless channel that each wireless access point 7 should use in view of the number and geographical location of surrounding wireless access points 7. Such managed spectral allocation is designed to minimise the interference between the different access points. For example, in Figure 1, a first wireless access point 7a is using channel 1 while a second wireless access point 7b is using channel 6. In this configuration, and absent any other wireless access points transmitting on overlapping channels, neither access point 7 causes interference to the other access point 7.

Whilst the quality of wireless signal at any given location will typically vary with time due to the number of connected devices and environmental fluctuations such as doors moving etc. Large fluctuations are not common unless a source of interference from another wireless device is present. Interference on the wireless radio spectrum used by the access points 7 will manifest as degradation or failure of the wireless data communications between wireless access points 7 and any connected wireless devices 9.

In conventional systems, the network administrator is only made aware of such interference when users log faults relating to a degradation of service. Then the task of identifying and rectifying the problem is not trivial and can lead to inconsistent resolution.

In the system shown in Figure 1, an interference management server 11 is a part of the WLAN 1 and is therefore connected to, and able to directly connect with, all of the wired devices 3 and wireless access points 7 via the network backbone 5.

The interference management server 11 is aware of the location of each wireless device (in this embodiment the information is provided by the network administrator). The interference management server 11 can therefore decide how to allocate channels to access points 7, perhaps with input from a network administrator. The interference management server 11 then notifies each access point 7 using a conventional remote management protocol such as TR069 of the channel it should be using and therefore each access point 3 is configured so that the network as a whole is more efficient due to a reduction in interference and CSMA/CA collision handling on the air medium.

The interference management server 11 is also responsible for detecting the presence of potential sources of interference on the WLAN 1 and any other device which are acting in a rogue manner. The interference management server 11 furthermore attempts to resolve the situation without any intervention from the network administrator.

Types of rogue/sources of interference

Within such a network there are a number of possible scenarios in which a device or set of devices could be deemed as exhibiting rouge behaviour and therefore require resolution.

- Unauthorised access point connected to the network;
- Misconfigured authorised access point;
- Unauthorised wireless device; and
- Devices which are not part of the network but still cause interference.

Unauthorised access point connected to the network

The authorised access points 7 are access points which have been installed by a network administrator for the purpose of providing wireless devices 9 with data connectivity to the WLAN 1. The interference management server 11 is therefore aware of the devices and their location so that the interference management server 11 can specify which wireless channel and other transmission characteristics the authorised access point 7 should possess.

However, it is recognised that some users of the WLAN 1 may bring their own "unauthorised" access points 13 and connect them to the WLAN 1 via an available Ethernet port to the network backbone 5. Since the operating parameters of the unauthorised access point 13 are not managed by the interference management server 11, it may cause interference to authorised access points 7 due to transmission on an overlapping channel. For example, if the unauthorised access point 13 is transmitting on channel 3 it can potentially cause interference to both authorised access points 7a and 7b. Equally, if the unauthorised access point 13 is transmitting on the same channel as one of the authorised access points 7 it will cause co-channel interference. Furthermore since the authorised wireless devices 9 generally decide to associate with an access point based on signal strength, they may connect to the unauthorised access point 13 in preference to an authorised wireless access point 7 and thereby increase the utilisation of the unauthorised access point 13 on the radio spectrum beyond just responding to probe requests.

Since the unauthorised access point 13 is connected to the WLAN 1, the interference management server 11 can directly communicate with the unauthorised access point 13 in order to resolve the situation once it has been detected. As will be explained later, depending on the situation, this may involve asking it to change channel, or simply blocking it from using the network by a form of MAC address filtering. Any connected devices would see the loss of connectivity to the network and choose an authorised wireless access point 7.

Misconfigured authorised access point

Although the interference management server 11 specifies the radio frequency channel that any particular authorised access point 7 should use, it is possible that the access point 7 will not be configured with the recommended parameters. Aside from not being on the correct channel, the transmission power may also be different. In particular, a misconfigured access point which has a transmission power which is too high will cause interference over a wider area to neighbouring wireless devices 7. A device may also be discovered to be misconfigured even if it is using its intended configuration. For example, if an access point has an agreement to not interfere with other neighbouring areas. If a barrier is removed or the power settings were incorrectly judged during planning the device may be detected in one of the areas that it agreed not to cause interference.

The interference management server 11 is connected to the authorised wireless access points via the network backbone 5 and therefore once the misconfiguration is detected, the interference network manager 11 can communicate with the misconfigured wireless access point 7 to try to change the incorrect parameters.

Unauthorised wireless device

In this embodiment network, the interference management server 11 maintains a whitelist of authorised connected devices 9. Therefore only devices 9 which are allowed to access the WLAN 1 will be allowed to connect to an authorised access point 7. Any other wireless devices 15 are not authorised.

The whitelist is stored in the interference management server 11 and by comparing a new network device against the list, the unauthorised device will not be allowed to enter the network. However, even though unauthorised devices cannot connect to the WLAN 1, they can still be a source of interference due to their repeated transmission of probe or association requests for available access points. This extra traffic can affect the transmissions by authorised senders and receivers.

The interference management server 11 can try to mitigate the interference by contacting the unauthorised device 15 to reduce or stop its probe requests, send a message to the user of the unauthorised device 15 or cause the authorised access points 7 to ignore the unauthorised wireless device 15.

Sources of interference which are not part of the network

In addition to devices located within the WLAN 1, there are many external sources of interference which will affect the wireless performance of the WLAN 1. The interference may be from a network device forming part of a different WLAN which is not connected to WLAN 1, a networking device operating under a different wireless protocol such as Bluetooth, or a non-networking device which nevertheless causes interference in the Wi-Fi frequency range such as a microwave oven.

The options for resolving the interference will depend on the type, duration and level of the interference. For example, most non-networking sources of interference are generally disruptive but of a limited duration and so in one case the interference management server 11 will just note the source of interference based on a profile and check for when it has been resolved.

Sensing new devices

Before any interference can be resolved, it is first necessary to detect the presence of devices which may be potential sources of interference. In this way, it may be possible to block or alter the behaviour of the device before it causes interference. In conventional systems, interference is not inferred until a user has called the network administrators to report a deterioration or loss of service. In many cases interference might not be investigated due to a report in deterioration of service or it may be one of the later options investigated (e.g. after checking backhaul links, routing settings etc.)

In this embodiment, the interference management server 11 receives notifications of new devices capable of interacting with the WLAN 1 from a number of sources which will be collectively referred to as reporting nodes.

- Devices attaching directly to the network backbone 5 – When a new device such as an authorised access point 7, an unauthorised access point 13 or a desktop device connects to the WLAN via an Ethernet port to the network backbone 5 it will request an IP address from a DHCP server (not shown). In this embodiment, the DHCP server is configured to notify the interference management server 11 when it receives a request for an IP address. Alternatively, the DHCP server

is not modified but a listening node on the network is configured to listen to network traffic and detect the issuance of a new IP address before notifying the interference management server 11.

- Devices attaching via an access point - wireless devices wishing to connect to an access point which is itself connected to the network backbone 5 must perform an association and authentication routine before it can connect to the WLAN 1. In this embodiment, the authorised access points 7 are configured to inform the interference management server 11 when a new device attempts to associate with an authorised access point.

- Other devices near the WLAN - whilst the authorised access points can inform the interference management server 11 regarding new devices which attempt to connect to them, other devices may be present which can also cause interference. To detect these devices, a set of network sensors 17 are present to monitor any transmissions in the 2.4Ghz and 5Ghz range emitted by Wi-Fi devices which connect to unauthorised access points, Bluetooth devices, microwave ovens and DECT phones. In this embodiment, the interference management server 11 also includes equivalent function to a network sensor 17 so that it can detect wireless devices in its vicinity.

Format of notification message

Each of the reporting devices such as the DHCP server, wireless access point 7 and sensor network sends a notification message to the interference management server 11 whenever a new device is detected. In order to help the interference management server 11 identify whether the interference is from a rogue device, the notification message contains a number of information fields including:

- An identifier for the reporting node – such as MAC address, IP address;
- The time the possibly rogue device was first detected;
- The time the report was sent;
- The type of device being reported, example classes include: Wi-Fi AP, Wi-Fi client, Bluetooth, LTE cell, LTE handset, unknown interference
- The location of the reporting device
- Location (depends on reporter's capabilities) – grid reference, room number, approximate position relative to the reporting device, not known
- Frequencies: Value in Hz, channel number for a particular protocol, description of a channel hopping pattern
- Signal level (dependent on device being reported) – received power, RSSI, RSRP

- Signal characteristics – heavy/medium/light use, constant/intermittent/pulse. Transmission burst distribution, quiet time distribution

The format of the notification messages will vary in accordance with the type of sub-system which is doing the monitoring.

For example, the DHCP server notification message will include a reporting device identifier, time of new device detection, and time of the report. It does not have access to any wireless attribute information and so these message fields are not included. In contrast, a network sensor will be able to include a lot of wireless attributes of the new and possibly rogue device.

Interference monitoring server

Figure 2 shows the internal components of the interference management server 11 in the first embodiment. The role of the interference management server 11 is to process reports that interference has been detected, classify and determine a severity for the interference and attempt to resolve the interference.

The interference management server 11 has a number of network interfaces 21 in order to communicate with the authorised wireless access points 7, any wired devices connected to the network backbone 5 of the LAN 1, and also to the network sensors 17. As mentioned above, interference management server 11 also has a wireless monitor function so that it can detect devices in its vicinity if required.

The monitoring sub-systems are configured to monitor for the presence of new devices operating in the wireless spectrum range used by authorised access points 7 since unauthorised or misconfigured devices may be potential sources of interference. When a new device is detected, each sub-system notifies the interference management server 11 via the network interface 21 and then returns to listening for new devices.

The sensing sub-systems only need to report the presence of devices attempting to join the network, the determination of whether they are authorised or rogue devices is handled by the interference management server 11. Once a device notification has been received at the network interface 21, a rogue identifier 23 is responsible for determining whether the new device is an authorised or rogue device.

The rogue identifier 23 stores the data in the received notification messages into a rogue device data structure 22 and then compares the data against two data stores; a connected device store 25 and a

whitelist of authorised devices 27. The connected device store 25 contains data relating to which devices have been previously identified by the rogue identifier 23. Since the notification sub-systems are arranged to simply forward notification messages, they will often send duplicate notifications for the same device when a DHCP renewal request is issued or where the device travels out of range of the WLAN and then subsequently re-joins performs re-association to an authorised access point 7. Another reason for notifications is that separate devices send notifications about the same device. For example, a device with a strong signal could be identified by neighbouring access points and many sensor devices.

To avoid carrying out extra processing, the rogue identifier 23 maintains a list of devices it has already encountered and processed so it can quickly determine how to process the device.

For new devices which have not joined the WLAN 1 before, the rogue identifier 23 uses a whitelist of authorised devices 27 in order to see whether the new device is authorised. The whitelist is populated by a user administrator and the presence of a device on the whitelist is used to influence the subsequent processing. The device is then added to the list of connected devices in the connected device store 25.

How to identify a rogue device

The rogue identifier 23 tests the new device against a set of network administrator rules to make a determination of whether a device is a rogue. Example conditions include, detection of an unexpected transmission (based on time, frequency, modulation, power, etc.), or it could be detection of a transmission whose lower layer packet headers identify that it is not a allowed/expected device, e.g. a MAC address.

In this embodiment, for the WLAN, the rogue identifier 23 is configured by the network administrators to determine any device which is not on the whitelist as a rogue. However, devices which are on the whitelist are still sent on for further examination in case they are misconfigured.

Once the device has been logged with the rogue identifier 23, details regarding the new device are updated in the rogue device data structure 22 and a message is passed to a rogue behaviour classifier 29 containing the location of the data structure 22.

- The data fields of the data structure 22 include: The time that the rogue device was first detected

- The most recent report send time (since a device may be detected by multiple reporting nodes)
- Any identifiers such as IP address or MAC address
- Used frequencies: Value in Hz, channel number for a particular protocol, description of a channel hopping pattern
- The type of wireless protocol: Unknown, LTE, Wi-Fi, GSM, Bluetooth
- Any protocol specific details (different categories for different protocols): Modulation(s), regional setting, transmit power (if known)
- The most recent signal level detected by the reporting node
- The location of the reporting node(s)
- Device Location (depends on reporter's capabilities + extra processes, e.g. triangulation, that can be done by the rogue manager)
- Signal characteristics – heavy/medium/light use, constant/intermittent/pulse.
- Transmission burst distribution, quiet time distribution

Classifying a rogue

Once a rogue device has been identified by the rogue identifier 23, the rogue behaviour classifier 29 processes the details entered into the data structure 22 by the rogue identifier 23 to assign a classification to the rogue device based on a determination of the types of interference that could be caused by the rogue device.

The classifier 29 uses information provided by a network administrator. A classification map 31 containing a list of all the possible rogue classifications.

Once a rogue device has been identified, it is classified in accordance with its characteristics and the type of interference it could cause. In this finer form of identification the attributes of the rouge device are used, for example, the protocol in use, power, frequency, modulation, regional settings etc. Importantly, this stage also identifies whether it is possible to communicate with the rogue. Since several sensor sub-systems may detect the same device, the sensor which first detected the rogue device might not be the best device to communicate with it.

Example rogue device classifications for WLAN 1 are:

- Not an access point;
- Authorised access point on wrong operating channel;
- Authorised access point with transmissions exceeding threshold Max EIRP;

- Non-authorised access point;
- Non-authorised access point and having incorrect regional settings;
- Non-authorised access point with transmissions exceeding threshold Max EIRP; and
- Non-authorised access point using a channel that interferes with authorised access point.

Of course, a rogue device may fall within several classifications.

The classifier processor 29 matches the characteristics of an identified rogue device to a classification based on information received from the sensor subsystems and updates the data structure 22.

Severity

The classification process by the rogue classifier 29 results in the rogue device being assigned a classification label based on the type of interference it could cause.

The impact a particular type of the interference will have on a wireless network varies in accordance with the use and context of that network.

The interference management server 11 includes a severity rating processor 33 and severity map 35. The severity map contains data provided by a network administrator relating to how severe each classification is the operation of the particular WLAN at a certain time. While the classifications are absolute, the severity is affected by the type of network, commercial agreements or even the time of day.

For example, if a rogue device is in a classification such as being on the wrong channel where it can potentially cause significant interference with a live broadcast of a premium sporting event, or it could prevent allied communications in a warzone, then it would have a high if not maximum severity mapping. Conversely, if the same classification is assigned for a low data rate and low utilisation wireless network, then the device may be given a low severity rating. Other reasons for severity ratings can simply be an unlicensed user, accessing spectrum in a licensed band. For example, a cellular femto cell could be connected to the internet and run in a location where the operator does not have a license.

The severity processor 33 is responsible for receiving details of the rogue device from the rogue classifier 29, looking up the current severity rating associated with that classification and adding the severity information to the data associated with that rogue device in the rogue device data structure 22.

Remedial action

Having classified and assigned a network specific severity rating to the rogue device, the next step is to determine whether remedial action is required to prevent the risk of interference to the WLAN 1 and if appropriate, to attempt the remedial action.

An action processor 37 is responsible for trying to prevent interference that could be caused by the rogue device. The action processor uses the severity data provided by the severity rating processor and list of permissible remedial actions held in a data store. The list is stored in a remedial actions store 39 and each entry relates to or more possible actions in relation to the possible severity ratings.

The network administrators provide the information stored in the remedial actions store 39. Possible actions will now be described.

In this embodiment, when a device is determined by the rogue classifier to be a device operating in the wrong regional settings (such as on Wi-Fi channel 14), the severity processor determines from the severity map 35 that the network administrators did not regard this as a serious problem and therefore the device is assigned a low severity since the rogue device does not cause any noticeable performance degradation to the authorised access points 7 in the WLAN 1 and the current settings are within the operating parameters of other local regional settings. In this case, the remedial actions store may have a mapping to take no action except merely logging the attributes of the rogue device in the rogue device data structure 22.

In 5 Ghz Wi-Fi installations, access points can operate in the U-NII-1 band for channels 36-48 and also in the U-NII-2 bands for channels 48-64 and 100-136 in Europe. However, the bands have different restrictions which are not found in the 2.4 Ghz Wi-Fi. For example, the U-NII channels 100-136 are in an extended band which is subject to Dynamic Frequency Selection (DFS) controls.

Therefore in this embodiment, the network administrators have set the following severity cases:

- Lowest – The device has the wrong regional settings, but is not actually able to use UNII-2 extended band;
- Low – The device is not operating in the UNII-2 extended band but can switch to an extended band channel;
- Med – The device is operating in the UNII-2 extended band but radar primary user is not active; and
- High – the device is operating in the UNII-2 extended band, and the primary radar user is transmitting in the extended band.

Therefore in the remedial actions store 39, the following actions may be stored to try to pre-emptively resolve the potential interference.

Low severity

1. Try to communicate with the device to request that the regional settings are set to the local region;
2. Communicate with the rogue device to request that U-NII-2 is disabled;
3. Use containment to reduce the transmissions from the rogue device.

Medium severity

1. Communicate with the device to request immediate channel change to a channel outside of the UNII-2 extended band;
2. Communicate with the device to request that its regional settings are set to match the local region;
3. Communicate with the device to request that the UNII-2 extended band is disabled;
4. Use containment to reduce the transmissions from the rogue device.

Similar remedial actions are stored for the high severity action list, however, in this case the communication with the rogue device must be via a wired interface since the remedial actions by the interference management server 11 would themselves violate the DFS restrictions if transmitted using WiFi.

Reporting to network administrator

Regardless of the severity level and rogue characteristics, the remedial actions cannot be actioned if the interference management server 11 cannot communicate with the rogue device. Therefore the fall-back position for the action processor 37 is to compose an alert (with priority that is appropriate for the severity of the rogue interference) message to the system administrators responsible for maintaining the network. The alert message contains details regarding the severity rating, what the rogue device is doing and information relating to where it might be located.

The network administrators can then be notified and a manual search and inspection for the rogue access point can be initiated. Since the alert message is generated and received as soon as the rogue device is detected, even rogue devices which cannot be automatically fixed can be investigated by the network administrators armed with data gathered by the network sensors and the interference management server.

Finally, the interference management server 11 also includes an administrator user interface 41 for allowing the network administrator to input data into the various lists and data stores such as whitelists, classification to severity relationships and severity to remedial action relationships.

Processing of the network sensors

Figure 3 shows the processing of a sensor network node or connected wireless device.

In step s1, the sensor node 17 tunes to one of the monitored channels and listens for new devices. In step s3, a test is performed if a device has been detected operating in the channel. If a device is detected, or several devices are detected, then in step s5 a the sensor node generates a notification message containing information about the device(s) and sends it to the interference management server and processing proceeds to step s7 where the next channel is tested. If device is not detected, then processing also proceeds to check the next channel and the processing steps are repeated for the new channel.

The above processing to scan the vicinity of the sensor node is repeated periodically, for example every 30 seconds. Similarly, every other sensor node in the sensor network independently performs the same scanning method and reports to the interference management server 11.

With this processing, the network sensor nodes can detect the devices within the range of the WLAN 1, even when these devices are not part of the WLAN 1.

Interference Management Server Processing

The operation of the interference management server will now be described with reference to Figure 4.

Figure 4 shows the processing of the management server. In step s11 a check is performed by the network interfaces to see whether an notification message has been received from a reporting node.

Since the reporting nodes only notify the interference management server 11 about the presence of a devices, in step s13 the device identity processor identifies whether the device is a rogue device using existing data in the notification message, connected devices store 25 and the whitelist store 27.

In step s15 the rogue behaviour classifier 29 determines the type of non-compliance behaviour exhibited by the rogue device.

Next in step s17, the severity of the rogue's behaviour is determined by the severity rating processor 33. Whilst the type of misconfiguration is an absolute condition, the severity of the non-compliance is relative to the surrounding network. The correlation between classification and severity is supplied by the network administrator.

Once a severity rating has been applied, in step s19 the action processor 37 tries to resolve the interference caused by the rogue device in a manner determined by administrator provided rules. An instruction is generated and, depending on the type of device which is causing the interference, the instruction is sent to the device requesting it to reconfigure itself in a manner set out by the action processor, or to a proxy device in a case where the interference management server 11 cannot directly communicate with the device.

In step s21 the action processor 37 checks whether the interference or potential interference related to the rogue device has in fact been resolved by looking at later reports from the reporting sensing nodes relating to that same device, i.e. to check if it is no longer present in the case of devices which are not authorised to be on the network, or if the device is present but now operating in a correct manner in the case of misconfigured devices.

If it has, then in step s23 the action processor 37 notifies the device identity processor 23 that the device can be placed in the list of allowed devices and processing ends for that particular notification message. However, if the recommended remedial action was not successful, then in step s25 a report is generated for the network administrator so that the device and potential interference can be rectified manually. The report contains information gathered about the properties of the device causing the interference including its geographical location.

Finally processing ends for that particular instance of interference being detected.

In the first embodiment, an interference management server 11 is deployed in a WLAN 1 with a sensor network in order to detect rogue devices which may go on to cause a form of interference to the WLAN 1. When new devices are detected, the interference management server 11 takes steps to automatically reduce the likelihood of that device causing interference in the wireless domain to authorised devices. This is achieved by identifying rouges, classifying the nature of the rogue, determining a severity of the potential interference based on the current network conditions and taking one or more remedial actions.

As described, the first embodiment provides several advantages over a conventional network management system, namely:

1) speed of treatment – rogue devices can be handled very quickly without the delays associated with human intervention;

2) thorough policing – the non-compliant conditions can be handled with consistency;

3) differentiation – policies can be used to apply different remedies in different scenarios (such as time of day) and locations; and

4) more effective workforce – by removing some tasks via automation, and providing quicker alerts and more information for tasks that do require workforce engagement.

Second embodiment

In the first embodiment, the interference management device is used to detect and attempt to resolve interference that might affect a single network. In this situation the interference management server is directly connected to the network backbone of the WLAN and can therefore directly communicate with authorised devices which may be able to resolve the interference.

In a second embodiment, the interference management server is used to reduce interference for a particular geographical area having a densely situated number of wireless networks. Examples of such environments are a sporting or press event with a large number of Wi-Fi access points. In these situations, any authorised equipment taken into the event is generally registered with the company managing the event, and commercial agreements may be in place to ensure that certain parties have access to spectrum to ensure a particular quality of service. For example exclusive broadcasting/transmission rights to external networks, dedicated spectrum for inter or intra network communications, etc.

Figure 5 shows a geographical area 101 containing a number of Wi-Fi wireless access point networks 103. Two of the wireless networks 103 are generated by two authorised wireless access point 105, while a third wireless network is generated by an unauthorised wireless access point 107. A fourth wireless network 103 is generated by an incorrectly configured wireless access point 109. Other cellular network access points operating other wireless protocols are also present, in Figure 5 a LTE cellular data network transmitter 111 and a small cells transmitter 113 is also shown.

An interference management server 115 is present to detect interference and in particular whether there are rogue devices which are causing interference. To detect devices which may be the source of

such interference, a plurality of network sensors 117 are placed throughout the geographical area 101 and each sensor 117 is linked to the interference management server 115.

The network sensors 117 may include detectors for at least one type of wireless network protocol, such as Wi-Fi, LTE, Bluetooth, small/femto/pico Cells, whitespace or any other wireless signal. As with the first embodiment, the network sensors 117 are configured to continuously monitor for devices and when a device is detected by a sensor, that sensor notifies the interference management server 115.

The operation of the interference management server 115 in the second embodiment is similar to the operation in the first embodiment but the data stored in the various data stores would differ to suit the particular geographical area 101.

The whitelist would contain a list of devices which have been registered with the event management company as being authorised devices along with the entity which owns that equipment. Any devices which are detected but are not present would be regarded as rogue devices. However, since authorised devices can be misconfigured, the interference management server 115 still processes devices on the whitelist.

Rogues can still be classified and assessed for severity as in the first embodiment. In the action processor, the types of action that can be taken are more restricted given that the interference management server will often not have direct access to the devices which may be causing interference.

In this embodiment, commercial agreements have been established which grant the interference management server 115 access to certain interfaces or a set of configuration commands to each of the networks being utilised in the sporting event. For example, each wireless network maintains a proxy server which can reconfigure that particular wireless network in accordance with the resolution commands set out by the interference management server 115. In this way, sources of interference can be resolved automatically as in the first embodiment.

The second embodiment relates to an interference network monitor 115 which resolves network interference without being part of the network 103. It is of particular relevance to events or exhibitions where multiple networks are present and any interference is likely to affect a large number of devices.

Alternatives and modifications

In the embodiments, the interference management server is configured to attempt automatic resolution of the detected interference in as many severity cases as possible.

However, even if no automatic resolution is performed, there are still benefits to the operation of the networks by virtue of detecting any interference as soon as possible. Therefore in a simple case, the output of the action processor is to notify the network administrators whenever a rogue is detected with information relating to the location of the rouge device and details of the rogue behaviour so that the operators of misconfigured devices can take appropriate action. Similarly, for unregistered devices, especially rogue access points, the event managers can be notified and if location data is available they can manually search for the rogue device.

Claims

1. A management apparatus for managing wireless devices in a wireless network environment comprising:

a network interface for receiving device related characteristic data relating to a device present in the wireless network environment;

identifying means for identifying whether said device is a possible source of wireless interference to other devices in the wireless network environment;

assessment means for assessing, in the event said device is identified as a possible source of interference, a severity score indicative of the impact said device may cause to the wireless network environment; and

resolving means for determining in accordance with said severity score, at least one configuration action for rectifying the source of interference and generating instructions to carry out the at least one configuration action.

2. A management apparatus according to claim 1, further comprising a data store storing:

a first set of rules for use by the identifying means for determining whether said device is a possible source of wireless interference to other devices in the wireless network environment;

a second set of rules for use by the assessment means for assessing the severity of the interference to the wireless network environment;

a third set of rules for use by the resolving means for determining at least one configuration action for rectifying the source of interference and attempting the at least one action.

3. A management apparatus according to claim 1 or claim 2, wherein the generated instructions are transmitted to the device identified as being a possible source of interference.

4. A management apparatus according to claim 1 or claim 2, wherein the generated instructions are transmitted to an intermediary apparatus which is able to reconfigure the device identified as being a possible source of interference.

5. A network management system for detecting and correcting wireless interference comprising:

an apparatus as set out in any of claims 1 to 4; and

a plurality of sensors for detecting devices which may cause interference to other wireless networking devices.

6. A network management system according to claim 5, wherein the sensors are configured to detect wireless devices operating in accordance with at least one of the Wi-Fi, cellular data communication, Bluetooth protocols and other wireless devices transmitting in the same radio frequency spectrum used by said protocols.

7. A method of managing wireless devices in a wireless network environment comprising:

receiving device related characteristic data relating to a device present in the wireless network environment;

identifying whether said device is a possible source of wireless interference to other devices in the wireless network environment; and

in the event said device is identified as a possible source of interference:

assessing a severity score indicative of the impact said device may cause to the wireless network environment; and

determining in accordance with said severity score, at least one configuration action for rectifying the source of interference and generating instructions to carry out the at least one configuration action.

8. A method according to claim 7, further comprising a data store storing:

using a first set of rules in the identifying step for determining whether said device is a possible source of wireless interference to other devices in the wireless network environment;

using a second set rules in the severity assessment step for assessing the severity of the interference to the wireless network environment;

using a third set of rules in the determining step to determine at least one configuration action for rectifying the source of interference and attempting the at least one action.

9. A method according to claim 7 or claim 8, further comprising transmitting the generated instructions to the device identified as being a possible source of interference.

10. A method according to claim 7 or claim 8, further comprising transmitting the generated instructions to an intermediary apparatus which is able to reconfigure the device identified as being a possible source of interference.

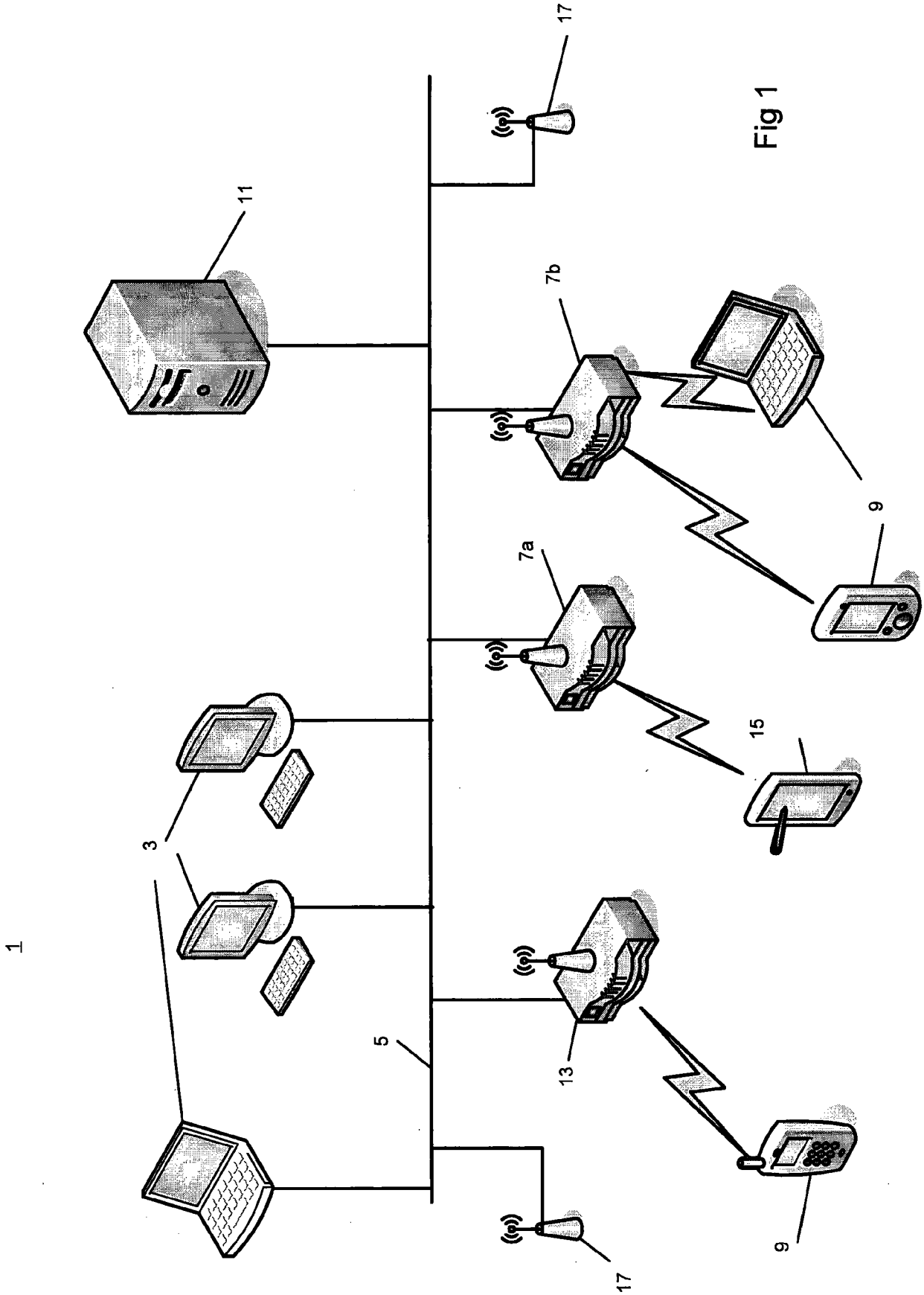

Fig 1

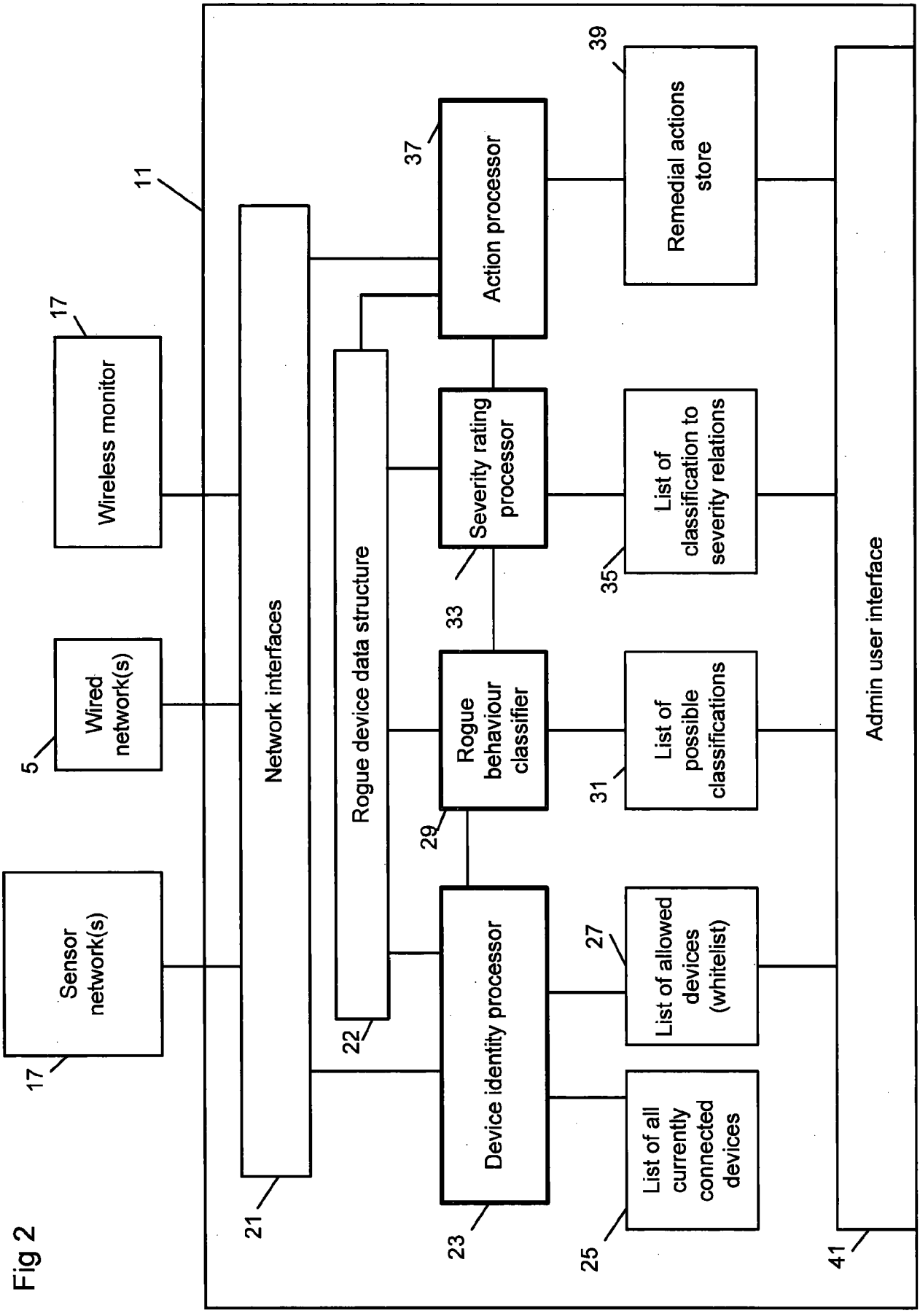
11
Network interfaces
21
Wireless monitor
17
Wired network(s)
5
Sensor network(s)
17
Rogue device data structure
22
Action processor
37
Severity rating processor
33
Rogue behaviour classifier
29
Device identity processor
23
Remedial actions store
39
List of classification to severity relations
35
List of possible classifications
31
List of allowed devices (whitelist)
27
List of all currently connected devices
25
Admin user interface
41

Fig 2

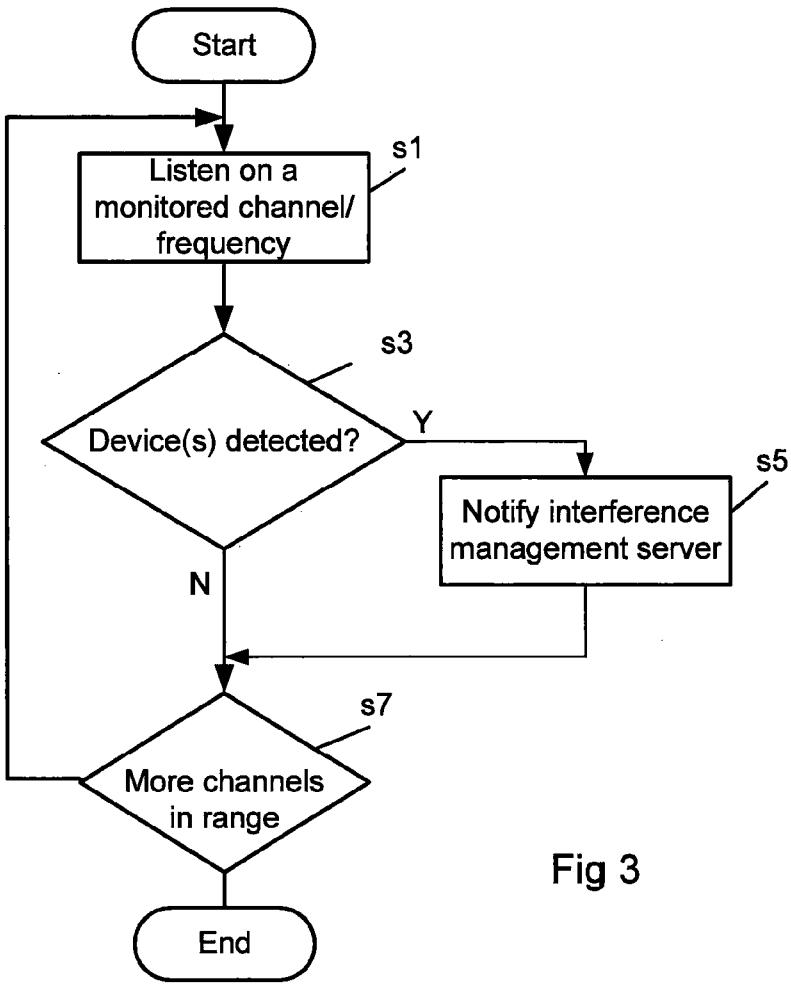
Start
Listen on a monitored channel/ frequency
s1
Device(s) detected?
s3
Y
N
Notify interference management server
s5
More channels in range
s7
End

Fig 3

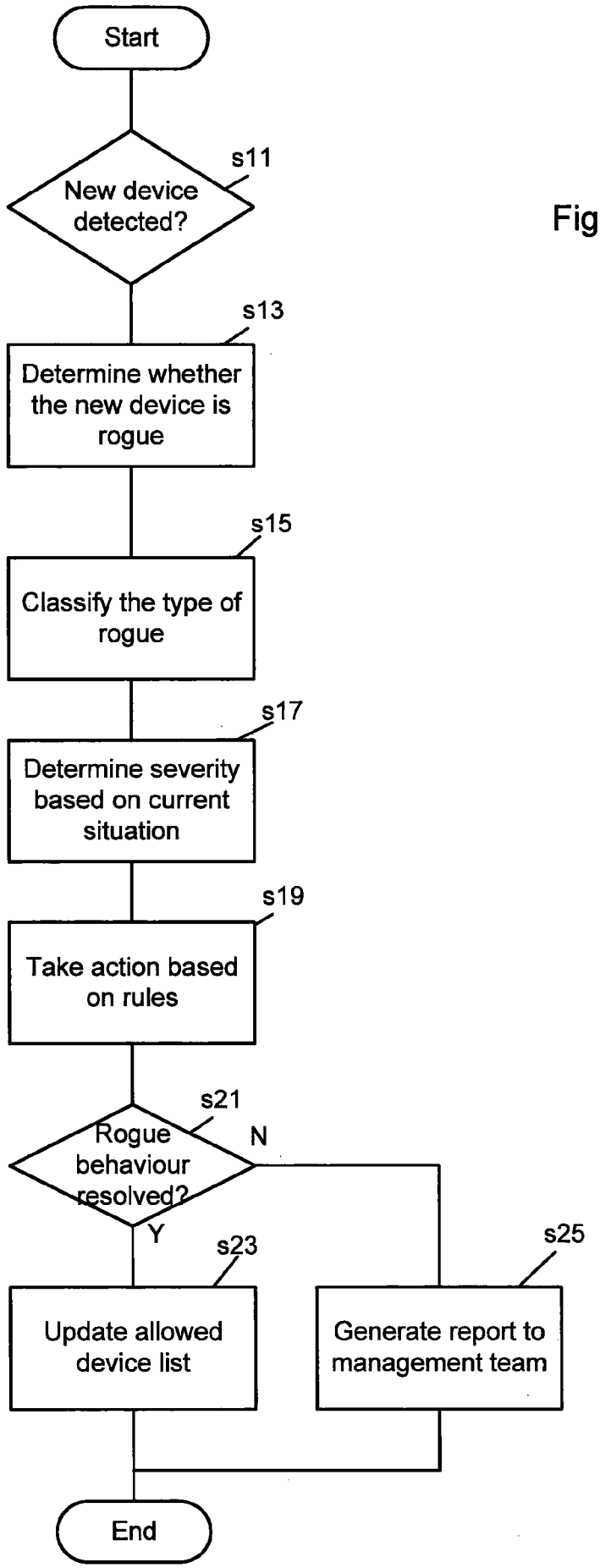
Start
s11
New device detected?
s13
Determine whether the new device is rogue
s15
Classify the type of rogue
s17
Determine severity based on current situation
s19
Take action based on rules
s21
Rogue behaviour resolved?
N
Y
s23
Update allowed device list
s25
Generate report to management team
End

Fig. 4

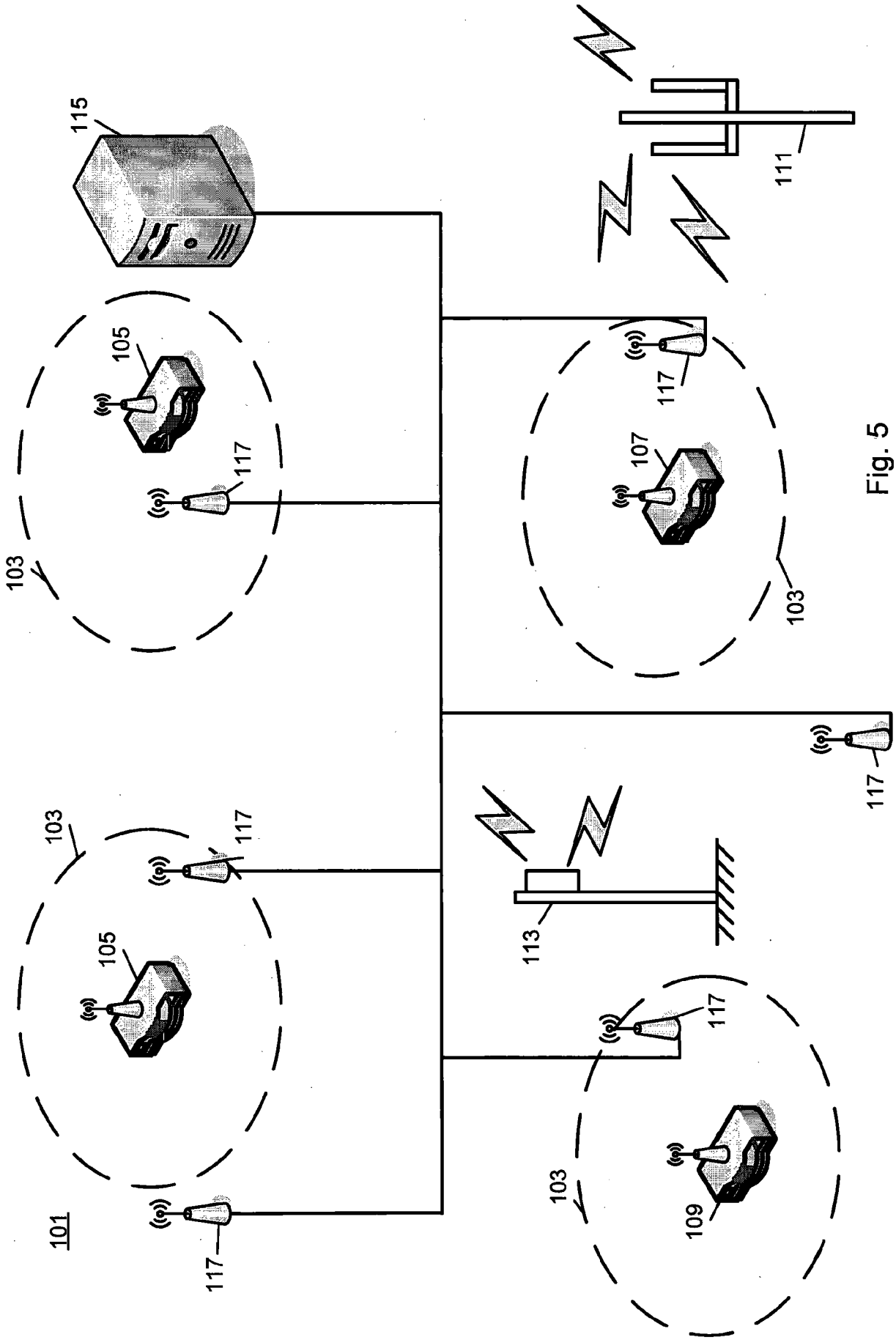
115
111
105
117
103
107
117
103
117
103
105
117
101
117
113
117
103
109

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2014/000495

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/12
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/137915 A1 (DIENER NEIL R [US] ET AL) 15 July 2004 (2004-07-15) paragraphs [0063], [0064], [0065], [0066], [0086], [0087], [0091], [0100], [0147], [0161], [0162], [0275], [0277]; figures 1,3,5,7,8	1-10
X	US 2013/003591 A1 (NOVAK ROBERT [CA] ET AL) 3 January 2013 (2013-01-03) paragraphs [0036], [0041], [0043], [0056], [0057], [0061], [0065], [0066], [0076], [0082], [0085], [0092]; figures 5A,5B, 6A, 6B, 8, 9, 10, 11	1-10

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 January 2015	29/01/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Stefan, Andrei

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2014/000495

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/315174 A1 (SAVOOR RAJ [US] ET AL) 28 November 2013 (2013-11-28) paragraphs [0022], [0024], [0030] - [0033]	1,2,5-8
A	US 2006/019679 A1 (RAPPAPORT THEODORE S [US] ET AL) 26 January 2006 (2006-01-26) paragraphs [0203], [0204], [0231], [0232]	1-10
A	US 2009/182862 A1 (THOMSON ALLAN [US] ET AL) 16 July 2009 (2009-07-16) paragraphs [0013], [0023], [0024]; figures 1, 2, 4	1-10

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2014/000495

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004137915 A1	15-07-2004	NONE	
US 2013003591 A1	03-01-2013	CA 2808472 A1	29-03-2012
		CN 103119978 A	22-05-2013
		CN 103120003 A	22-05-2013
		CN 103155625 A	12-06-2013
		EP 2620009 A1	31-07-2013
		EP 2620010 A1	31-07-2013
		EP 2620028 A1	31-07-2013
		TW 201218829 A	01-05-2012
		TW 201218830 A	01-05-2012
		TW 201220907 A	16-05-2012
		US 2013003591 A1	03-01-2013
		US 2013005240 A1	03-01-2013
		US 2013064197 A1	14-03-2013
		WO 2012037637 A1	29-03-2012
		WO 2012037669 A1	29-03-2012
		WO 2012037670 A1	29-03-2012
US 2013315174 A1	28-11-2013	CA 2647132 A1	22-11-2007
		EP 2018776 A2	28-01-2009
		US 2007263587 A1	15-11-2007
		US 2012087268 A1	12-04-2012
		US 2013315174 A1	28-11-2013
		WO 2007133902 A2	22-11-2007
US 2006019679 A1	26-01-2006	DE 112005001761 T5	24-05-2007
		KR 20070089119 A	30-08-2007
		US 2006019679 A1	26-01-2006
		WO 2006012554 A2	02-02-2006
US 2009182862 A1	16-07-2009	NONE	