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

(11) EP 3 540 707 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
18.09.2019 Bulletin 2019/38

(51) Int Cl.:
G08B 29/04 *(2006.01)* ***H04K 3/00*** *(2006.01)*

(21) Application number: **18161928.9**

(22) Date of filing: **15.03.2018**

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

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

(72) Inventor: **Skarp, Filip**
24741 Södra Sandby (SE)

(74) Representative: **Hansson Thyresson AB**
PO Box 73
201 20 Malmö (SE)

(54) A METHOD AND A DEVICE OF DETECTING RADIO DISTURBANCES IN A RADIO COMMUNICATION SYSTEM

(57) A method and a detector for detecting radio disturbances in a radio communication system comprising a gateway device and a peripheral device, each arranged to send radio signals to and to receive radio signals from the other. The method comprises measuring the power level (Pm) of separate information segments of the radio signals received by one device from the other device, determining a statistical value (Pd) of measured power level values, comparing a selected measured power level with the statistical value, and producing an alert signal, indicating a radio disturbance, if the difference between the selected measured power level and the statistical value exceeds a threshold. The detector comprises a power level detector (62), a processing unit (64) operatively connected to the power level detector (62), and a memory unit (66) storing a plurality of statistical values.

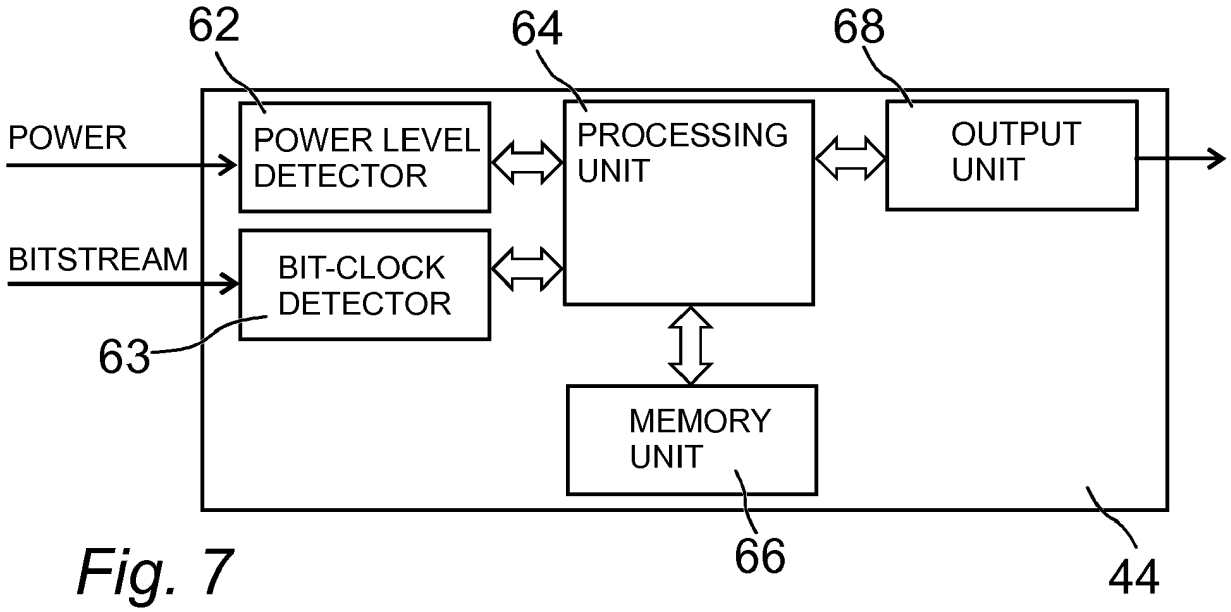

Fig. 7

EP 3 540 707 A1

Description

TECHNICAL FIELD

[0001] The invention relates to a method and a device of detecting radio disturbances in a radio communication system.

PRIOR ART

[0002] A prior art alarm system for handling jamming situations is disclosed in EP2541518. A first alarm installation is arranged to supervise a second alarm installation and to monitor radio signals exchanged in said second alarm installation. Absence of monitored radio signals will result in the generation of a jamming alarm signal. It should be noted that if communication between a peripheral device and a gateway in either alarm installation is interrupted during a longer time period, such as several minutes, a supervision alarm can be generated in that alarm installation.

SUMMARY OF THE INVENTION

[0003] In accordance with a first aspect there is provided a method of detecting radio disturbances in a radio communication system comprising a gateway device and a peripheral device, each arranged to send radio signals to and to receive radio signals from the other. The method comprises

i. measuring the power level (Pm) of separate information segments of the radio signals received by one device from the other device,
ii. determining a statistical value (Pd) of measured power level values,
iii. comparing a selected measured power level with the statistical value, and
iv. producing an alert signal, indicating a radio disturbance, if the difference between the selected measured power level and the statistical value exceeds a threshold.

[0004] As a result, more sophisticated jamming methods can be detected, and a jamming alarm can be set, should jamming attempts be made. A jamming alarm can comprise generation of an alarm signal in premises where the radio communication system is installed and/or forwarding an alarm signal to a remote central monitoring station where further steps for managing the situation can be taken. The method will provide a higher security in detecting sophisticated targeted jamming attempts in radio communication systems in general and on alarm systems specifically, even where a jamming signal disturbs or destroys specific information segments exchanged in radio communication.

[0005] The disclosed method can be used in a home wireless communications system comprising a plurality of wireless nodes including a first gateway at least one wireless peripheral device and, in some installations, at least one second gateway. The home wireless communications system forms an installation that can include a conventional home security system that comprises at least one wireless alarm detector and at least one gateway. If any of the devices or nodes fail - some action is taken, such as notifying the home owner or triggering a tamper alarm. The tamper alarm can comprise generation of an alarm signal in premises where the radio communication system is installed and/or forwarding an alarm signal to a remote central monitoring station where further steps for managing the situation can be taken.

[0006] A home wireless communications system in general can be any type of wireless system comprising a plurality of peripheral wireless nodes, such as an intruder alarm, and a central unit. Specifically, it can be a security system having a plurality of wireless detectors, sensitive to the presence or passage of persons and objects, communicating with a central unit such as a gateway using wireless communication.

[0007] Intentional radio disturbance measures or interference can be caused by a radio jammer that is a device that deliberately blocks, jams or interferes with authorized wireless communications. In some cases, jammers work by the transmission of radio signals that disrupt communications by decreasing the signal-to-noise ratio. The concept can be used in wireless data networks to disrupt information flow. Jamming is usually distinguished from interference that can occur due to device malfunctions or other accidental circumstances. Some kinds of unintentional 'jamming' exist. One form occurs when an operator transmits on a busy frequency without first checking whether it is in use, or without being able to receive signals from stations using the frequency. Another form of unintentional jamming occurs when equipment accidentally radiates a signal of a frequency that will disturb communication using that frequency.

[0008] One application of home wireless communications systems is alarm systems. Security and alarm systems used today normally comprise a control panel and a gateway that is connected to a central station, either by a telephone line or by a wireless telecommunications system such as GSM or other radio frequency systems. The connection can also be through the internet. The control panel can be provided with an input device or be activated and controlled by a control device such as a keypad which can be a wireless remote device.

[0009] In digital communication systems using packets, sophisticated jamming methods include packet sniping that will destroy communication between gateways and peripheral devices without raising the background noise continuously. A packet sniping jammer normally would incorporate an intelligent receiver chain and listen for packets or power in the air during digital wireless communication. In this context, a packet comprises a dataset of preamble, sync-word, payload and cyclic redundancy check (CRC). Once the start of a packet is detected the

jammer may emit a short surge of power lasting only a fraction of the packet length (the actual length would be based on the protocol being jammed, if for instance error correctional coding is used more bits would have to be jammed to ensure a destroyed packet). This would destroy one or a plurality of bits somewhere in the packet causing the packet to, for instance be ignored due to destroyed sync word, be filled with complete nonsense or fail cyclic redundancy check (CRC).

[0010] In various embodiments, the power of the incoming signal is continuously measured and changes in that power are detected in a detector. By measuring the energy per bit of the received bit stream it is possible to detect step changes, both positive and negative, that would arise from packet sniping. The continuous measurement of power could be done at any suitable position in the receiver chain. The measurement is done with a sufficiently high bandwidth (the power measurement speed should be in the order of the bitrate of the received signal). Depending on the receiver architecture the power measurements could be done by measuring the power of the incoming signal in relevant radio receiver parts, such as the Automated Gain Control (AGC), the Intermediate Frequency Amplifier (IF AMP) or the Analog to digital converter (ADC). The power measurement can also be made by measuring the level of the digital IQ data. In practice, different measurement methods are used depending on receiver architecture.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Non-limiting embodiments of the invention will now be described with reference to the figures in which:

Fig. 1 is a schematic view of an installation of a home wireless system,

Fig. 2 is a schematic diagram showing power of a received radio signal in a simple jamming situation in the time domain,

Fig. 3 is a schematic diagram showing power of a received radio signal in the time domain where a jamming signal is generated by a sniping jammer in a more sophisticated way,

Fig. 4 schematically shows signal measurements of the signal shown in Fig. 3,

Fig. 5 is a schematic diagram showing an analogue type receiver comprising one embodiment of a detector in accordance with the invention,

Fig. 6 is a schematic diagram showing a digital type receiver comprising one embodiment of a detector in accordance with the invention,

Fig. 7 is a schematic diagram showing one embodiment of a detector in accordance with the invention,

Fig. 8 is a schematic diagram showing a typical installation including two communication units comprising a detector in accordance with the invention,

Fig. 9 is a table showing part of a correctly received bit stream package and corresponding energy levels, and

Fig. 10 is a table showing part of a received jammed bit stream package and corresponding energy levels.

DETAILED DESCRIPTION

[0012] Fig. 1 shows a home wireless system installed in a building 10. The home wireless system is an alarm system installation and comprises a plurality of wireless peripheral nodes including wireless peripheral devices, a first gateway 12 and a second gateway 12'. The second gateway 12' is mains powered and normally is not provided with battery backup. One wireless peripheral node is a first infrared detector 14 mounted in the corner of a room close to the ceiling. The first infrared detector 14 has a sensing area that covers the first gateway 12. A first perimeter alarm detector 16 is mounted at a window 17 in the same room. The infrared detector operates in a conventional manner to detect presence and movements of objects emitting infrared radiation. The perimeter alarm detector also operates in a conventional manner to detect when a door or a window is opened. In various embodiments the perimeter alarm detector comprises a magnetic sensor that will detect when a magnet attached to the door or window is moved.

[0013] Second gateway 12' is arranged in a second room separated from the room where the first gateway 12 is arranged. A second infrared detector 14' is mounted in the same room as the second gateway 12' to cover it within its operative area and a second perimeter alarm detector 16' is mounted at a second window 17' in the same room. A keypad 19 is mounted close to a front door 20 of the building 10. The keypad 19 is used by an operator of the alarm system to arm and to disarm the alarm system. The keypad 19 also is a wireless peripheral node. The front door 20 is covered by a third perimeter alarm detector 21. Another type of wireless peripheral device is a smoke detector 23 mounted in the ceiling of the building. In various embodiments a plurality of smoke detectors 23 are arranged throughout the building 10 to ensure that fire can be detected at an early stage.

[0014] Depending on different circumstances the first gateway 12 and the second gateway 12' are connected to a remote central monitoring station 22 either through a wired connection 24 or through a wireless connection such as GSM or a similar digital cellular network 34. The connection to the remote central monitoring station 22 can also be through the internet 26. In the embodiment shown in Fig. 1, internet connection is provided through a wireless router 32 that is connected to internet by fibre, cable or Digital Subscriber Line, such as ADSL. In the embodiment shown in Fig. 1 second gateway 12' is connected by wire 33 to wireless router 32. The wired connection 24 can be part of a public switched telephone network 25. In various embodiments the remote central

monitoring station 22 comprises an interface module 27, a database 28 and a web server 29. The database 28 stores installation and application data relating to the installation including all wireless network nodes and alarm settings.

[0015] The first gateway 12 is capable of communicating with the second gateway 12' because of the more powerful radio transmitting units even though some peripheral nodes cannot. By placing gateways strategically within a building, it is possible to guarantee that every peripheral node has an adequate RF link with at least one gateway. As long as each gateway can communicate directly with at least one other gateway and directly or indirectly with all of the other gateways, the installation will function properly. To achieve full redundancy the installation should include enough gateways for every peripheral node to be able to communicate with at least two gateways.

[0016] An installation such as the alarm system shown in Fig. 1 holds a large amount of dynamic state information, such as arm state, alarm status, peripheral battery status, etc. in a total system state information dataset. Similar information is stored also in other types of home wireless systems. Each gateway or controller continuously receives inputs from different authenticated sources such as peripheral nodes, a remote central monitoring station (RCMS), adjacent systems, etc. that affects a distributed state of the application or system.

[0017] In various embodiments, a second gateway can utilize the RF communication link of another gateway for tunneling messages to an RCMS. For example, if the second gateway up-link to RCMS is very slow or unreachable, or has a higher cost, another gateway up-link can be utilized.

[0018] The schematic diagram in Fig. 2 shows power levels of received radio signals in a jamming situation in the time domain where a jamming signal 40 is transmitted as noise. Message signals 42 received at a power level PA are concealed or at least not fully readable when a noise level PN extends above message signal level PA. When a jamming situation as shown in Fig. 2 is detected in prior art systems a jamming alarm can be generated.

[0019] The schematic diagram in Fig. 3 shows a jamming situation in the time domain where a jamming signal is generated by a sniping jammer in a more sophisticated way. A sniping jammer normally comprises a more intelligent receiver chain and will listen for message signals 42 or power in the air. Once a message signal 42 such as a packet is detected the jammer emits a short surge 43 of power at power level PN lasting at least and normally only a fraction of the packet length. The actual length normally would be based on the protocol being jammed. If error correctional coding is used more bits would have to be jammed to ensure a destroyed packet. This would destroy one or a plurality of bits somewhere in the packet causing the packet to, for instance be ignored due to destroyed the sync word being destroyed, be filled with complete nonsense or fail cyclic redundancy check (CRC). However, these effects are not automatically detected as a jamming situation.

[0020] The diagram in Fig. 4 illustrates a situation starting with receiving a normal radio signal during four consecutive time periods, each time period Tn including one information segment. In the signal format used in Fig. 4 one information segment extends over a time period of Tb. The power level value of each time period is referred to as Pm. There is normally a variation of the received power values Pm over time. A statistical value Pd of measured power levels Pm is continuously determined based on power levels of previously received information segments. In various embodiments, Pm is measured over a limited time period Tm, such as 1 s.

[0021] A basic statistical value is a mean value as indicated with a dashed line in Fig. 4 indicates that the received power level may vary up and down over time. The mean value is continuously determined based on power levels of previously received information segments or determined continuously for each information segment. In various embodiments, the statistical value is the standard deviation of a set of or all power level values Pm. The set of power level values can be based on a plurality of values, values measured over a time period, or all or a subset of values of a specific information segment.

[0022] At time tj a jamming signal 44 is broadcast and received during a time period where an information segment also is broadcast. The jamming signal 44 has a power level Pj which is different from the power level Pm of the information segment and also different from the mean value Pd. Power level Pj is greater than the mean power level. The difference is Pe. If the power level Pj deviates more from the mean value or the statistical value than a reference or threshold value power level Pj is determined to indicate that intentional or unintentional radio disturbance measures have occurred. As a result, an alarm signal is generated. The threshold value can be two to five times the standard deviation or preferably around three times the standard deviation.

[0023] A detector 44 for detecting intentional or unintentional radio disturbance measures is connected to an appropriate location in a receiver chain where the measurement can be done with high enough bandwidth (the power measurement speed should be in the order of the bitrate of the received signal but any bandwidth allowing for more than one measurement per information segment will be usable). The exact location depends on the receiver architecture. The detector will produce an alert signal when intentional or unintentional radio disturbance measures are detected.

[0024] In an analogue receiver as shown in Fig. 5, an antenna 46 is connected to a Low Noise Amplifier (LNA) 48 in a conventional manner. An output of LNA 48 is connected to a mixer 50 mixing the amplified signal with an adjustable frequency signal from an oscillator 52. The mixer is connected also to an Intermediate Frequency stage with an amplifier (IF AMP) 54, an output of which

is connected to a filter 56 in a conventional way.

[0025] In the embodiment shown in Fig. 5, IF AMP 54 comprises an Automatic Gain Control (AGC) 58. In various embodiments, AGC 58 generates a signal that is indicative of the power of the received signal. The generated signal is sent to detector 44 through an output of AGC 58 that is connected to detector 44. An output of filter 56 is connected to an analog-to-digital converter (ADC) 60 providing a bitstream of digital data and a power level output. The power level output is connected to detector 44. A signal at the power level output is indicative of the power of the received signal and thus can be used for detecting intentional or unintentional radio disturbance measures.

[0026] In a digital receiver, as shown in Fig. 6, antenna 46 is connected to LNA 48 in a conventional manner. The signal amplified in LNA 48 is processed in ADC providing a bitstream of digital data and a power level output. The power level output is connected to detector 44. A signal at the power level output is indicative of the power of the received signal and thus can be used for detecting intentional or unintentional radio disturbance measures.

[0027] The basic components of an embodiment of a detector 44 in accordance with the invention are shown in Fig. 7. Detector 44 could be physical device or be software implemented. A power level detector 62 is connected to an appropriate position in a radio receiver to continuously detect a power level signal indicative of the power of information segments in a radio received signal. A bit-clock detector 63 is connected to an appropriate position in a radio receiver to continuously detect a bit-clock to provide basis for synchronization. Values of power levels are processed by a processing unit 64 and stored in a memory unit 66. In various embodiments, the processing of power levels comprises calculating at least one statistical value. Normally, a mean value of power level values is continuously calculated.

[0028] In various embodiments, power level detector 62 is connected to an appropriate position in a radio receiver to continuously detect a power level signal indicative of the power of separate information segments in a radio received signal. Detector 44 can be used also to measure continuously power of a received package of data and to detect if any steps in power should occur. As soon as the start of a package is detected an evaluation of power starts. Regardless of bit synchronization an alarm will be generated, should there be a positive or negative power step.

[0029] The processing further comprises repeatedly comparing a present value of the power level of at least one information segment of a received signal with said statistical value. When a present power level value, or a set of recently received power level values, differs from the statistical value by more than a threshold value intentional or unintentional radio disturbance measures is considered to be present. When the processing results in detecting intentional or unintentional radio disturbance measures processing unit 64 instructs an output unit 68 to produce an alert signal and to forward the alert signal to a central unit, as described in more detail below.

[0030] A basic installation of a radio system is shown in Fig. 8. This embodiment relates to a home alarm system comprising first gateway 12, second gateway 12' and at least one wireless peripheral device, such as an infrared detector 14. First gateway 12, second gateway 12' and infrared detector 14 all communicate using radio communication. At least one gateway is repeatedly communicating with remote central monitoring station 22 as disclosed above. A sniping jammer device 70 has been moved to a position where radio signals in the installation can be received and radio disturbance measures can be taken.

[0031] First and second gateways 12, 12' comprise first communication units 72 and second communication units 74. First communication units 72 is used for communicating with remote central monitoring station 22 either through a wired connection 24 or through a wireless connection such as GSM or a similar digital cellular network. The connection to the remote central monitoring station 22 can also be through a wired connection, such as a public switched telephone network or the internet.

[0032] Second communication units 74 is mainly used for communication within the installation between gateways and between gateways and peripheral nodes. Each gateway is controlled by a central unit 76 and comprise a power unit 78, normally a battery. At least one gateway is provided with a detector 44 continuously monitoring radio communication received in the gateway. When detector 44 detects intentional or unintentional radio disturbance measures in the radio communication system an alert signal is transferred to central unit 76. An alarm signal then can be generated in the gateway and forwarded to the remote central monitoring station 22 in an appropriate way.

[0033] By combining the power data with the continuous bit stream, it is possible to detect intentional or unintentional radio disturbance measures. The table in Fig. 9 describes a part of a correctly received package with the bits as "1" and "0" in the top row and the energy level as "A" to "Z" in the second row. In the table in Fig. 10 a packet sniping activation is present. Higher energy levels during packet jamming are indicated with a Vresulting in a different and disturbed bit stream.

[0034] A step in power would be easily detected and by pairing the power step with the bit pattern before and after the power step it can be determined that there was a package en route to the receiver that was sniped. The sniping detection could also be solely based on short changes in power if the received bit stream ignoring the packet recognition factor although this would most likely cause some false alarms since neighboring systems and other RF protocols could be mistaken for snipers.

[0035] If the method is run on two independent receive paths (for instance in systems with Rx diversity or receiver antenna switching) it would also be possible to detect snipers trying to mimic the power level of the received

signals in order to mask the sniper. This kind of jammer would have to be very sophisticated and know the location of the receiver, the transmitter and its relation to both. It would also have to have detailed knowledge of the receiver RSSI in relation to the transmitter. The signal from the sniper would not be received with the same intensity on both receivers and even if the sniper was perfectly power matched to one the receivers it would be out of phase and power with the other.

[0036] In various embodiments, calculating the statistical value comprises calculation of a standard deviation of power level values of separate information segments. By using the standard deviation situations where the power levels normally vary can still be handled without producing too high an amount of faulty alert and alarm signals. If a present power level value deviates more than three times the standard deviation it is very likely that intentional or unintentional radio disturbance measures have been taken. It is possible to use also a threshold of twice the standard deviation or equal to the standard deviation to produce the alert and alarm signal.

[0037] While certain illustrative embodiments of the invention have been described in particularity, it will be understood that various modifications will be readily apparent to those skilled in the art without departing from the scope and spirit of the invention. Accordingly, it is not intended that the scope of the claims appended hereto be limited to the description set forth herein but rather that the claims be construed as encompassing all equivalents of the present invention which are apparent to those skilled in the art to which the invention pertains.

Claims

1. A method of detecting radio disturbances in a radio communication system comprising a gateway device and a peripheral device, each arranged to send radio signals to and to receive radio signals from the other, the method comprising the steps:

    i. measuring the power level (Pm) of separate information segments of the radio signals received by one device from the other device,
    ii. determining a statistical value (Pd) of measured power level values,
    iii. comparing a selected measured power level with the statistical value, and
    iv. producing an alert signal, indicating a radio disturbance, if the difference between the selected measured power level and the statistical value exceeds a threshold.

2. The method of claim 1, wherein the selected measured power level is the power level of at least one information segment of the received radio signals.

3. The method as claimed in claim 1 or claim 2, wherein said radio signal transmitters and said radio receivers are communicating with information divided into a plurality of information segments and each of said information segments is communicated for a time (Tb) where said statistical value (Pd) and said power level values (Pm) are repeatedly updated.

4. The method as claimed in any of the preceding claims, wherein said statistical value (Pd) is the standard deviation and the threshold value is plus minus three times said standard deviation.

5. The method as claimed in any of the preceding claims , wherein said radio communication system is a home alarm system.

6. The method as claimed in claim 1, wherein said statistical value (Pd) is the mean value of power level values (Pm) over a predetermined time period (Tm) and the threshold value is plus minus two to five times of said mean value.

7. The method as claimed in anyone of the preceding claims, wherein the power level signal is obtained at a bandwidth corresponding to an order of separate information segments in a radio signal received in said receiver.

8. The method as claimed in anyone of the preceding claims, further comprising measuring power of an incoming radio signal to a radio receiver at an Automated Gain Control (AGC) unit of the receiver.

9. The method as claimed in anyone of claim 1-7, further comprising measuring power of an incoming radio signal to a radio receiver at an analogue to digital converter (ADC).

10. The method as claimed in anyone of the preceding claims, further comprising measuring receiving the power level signal in said radio signal receiver of the gateway.

11. A detector (44) for detecting radio disturbances in a radio communication system comprising a gateway device and a peripheral device, each arranged to send radio signals to and to receive radio signals from the other, wherein the detector (44) comprises:

    a power level detector (62),
    a processing unit (64) operatively connected to the power level detector (62),
    a memory unit (66) storing a plurality of statistical values of detected power levels, wherein said processing unit (64) is arranged to:

        i. measure the power level (Pm) of separate information segments of the radio signals

received by one device from the other device,
ii. determine a statistical value (Pd) of measured power level values,
iii. compare a selected measured power level with the statistical value,
iv. produce an alert signal, indicating a radio disturbance, if the difference between the selected measured power level and the statistical value exceeds a threshold.

12. The detector as claimed in claim 11, wherein the power level detector (62) is connected to an analogue to digital converter (ADC) of the radio signal receiver.

13. The detector as claimed in claim 11, wherein the power level detector (62) is connected to an Automated Gain Control (AGC) unit of the receiver.

14. The detector as claimed in anyone of claim 10-13, wherein the detector (44) is operatively connected to the radio signal receiver of the gateway.

15. The detector as claimed in anyone of claim 10-14, wherein the detector (44) is provided with a first input receiving power level of the power of separate information segments in a radio signal received in said radio signal receiver, and with a second input receiving separate information segments in a radio signal received in said receiver.

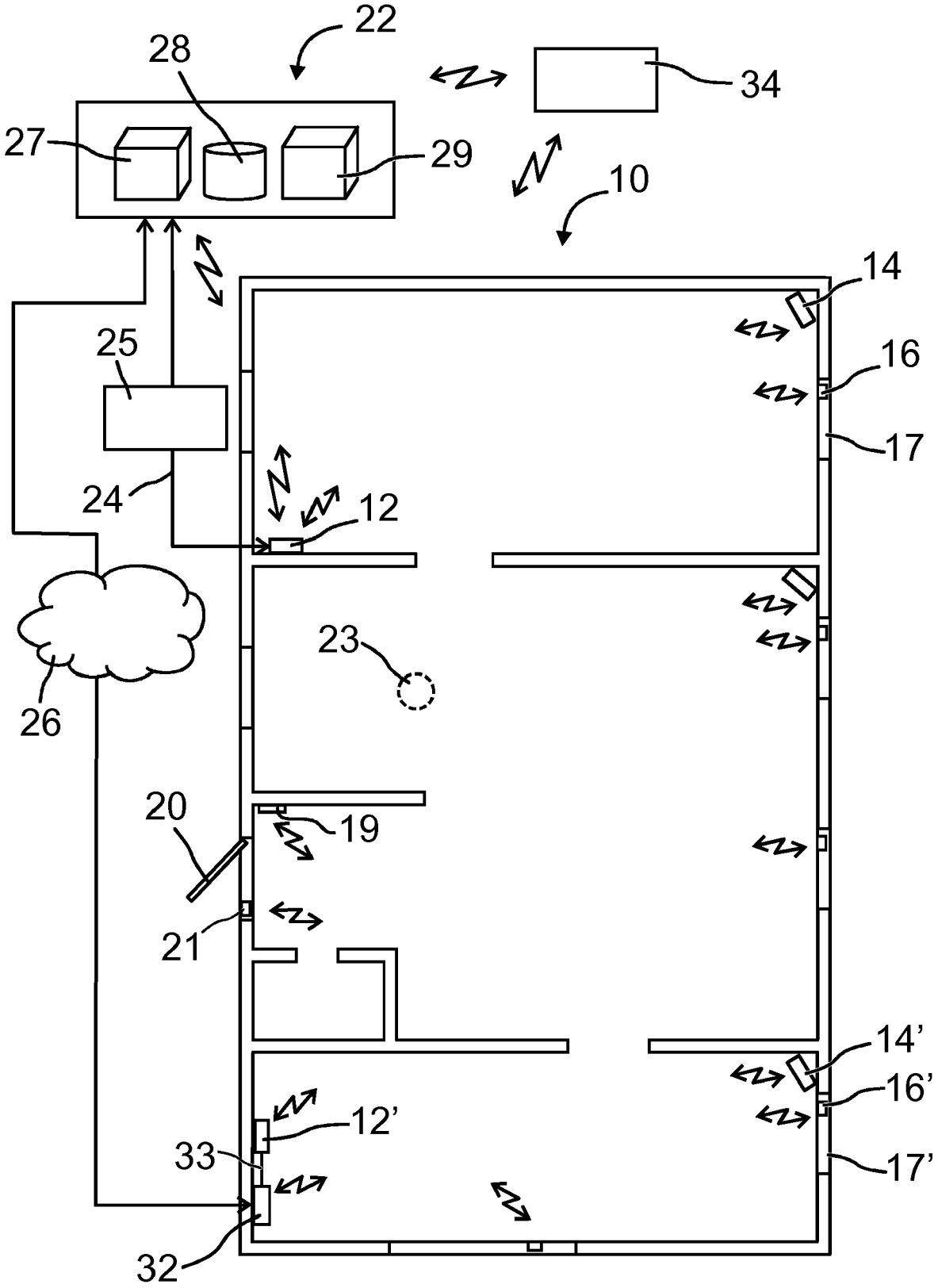

Fig. 1

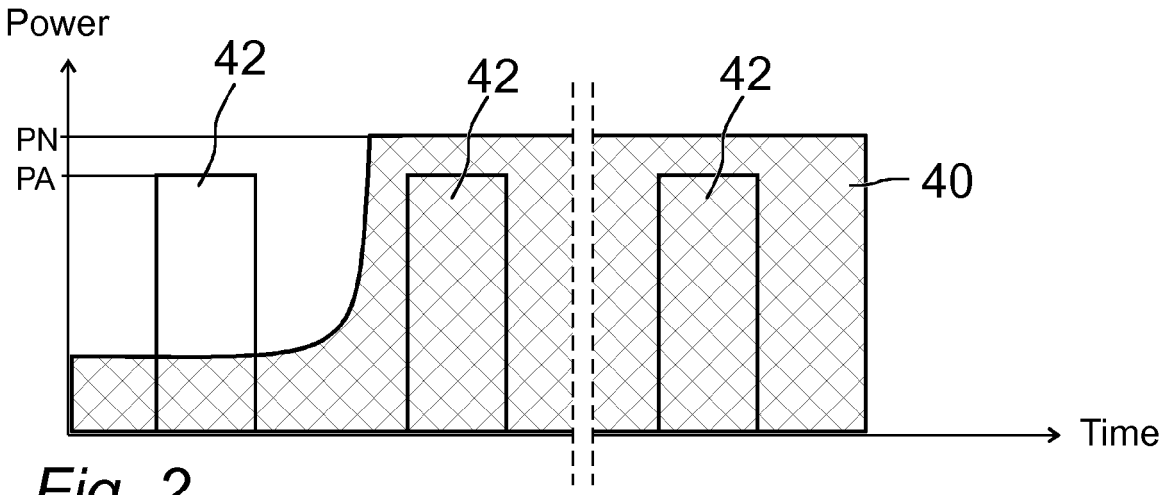

Fig. 2

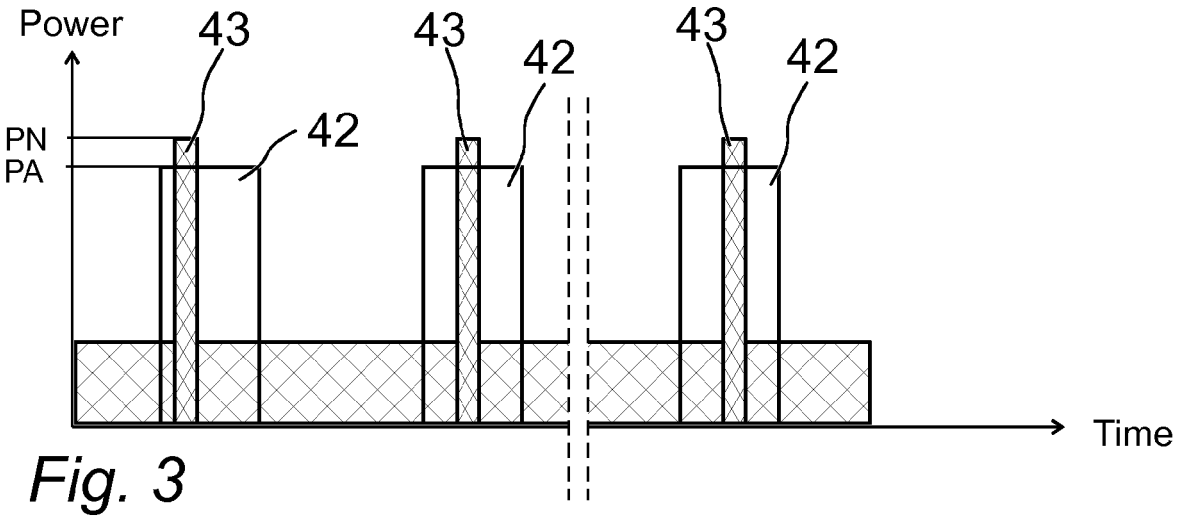

Fig. 3

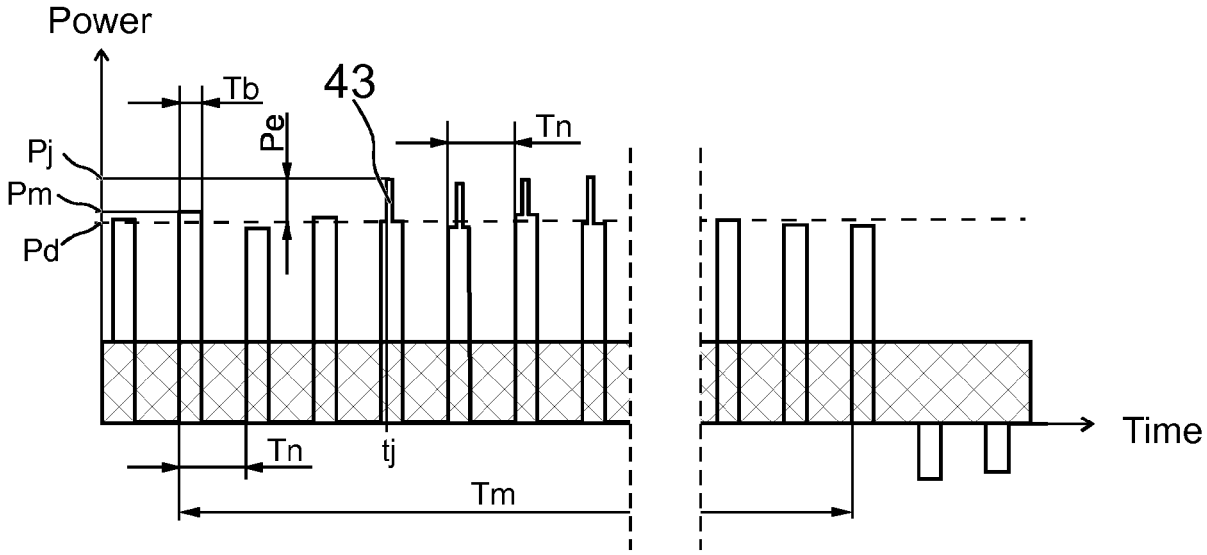

Fig. 4

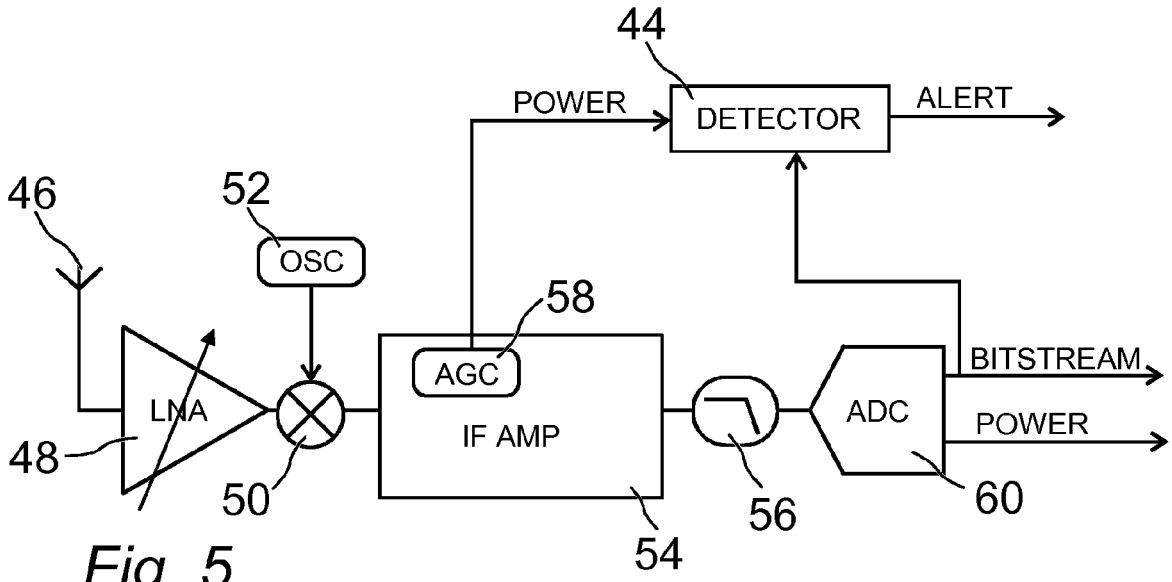

Fig. 5

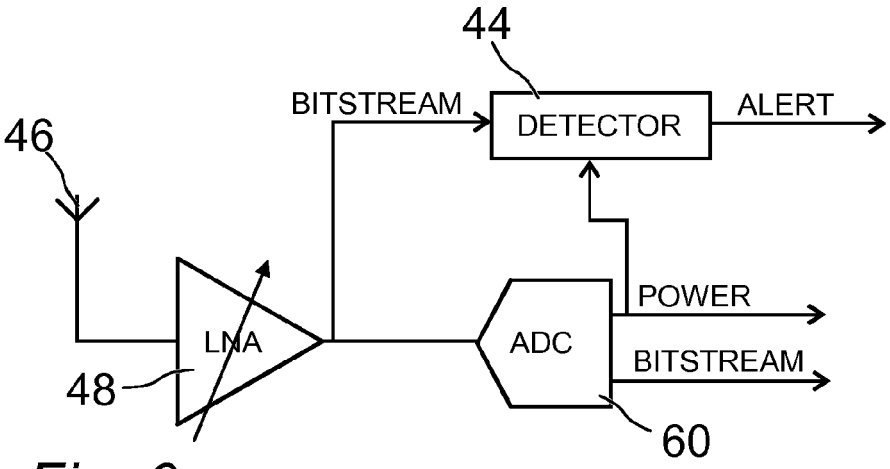

Fig. 6

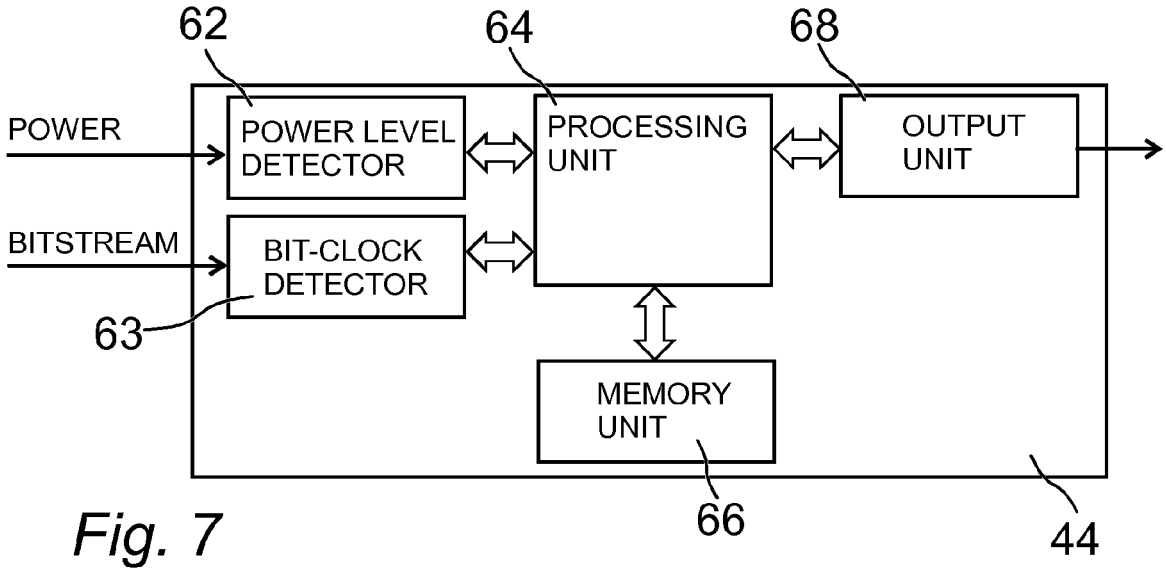

Fig. 7

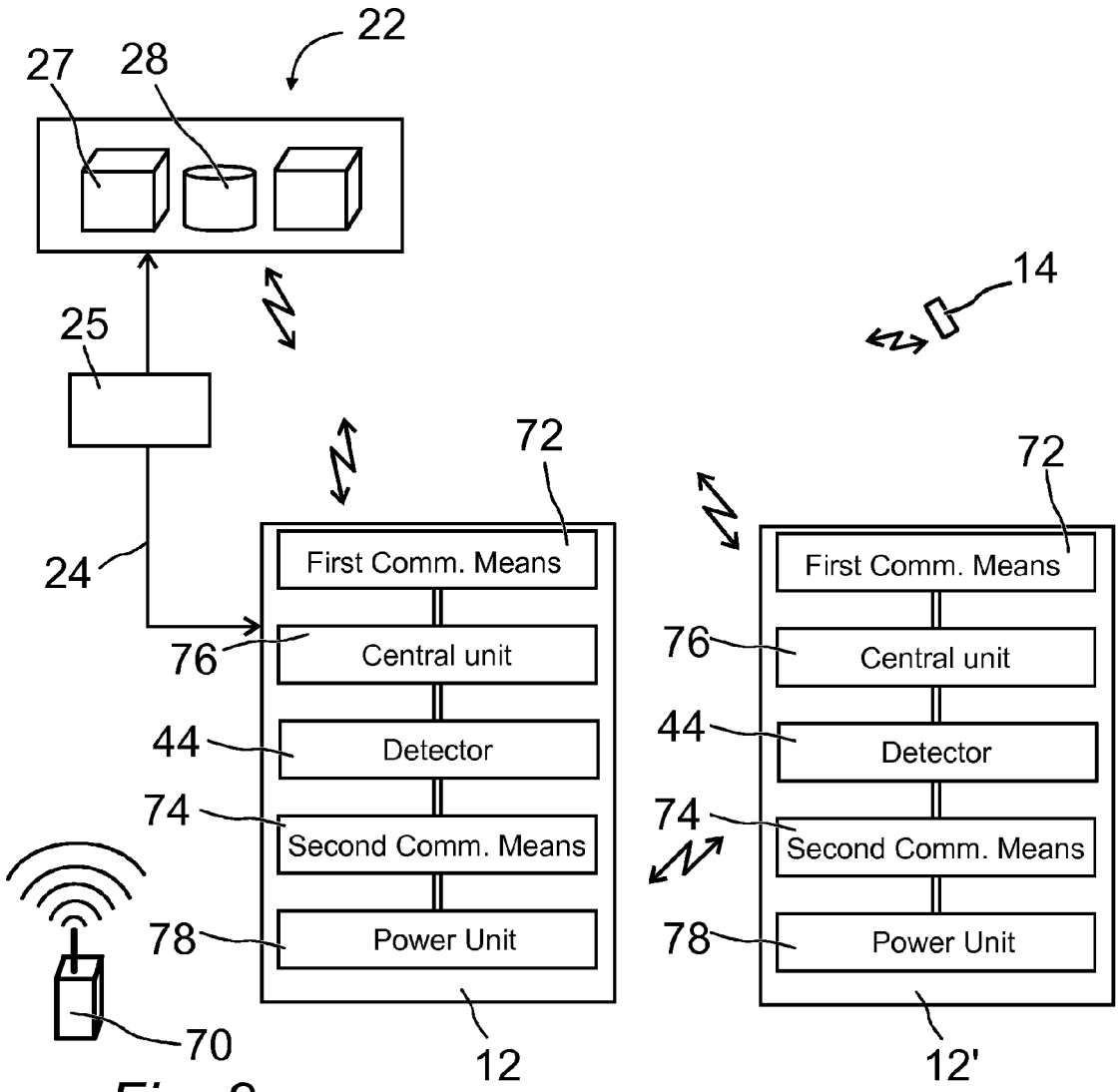

Fig. 8

1	0	1	0	1	0	1	1	0	0	1	0	1	1	0	1
G	G	G	G	H	H	H	H	H	G	G	G	G	G	G	G

Fig. 9

1	0	1	0	1	0	1	**1**	**1**	**1**	**1**	**1**	**1**	1	0	1
G	G	G	G	H	H	H	***V***	***V***	***V***	***V***	***V***	***V***	G	G	G

Fig. 10

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 18 16 1928

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	EP 2 733 853 A1 (GEMALTO M2M GMBH [DE]) 21 May 2014 (2014-05-21) * abstract; figure 2 * * paragraph [0098] *	1-15	INV. G08B29/04 H04K3/00
A	EP 3 026 835 A1 (GEMALTO M2M GMBH [DE]) 1 June 2016 (2016-06-01) * abstract; figure 5 * * paragraph [0006] * * paragraph [0017] * * paragraph [0023] - paragraph [0029] *	1-15	
A	US 6 229 998 B1 (HAMDY WALID [US] ET AL) 8 May 2001 (2001-05-08) * abstract; figure 1 * * column 5, line 62 - column 6, line 25 *	1-15	

TECHNICAL FIELDS SEARCHED (IPC)

G08B
H04K

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	25 September 2018	Wagner, Ulrich

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 18 16 1928

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.

25-09-2018

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2733853 A1	21-05-2014	EP 2733853 A1	21-05-2014
		EP 2920886 A1	23-09-2015
		US 2015270922 A1	24-09-2015
		WO 2014076283 A1	22-05-2014
EP 3026835 A1	01-06-2016	CA 2966803 A1	02-06-2016
		CN 107005337 A	01-08-2017
		EP 3026835 A1	01-06-2016
		EP 3224974 A1	04-10-2017
		US 2017366294 A1	21-12-2017
		WO 2016083390 A1	02-06-2016
US 6229998 B1	08-05-2001	AT 274258 T	15-09-2004
		AT 345599 T	15-12-2006
		AU 4642700 A	14-11-2000
		CN 1346545 A	24-04-2002
		DE 60013108 D1	23-09-2004
		DE 60013108 T2	18-08-2005
		DE 60031895 T2	30-08-2007
		EP 1166458 A1	02-01-2002
		EP 1337050 A2	20-08-2003
		HK 1042996 A1	01-08-2008
		JP 4485695 B2	23-06-2010
		JP 2002542651 A	10-12-2002
		KR 20010108483 A	07-12-2001
		US 6229998 B1	08-05-2001
		WO 0062437 A1	19-10-2000

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

- EP 2541518 A **[0002]**