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

(11) EP 3 543 976 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
25.09.2019 Bulletin 2019/39

(51) Int Cl.:
G08B 13/00 $^{(2006.01)}$ ***G08B 25/10*** $^{(2006.01)}$
G08B 29/04 $^{(2006.01)}$

(21) Application number: **18163170.6**

(22) Date of filing: **21.03.2018**

(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**
247 41 Södra Sandby (SE)

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

(54) A METHOD FOR INCREASING SPECIFICITY OF JAMMING DETECTION IN A HOME ALARM SYSTEM

(57) A method and a system for detecting an interference signal and classifying the interference signal into two or more classes by
- repeatedly measuring (201) a received signal strength indicator (RSSI) of a received signal;
- repeatedly calculating an average value (205) of the received signal strength indicator over a first time-period;
- repeatedly calculating a variance value (210) of the received signal strength indicator over a second time-period, said second time period at least partly overlapping said first time period;
- comparing the calculated average value (215) to a predetermined threshold average value;
- comparing the calculated variance value (220) to a predetermined threshold variance value; and
- classifying the signal into one of two or more classes (235) based on the comparisons (215, 220), one class being indicative of a jamming condition.

The system comprises an antenna, a transceiver and a processor.

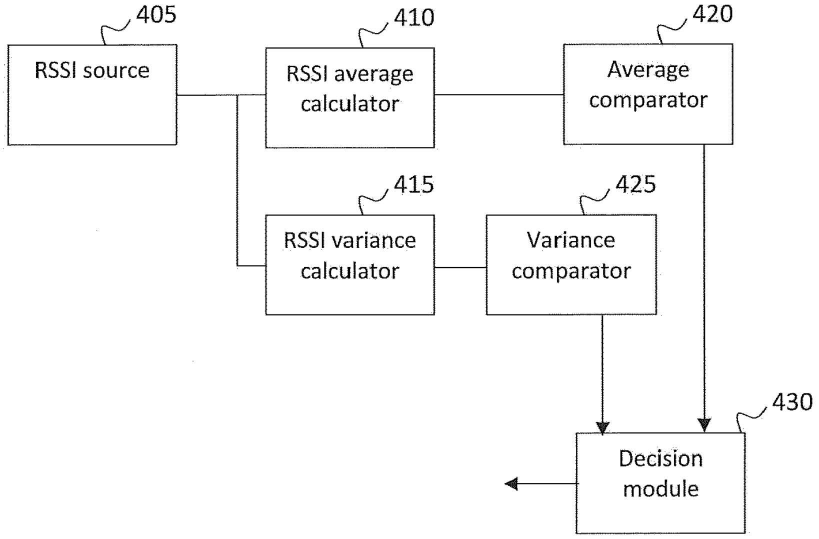

Fig. 4

Printed by Jouve, 75001 PARIS (FR)

Description

TECHNICAL FIELD

[0001] The invention relates to a method and a system for detecting jamming of systems using wireless communication. In particular it relates to a method and a system for differentiating between interference originating from a jamming device and interference originating from a nearby wireless system.

BACKGROUND

[0002] Alarm systems comprising detectors and gateways are commonly used in private houses and office premises. Detectors are more and more frequently connected through wireless communication means to a central unit, also known as a gateway, which in turn is connected to a central monitoring station (CMS) such as a remote alarm receiving centre. In case of an alarm situation one or more detector(s) transmits an alarm signal to the gateway and the gateway transmits an alarm signal to the central monitoring station, should the alarm system be in an armed state.

[0003] A burglar or other intruder may use electronic jamming devices to jam wireless signals between the detector(s) and the gateway or between the gateway and the central monitoring station. The present invention relates to a method and means for detection of jamming interference from such jamming devices, and for detecting nearby wireless communication interference and differentiating the two from each other.

[0004] If nothing else is explicitly stated in the present document, it is the communication between the gateway and its associated detectors and sensors that is subject to jamming.

PRIOR ART

[0005] Prior art jamming detection exist in different forms. Detectors, sensors and gateways normally communicate via radio links or by other wireless means. Radio signals also can be used for communication with the remote alarm receiving centre. As in all applications radio signals are vulnerable to disturbances and of course to deliberate jamming attempts.

[0006] GB2457102 discloses an alarm comprising a repeater which is arranged to detect a jamming signal and to transmit a jamming alert signal at a frequency other than a jammed frequency in the event that a jamming signal is detected.

[0007] Another way of handling jamming problems is disclosed in RU2399095. The system in RU2399095 comprises a plurality of microcells in a multilevel hierarchical structure. A plurality of relay nodes is used to ensure that alarm messages are transmitted even if one microcell is jammed.

SUMMARY OF THE INVENTION

[0008] According to a first aspect of the present invention, there is provided a method of detecting an interference signal and classifying the origin of the interference signal into one of two or more classes. The method comprises the following steps:

- measuring (201) a received signal strength indicator (RSSI) of a received signal;
- calculating an average value (205) of the received signal strength indicator during a first time period;
- calculating a variance value (210) of the received signal strength during a second time period, said second time period at least partly overlapping said first time period;
- comparing the calculated average value (215) to a predetermined threshold average value;
- comparing the calculated variance value (220) to a predetermined threshold variance value;
- classifying the signal into one of two or more classes (235) based on the comparisons (215, 220) during overlapping time periods, one class being indicative of a jamming condition.

[0009] An advantage of an alarm system with a method of the present invention is that jamming can be detected earlier and more accurately. The method facilitates differentiation between radio frequency interference originating from a jammer and radio frequency interference originating from an adjacent wireless system.

[0010] A feature of the present invention is that unintentional interference from other benign wireless systems can be differentiated from malicious RF jamming. This differentiation will ultimately result in a decrease of the number of false alarms. The present invention provides a method of detecting jamming of intruder alarm systems or jamming of other wireless systems. The method is particularly advantageous for such systems because the number of false alarms due to detection of interference from other wireless systems can be reduced without reducing the number of true alarms, i.e. alarms due to the detection of interference from a jamming device.

[0011] The present invention provides a way to detect and differentiate radio interference originating from a jamming device, a so-called jammer, from interference originating from a nearby wireless system. When a jamming condition is detected an alarm can be generated. An alarm or alert signal can also be forwarded to a central monitoring station where further actions can be taken in a response to the jamming condition.

[0012] The jammers used today are based on noise generators. These jammers generate a broadband noise. More advanced models may use filtering to only jam parts of the spectrum - but it is still using noise to jam the system. Since noise per definition will be random it will exhibit a high degree of variance around a constant mean.

[0013] By continuously measuring the received signal strength, a so called Received Signal Strength Indicator (RSSI) and repeatedly calculating the mean and variance of the signal over a predetermined number of the latest received signal strength measurements one would have all the data needed to differentiate between noise and signal. If the average and variance is "high", there is a jammer present, if the average is high but the variance low, a carrier is present. The fact that a carrier is present is considered equivalent to the fact that a nearby wireless system is present and is transmitting.

[0014] According to a further aspect, there is provided an alarm system for detecting a possible jamming signal, the system comprising:

- an antenna;
- a transceiver;
- a processor;

wherein the system is configured to detect possible jamming and to classify the possible jamming signal as a jamming condition to indicate whether it is an interference from a carrier originating from a nearby benign wireless system or a jammer.

[0015] An advantage of such a system is that the number of false alarms would decrease making it easier for an alarm operator to decide when to send out a watchman, and when not to, decreasing the time and money spent on false alarms.

[0016] The system preferably comprises

- an RSSI source of the transceiver;
- an RSSI average calculator unit (410) for calculating an RSSI average;
- an RSSI variance calculator unit (415) for calculating an RSSI variance
- an average comparator unit (420) for comparing RSSI average with a predetermined average threshold;
- a variance comparator unit (425) for comparing RSSI variance with a predetermined variance threshold;
- a decision module unit (430) for deciding a class based on the comparisons.

[0017] By studying RSSI average and variance a good estimate on whether the received signal is originating from a nearby installation or from a jamming device, since jamming device signals and carrier waves from a nearby installation normally have different characteristics.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] Non-limiting embodiments of the invention will now be described with reference to the figures in which:

Fig. 1 shows a schematic diagram of a radio receiving module according to prior art.

Fig. 2 shows a flowchart of a method for differentiating whether a high received signal strength indicator is caused by a jammer or caused by a transmission originating from a nearby wireless system.

Fig. 3 shows a schematic block diagram of a wireless system

Fig. 4 shows a schematic block diagram of a jammer/carrier detector

DETAILED DESCRIPTION

[0019] In jamming detection, it is usually beneficial to detect jamming early and accurately. The present invention provides a method and a system for differentiating between a jammer and an adjacent wireless system or a similar radio condition environment thus resulting in a more accurate jamming detection.

[0020] The accuracy of a jamming detector could be estimated by studying the two measures called "sensitivity" and "specificity". Sensitivity or "true positive rate" is a measure of the proportion of positives that are correctly identified as such, i.e., the percentage of true jamming signals that are correctly identified as such. Specificity or "true negative rate" is a measure of the proportion of negatives that are correctly identified as such, i.e., the percentage of noise and interference signals not coming from a jammer, that are correctly identified as being not jamming signals.

[0021] For alarm system operators, there is a trade-off between these values because it is desirable to detect jamming (high sensitivity), but it is also desirable to limit the number of false positives, since these will increase costs, without adding value. A high number of false positives may also lower the confidence in the system among customers.

[0022] One way to lower false positive rate is to target interference that originates from adjacent home alarm systems or similar installations. The jammers used today normally are based on noise generators. These jammers generate a broadband noise. More advanced models may use filtering to only jam parts of the spectrum - but most are still using noise to jam the system. Since noise per definition will be random it will exhibit a high degree of variance around a constant mean. A regular transmission from an alarm system will not exhibit those noise characteristics, instead there will be a low variance. The average may still be high though, depending on distance to the nearby system and transmitted power.

[0023] In accordance with the disclosed embodiment, signal strength average and variance data are used to distinguish between carriers and noise. Furthermore, it may be used to either continuously or intermittently monitor possible jamming and non-malicious neighbouring signals. The method comprises steps to determine the values of the average and variance of received radio frequency energy, or RSSI, in those particular bandwidth(s) used for communication. If the average and variance values are both "high", there is a high probability that a jammer and a jamming condition is present. If the average is high but the variance is low, there is a high probability that a carrier is present. The four use cases are summarized in the table below:

Table 1. How received signal average and variance predict signal origin

	Low variance	High variance
Low average	Weak carrier	Noise
High average	Carrier	Jammer

[0024] Thus, embodiments of the present invention provide methods of detecting an interference signal and classifying the origin of the interference signal into one of two or more classes. In the present embodiment, the method comprises the following steps:

- repeatedly measuring (201) a received signal strength indicator (RSSI) of a received signal;
- repeatedly calculating an average value (205) of the received signal strength indicator over a first time period;
- repeatedly calculating a variance value (210) of the received signal strength indicator over a second time period, said second time period at least partly overlapping said first time period;
- comparing the calculated average value (215) to a predetermined threshold average value;
- comparing the calculated variance value (220) to a predetermined threshold variance value;
- classifying the signal into one of two or more classes (235) based on the comparisons (215, 220) during overlapping time periods, one class being indicative of a jamming condition.

[0025] The classes are preferably the classes defined in table 1, i.e., "Weak carrier", "Noise", "Carrier", and "Jammer". The classes may as an alternative be "Jammer" and "Non-jammer". The class "Jammer" corresponds to a jamming condition.

[0026] Fig. 1 shows a schematic diagram of a radio receiving portion of a wireless system according to prior art. The system is configured to provide a so-called received strength signal indicator. An antenna 101 is connected to a low noise amplifier 105. The output from the low noise amplifier 105 is connected to a mixer 110. The mixer also receives input from a local oscillator 115. The mixer output is filtered by a filter 120 and fed to an amplifier 125. Output from the amplifier 125 is fed to a channel filter 130. Output from the channel filter 130 is fed to a detector 135. Output from detector 135 is fed to a demodulator 140. Output 145 from the demodulator may include received signal strength indicator.

[0027] Fig. 2 shows a flowchart of a method for differentiating whether a high received signal strength indicator is caused by a jammer or caused by a transmission originating from a nearby and harmless, wireless system. The method comprises the following steps:

- Providing 201 an RSSI signal representative of received signal strength of the studied frequency band;
- Providing 207 a first window size representative of the time window of RSSI signal to use for producing values of the RSSI average signal
- Producing 205 an RSSI average signal, based on the RSSI signal, and representative of a moving average created with the aid of the first window size;
- Providing 212 a second window size representative of the time window of RSSI signal to use for producing values of the RSSI variance signal
- Producing 210 an RSSI variance signal, based on the RSSI signal, and representative of a moving variance created with the aid of the second window size;
- Providing 217 a threshold for the RSSI average, above which threshold it is highly likely that a nearby system or jammer is emitting radio frequency energy in the studied frequency band
- Comparing 215 the RSSI average signal with the provided threshold for average;
- Providing 218 a variance threshold for the RSSI variance, above which threshold it is highly likely that it is a nearby jammer that is emitting radio frequency energy in the studied frequency band, but below which threshold it is highly likely that any emitted radio frequency energy in the frequency band studied, originates from a nearby wireless system.
- Comparing 220 the RSSI variance signal with the provided threshold for variance;
- Deciding 235 based on the comparisons 215, 220 whether a jammer is active.

[0028] Variance and average threshold values are predetermined and set in dependence of radio signal conditions in the environment of the wireless system. The predetermined average value normally is set to a level where the RSSI of a standard wireless system will be. The predetermined variance value normally is set to a level somewhat higher than where a standard carrier is present.

[0029] Fig. 3 shows a schematic block diagram of a wireless system according to an embodiment of the present invention. An antenna 302 is connected to a radio transceiver unit TXU 305, such as e.g. Ti 1121 from Texas Instruments. The radio transceiver unit 305 is connected to a processor, preferably a microcontroller unit MCU 310. The microcontroller unit MCU is configured to instruct the transceiver unit TXU to provide a first stream of instantaneous values of received signal strength indicator (RSSI) to the microcontroller unit 310.

[0030] Further, the microcontroller 310 is configured to provide a second stream of values, each value calculated as an average of a predetermined number of the last values of the first stream. The microcontroller 310 is further configured to provide a third stream of values, each value calculated as a value corresponding to or being the variance of the first stream.

[0031] The microcontroller 310 is further configured to decide, based on the second and third stream of values, if a jamming device is active. Preferably, the decision is based on whether the average is high at the same time as variance is high, as can be seen in Table 1 above.

[0032] Fig. 4 shows a schematic block diagram of a jammer-carrier detector. An RSSI source unit 405 is connected to an RSSI average calculator unit 410 to provide an RSSI stream of values. The RSSI source unit 405 also provides RSSI values to an RSSI variance calculator unit 415. The RSSI average calculator unit 410 is configured to produce an RSSI average stream of values, in each moment representative of the average RSSI taken during a first time period incorporating a first predetermined number of the last samples of the RSSI signal.

[0033] The RSSI variance calculator unit 415 is configured to produce an RSSI variance stream of values, in each moment representative of the variance of the RSSI stream of values taken during a second time period incorporating a second predetermined number of the last samples of the RSSI signal. In various embodiments, first and second sliding time windows start at the same time and have equal length.

[0034] Each value of the stream of averaged values are compared to a predetermined average threshold value in an average comparator unit 420.

[0035] Each value of the stream of variance values are compared to a predetermined variance threshold value in a variance comparator unit 425.

[0036] The result of the comparisons in the average comparator unit 420 and in the variance comparator unit 425 are fed to a decision module unit 430. The decision module unit 430 is configured to provide, based on the result of the comparisons, a classification indicating whether the received signal belongs to one of the following classes:

- Class 1: There is a jamming signal present, or
- Class 2: There is radio frequency energy present originating from a nearby benign wireless system;
- Class 3: There is neither any jammer nor any actively sending nearby benign wireless system present.

[0037] There may also be provided a further alternative, such as an indication that, based on the received radio frequency energy, it is not possible to give a definite classification.

[0038] The classification result is preferably used to take decision on generating an alarm signal and/or sending an alarm signal to a remote alarm receiving centre or wait and see how the received energy develops.

Claims

1. A method of detecting an interference signal and classifying the origin of the interference signal into one of two or more classes, the method comprising the following steps:

- measuring (201) a received signal strength indicator (RSSI) of a received signal;
- calculating an average value (205) of the received signal strength indicator during a first time-period;
- calculating a variance value (210) of the received signal strength indicator during a second time period, said second time period at least partly overlapping said first time period;
- comparing the calculated average value (215) to a predetermined threshold average value;
- comparing the calculated variance value (220) to a predetermined threshold variance value; and
- classifying the signal into one of two or more classes (235) based on the comparisons (215, 220), one class being indicative of a jamming condition.

2. The method according to claim 1, further comprising calculating the average value and the variance value over the same time period.

3. The method according to claim 1, further comprising classifying the received signal as a jamming signal when the average value exceeds the predetermined threshold average value and the variance value exceeds the predetermined threshold variance value.

4. An alarm system for detecting a possible jamming condition, the system comprising:

- an antenna;
- a transceiver;
- a processor;

characterised in that the system is configured to:

- measuring (201) a received signal strength indicator (RSSI) of a received signal;
- calculating an average value (205) of the received signal strength indicator over a first time-period;
- calculating a variance value (210) of the received signal strength indicator over a second time-period, said second time period at least partly overlapping said first time period;
- comparing the calculated average value (215) to a predetermined threshold average value;
- comparing the calculated variance value (220) to a predetermined threshold variance value; and
- classifying the signal into one of two or more classes (235) based on the comparisons (215,

220), one class being indicative of a jamming condition.

5. The system of claim 4 further comprising:

- an RSSI source;
- an RSSI average calculator unit (410) for calculating an RSSI average;
- an RSSI variance calculator unit (415) for calculating an RSSI variance
- an average comparator unit (420) for comparing RSSI average with a first threshold;
- a variance comparator unit (425) for comparing RSSI average with a second threshold;
- a decision module unit (430) for deciding a class based on the comparisons.

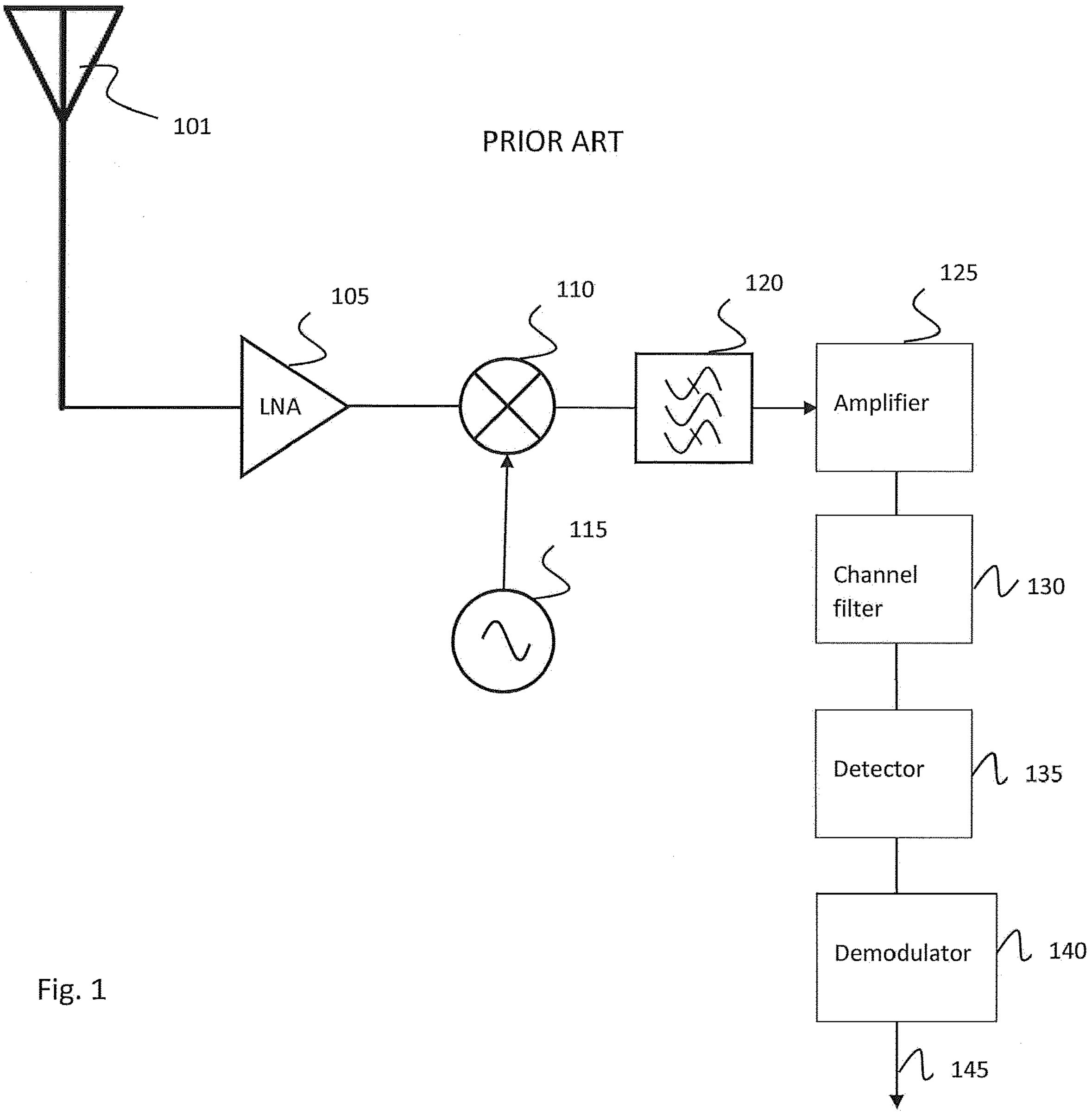
101
PRIOR ART
105
LNA
110
120
125
Amplifier
115
Channel filter
130
Detector
135
Demodulator
140
145

Fig. 1

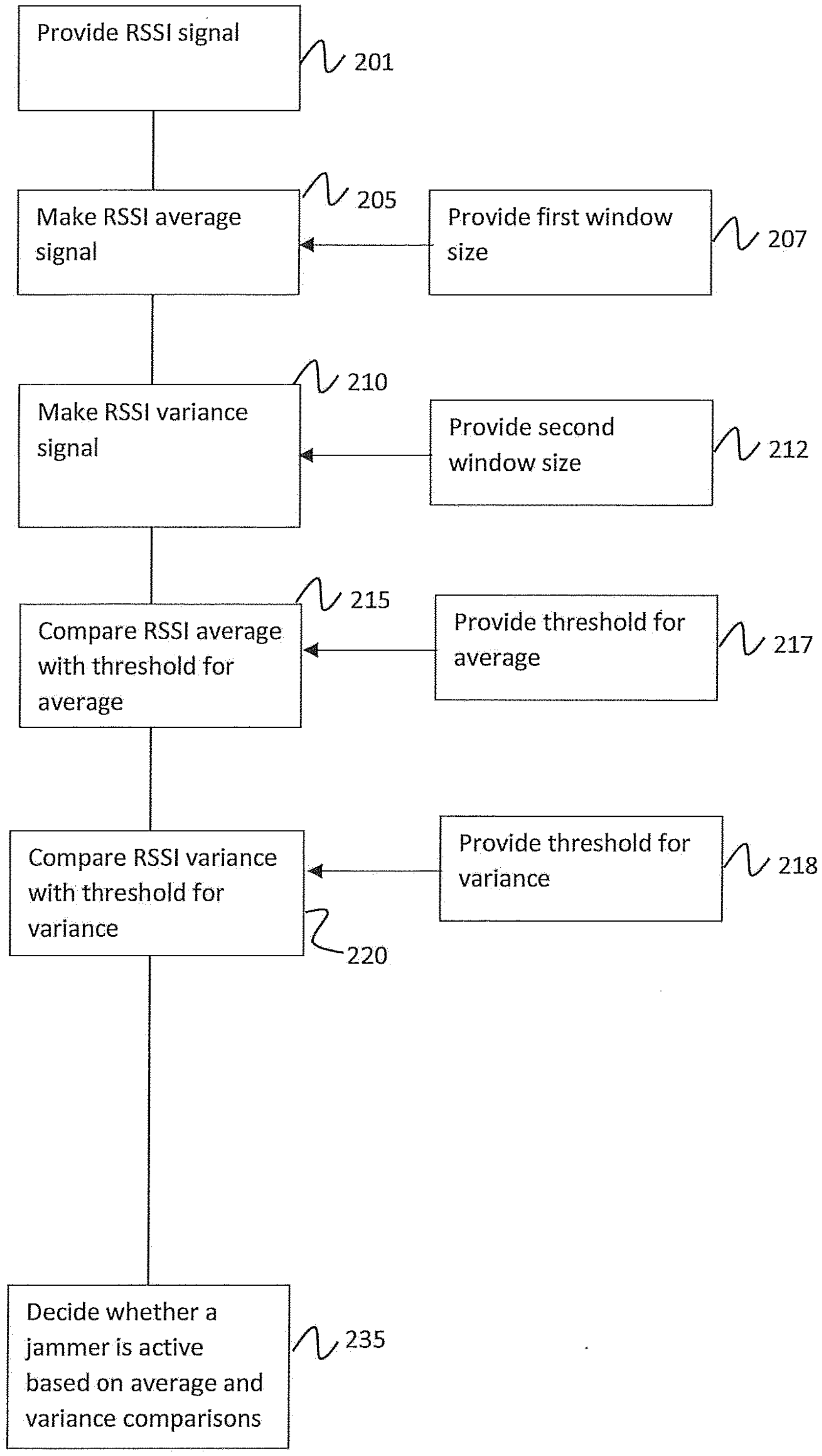
Provide RSSI signal
201
Make RSSI average signal
205
Provide first window size
207
Make RSSI variance signal
210
Provide second window size
212
Compare RSSI average with threshold for average
215
Provide threshold for average
217
Compare RSSI variance with threshold for variance
220
Provide threshold for variance
218
Decide whether a jammer is active based on average and variance comparisons
235

Fig. 2

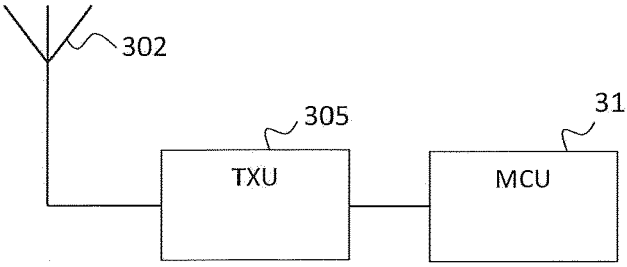
302
305
310
TXU
MCU

Fig. 3

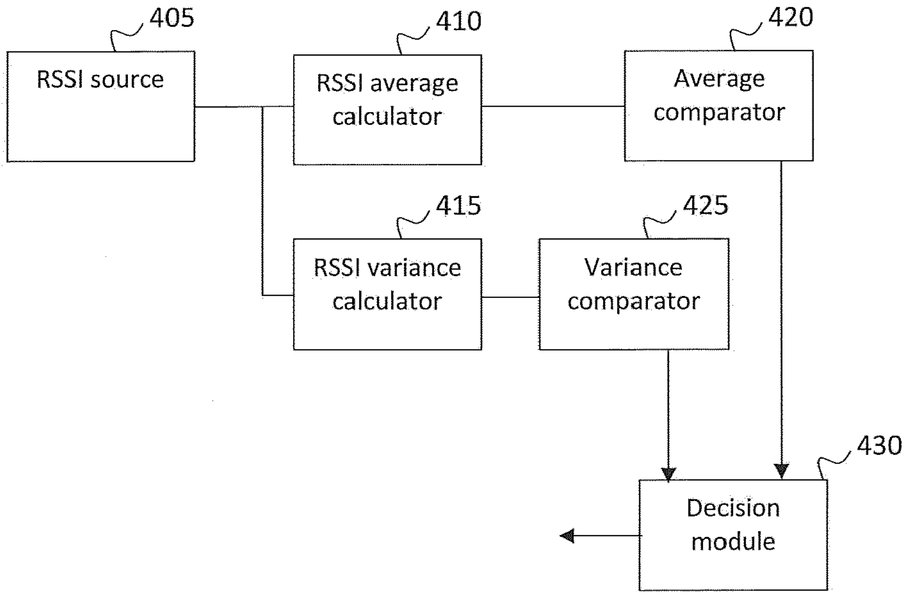
405
RSSI source
410
RSSI average calculator
420
Average comparator
415
RSSI variance calculator
425
Variance comparator
430
Decision module

Fig. 4

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 18 16 3170

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X A	US 2010/248667 A1 (DAUGHERTY JR THOMAS H [US] ET AL) 30 September 2010 (2010-09-30) * paragraph [0002] * * paragraph [0012] * * paragraph [0016] * * paragraph [0026] * * paragraphs [0032], [0033] * * claim 5 * * figures 1,4 * -----	1,2,4,5 3	INV. G08B13/00 G08B25/10 G08B29/04
A	US 5 950 110 A (HENDRICKSON ROBERT C [US]) 7 September 1999 (1999-09-07) * the whole document * -----	1-5	
			TECHNICAL FIELDS SEARCHED (IPC)
			G08B

The present search report has been drawn up for all claims

1

Place of search	Date of completion of the search	Examiner
Munich	11 September 2018	Meister, Mark

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
&amp; : member of the same patent family, corresponding document

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 18 16 3170

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.

11-09-2018

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010248667 A1	30-09-2010	NONE	
US 5950110 A	07-09-1999	NONE	

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

- GB 2457102 A **[0006]**
- RU 2399095 **[0007]**