

Marcas – Patentes
Modelos – Diseños
Nombres Comerciales – Enseñas
Propiedad Intelectual
Registros en el Exterior
Registros Sanitarios INVIMA – ICA
Acciones Judiciales – Administrativas
Derecho Comercial – Industrial
Asesoría – Contratos – Otros
Corresponsalia a Nivel Mundial

MDE

Mario Delgado Echeverry e Hijos Ltda.

Abogados Consultores – Marcas y Patentes

Bogotá D.C. - Colombia
Avda. Kra. 24 Park Way No. 37 – 31 Of.
202
Tels. (571) 2444096 – 3690624
Fax (571) 2442496 A.A. No. 6207
E-mail: mde@mdelaw.com
mdelawof@cablenet.co
mdeabogados@cablenet.co

Miembros ACPI – ASIPI - AIPPI

**SEÑOR
SUPERINTEDENTE DE INDUSTRIA Y COMERCIO
DIVISIÓN DE NUEVAS CREACIONES
E. S. D.**

Superintendencia de Industria y Comercio

Radicado: 16119034 38 Folios
Dependencia: Desc Fecha: 2016-07-28 16:28:21
Tipo aplicación: Documentos independientes

Ref.: Expediente No.: 16 119.034

Patente de invención: METODO Y DISPOSITIVO DE DETECCION DE INTERFERENCIA DELIBERADA

Atentamente se dirige a usted **JAIME EDUARDO DELGADO VILLEGAS**, Abogado, mayor y vecino de Bogotá D.C., e identificado como aparece al pie de mi firma, me dirijo a su Digno Despacho para manifestarle lo siguiente:

En mi condición de apoderado de la sociedad **SECURITAS DIRECT AKTIEBOLAG**, domiciliada en Suecia, presenté ante su Digno Despacho la solicitud de registro de la patente de invención mencionada en la referencia.

2. Debido a lo anterior me permito adjuntar lo siguiente:

- Copia legalizada de la primera solicitud de la patente de invención de la referencia, presentada ante la Oficina de Europea de Patentes el 8 de mayo de 2015 bajo el número 15382243.2 a nombre de **SECURITAS DIRECT AKTIEBOLAG**.

Con el anterior documento, dejo completa mi solicitud y por lo tanto solicito se continúe con el trámite normal de registro del diseño industrial de la referencia.

Marcas – Patentes
Modelos – Diseños
Nombres Comerciales – Enseñas
Propiedad Intelectual
Registros en el Exterior
Registros Sanitarios INVIMA – ICA
Acciones Judiciales – Administrativas
Derecho Comercial – Industrial
Asesoría – Contratos – Otros
Corresponsalia a Nivel Mundial



Mario Delgado Echeverry e Hijos S.A.S .

Abogados Consultores – Marcas y Patentes

Bogotá D.C. - Colombia
Av. Kr.24 Park Way No. 37 – 31 Of. 202
Tels.(571) 2444096 – 3690624
(571) 2444938 - 3687752
Fax (571) 2442496 A.A. No. 6207
E-mail: mde@mdelaw.com
mdelawof@cablenet.co
mdeabogados@cablenet.co

Miembros ACPI – ASIPI - AIPPI

Atentamente,



JAIME EDUARDO DELGADO VILLEGAS
C.C. No. 19.270.955 de Bogotá
T.P. No. 43.308 del C. S. de la J.

Bescheinigung

Certificate

Attestation

Die angehefteten
Unterlagen stimmen mit der
als ursprünglich eingereicht
geltenden Fassung der auf
dem nächsten Blatt
bezeichneten europäischen
Patentanmeldung überein.

The attached documents are
exact copies of the text in
which the European patent
application described on the
following page is deemed to
have been filed.

Les documents joints à la
présente attestation sont
conformes au texte,
considéré comme
initialement déposé, de la
demande de brevet
européen qui est spécifiée à
la page suivante.

Patentanmeldung Nr.

Patent application No.

Demande de brevet n°

15382243.2 / EP15382243

The organization code and number of your priority application, to be used for filing abroad under the Paris Convention, is EP15382243.

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.



V. Joseph

Anmeldung Nr:
Application no.: 15382243.2
Demande no :

Anmeldetag:
Date of filing: 08.05.15
Date de dépôt :

Anmelder / Applicant(s) / Demandeur(s):

Securitas Direct AB
PO Box 392
201 23 Malmö/SE

Bezeichnung der Erfindung / Title of the invention / Titre de l'invention:

(Falls die Bezeichnung der Erfindung nicht angegeben ist, oder falls die Anmeldung in einer Nicht-Amtssprache des EPA eingereicht wurde, siehe Beschreibung bezüglich ursprünglicher Bezeichnung.

If no title is shown, or if the application has been filed in a non-EPO language, please refer to the description for the original title.

Si aucun titre n'est indiqué, ou si la demande a été déposée dans une langue autre qu'une langue officielle de l'OEB, se référer à la description pour le titre original.)

JAMMING DETECTION METHOD AND DEVICE

In Anspruch genommene Priorität(en) / Priority(Priorities) claimed / Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen / State/Date/File no. / Pays/Date/Numéro de dépôt:

Am Anmeldetag benannte Vertragsstaaten / Contracting States designated at date of filing / Etats contractants désignées lors du dépôt:

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

JAMMING DETECTION METHOD AND DEVICE

5

DESCRIPTION**FIELD OF THE INVENTION**

10 The present invention has its application within the security sector and, especially, in the industrial area engaged in providing intruder and theft alarms.

BACKGROUND OF THE INVENTION

15 Modern security and surveillance systems, such as those providing intruder or burglar alarms, typically comprise a central control panel connected to a plurality of peripherals such as video cameras, microphones, pressure sensors, temperature sensors, movement detectors, etc. When a possible threat is detected by any of the peripherals, said peripheral alerts the central control panel, which in turn transmits an alert signal to a remote centralized back-end service. Communications between peripherals and
20 control panel, and between control panel and back-end services can be performed either through wired or through wireless communication systems. However, wired communications can be easily tampered, effectively disengaging the security system. Wireless communications are hence regarded as being more secure, but they can also be subjected to attacks through intentional jamming. When this occurs, the wireless
25 communication channel is actively interfered, reducing the signal to noise ratio of the transmitted signals and rendering communication impossible. Although less likely, a similar scenario can occur as a result of unintentional interferences from nearby radio frequency systems.

30 In order to establish defences against this kind of accidental or active jamming, several alternatives have been proposed in the state of the art. For example, patent document GB-2457102-A discloses an intruder detection system where the alarm signal is transmitted wirelessly. In case of jamming, the interference is detected by a sensor, and the transmission frequency is modified to avoid the jammed frequency range.

However, modifying the frequency may not be enough to avoid the jamming. If the intruder manages to completely jam all the frequency band within which said transmission frequency can be tuned, the alarm signal will still not be received.

5 Patent document US-2014/0369452-A1 presents an alternative approach based on a multi-channel communication link between the transmitter and the receiver of a global navigation satellite system (GNSS) network. When jamming is detected, the number of channels used for data transmission is progressively reduced, increasing jamming resilience. Nevertheless, this approach could not be straightforwardly applied to
10 wireless communication networks used in security systems such as Industrial Scientific and Medical (ISM) radio networks and Global System for Mobile Communications (GSM) networks. Furthermore, the maximum achievable jamming protection is limited by the channel bandwidth of the architecture of the network used for the communication link, which could prove insufficient in some scenarios.

15 Finally, patent document US-4117405-A1 discloses an alarm transmission system relying on an ultra narrow band network (UNB), given its inherent resistance against jammers. The system comprises a plurality of alarm stations, each of them locked to a finely tuned local oscillator. A distinctive local oscillator frequency is assigned to each
20 alarm station. However, although some jamming resistance is incorporated, the actual presence of jamming is neither checked nor notified to the back-end service, hence giving the intruders more freedom during their tampering attempt. Furthermore, by using a fixed frequency in each station, the system is more predictable and easily tampered, and it requires significant resources to be employed in calibration and
25 frequency drift corrections. Finally, UNB networks are devised for multi-point to point services in which each element rarely needs to access the communication medium. Using the UNB by default in all communications between elements of the security system limits the total traffic and the number of deployable alarm stations.

30 Therefore, there is still the need in the state of the art of a jamming detection technique that effectively protects security systems against aggressive jamming of their wireless communications. Furthermore, it is still desirable that said jamming detection technique does not limit the number of elements connected to the back-end service or the data load among them when no jamming is present, and that it presents a reduced energy

consumption for increased autonomy, and therefore, a more prolonged and reliable protection.

SUMMARY OF THE INVENTION

5

The current invention solves all the aforementioned problems by disclosing a jamming detector that relies on an ultra narrowband network for alarm signal transmission in the presence of jamming, without affecting the normal operation of said security system when no jamming is present.

10

In a first aspect of the invention, a jamming detection device is disclosed. The device comprises a transceiver configured to periodically scan one or more frequency bands used for signal transmission between elements of a security system such as an intruder or theft alert system. When jamming is detected within at least one of said frequency bands, the device is configured to send an alarm signal through an ultra narrow band network, significantly more resilient to malicious jamming than conventional networks.

15

Preferably, the device is configured to periodically scan the following networks:

20

- An Industrial Scientific and Medical (ISM) radio network connecting one or more peripherals of the security system and a central control panel installed in the same location as the peripherals. Peripherals can comprise detectors such as video cameras, temperature sensors, movement sensors, etc.; alarms such as visual signs or sound systems; user-activated devices, or any other device associated to the security system. More preferably, the ISM network is established over the 868 MHz band for radio communications in Europe and in the 915 MHz band in America.

25

30

- A Global System for Mobile Communications (GSM) network connecting the control panel and a remote back-end service of the security system, typically used for alarm signal transmission in the absence of jamming. More preferably, the device scans both the 900 MHz and the 1800 MHz frequency bands of the GSM network for the presence of jamming.

Also preferably, the Ultra Narrowband (UNB) network used by the device for transmitting the alarm signal is established in a frequency band partially or fully overlapping the ISM radio network connecting the peripherals and the control panel.

5 According to the aforementioned preferred option for said ISM network, the ultra narrowband network is established over the 868 MHz radio frequency band.

In order to be able to scan all the relevant frequency bands with the same transceiver, said transceiver preferably comprises a local oscillator generating multiple harmonics of its main frequency. For example, this can be implemented with a local oscillator generating a signal with a rectangular waveform, which results in a significant third order harmonic generation. This enables to scan different frequency bands by tuning different harmonics of the generated signal. In the same example, the first order harmonic can be used to scan the 868 MHz band of the ISM network and the 900 MHz band of the GSM network, whereas the third order harmonic is used to scan the 1800 MHz band of said GSM network.

Some preferred options for medium access control and signal modulation for the alarm signal transmission in the ultra narrowband network include random frequency hopping and binary-phase-shift-keying modulation. As a result, the alarm signal is preferably transmitted using a signal bandwidth equal or lesser than 200 Hz. The central frequency of said signal bandwidth is randomly chosen within a 200 KHz band of the UNB network.. Given this extremely narrow signal bandwidth and the unpredictability of the precise frequency over which the alarm signal is transmitted, active jamming systems are unable to interfere with the operation of the UNB network.

When jamming is detected during the scanning of the different frequency bands, the alarm signal generated by the device preferably comprises an identifier of the at least a frequency band being jammed and a first numerical value representing a jamming intensity. The first numerical value may be, for example, a radio frequency signal intensity measurement, or a number of channels of a frequency band in which the measured intensity exceeds a given threshold. Once the device detects that the jamming is finished, an alarm signal is also generated comprising a second

numerical value indicating the duration of the jamming.

Furthermore, the jamming detection device may include additional features which are capable of generating alarm signals that are transmitted over the UNB network:

5

- An accelerometer for tampering detection. When a measurement of the accelerometer exceeds at least a first threshold, an alarm message is generated. This prevents any intruder from manually disabling the jamming detection device before attempting to jam the security system communications.

10

- A thermometer. When a measurement of the accelerometer exceeds at least a second threshold, an alarm message is generated. Said second threshold can delimit an absolute temperature range, or it can be applied to a temperature gradient which combines multiple thermometer measurements.

15

- A user interface that enables a user of the security system to send alarm messages at any desired time. The interface may be as simple as a button that the user can press during a risk scenario, or include more complex input and output capabilities such as screens, microphones, etc. This feature also enables the user to check that UNB communications are working properly.

20

In another aspect of the present invention, a method for jamming detection in a security system is disclosed. The method comprises the following steps:

25

- Scanning at least a frequency band of a security system to detect jamming. The scanned frequency bands preferably comprise a 868 MHz frequency band (or 915MHz in America) in a ISM network connecting a control panel and the peripherals, and a 900 MHz and a 1800 MHz frequency bands in a GSM network connecting the control panel and the back-end services.

30

- When jamming is detected during the frequency band scans, sending an alarm signal to the back-end service through an ultra narrowband network. This step may preferably comprise applying random frequency hopping and/or binary-phase-shift-keying modulation to the transmitted alarm signal. Preferably, this step

comprises transmitting the alarm signal through a channel with a 200 Hz bandwidth or less. Furthermore, this step may comprise including in the alarm signal an identifier of the at least a frequency band being jammed, a first numerical value representing a jamming intensity. When the jamming is determined to have finished,
5 a second numerical value representing a jamming duration is also transmitted.

Preferably, the method further comprises measuring a displacement of an accelerometer and transmitting an alarm signal through the UNB network when said displacement exceeds a first threshold.

10 Preferably, the method further comprises measuring a temperature of a thermometer and transmitting an alarm signal through the UNB network when said temperature exceeds a second threshold. Said second threshold may be an absolute temperature range and/or a temperature gradient range.

15 Preferably, the method further comprises transmitting an alarm signal through the UNB network when receiving a user command through a user interface.

20 With the disclosed method and device, security and surveillance systems become resilient to intentional or accidental jamming of their wireless communications. When no jamming is present, the method and device do not impose any limitation on the normal operation of the security system. The jamming detector is also protected from physical tampering of the device, as well as from sudden temperature changes caused, for example, by a nearby fire or from certain tampering instruments.
25 Furthermore, the disclosed ultra narrow band network greatly optimizes energy consumption during data transmission towards the base station, therefore increasing the autonomy of the jamming detection device. These and other advantages will be apparent at the light of the detailed description of the invention.

30 Additional advantages and features of the invention will become apparent from the detailed description that follows and will be particularly pointed out in the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

For the purpose of aiding the understanding of the characteristics of the invention, according to a preferred practical embodiment thereof and in order to complement this description, the following figures are attached as an integral part thereof, having an illustrative and non-limiting character:

Figure 1 shows a schematic scenario to which the jamming detection device of the invention is applied, according to a particular embodiment thereof.

Figure 2 presents with further detail the components comprised by the jamming detection device according to a particular embodiment thereof.

Figure 3 depicts a simplified flowchart of a jamming detection algorithm according to a particular embodiment of the device and method of the invention.

Figure 4 illustrates a possible coding of the alarm signals sent by the jamming detection device and method according to a particular embodiment thereof.

DETAILED DESCRIPTION OF THE INVENTION

The matters defined in this detailed description are provided to assist in a comprehensive understanding of the invention. Accordingly, those of ordinary skill in the art will recognize that variation changes and modifications of the embodiments described herein can be made without departing from the scope and spirit of the invention. In particular, note that any particular embodiment or feature of the device of the invention may be applied to the method of the invention and vice versa. Also, description of well-known functions and elements are omitted for clarity and conciseness.

In this text, the term "ultra narrow band network" refers to any wireless network in which the spectrum of a transmitted signal is confined to a small spectral range, being said spectral range actively limited through signal modulation and/or signal processing techniques. The ultra narrow band network is therefore a network with a narrower

transmission bandwidth and increased resistance against jamming than any other network used for communications within the security system. An ultra narrow band network can be defined by having a ratio between a channel bandwidth and the total frequency bandwidth of the UNB network below a given threshold. Alternatively, the UNB network can be defined by having a ratio between channel bandwidth and carrier frequency below a given threshold, or by having an absolute channel bandwidth below another given threshold. In the particular embodiments disclosed herein, a channel bandwidth of 200 Hz or less is used.

Note that the specific ranges of the frequency bands mentioned in this description may be subjected to changes according to each particular embodiment and to the regulations of each particular country. Also note that in the preferred embodiments of the invention, the jamming detection device is described for simplicity as a stand-alone device. Nevertheless, its components and features could be also integrated within other components of the security system, such as the main control panel or any peripheral intruder sensor.

Figure 1 schematically depicts the main elements of a scenario in which particular embodiments of the jamming detection method and device of the invention are applied, namely a wireless security system where a malicious jamming is attempted. The security system comprises a plurality of peripherals (1) such as video cameras, microphones, pressure sensors, temperature sensors, alarms, etc. Peripherals (1) are connected to the central control panel (3) through an ISM network (2). The control panel (3) is also connected to the back-end service (5) through a GSM network (4). Note that alternative wireless technologies may be applied to each of the communication links. In the particular case of the connection between the control panel (3) and the back-end service (5), 3G or 4G technologies may be used. Nevertheless, 3G and 4G modems incorporated in control panels typically scale down to GSM connections when jamming is detected, so protecting GSM network (4) from jamming attacks implicitly protects said 3G and 4G networks. In particular, the ISM network (2) is established over the 868 MHz frequency band (201) (915MHz in America), whereas the GSM network (4) is established over the 900 MHz frequency band (401) and the 1800 MHz frequency band (402).

In Europe, The ISM 868 MHz frequency band (201) comprises the range between 863 MHz and 870 MHz and is used by license-free device. In America the ISM 915MHz frequency band comprises the range between 902 MHz and 928 MHz and is also used by license-free device. The 900 MHz frequency band (401) ranges from 880 MHz to 960 MHz and is used by cell operators for GSM and 3G communications. The 1800 MHz frequency band (402) ranges from 1710 MHz to 1880 MHz and is used by cell operators for GSM and 4G communications. Notice that the security system is independent from the present invention, which only requires the knowledge of the frequency band (or bands) which need to be protected from jamming. Also notice that particular embodiments of the present invention may comprise scanning different frequency bands and/or different communication networks.

A threat to the security system, such as a jammer (6) is also depicted, targeting both the ISM network (2) and the GSM network (4). Both attacks are detected by a jamming detection device (7). The jamming detection device (7) is connected to the back-end service (5) through an ultra narrowband network (8), resilient to jamming. In particular, transmissions over the UNB network (8) are also performed in the 868 MHz frequency band (801). The jamming detection device (7) periodically scans for jamming all the frequency bands used by the security system. When jamming is detected, an alert signal is sent through the UNB network (8) to the back-end service (5). The UNB network (8) may comprise any number of stations receiving the signal simultaneously and sending said signal to the back-end service (5).

Figure 2 presents in further detail the components of the jamming detection device (7), as well as the networks with which the device (7) interacts. The device (7) comprises a transceiver (701) with a local oscillator (702). For example, the transceiver (701) may be a low-current transceiver covering the sub-GHz frequency bands. A single local oscillator (702) is used for both transmission and reception modes, since both do not occur at the same time. In particular, the local oscillator (702) is implemented by combining an integrated voltage-controlled oscillator (VCO) and a $\Delta\Sigma$ fractional-N Phase-Locked Loop (PLL). Since the resulting waveform presents a squared or rectangular shape, its third harmonic component can be used to scan frequency bands above the natural 1 GHz limit of the transceiver (701). When transmitting through UNB network (8), the transceiver (701) applies random frequency hopping and binary-

phase-shift-keying modulation.

5 The device (7) also comprises a processor (703) which coordinates the rest of the elements of the device (7) and implements the decision algorithms leading to the transmission of alarm signals. The processor may be implemented in a computer, a digital signal processor, a field-programmable gate array, an application-specific integrated circuit, a micro-processor, a micro-controller, or any other form of programmable hardware, being preferred the low-consumption integrated options. Furthermore, the processor (703) comprises a computer program which implements
10 the method of the invention when executed, therefore controlling the device of the invention and processing the measured data.

The device (7) comprises several additional sensors and elements that can result in the generation of an alarm signal for other causes beyond jamming detection. In
15 particular, the device (7) comprises a user interface (704), an accelerometer (705), a thermometer (706) and a battery (707). All these elements improve the security of the device (7) itself, and therefore improve its robustness for jamming detection in a synergic manner.

20 In a preferred embodiment, the user interface (704) simply comprises a button and a visual indicator such as a LED light. Nevertheless, alternative embodiments may comprise more complex user interfaces (704) such as screens, touch screens, microphones, speakers, etc. The interface (704) may be used by the user to send alarm messages or any other request through the UNB network (8); as well as to
25 communicate the user the status of the device (7) or any additional information. Notice that there may be particular embodiments in which the user has no active involvement in the operation of the device (7), and therefore the device (7) presents no user interface.

30 The accelerometer (705) prevents the device from being tampered by generating and alarm message when any movement of the device is detected. A first predefined threshold is established to determine whether a measurement of the accelerometer (705) corresponds to normal operation conditions such as vibrations and movement in the room, or to a possible tampering attempt.

The thermometer (706) can generate alarm messages both when an absolute temperature range is exceeded, and when a temperature gradient exceeds some predefined values. The thermometer (706) can be implemented with any temperature sensing technology of the state of the art, as a great precision or tolerance are not required for this purposes. For example, the thermometer (706) can be a temperature sensor with a 2 °C tolerance, generating alarm messages when the measured temperature exceeds 50 °C, is reduced under 0°C, or the temperature gradient exceeds a 10 °C variation within a minute. In order to reduce energy consumption, the thermometer (706) is preferably an on-chip temperature sensor.

The device comprises a battery (707) to guarantee jamming protection even if the electrical network is compromised. Furthermore, the use of a UNB network (8) with random frequency hopping in which most of the signal processing load (such as transmission frequency search and frequency compensations) occurs in the receiving base station and network nodes, greatly reduces energy consumption at the device (7), and therefore increases its autonomy and protection capabilities. Nevertheless, when the battery (707) energy level is reduced below a safety threshold and needs to be charged or replaced, an alarm message may be sent to the back-end service. Additionally or alternatively, a message notifying the user of the low battery (707) energy level can be transmitted through the user interface (704)

Figure 3 presents a particular embodiment of the decision algorithm leading to the transmission of alarm signals in the presence of jamming, implemented by the processor (703) with the data provided by the transceiver (701). The steps of the decision algorithm are periodically performed every T_1 (710), where T_1 is a configurable period with a preferred value of 20 seconds. First, the presence of jamming in the GSM network is checked (711), based on the scans performed by the transceiver (701). In order to determine if the frequency band is being jammed, the average RF power is adaptively measured. When the difference between the measured RF power at a given instant and its moving average exceeds a given threshold, the band is considered to be jammed. Notice that any alternative decision algorithm or signal processing technique may be implemented in order to determine the presence of jamming based on signal power levels in the band under analysis.

If jamming is detected, the device waits for a safety period T_2 before checking again (712). This prevents the system from sending alarm messages for false alarms or transitory interferences. T_2 is a configurable period with a preferred value of 6 seconds.

5 If the jamming continues, an alarm indicating that the GSM network is being jammed is sent (713) to the back-end service (5). Otherwise, if no jamming is initially detected, or the jamming stops before T_2 , no message is sent, and jamming in the ISM network is checked (714). As in the previous case, if jamming is detected, its continuity is checked again after a T_2 interval (715). If jamming is still present in the ISM network, the
10 corresponding alarm message is transmitted (716).

Finally, the content of alarm messages caused by several causes are shown in figure 4. Note that alternative information may be coded in each message according to particular embodiments within the scope of the invention as claimed. Likewise,
15 information coding, field length and other particulars of the communication protocol may be applied. Also note that the device (7) and the back-end service (5) may exchange any additional message beyond alarms, such as keep-alive signals, remote configuration information, statistical data transmission, etc.

20 In the particular embodiment shown in figure 4, all alarm messages comprise a header (901) and a frame type (902), regardless of the nature of the alarm. If needed, they may also comprise an event type (903) that complements the frame type (902) in order to define the purpose of the message. For example, the header may comprise an identifier corresponding to a device or to a plurality of devices in the UNB network (8),
25 and any control information such as information regarding failed transmission attempts. The frame type (902) may identify, for example, if the transmitted message is an alarm, a booting message, a periodic keep-alive message, a debug message, a user command, a network test, or any other kind of message required by a particular embodiment of the protocol. The event type (903) field provides further details
30 regarding the particular frame type (902), such as the nature of the alarm in alarm messages.

The fields of each alarm message depend on the particular nature of the alarm. The corresponding payload of each alarm message may be constant or vary among alarm

messages depending on the particular embodiment of the protocol. For example, a jamming alarm message (9a) is sent as a result of jamming detection through frequency band scans. Its payload comprises an status field (904), that is, an identifier of the frequency band or bands (201, 401, 402) being jammed; and at least
 5 a first numerical value representing a jamming intensity (906), also named 'radio level' in the figure for conciseness. Jamming intensity (906) may be indicated separately for each analysed frequency band (201, 401, 402), and may be represented, for example, by an intensity level measured by the transceiver, or by a number or fraction of channels in which intensity levels exceed a given threshold
 10 and are considered to be rendered unfit for transmission. After the jamming is finalized and normal operation is restored, a second numerical value representing a jamming duration (905) can also be transmitted.

A user-triggered alarm message (9b) is sent as a result of the user interaction with the user interface (704), such as the user pressing a button. The message may comprise
 15 various information useful to the back-end service (5), such as the button duration (907), that is, the length of time the button has been pressed; an accelerometer measurement (908); an status field (904) similar to the jamming alarm message (9a), a battery level (909) and a button level (910) in the case of capacitive buttons.

20 A tamper alarm message (9c) is sent as a result of a measurement of the accelerometer (705) exceeding a threshold. It comprises said accelerometer measurement (908), and it may comprise further information such as the jamming intensity (906) and any further data describing the event detected by the accelerometer
 25 (911). Accelerometer measurement (908) is typically indicated separately for each of the three axis of the accelerometer (705).

A temperature alarm message (9d) typically comprises a thermometer measurement (912), and may comprise further information about the reason of the message in the event type (903) field, such as the alert being caused by a high temperature, a low
 30 temperature or a high temperature gradient. Likewise, a battery alarm message (9e) typically comprises a measurement of the battery level (909), and is transmitted when said battery level (909) is reduced below a safety threshold.

Note that in this text, the term "comprises" and its derivations (such as "comprising", etc.) should not be understood in an excluding sense, that is, these terms should not be interpreted as excluding the possibility that what is described and defined may include further elements, steps, etc.

5

In the context of the present invention, the term "approximately" and terms of its family (such as "approximate", etc.) should be understood as indicating values very near to those which accompany the aforementioned term. That is to say, a deviation within reasonable limits from an exact value should be accepted, because a skilled person in the art will understand that such a deviation from the values indicated is inevitable due to measurement inaccuracies, etc. The same applies to the terms "about" and "around" and "substantially".

10

CLAIMS

1. Jamming detection device (7) comprising a transceiver (701) configured to periodically scan at least a frequency band (201, 401, 402) of a security system to
5 detect jamming, characterized in that, if jamming is detected in the at least one frequency band (201, 401, 402), the transceiver (701) is configured to send an alarm signal to a back-end service (5) through an ultra narrow band network (8).
2. Jamming detection device (7) according to claim 1, characterized in that the
10 transceiver (701) is configured to periodically scan at least a first frequency band (201) of a Industrial Scientific and Medical radio network (2) connecting at least a peripheral (1) and a control panel (3) of the security system.
3. Jamming detection device (7) according to claim 2, characterized in that the at
15 least one first frequency band (201) of the Industrial Scientific and Medical radio network (2) is centred at 868 MHz.
4. Jamming detection device (7) according to any of claims 2 and 3, characterized
20 in that the alarm signal is sent over a second frequency band (801) of the ultra narrow band network (8), being the second frequency band overlapped with the at least one first frequency band (201) of the Industrial Scientific and Medical radio network (2).
5. Jamming detection device (7) according to any of the previous claims,
25 characterized in that the transceiver (701) is configured to periodically scan at least a third frequency band (401, 402) of a Global System for Mobile Communications network (4) connecting the control panel (3) and the back-end service (5) of the security system.
- 30 6. Jamming detection device (7) according to claim 5 characterized in that the transceiver (701) is configured to periodically scan a 900 MHz frequency band (401) and a 1800 MHz frequency band (402) of the Global System for Mobile Communications network (4).

7. Jamming detection device (7) according to any of the previous claims, characterized in that the transceiver (701) comprises a local oscillator (702) configured to generate a plurality of harmonics, being at least one frequency band (201, 401, 402) scanned using a third order harmonic.

5

8. Jamming detection device (7) according to any of the previous claims, characterized in that the transceiver (701) comprises modulation means configured to apply random frequency hopping to the alarm signal when accessing the Ultra Narrowband Network (8).

10

9. Jamming detection device (7) according to any of the previous claims, characterized in that the transceiver (701) comprises modulation means configured to apply a binary-phase-shift-keying modulation to the alarm signal when accessing the Ultra Narrowband Network (8).

15

10. Jamming detection device (7) according to any of the previous claims, characterized in that the transceiver (701) comprises modulation means configured to send the alarm signal through a channel of the Ultra Narrowband Network (8) with a bandwidth lesser or equal than 200 Hz.

20

11. Jamming detection device (7) according to any of the previous claims, characterized in that the device (7) further comprises an accelerometer (705), and in that the transceiver (701) is configured to send an alarm signal to the back-end service (5) through the ultra narrow band network (8) when a measurement of the accelerometer (705) exceeds a first predefined threshold.

25

12. Jamming detection device (7) according to any of the previous claims, characterized in that the device (7) further comprises a thermometer (706), and in that the transceiver (701) is configured to send an alarm signal to the back-end service (5) through the ultra narrow band network (8) when a measurement of the thermometer (706) exceeds a second predefined threshold.

30

13. Jamming detection device (7) according to any of the previous claims, characterized in that the device (7) further comprises a user interface (704), and in

that the transceiver (701) is configured to send an alarm signal to the back-end service (5) through the ultra narrow band network (8) when a user inputs a command through the user interface (704).

- 5 14. Jamming detection method comprising:
 - periodically scanning at least a frequency band (201, 401, 402) of a security system to detect jamming;characterized in that the method further comprises:
 - if jamming is detected in the at least one frequency band (201, 401, 402),
10 sending an alarm signal to a back-end service (5) through an ultra narrow band network (8).

- 15 15. Jamming detection method characterized in that the step of sending the alarm signal further comprises sending an identifier (904) of the at least a frequency band (201, 401, 402) being jammed and at least a first numerical value representing a jamming intensity (906).

ABSTRACT**JAMMING DETECTION METHOD AND DEVICE**

Jamming detection device (7) and method, which scan one or more frequency
5 bands (201, 401, 402) and, if jamming is detected in said frequency bands (201,
401, 402), transmits an alarm signal through an ultra narrow band network (8).
Preferably, both an ISM network (2) connecting a control panel (3) and at least one
peripheral (1), and a GSM network (4) connecting the control panel (3) and a back
end service (5), are scanned. Also preferably, the ultra narrow band network (8) is
10 implemented over the same frequency band (801) as the ISM network (2)
connecting the control panel (3) and the least one peripheral (1).

[Fig. 1]

15

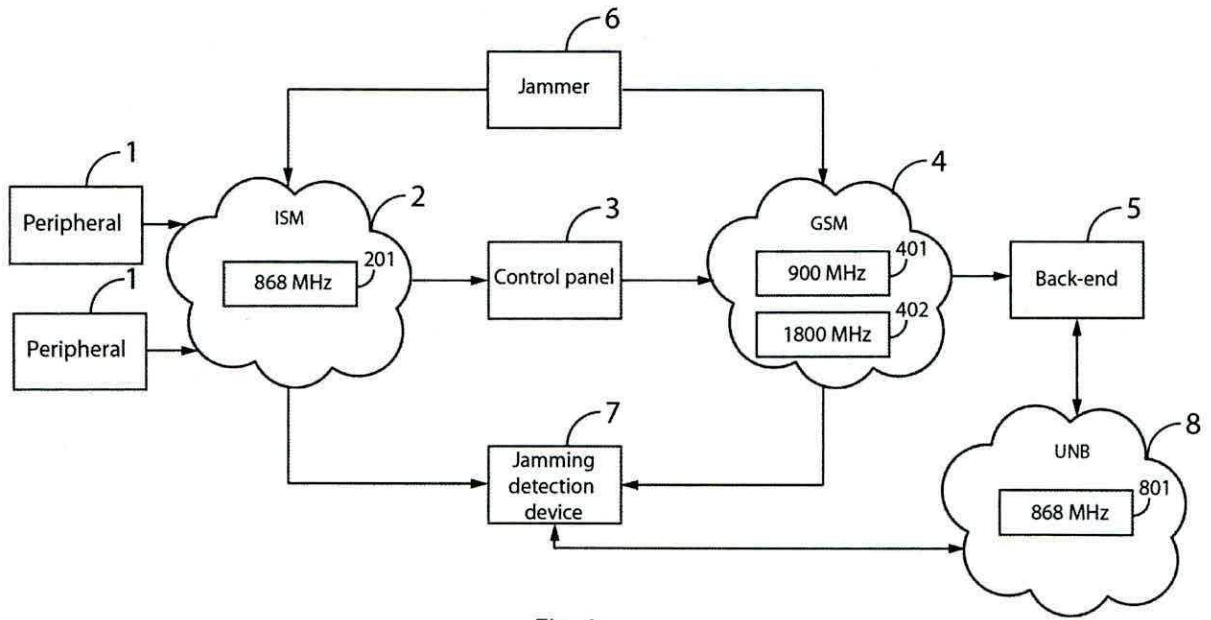


Fig. 1

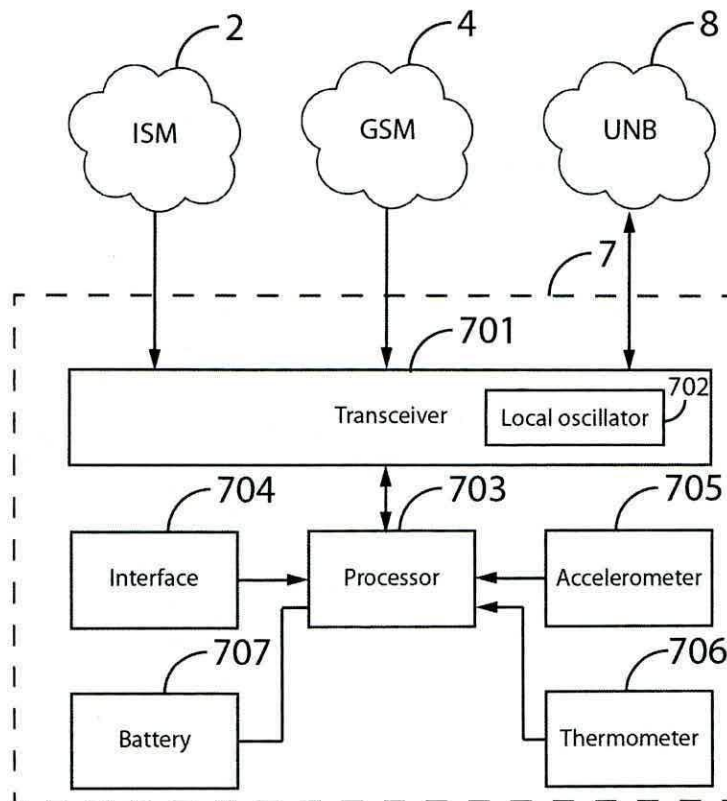


Fig. 2

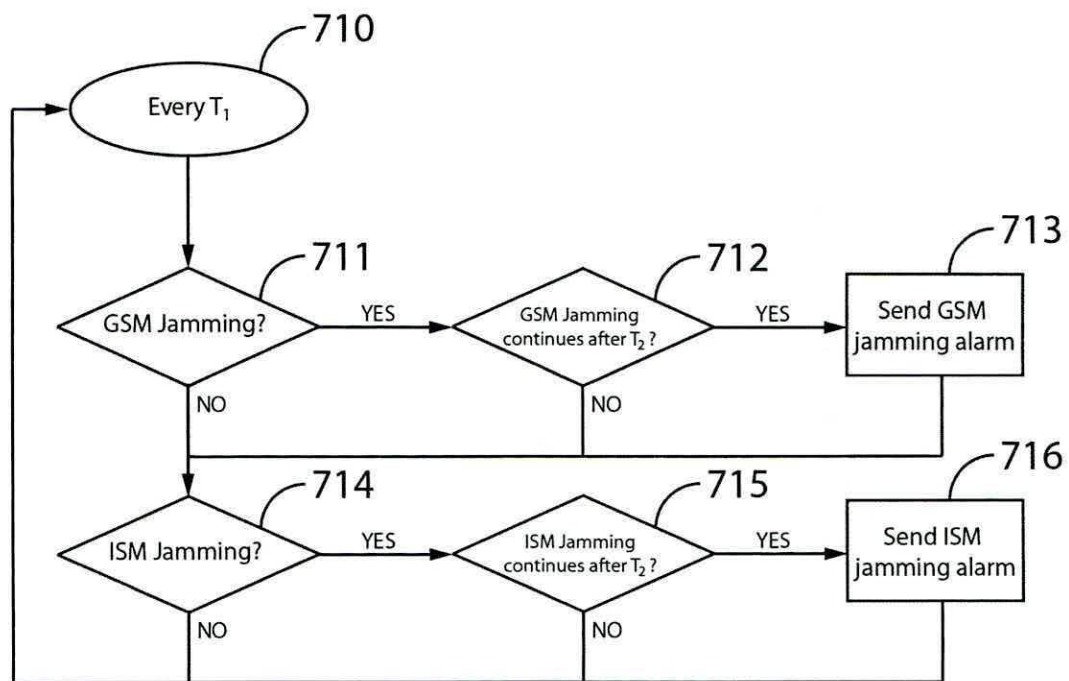


Fig. 3

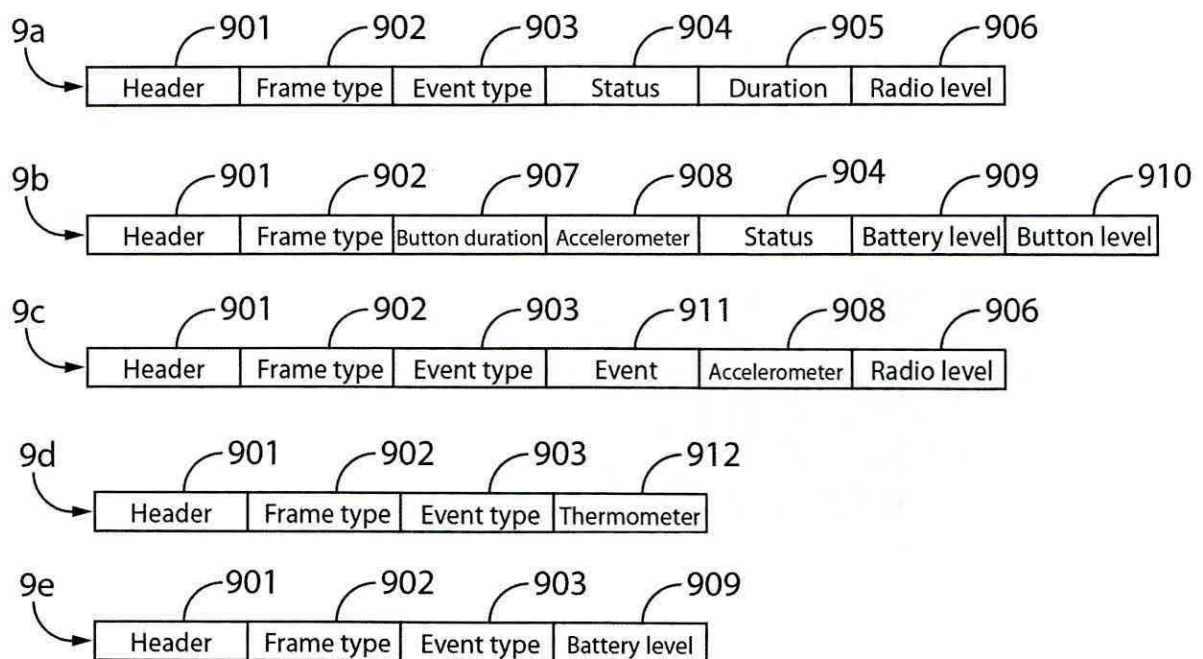


Fig. 4

17
16

Oficina Europea de Patentes

Certificado

Los documentos adjuntos son copias exactas del texto en el cual se describe en las siguientes hojas la solicitud de Patente Europea que ha sido solicitada.

Número de solicitud de Patente.

15382243.2/ EP15382243

El código y número de la organización de su patente prioritaria, para ser usada como solicitud en el extranjero bajo la Convención de París, es EP15382243.

Por el Presidente de la Oficina Europea de Patentes,

(FIRMA)

V. Joseph

18
17

No. de solicitud: 15382243.2

Fecha de solicitud: 08.05.15

Solicitante:

Securitas Direct AB
PO Box 392
201 23 Malmö/SE

Título de la invención: (Si no se muestra ningún título, o si la solicitud ha sido rellena en un idioma no oficial de la EPO, por favor remítase a la descripción para el título original.)

MÉTODO Y DISPOSITIVO DE DETECCIÓN DE INTERFERENCIA DELIBERADA

Prioridad reclamada/Estado/Fecha/Número de solicitud:

Estados designados en la fecha de solicitud:

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

MÉTODO Y DISPOSITIVO DE DETECCIÓN DE INTERFERENCIA DELIBERADA

DESCRIPCIÓN

CAMPO DE LA INVENCION

La presente invención tiene su aplicación en el sector de la seguridad y, especialmente, en el área industrial que participa en proporcionar alarmas de intrusos y robo.

ANTECEDENTES DE LA INVENCION

Los sistemas de seguridad y vigilancia modernos, tales como aquellos que proporcionan alarmas de intrusos o ladrones, comprenden normalmente un panel de control central conectado a una pluralidad de periféricos tales como cámaras de vídeo, micrófonos, sensores de presión, sensores de temperatura, detectores de movimiento, etc. Cuando se detecta una posible amenaza mediante cualquiera de los periféricos, dicho periférico alerta al panel de control central, que a su vez transmite una señal de alerta a un servicio de gestión central remoto. Las comunicaciones entre los periféricos y el panel de control, y entre el panel de control y los servicios de gestión central pueden realizarse a través de sistemas de comunicación cableados o a través de inalámbricos. Sin embargo, las comunicaciones cableadas pueden manipularse fácilmente, desconectando de manera eficaz el sistema de seguridad. Las comunicaciones inalámbricas se consideran por lo tanto como que son más seguras, pero pueden verse sometidas también a ataques a través de interferencia deliberada intencionada. Cuando esto ocurre, el canal de comunicación inalámbrico está interferido de manera activa, que reduce la relación de señal a ruido de las señales transmitidas y que representa comunicación imposible. Aunque menos probable, un escenario similar puede ocurrir como resultado de interferencias no intencionadas desde sistemas de frecuencia de radio cercanos.

Para establecer defensas frente a este tipo de interferencia deliberada accidental o activa, se han propuesto varias alternativas en el estado de la técnica. Por ejemplo, el documento de patente GB-2457102-A divulga un sistema de detección de intrusos donde la señal de alarma se transmite inalámbricamente. En caso de interferencia deliberada, se detecta la interferencia mediante un sensor, y la frecuencia de

transmisión se modifica para evitar el intervalo de frecuencia de interferencia deliberada. Sin embargo, modificar la frecuencia puede no ser suficiente para evitar la interferencia deliberada. Si el intruso gestiona para interferir deliberadamente por completo toda la banda de frecuencias en la que puede sintonizarse dicha frecuencia de transmisión, tampoco se recibirá la señal de alarma.

El documento de patente US-2014/0369452-A1 presenta un enfoque alternativo basado en un enlace de comunicación multi-canal entre el transmisor y el receptor de una red de sistema de satélite de navegación global (GNSS). Cuando se detecta interferencia deliberada, el número de canales usados para transmisión de datos se reduce progresivamente, aumentando la resistencia de interferencia deliberada. Independientemente, este enfoque no podría aplicarse de manera directa a redes de comunicación inalámbrica usadas en sistemas de seguridad tales como las redes de radio Industrial, Científica y Médica (ISM) y redes del Sistema Global para Comunicaciones Móviles (GSM). Adicionalmente, la máxima protección de interferencia deliberada conseguible está limitada por el ancho de banda del canal de la arquitectura de la red usada para el enlace de comunicación, que podría resultar ser insuficiente en algunos escenarios.

Finalmente, el documento de patente US-4117405-A1 divulga un sistema de transmisión de alarma que se basa en una red de banda ultra estrecha (UNB), dada su resistencia intrínseca frente a interferencias deliberadas. El sistema comprende una pluralidad de estaciones de alarma, cada una de las cuales está bloqueada a un oscilador local ajustado con precisión. Se asigna una frecuencia de oscilador local distintiva a cada estación de alarma. Sin embargo, aunque se incorpora alguna resistencia a interferencia deliberada, la presencia real de interferencia deliberada no se comprueba ni notifica al servicio de gestión central, proporcionando por lo tanto a los intrusos más libertad durante su intento de manipulación. Adicionalmente, usando una frecuencia fija en cada estación, el sistema es más predecible y fácilmente manipulable, y requiere que se empleen recursos significativos en la calibración y correcciones de desvío de frecuencia. Finalmente, las redes UNB están diseñadas para servicios multi-punto a punto en los que cada elemento raramente necesita acceder al medio de comunicación. Usando la UNB por defecto en todas las comunicaciones entre elementos del sistema de seguridad limita el tráfico total y el número de estaciones de alarma desplegables.

21
20

Por lo tanto, existe aún la necesidad en el estado de la técnica de una técnica de detección de interferencia deliberada que proteja eficazmente sistemas de seguridad frente a interferencia deliberada agresiva de sus comunicaciones inalámbricas. Adicionalmente, es deseable aún que dicha técnica de detección de interferencia deliberada no limite el número de elementos conectados al servicio de gestión central o a la carga de datos entre ellos cuando no está presente interferencia deliberada, y que presente un consumo de energía reducido para autonomía aumentada, y por lo tanto, una protección más prolongada y fiable.

10 SUMARIO DE LA INVENCION

La invención actual resuelve todos los problemas anteriormente mencionados divulgando un detector de interferencia deliberada que se basa en una red de banda ultra estrecha para transmisión de señal de alarma en presencia de interferencia deliberada, sin afectar la operación normal de dicho sistema de seguridad cuando no está presente interferencia deliberada.

En un primer aspecto de la invención, se divulga un dispositivo de detección de interferencia deliberada. El dispositivo comprende un transceptor configurado para explorar periódicamente una o más bandas de frecuencia usadas para transmisión de señal entre elementos de un sistema de seguridad tal como un sistema de alerta de intrusos o robo. Cuando se detecta interferencia deliberada en al menos una de dichas bandas de frecuencia, el dispositivo está configurado para enviar una señal de alarma a través de una red de banda ultra estrecha, significativamente más resistente a interferencia deliberada maliciosa que las redes convencionales.

25

Preferentemente, el dispositivo está configurado para explorar periódicamente las siguientes redes:

- 5 - Una red de radio Industrial, Científica y Médica (ISM) que conecta uno o más periféricos del sistema de seguridad y un panel de control central instalado en la misma localización que los periféricos. Los periféricos pueden comprender detectores tales como cámaras de vídeo, sensores de temperatura, sensores de movimiento, etc.; alarmas tales como indicadores visuales o sistemas de sonido; dispositivos activados por usuario, o cualquier otro dispositivo asociado al sistema de seguridad. Más preferentemente, la red ISM se establece sobre la banda de 10 868 MHz para comunicaciones de radio en Europa y en la banda de 915 MHz en Estados Unidos.
- 15 - Una red del Sistema Global para Comunicaciones Móviles (GSM) que conecta el panel de control y un servicio de gestión central remoto del sistema de seguridad, normalmente usada para transmisión de señal de alarma en ausencia de 15 interferencia deliberada. Más preferentemente, el dispositivo explora tanto las bandas de frecuencia de 900 MHz como de 1800 MHz de la red de GSM para la presencia de interferencia deliberada.

También preferentemente, la red de banda ultra estrecha (UNB) usada mediante el dispositivo para transmitir la señal de alarma se establece en una banda de 20 frecuencia que solapa parcial o completamente la red de radio de ISM que conecta los periféricos y el panel de control. De acuerdo con la opción preferida anteriormente mencionada para dicha red ISM, la red de banda ultra estrecha se establece sobre la banda de frecuencia de radio de 868 MHz.

Para poder explorar todas las bandas de frecuencia relevantes con el mismo 25 transceptor, dicho transceptor preferentemente comprende un oscilador local que genera múltiples armónicos de su frecuencia principal. Por ejemplo, este puede implementarse con un oscilador local que genera una señal con una forma de onda rectangular, que da como resultado una generación de armónico de tercer orden significativo. Esto posibilita explorar diferentes bandas de frecuencia sintonizando 30 diferentes armónicos de la señal generada. En el mismo ejemplo, el armónico de primer orden puede usarse para explorar la banda de 868 MHz de la red ISM y la banda de 900 MHz de la red de GSM, mientras que el armónico de tercer orden se

usa para explorar la banda de 1800 MHz de dicha red de GSM.

Algunas opciones preferidas para control de acceso al medio y modulación de señal para la transmisión de señal de alarma en la red de banda ultra estrecha incluyen salto de frecuencia aleatoria y modulación por desplazamiento de fase binaria. Como
5 resultado, la señal de alarma se transmite preferentemente usando un ancho de banda de señal igual o menor de 200 Hz. La frecuencia central de dicho ancho de banda se elige aleatoriamente en una banda de 200 KHz de la red de UNB. Dado este ancho de banda de señal extremadamente estrecha y la no capacidad de predicción de la frecuencia precisa sobre la que se transmite la señal de alarma, los
10 sistemas de interferencia deliberada activos no pueden interferir con la operación de la red de UNB.

Cuando se detecta interferencia deliberada durante la exploración de las diferentes bandas de frecuencia, la señal de alarma generada mediante el dispositivo comprende preferentemente un identificador de al menos una banda de frecuencia
15 que está interfiriéndose deliberadamente y un primer valor numérico que representa una intensidad de interferencia deliberada. El primer valor numérico puede ser, por ejemplo, una medición de intensidad de señal de frecuencia de radio, o un número de canales de una banda de frecuencia en la que la intensidad medida supera un umbral dado. Una vez que el dispositivo detecta que la interferencia deliberada ha finalizado,
20 se genera también una señal de alarma que comprende un segundo valor numérico que indica la duración de la interferencia deliberada.

Adicionalmente, el dispositivo de detección de interferencia deliberada puede incluir características adicionales que pueden generar señales de alarma que se transmiten a través de la red de UNB:

- 25 - Un acelerómetro para detección de manipulación. Cuando una medición del acelerómetro supera al menos un primer umbral, se genera un mensaje de alarma. Esto evita que cualquier intruso desactive manualmente el dispositivo de detección de interferencia deliberada antes de intentar interferir deliberadamente las comunicaciones del sistema de seguridad.
- 30 - Un termómetro. Cuando una medición del acelerómetro supera al menos un segundo umbral, se genera un mensaje de alarma. Dicho segundo umbral puede

delimitar un intervalo de temperatura absoluta, o puede aplicarse a un gradiente de temperatura que combina múltiples mediciones de termómetro.

- Una interfaz de usuario que posibilita a un usuario del sistema de seguridad enviar mensajes de alarma en cualquier momento deseado. La interfaz puede ser tan sencilla como un botón que el usuario puede presionar durante un escenario de riesgo, o incluir capacidades de entrada y salida más complejas tales como pantallas, micrófonos, etc. Esta característica también posibilita al usuario comprobar que las comunicaciones de UNB funcionan apropiadamente.

En otro aspecto de la presente invención, se divulga un método para detección de interferencia deliberada en un sistema de seguridad. El método comprende las siguientes etapas:

- Explorar al menos una banda de frecuencia de un sistema de seguridad para detectar interferencia deliberada. Las bandas de frecuencia exploradas preferentemente comprenden una banda de frecuencia de 868 MHz (o 915 MHz en Estados Unidos) en una red ISM que conecta un panel de control y los periféricos, y unas bandas de frecuencia de 900 MHz y de 1800 MHz en una red de GSM que conecta el panel de control y los servicios de gestión central.

- Cuando se detecta interferencia deliberada durante las exploraciones de banda de frecuencia, se envía una señal de alarma al servicio de gestión central a través de una red de banda ultra estrecha. Esta etapa puede comprender preferentemente aplicar salto de frecuencia aleatoria y/o modulación por desplazamiento de fase binaria a la señal de alarma transmitida. Preferentemente, esta etapa comprende transmitir la señal de alarma a través de un canal con un ancho de banda de 200 Hz o menor. Adicionalmente, esta etapa puede comprender incluir en la señal de alarma un identificador de al menos una banda de frecuencia que se está interfiriendo deliberadamente, un primer valor numérico que representa una intensidad de interferencia deliberada. Cuando se determina que ha finalizado la interferencia deliberada, se transmite también un segundo valor numérico que representa una duración de interferencia deliberada.

- Preferentemente, el método comprende adicionalmente medir un desplazamiento de un acelerómetro y transmitir una señal de alarma a través de la red de UNB cuando

dicho desplazamiento supera un primer umbral.

Preferentemente, el método comprende adicionalmente medir una temperatura de un termómetro y transmitir una señal de alarma a través de la red de UNB cuando dicha temperatura supera un segundo umbral. Dicho segundo umbral puede ser un
5 intervalo de temperatura absoluta y/o un intervalo de gradiente de temperatura.

Preferentemente, el método comprende adicionalmente transmitir una señal de alarma a través de la red de UNB cuando se recibe un comando de usuario a través de una interfaz de usuario.

Con el método y dispositivo divulgados, los sistemas de seguridad y vigilancia se
10 hacen más resistentes a interferencia deliberada intencionada o accidental de sus comunicaciones inalámbricas. Cuando no está presente interferencia deliberada, el método y dispositivo no imponen ninguna limitación en la operación normal del sistema de seguridad. El detector de interferencia deliberada está protegido también de manipulación física del dispositivo, así como de cambios de temperatura
15 repentinos producidos, por ejemplo, por un fuego cercano o desde ciertos instrumentos de manipulación. Adicionalmente, la red de banda ultra estrecha divulgada optimiza enormemente el consumo de energía durante la transmisión de datos hacia la estación base, aumentando por lo tanto la autonomía del dispositivo de detección de interferencia deliberada. Estas y otras ventajas serán evidentes a la luz
20 de la descripción detallada de la invención.

Se harán evidentes ventajas y características adicionales de la invención a partir de la descripción detallada que sigue y que se señalarán particularmente en las reivindicaciones adjuntas.

25 BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para el fin de ayudar al entendimiento de las características de la invención, de acuerdo con una realización práctica preferida de la misma y para complementar esta descripción, se adjuntan las siguientes figuras como una parte integral de la misma, teniendo un carácter ilustrativo y no limitante:

La Figura 1 muestra un escenario esquemático al que se aplica el dispositivo de detección de interferencia deliberada de la invención, de acuerdo con una realización particular del mismo.

5 La Figura 2 presenta con mayor detalle los componentes comprendidos mediante el dispositivo de detección de interferencia deliberada de acuerdo con una realización particular del mismo.

La Figura 3 representa un diagrama de flujo simplificado de un algoritmo de detección de interferencia deliberada de acuerdo con una realización particular del dispositivo y el método de la invención.

10 La Figura 4 ilustra una posible codificación de las señales de alarma enviadas mediante el dispositivo y método de detección de interferencia deliberada de acuerdo con una realización particular de los mismos.

DESCRIPCIÓN DETALLADA DE LA INVENCION

15 Las materias definidas en esta descripción detallada se proporcionan para ayudar a un entendimiento comprensivo de la invención. Por consiguiente, los expertos en la materia reconocerán que pueden realizarse cambios de variación y modificaciones de las realizaciones descritas en el presente documento sin alejarse del alcance y espíritu de la invención. En particular, obsérvese que cualquier realización o característica particular del dispositivo de la invención puede aplicarse al método de
20 la invención y viceversa. También, se omite la descripción de funciones y elementos bien conocidos por claridad y brevedad.

En este texto, la expresión "red de banda ultra estrecha" se refiere a cualquier red inalámbrica en la que el espectro de una señal transmitida está confinado a un pequeño intervalo espectral, estando dicho intervalo espectral activamente limitado a
25 través de técnicas de modulación de señal y/o procesamiento de señal. La red de banda ultra estrecha es por lo tanto una red con un ancho de banda de transmisión más estrecho y resistencia aumentada frente a interferencia deliberada que cualquier otra red usada para comunicaciones en el sistema de seguridad. Una red de banda ultra estrecha puede definirse teniendo una relación entre un ancho de banda de
30 canal y el ancho de banda de frecuencia total de la red de UNB por debajo de un

umbral dado. Como alternativa, la red de UNB puede definirse teniendo una relación entre el ancho de banda del canal y la frecuencia de portadora por debajo de un umbral dado, o teniendo un ancho de banda del canal absoluto por debajo de otro umbral dado. En las realizaciones particulares divulgadas en el presente documento, se usa un ancho de banda de canal de 200 Hz o menos.

Obsérvese que los intervalos específicos de las bandas de frecuencia mencionadas en esta descripción pueden someterse a cambios de acuerdo con cada realización particular y a los reglamentos de cada país particular. Obsérvese también que en las realizaciones preferidas de la invención, el dispositivo de detección de interferencia deliberada se describe por simplicidad como un dispositivo independiente. Independientemente, sus componentes y características podrían integrarse también en otros componentes del sistema de seguridad, tal como el panel de control principal o cualquier sensor de intrusos periférico.

La Figura 1 representa esquemáticamente los principales elementos de un escenario en el que se aplican realizaciones particulares del método y dispositivo de detección de interferencia deliberada de la invención, en concreto un sistema de seguridad inalámbrico donde se intenta una interferencia deliberada maliciosa. El sistema de seguridad comprende una pluralidad de periféricos (1) tal como cámaras de vídeo, micrófonos, sensores de presión, sensores de temperatura, alarmas, etc. Los periféricos (1) están conectados al panel de control (3) central a través de una red ISM (2). El panel de control (3) está conectado también al servicio de gestión central (5) a través de una red de GSM (4). Obsérvese que pueden aplicarse tecnologías inalámbricas alternativas a cada uno de los enlaces de comunicación. En el caso particular de la conexión entre el panel de control (3) y el servicio de gestión central (5), pueden usarse tecnologías de 3G o 4G. Independientemente, los módems de 3G y 4G incorporados en paneles de control normalmente escalan hacia abajo a conexiones de GSM cuando se detecta interferencia deliberada, por lo que proteger la red de GSM (4) de ataques de interferencia deliberada protege implícitamente dichas redes de 3G y 4G. En particular, la red ISM (2) se establece sobre la banda de frecuencia (201) de 868 MHz (915 MHz en Estados Unidos), mientras que la red de GSM (4) se establece sobre la banda de frecuencia (401) de 900 MHz y la banda de frecuencia (402) de 1800 MHz.

28
27

En Europa, la banda de frecuencia (201) de 868 MHz ISM comprende el intervalo entre 863 MHz y 870 MHz y se usa mediante dispositivos de licencia libre. En Estados Unidos la banda de frecuencia de 915 MHz ISM comprende el intervalo entre 902 MHz y 928 MHz y se usa también mediante dispositivos de licencia libre. La
5 banda de frecuencia (401) de 900 MHz varía de 880 MHz a 960 MHz y se usa mediante operadores celulares para comunicaciones de GSM y de 3G. La banda de frecuencia (402) de 1800 MHz varía de 1710 MHz a 1880 MHz y se usa mediante operadores celulares para comunicaciones de GSM y de 4G. Obsérvese que el sistema de seguridad es independiente de la presente invención, que únicamente
10 requiere el conocimiento de la banda (o bandas) de frecuencia que necesitan protegerse de interferencia deliberada. Obsérvese también que las realizaciones particulares de la presente invención pueden comprender explorar diferentes bandas de frecuencia y/o diferentes redes de comunicaciones.

Se representa también una amenaza para el sistema de seguridad, tal como un
15 equipo interferente (6), que se dirige tanto a la red ISM (2) como a la red de GSM (4). Ambos ataques se detectan mediante un dispositivo de detección de interferencia deliberada (7). El dispositivo de detección de interferencia deliberada (7) está conectado al servicio de gestión central (5) a través de una red de banda ultra estrecha (8), resistente a interferencia deliberada. En particular, las transmisiones a
20 través de la red de UNB (8) se realizan también en la banda de frecuencia (801) de 868 MHz. El dispositivo de detección de interferencia deliberada (7) explora periódicamente interferencias deliberadas por todas las bandas de frecuencia usadas mediante el sistema de seguridad. Cuando se detecta interferencia deliberada, se envía una señal de alerta a través de la red de UNB (8) al servicio de gestión central
25 (5). La red de UNB (8) puede comprender cualquier número de estaciones que reciben la señal simultáneamente y que envían dicha señal al servicio de gestión central (5).

La Figura 2 presenta en mayor detalle los componentes del dispositivo de detección de interferencia deliberada (7), así como las redes en las que interactúa el dispositivo
30 (7). El dispositivo (7) comprende un transceptor (701) con un oscilador local (702). Por ejemplo, el transceptor (701) puede ser un transceptor de baja corriente que cubre las bandas de frecuencia por debajo del GHz. Un único oscilador local (702) se usa para tanto los modos de transmisión como de recepción, puesto que ambos no

ocurren al mismo tiempo. En particular, el oscilador local (702) está implementado combinando un oscilador controlado por tensión integrado (VCO) y un oscilador enganchado en fase (PLL) fraccional-N $\Delta\Sigma$. Puesto que la forma de onda resultante presenta una forma cuadrada o rectangular, su tercer componente armónico puede usarse para explorar bandas de frecuencia por encima del límite de 1 GHz natural del transceptor (701). Cuando se transmite a través de la red de UNB (8), el transceptor (701) aplica salto de frecuencia aleatoria y modulación por desplazamiento de fase binaria.

El dispositivo (7) comprende también un procesador (703) que coordina el resto de los elementos del dispositivo (7) e implementa los algoritmos de decisión que conducen a la transmisión de las señales de alarma. El procesador puede implementarse en un ordenador, un procesador de señales digitales, un campo de matriz de puertas programables, un circuito integrado específico de la aplicación, un micro-procesador, un micro-controlador o cualquier otra forma de hardware programable, siendo preferidas las opciones integradas de bajo consumo. Adicionalmente, el procesador (703) comprende un programa informático que implementa el método de la invención cuando se ejecuta, controlando por lo tanto el dispositivo de la invención y procesando los datos medidos.

El dispositivo (7) comprende varios sensores y elementos adicionales que pueden dar como resultado la generación de una señal de alarma para otras causas más allá de la detección de interferencia deliberada. En particular, el dispositivo (7) comprende una interfaz de usuario (704), un acelerómetro (705), un termómetro (706) y una batería (707). Todos estos elementos mejoran la seguridad del propio dispositivo (7), y por lo tanto mejora su robustez para detección de interferencia deliberada de una manera sinérgica.

En una realización preferida, la interfaz de usuario (704) comprende simplemente un botón y un indicador visual tal como una luz LED. Independientemente, realizaciones alternativas pueden comprender interfaces de usuario (704) más complejas tales como pantallas, pantallas táctiles, micrófonos, altavoces, etc. La interfaz (704) puede usarse mediante el usuario para enviar mensajes de alarma o cualquier otra solicitud a través de la red de UNB (8); así como para comunicar al usuario el estado del dispositivo (7) o cualquier información adicional. Obsérvese que pueden existir

30
29

realizaciones particulares en las que el usuario no tiene implicación activa en la operación del dispositivo (7), y por lo tanto el dispositivo (7) no presenta interfaz de usuario.

5 El acelerómetro (705) evita que se manipule el dispositivo generando un mensaje de alarma cuando se detecta cualquier movimiento del dispositivo. Se establece un primer umbral predefinido para determinar si una medición del acelerómetro (705) corresponde a condiciones de operación normal tales como vibraciones y movimiento en la sala, o a un posible intento de manipulación.

10 El termómetro (706) puede generar mensajes de alarma tanto cuando se supera un intervalo de temperatura absoluta, como cuando un gradiente de temperatura supera algunos valores predefinidos. El termómetro (706) puede implementarse con cualquier tecnología de detección de temperatura del estado de la técnica, ya que no se requiere una enorme precisión o tolerancia para estos fines. Por ejemplo, el termómetro (706) puede ser un sensor de temperatura con una tolerancia de 2 °C,
15 que genera mensajes de alarma cuando la temperatura medida supera 50 °C, se reduce por debajo de 0 °C, o el gradiente de temperatura supera una variación de 10 °C en un minuto. Para reducir el consumo de energía, el termómetro (706) es preferentemente un sensor de temperatura en chip.

20 El dispositivo comprende una batería (707) para garantizar protección de interferencia deliberada incluso si la red eléctrica está comprometida. Adicionalmente, el uso de una red de UNB (8) con salto de frecuencia aleatoria en la que la mayoría de la carga de procesamiento de señal (tal como búsqueda de frecuencia de transmisión y compensaciones de frecuencia) ocurre en la estación base y nodos de red de recepción, reduce enormemente el consumo de energía en el dispositivo (7), y por lo
25 tanto aumenta su autonomía y capacidades protección. Independientemente, cuando el nivel de energía de la batería (707) se reduce por debajo de un umbral de seguridad y necesita cargarse o sustituirse, puede enviarse un mensaje de alarma al servicio de gestión central. Adicionalmente o como alternativa, puede transmitirse un mensaje que notifica al usuario del bajo nivel de energía de la batería (707) a través
30 de la interfaz de usuario (704).

La Figura 3 presenta una realización particular del algoritmo de decisión que conduce a la transmisión de señales de alarma en la presencia de interferencia deliberada,

implementado mediante el procesador (703) con los datos proporcionados mediante el transceptor (701). Las etapas del algoritmo de decisión se realizan periódicamente cada T_1 (710), donde T_1 es un periodo configurable con un valor preferido de 20 segundos. En primer lugar, se comprueba (711) la presencia de interferencia deliberada en la red de GSM, basándose en las exploraciones realizadas mediante el transceptor (701). Para determinar si la banda de frecuencia está interfiriéndose deliberadamente, se mide adaptivamente la potencia de RF media. Cuando la diferencia entre la potencia de RF medida en un instante dado y su media móvil supera un umbral dado, la banda se considera que está interferida deliberadamente.

5

10

Obsérvese que puede implementarse cualquier algoritmo de decisión alternativo o técnica de procesamiento de señal para determinar la presencia de interferencia deliberada basándose en niveles de potencia de señal en la banda bajo análisis.

Si se detecta interferencia deliberada, el dispositivo espera durante un periodo de seguridad T_2 antes de comprobar de nuevo (712). Esto evita que el sistema envíe mensajes de alarma por alarmas falsas o interferencias transitorias. T_2 es un periodo configurable con un valor preferido de 6 segundos. Si la interferencia deliberada continúa, una alarma que indica que la red de GSM se está interfiriendo deliberadamente se envía (713) al servicio de gestión central (5). De otra manera, si no se detecta inicialmente interferencia deliberada, o la interferencia deliberada se detiene antes de T_2 , no se envía mensaje, y se comprueba (714) la red ISM. Como en el caso anterior, si se detecta interferencia deliberada, se comprueba su continuidad de nuevo después de un intervalo (715) T_2 . Si la interferencia deliberada aún está presente en la red ISM, se transmite (716) el correspondiente mensaje de alarma.

15

20

Finalmente, se muestra el contenido de los mensajes de alarma producidos por varias causas en la Figura 4. Obsérvese que puede codificarse información alternativa en cada mensaje de acuerdo con realizaciones particulares dentro del alcance de la invención como se reivindica. De manera similar, puede aplicarse codificación de información, longitud de campo y otras particularidades del protocolo de comunicación. También obsérvese que el dispositivo (7) y el servicio de gestión central (5) pueden intercambiar cualquier mensaje adicional más allá de alarmas, tales como señales de mantenimiento de conexión, información de configuración remota, transmisión de datos estadísticos, etc.

25

30

- En la realización particular mostrada en la figura 4, todos los mensajes de alarma comprenden un encabezamiento (901) y un tipo de trama (902), independientemente de la naturaleza de la alarma. Si fuera necesario, pueden comprender también un tipo de evento (903) que complementa el tipo de trama (902) para definir el fin del mensaje. Por ejemplo, el encabezamiento puede comprender un identificador que corresponde a un dispositivo o a una pluralidad de dispositivos en la red de UNB (8), y cualquier información de control tal como información en relación con intentos de transmisión fallidos. El tipo de trama (902) puede identificar, por ejemplo, si el mensaje transmitido es una alarma, un mensaje de arranque, un mensaje de mantenimiento de conexión periódico, un mensaje de depuración, un comando de usuario, una prueba de red o cualquier otro tipo de mensaje requerido mediante una realización particular del protocolo. El campo tipo de evento (903) proporciona detalles adicionales en relación con el tipo de trama (902) particular, tal como la naturaleza de la alarma en los mensajes de alarma.
- 15 Los campos de cada mensaje de alarma dependen de la naturaleza particular de la alarma. La cabida útil correspondiente de cada mensaje de alarma puede ser constante o variar entre mensajes de alarma dependiendo de la realización particular del protocolo. Por ejemplo, un mensaje de alarma de interferencia deliberada (9a) se envía como resultado de detección de interferencia deliberada a través de exploraciones de banda de frecuencia. Su cabida útil comprende un campo de estado (904), es decir, un identificador de la banda o bandas de frecuencia (201, 401, 402) que están interfiriéndose deliberadamente; y al menos un primer valor numérico que representa una intensidad de interferencia deliberada (906), también denominado 'nivel de radio' en la figura por brevedad. La intensidad de interferencia deliberada (906) puede indicarse por separado para cada banda de frecuencia (201, 401, 402) analizada, y puede representarse, por ejemplo, mediante un nivel de intensidad medido mediante el transceptor, o mediante un número o fracción de canales en los que los niveles de intensidad superan un umbral dado y se considera que se presentan inadecuados para transmisión. Después de que finaliza la interferencia deliberada y se restaura la operación normal, puede transmitirse también un segundo valor numérico que representa una duración de interferencia deliberada (905).
- 20
- 25
- 30

Un mensaje de alarma accionado por el usuario (9b) se envía como resultado de la interacción del usuario con la interfaz de usuario (704), tal como que el usuario

5 presione un botón. El mensaje puede comprender diversa información útil para el servicio de gestión central (5), tal como la duración del botón (907), es decir, la longitud de tiempo que se ha presionado el botón; una medición de acelerómetro (908); un campo de estado (904) similar al del mensaje de alarma de interferencia deliberada (9a), un nivel de batería (909) y un nivel de botón (910) en el caso de botones capacitivos.

10 Un mensaje de manipulación de alarma (9c) se envía como resultado de una medición del acelerómetro (705) que supera un umbral. Comprende dicha medición de acelerómetro (908), y puede comprender información adicional tal como la intensidad de interferencia deliberada (906) y cualquier dato adicional que describe el evento detectado mediante el acelerómetro (911). La medición del acelerómetro (908) se indica normalmente por separado para cada uno de los tres ejes del acelerómetro (705).

15 Un mensaje de alarma de temperatura (9d) normalmente comprende una medición de termómetro (912), y puede comprender información adicional acerca de la razón del mensaje en el campo de tipo de evento (903), tal como la alerta que se produjo mediante una alta temperatura, una baja temperatura o un alto gradiente de temperatura. De manera similar, un mensaje de alarma de batería (9e) normalmente comprende una medición del nivel (909) de la batería, y se transmite cuando dicho
20 nivel de batería (909) se reduce por debajo de un umbral de seguridad.

Obsérvese que en este texto, el término "comprende" y sus derivaciones (tales como "que comprende", etc.) no deberían entenderse en un sentido excluyente, es decir, estos términos no deberían interpretarse como que excluyen la posibilidad de lo que se describe y define pueda incluir elementos adicionales, etapas, etc.

25 En el contexto de la presente invención, el término "aproximadamente" y los términos de su familia (tal como "aproximado", etc.) deberían entenderse como que indican valores muy cercanos a aquellos que acompañan el término anteriormente mencionado. Es decir, debería aceptarse una desviación dentro de límites razonables a partir de un valor exacto, puesto que un experto en la materia entenderá que una
30 desviación de este tipo a partir de los valores indicados es inevitable debido a las imprecisiones de las mediciones, etc. Lo mismo se aplica a los términos "acerca de" y "alrededor" y "sustancialmente".

REIVINDICACIONES

1. Dispositivo de detección de interferencia deliberada (7) que comprende un transceptor (701) configurado para explorar periódicamente al menos una banda de frecuencia (201, 401, 402) de un sistema de seguridad para detectar interferencia deliberada, caracterizado por que, si se detecta interferencia deliberada en la al menos una banda de frecuencia (201, 401, 402), el transceptor (701) está configurado para enviar una señal de alarma a un servicio de gestión central (5) a través de una red de banda ultra estrecha (8).
2. Dispositivo de detección de interferencia deliberada (7) de acuerdo con la reivindicación 1, caracterizado por que el transceptor (701) está configurado para explorar periódicamente al menos una primera banda de frecuencia (201) de una red de radio Industrial, Científica y Médica (2) que conecta al menos un periférico (1) y un panel de control (3) del sistema de seguridad.
3. Dispositivo de detección de interferencia deliberada (7) de acuerdo con la reivindicación 2, caracterizado por que la al menos una primera banda de frecuencia (201) de la red de radio Industrial, Científica y Médica (2) está centrada en 868 MHz.
4. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las reivindicaciones 2 y 3, caracterizado por que la señal de alarma se envía sobre una segunda banda de frecuencia (801) de la red de banda ultra estrecha (8), estando la segunda banda de frecuencia solapada con la al menos una primera banda de frecuencia (201) de la red de radio Industrial, Científica y Médica (2).
5. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por que el transceptor (701) está configurado para explorar periódicamente al menos una tercera banda de frecuencia (401, 402) de una red del Sistema Global para Comunicaciones Móviles (4) que conecta el panel de control (3) y el servicio de gestión central (5) del sistema de seguridad.
6. Dispositivo de detección de interferencia deliberada (7) de acuerdo con la reivindicación 5, caracterizado por que el transceptor (701) está configurado para explorar periódicamente una banda de frecuencia (401) de 900 MHz y una banda de

frecuencia (402) de 1800 MHz de la red del Sistema Global para Comunicaciones Móviles (4).

7. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por que el transceptor (701) comprende un oscilador local (702) configurado para generar una pluralidad de armónicos, explorándose al menos una banda de frecuencia (201, 401, 402) usando un armónico de tercer orden.

8. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por que el transceptor (701) comprende medios de modulación configurados para aplicar salto de frecuencia aleatoria a la señal de alarma cuando se accede a la red de banda ultra estrecha (8).

9. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por que el transceptor (701) comprende medios de modulación configurados para aplicar una modulación por desplazamiento de fase binaria a la señal de alarma cuando se accede a la red de banda ultra estrecha (8).

10. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por que el transceptor (701) comprende medios de modulación configurados para enviar la señal de alarma a través de un canal de la red de banda ultra estrecha (8) con un ancho de banda menor o igual de 200 Hz.

11. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por que el dispositivo (7) comprende adicionalmente un acelerómetro (705), y por que el transceptor (701) está configurado para enviar una señal de alarma al servicio de gestión central (5) a través de la red de banda ultra estrecha (8) cuando una medición del acelerómetro (705) supera un primer umbral predefinido.

12. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por que el dispositivo (7) comprende adicionalmente un termómetro (706), y por que el transceptor (701) está

configurado para enviar una señal de alarma al servicio de gestión central (5) a través de la red de banda ultra estrecha (8) cuando una medición del termómetro (706) supera un segundo umbral predefinido.

5 13. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las reivindicaciones anteriores, caracterizado por que el dispositivo (7) comprende adicionalmente una interfaz de usuario (704), y por que el transceptor (701) está configurado para enviar una señal de alarma al servicio de gestión central (5) a través de la red de banda ultra estrecha (8) cuando un usuario introduce un comando a través de la interfaz de usuario (704).

10 14. Método de detección de interferencia deliberada que comprende:

- explorar periódicamente al menos una banda de frecuencia (201, 401, 402) de un sistema de seguridad para detectar interferencia deliberada;

caracterizado por que el método comprende adicionalmente:

15 - si se detecta interferencia deliberada en la al menos una banda de frecuencia (201, 401, 402), enviar una señal de alarma a un servicio de gestión central (5) a través de una red de banda ultra estrecha (8).

20 15. Método de detección de interferencia deliberada caracterizado por que la etapa de enviar la señal de alarma comprende adicionalmente enviar un identificador (904) de la al menos una banda de frecuencia (201, 401, 402) que está siendo interferida deliberadamente y al menos un primer valor numérico que representa una intensidad de interferencia deliberada (906).

RESUMEN

MÉTODO Y DISPOSITIVO DE DETECCIÓN DE INTERFERENCIA DELIBERADA

- 5 Dispositivo (7) y método de detección de interferencia deliberada, que explora una o más bandas de frecuencia (201, 401, 402) y, si se detecta interferencia deliberada en dichas bandas de frecuencia (201, 401, 402), transmite una señal de alarma a través de una red de banda ultra estrecha (8). Preferentemente, se explora tanto una red ISM (2) que conecta un panel de control (3) y al menos un periférico (1), y una red de
- 10 GSM (4) que conecta el panel de control (3) y un servicio de gestión central (5). También preferentemente, la red de banda ultra estrecha (8) está implementada sobre la misma banda de frecuencia (801) que la red ISM (2) que conecta el panel de control (3) y el al menos un periférico (1).

[Fig. 1]

30
37

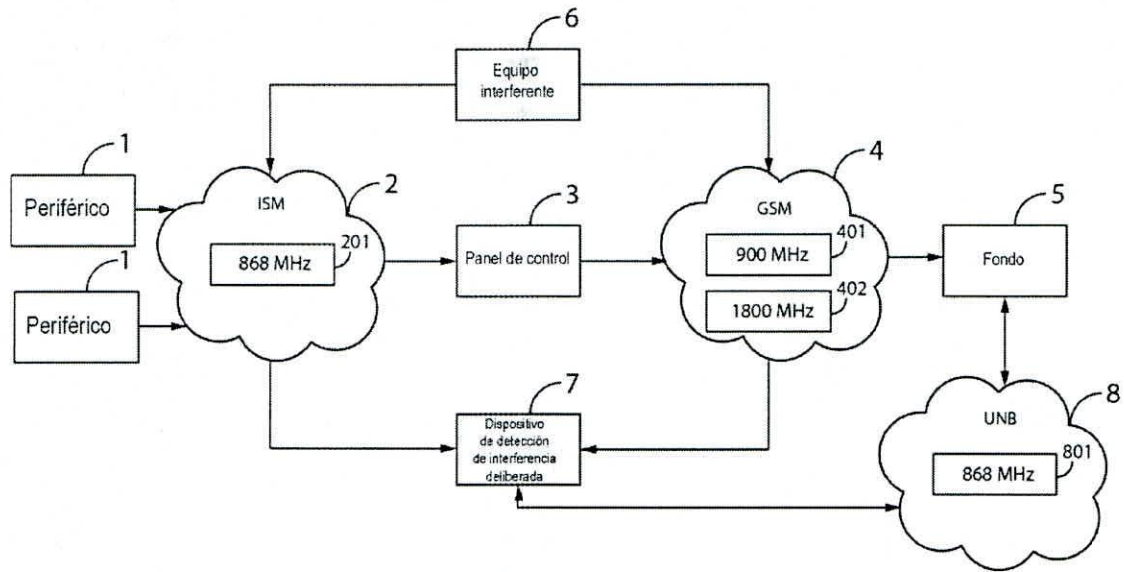


Fig. 1

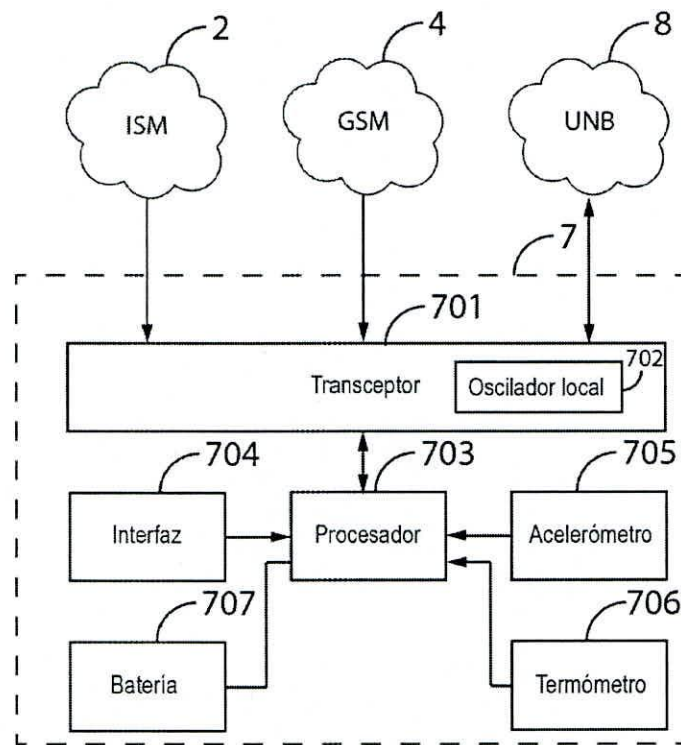


Fig. 2

39
38

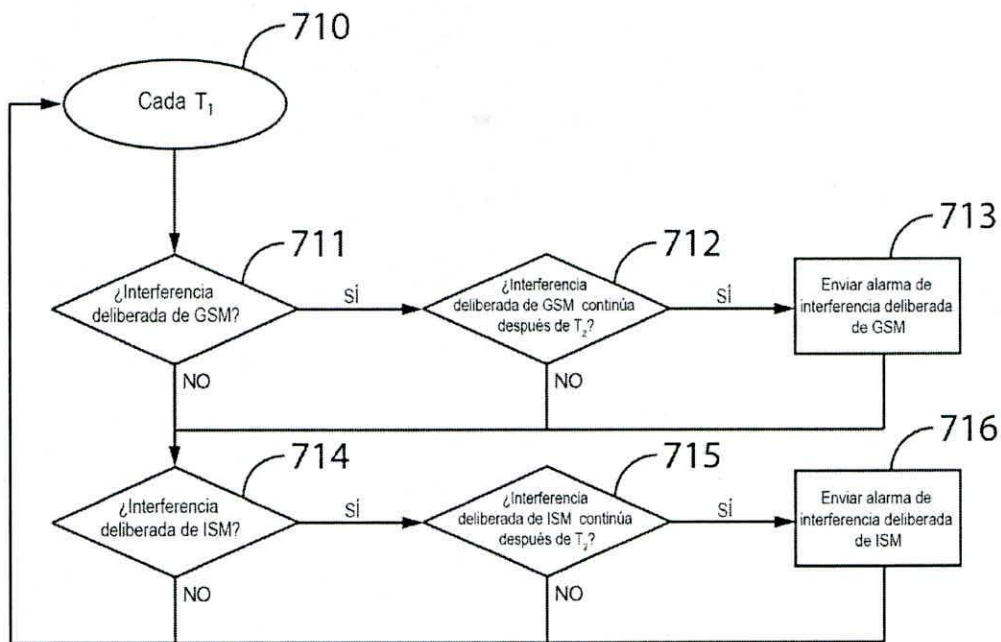


Fig. 3

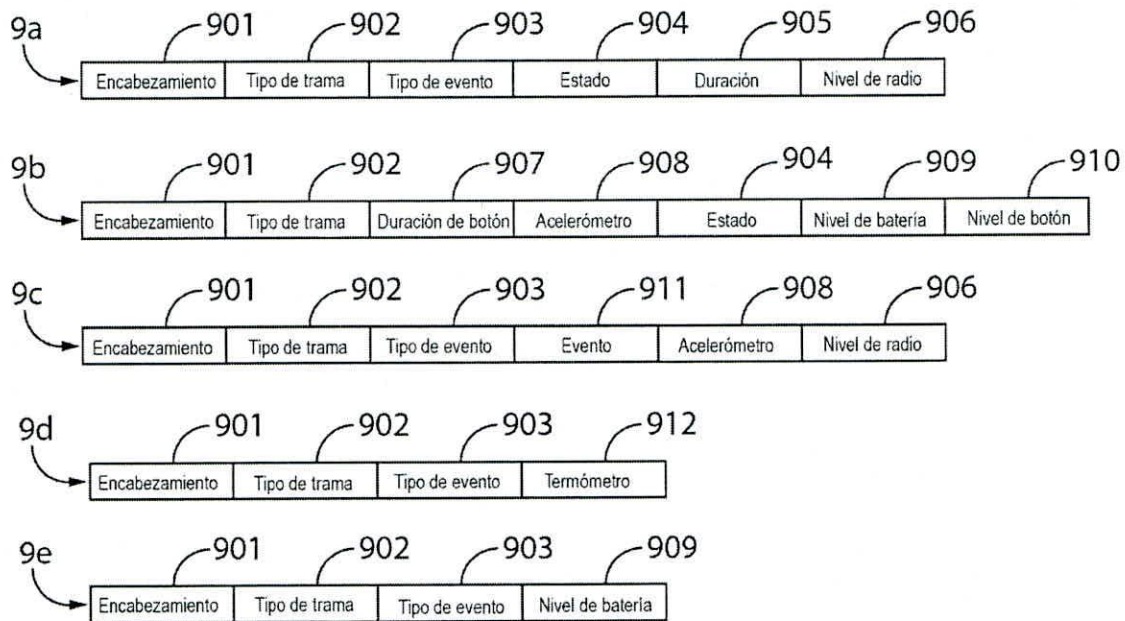


Fig. 4