(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 751 763**

(51) Int. CI.:

G08B 25/10 (2006.01)
G08B 26/00 (2006.01)
G08B 29/08 (2006.01)
G08B 29/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.05.2015 E 15382243 (2)**

(97) Fecha y número de publicación de la concesión europea: **24.07.2019 EP 3091519**

(54) Título: **Método y dispositivo de detección de interferencia deliberada**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.04.2020

(73) Titular/es:

VERISURE SÀRL (100.0%)
Chemin Jean-Baptiste Vandelle 3/3A
1290 Versoix, CH

(72) Inventor/es:

NORDMARK, PER LARS;
PIORNO IGLESIAS, ÁNGEL y
NOBLE ECHEVERRIA, JON

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método y dispositivo de detección de interferencia deliberada

Campo de la invención

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 invención

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 desvela 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 desvela 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, proporcionado 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.

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.

Sumario de la invención

La invención actual resuelve todos los problemas anteriormente mencionados desvelando 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.

Según la invención, se desvela un dispositivo de detección de interferencia deliberada como se define en la reivindicación 1. 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.

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

- 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 868 MHz para comunicaciones de radio en Europa y en la banda de 915 MHz en Estados Unidos.

- 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 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.

La red de banda ultra estrecha (UNB) usada mediante el dispositivo para transmitir la señal de alarma se establece en una banda de 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 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 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 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 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 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, 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:

- 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.

- 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 desvela 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 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 desvelados, los sistemas de seguridad y vigilancia se 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 repentinos producidos, por ejemplo, por un fuego cercano o desde ciertos instrumentos de manipulación. Adicionalmente, la red de banda ultra estrecha desvelada 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 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.

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.

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.

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 invención

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 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 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 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 desveladas 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 de 900 MHz (401) y la banda de frecuencia de 1800 MHz (402).

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 banda de frecuencia de 900 MHz (401) varía de 880 MHz a 960 MHz y se usa mediante operadores celulares para comunicaciones de GSM y de 3G. La banda de frecuencia de 1800 MHz (402) 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 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 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 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 (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 (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 el usuario el estado del dispositivo (7) o cualquier información adicional. Obsérvese que pueden existir 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.

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.

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 ºC, que genera mensajes de alarma cuando la temperatura medida supera 50 ºC, se reduce por debajo de 0 ºC, o el gradiente de temperatura supera una variación de 10 ºC en un minuto. Para reducir el consumo de energía, el termómetro (706) es preferentemente un sensor de temperatura en chip.

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 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 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. 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.

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.

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.

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).

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 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.

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).

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 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.

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 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) para un sistema de seguridad, comprendiendo el sistema de seguridad al menos un periférico (1) y un panel de control (3) conectados a través de al menos una primera banda de frecuencia (201) de una red de radio Industrial, Científica y Médica (2); estando conectado el panel de control (3) a un servicio de gestión central (5) a través de al menos una tercera banda de frecuencia de una red del Sistema Global para Comunicaciones Móviles (4);
en donde el dispositivo de detección de interferencia deliberada (7) comprende un transceptor (701) configurado para explorar periódicamente al menos una banda de frecuencia (201, 401, 402) del sistema de seguridad para detectar interferencia deliberada, incluyendo la al menos primera banda de frecuencia (201) de la red de radio Industrial, Científica y Médica (2), y la al menos tercera banda de frecuencia (401, 402) de una red del Sistema Global para Comunicaciones Móviles (4);
en donde, si la interferencia deliberada se detecta en la al menos primera banda de frecuencia (201) o en la al menos tercera banda de frecuencia (401, 402), el transceptor (701) se configura para enviar una señal de alarma al servicio de gestión central (5) a través de una red de banda ultra estrecha (8) sobre una segunda banda de frecuencia (801) de la red de banda ultra estrecha (8), estando la segunda banda de frecuencia parcial o totalmente superpuesta con la al menos una primera banda de frecuencia (201) de la red de radio Industrial, Científica y Médica (2).

2. Dispositivo de detección de interferencia deliberada (7) de acuerdo con la reivindicación 1, **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.

3. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las reivindicaciones 1-2, en donde el transceptor (701) está configurado para explorar periódicamente una banda de frecuencia de 900 MHz (401) y una banda de frecuencia de 1800 MHz (402) de la red del Sistema Global para Comunicaciones Móviles (4).

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

5. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las reivindicaciones anteriores, en donde 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).

6. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las reivindicaciones anteriores, en donde 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).

7. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las reivindicaciones anteriores, en donde 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 a 200 Hz.

8. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el dispositivo (7) comprende adicionalmente un acelerómetro (705), y en donde 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.

9. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el dispositivo (7) comprende adicionalmente un termómetro (706), y en donde 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.

10. Dispositivo de detección de interferencia deliberada (7) de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el dispositivo (7) comprende adicionalmente una interfaz de usuario (704), y en donde 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).

11. Sistema de seguridad que comprende:

- al menos un periférico (1) y un panel de control (3) conectados a través de al menos una primera banda de frecuencia (201) de una red de radio Industrial, Científica y Médica (2);
- estando conectado el panel de control (3) a un servicio de gestión central (5) a través de al menos una tercera banda de frecuencia de una red del Sistema Global para Comunicaciones Móviles (4);

en donde el sistema de seguridad comprende además un dispositivo de detección de interferencia deliberada de acuerdo con cualquier reivindicación anterior.

12. Método de detección de interferencia deliberada para un sistema de seguridad, comprendiendo el sistema de seguridad:

- al menos un periférico (1) y un panel de control (3) conectados a través de al menos una primera banda de frecuencia (201) de una red de radio Industrial, Científica y Médica (2);
- estando conectado el panel de control (3) a un servicio de gestión central (5) a través de al menos una tercera banda de frecuencia de una red del Sistema Global para Comunicaciones Móviles (4);

comprendiendo el método:

- explorar periódicamente al menos una banda de frecuencia (201, 401, 402) del sistema de seguridad para detectar interferencia deliberada, comprendiendo la al menos banda de frecuencia (201, 401, 402) explorada la al menos primera banda de frecuencia (201) de la red de radio Industrial, Científica y Médica (2), y la al menos tercera banda de frecuencia (401, 402) de una red del Sistema Global para Comunicaciones Móviles (4);

en donde el método comprende además:

- si se detecta interferencia deliberada en la al menos primera banda de frecuencia (201) o en la al menos tercera banda de frecuencia (401, 402), enviar una señal de alarma al servicio de gestión central (5) a través de una red de banda ultra estrecha (8) sobre una segunda banda de frecuencia (801) de la red de banda ultra estrecha (8), estando la segunda banda de frecuencia parcial o totalmente superpuesta con la al menos una primera banda de frecuencia (201) de la red de radio Industrial, Científica y Médica (2).

13. Método de detección de interferencia deliberada de la reivindicación 12, en donde 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).

14. Método de detección de interferencia deliberada de la reivindicación 13, en donde el método comprende además transmitir un segundo valor numérico que representa una duración de interferencia deliberada, cuando se determina que ha terminado la interferencia deliberada.

15. Método de detección de interferencia deliberada de cualquiera de las reivindicaciones 12-14, en donde enviar la señal de alarma al servicio de gestión central (5) mediante una red de banda ultra estrecha (8) comprende enviar la señal de alarma mediante un canal con ancho de banda de 200 Hz o menos.

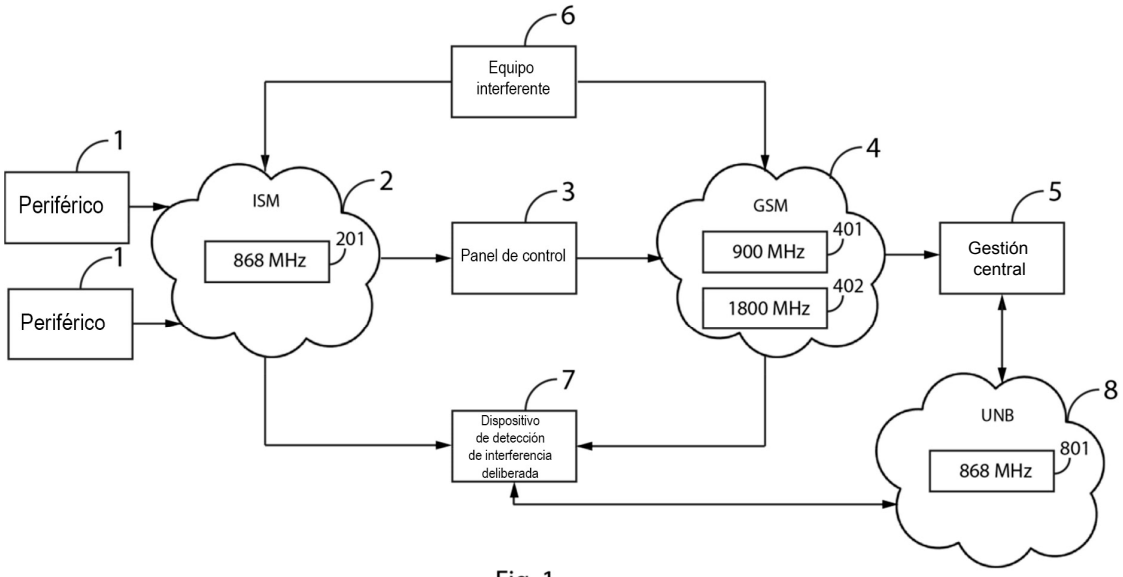
6
Equipo interferente
1
Periférico
1
Periférico
ISM
2
868 MHz
201
3
Panel de control
GSM
4
900 MHz
401
1800 MHz
402
5
Gestión central
7
Dispositivo de detección de interferencia deliberada
UNB
8
868 MHz
801

Fig. 1

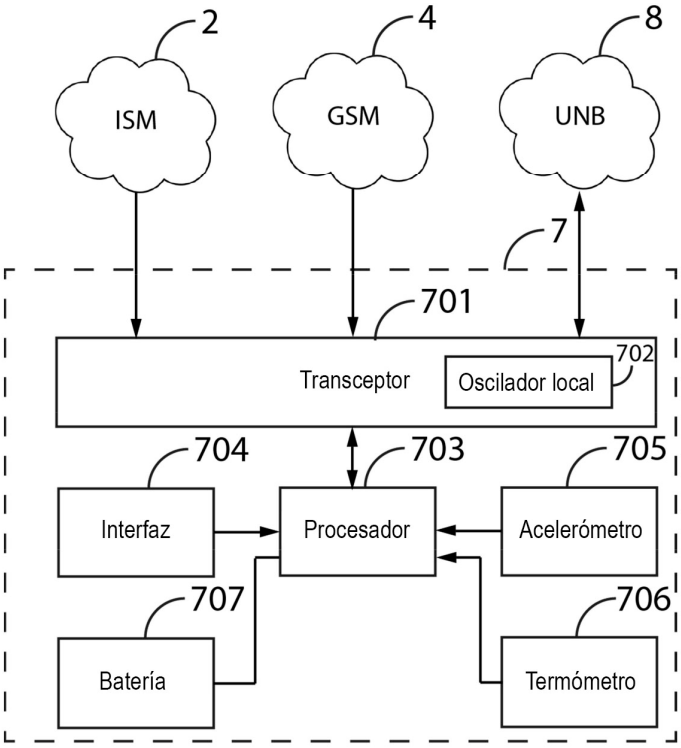
2
ISM
4
GSM
8
UNB
7
701
Transceptor
Oscilador local
702
704
703
705
Interfaz
Procesador
Acelerómetro
707
706
Batería
Termómetro

Fig. 2

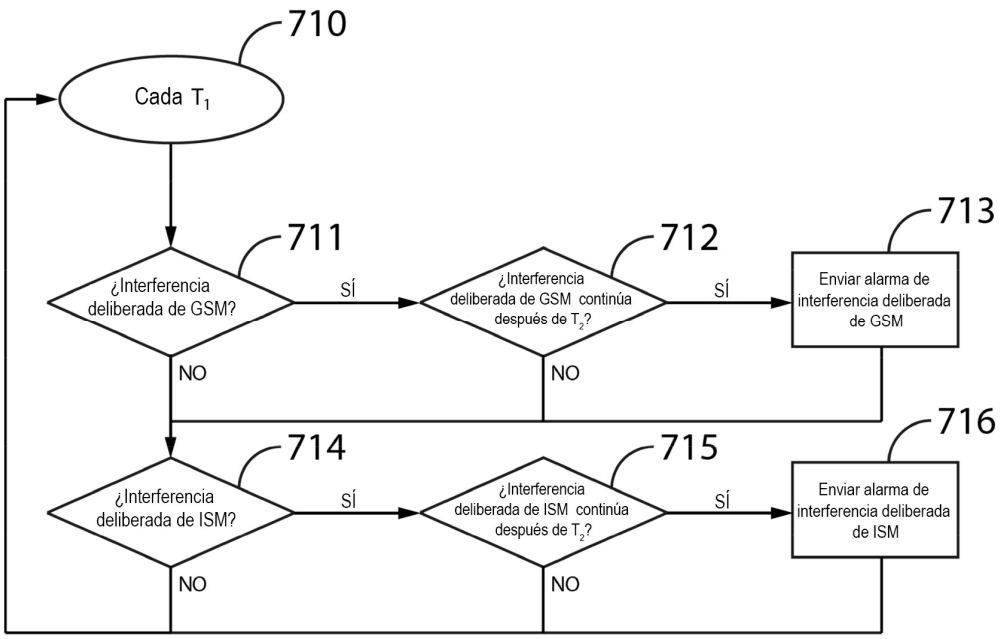
710
Cada T_1
711
¿Interferencia deliberada de GSM?
SÍ
712
¿Interferencia deliberada de GSM continúa después de T_2?
SÍ
713
Enviar alarma de interferencia deliberada de GSM
NO
NO
714
¿Interferencia deliberada de ISM?
SÍ
715
¿Interferencia deliberada de ISM continúa después de T_2?
SÍ
716
Enviar alarma de interferencia deliberada de ISM
NO
NO

Fig. 3

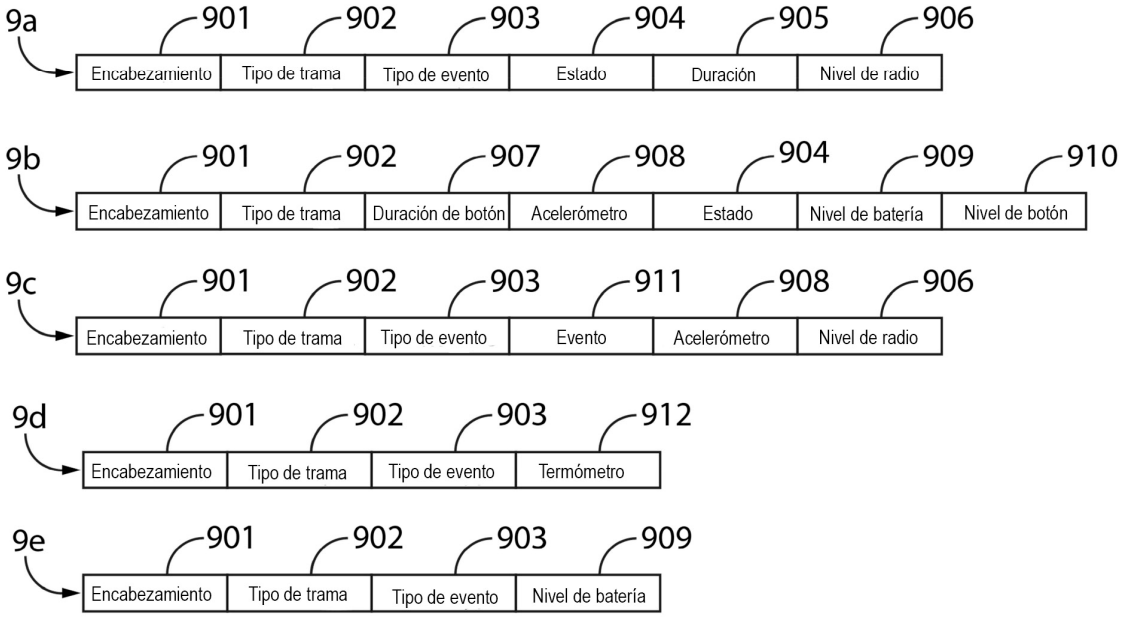
9a
901 Encabezamiento
902 Tipo de trama
903 Tipo de evento
904 Estado
905 Duración
906 Nivel de radio
9b
901 Encabezamiento
902 Tipo de trama
907 Duración de botón
908 Acelerómetro
904 Estado
909 Nivel de batería
910 Nivel de botón
9c
901 Encabezamiento
902 Tipo de trama
903 Tipo de evento
911 Evento
908 Acelerómetro
906 Nivel de radio
9d
901 Encabezamiento
902 Tipo de trama
903 Tipo de evento
912 Termómetro
9e
901 Encabezamiento
902 Tipo de trama
903 Tipo de evento
909 Nivel de batería

Fig. 4