(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 710 329**

(51) Int. CI.:

G08B 25/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.05.2017 E 17172597 (1)**

(97) Fecha y número de publicación de la concesión europea: **05.12.2018 EP 3252728**

(54) Título: **Sistema y método para un sistema de alarma**

(30) Prioridad:

23.05.2016 US 201662339980 P
28.07.2016 US 201662367657 P
04.09.2016 US 201662383432 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.04.2019

(73) Titular/es:

ESSENCE SECURITY INTERNATIONAL (E.S.I.) LTD. (100.0%)
Ackerstein Buildings, Building D, 7th Floor, 12 Abba Eben Boulevard
4672530 Herzlia Pituach, IL

(72) Inventor/es:

AMIR, HAIM y
AMIR, OHAD

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Sistema y método para un sistema de alarma

Antecedentes

La presente invención, en algunas realizaciones de la misma, se refiere a un sistema de alarma y, más específicamente, pero no en exclusiva, a la detección de un intento de un desarme no autorizado del sistema de alarma.

Un sistema de alarma típico instalado en instalaciones comprende uno o más sensores para detectar movimiento, presencia o intrusión, protegiendo una o más aberturas en las instalaciones o una o más áreas de las instalaciones. Las áreas protegidas pueden ser interiores o exteriores. Una compuerta, una puerta y una ventana son ejemplos de posibles aberturas protegidas por un sensor. Los uno o más sensores se conectan normalmente a un panel de control, que puede estar en comunicación con un centro de control. Tras detectar el movimiento de las instalaciones, la presencia de una persona u objeto en las instalaciones o un intento de entrar en las instalaciones, por ejemplo, detectando la abertura de una abertura protegida, al menos uno de los sensores envía una señal al panel de control que puede transmitir una señal al centro de control. Tras procesar la señal, el centro de control puede adoptar una o más acciones, por ejemplo llamar a un centro de emergencia o activar una señal de alarma visual o de audio.

Los sistemas de alarma se instalan en una amplia variedad de hogares, oficinas, negocios y otras ubicaciones. Un sistema de alarma típico puede tener uno de una pluralidad de posibles estados, incluyendo totalmente deshabilitado, totalmente activo y parcialmente activo. Por ejemplo, un sistema de alarma puede estar totalmente deshabilitado en una oficina durante las horas de trabajo. Cuando el sistema de alarma está totalmente deshabilitado, los uno o más sensores pueden no detectar movimiento, presencia o intrusión en las instalaciones, o el panel de control puede no transmitir una señal al centro de control. Una alarma puede estar totalmente activa en la oficina tras las horas de trabajo, cuando la oficina puede estar vacía. Cuando el sistema de alarma está totalmente activo, todos los uno o más sensores pueden estar activos para detectar movimiento, presencia o intrusión en las instalaciones. En un hogar, un sistema de alarma puede estar parcialmente activo por la noche, donde algunos de los unos o más sensores están activos y otros deshabilitados. Por ejemplo, en un estado posible parcialmente activo algunos sensores que protegen las aberturas exteriores de la casa tal como ventanas y puertas pueden estar activados, mientras que otros sensores para detectar movimiento en habitaciones de la casa pueden estar desactivados, para permitir que las personas que viven en la casa se muevan libremente por la casa. Como alternativa, el panel de control puede recibir todas las indicaciones de sensor pero puede transmitir al centro de control solo las indicaciones relevantes.

En algunos sistemas de alarma, la pluralidad de estados se controla usando una o más señales de frecuencia de radio (RF). En tales sistemas, el panel de control normalmente incluye un procesador de señal para recibir una o más de señales de RF desde un dispositivo de control, por ejemplo un llavero con una pluralidad de botones para controlar el estado del sistema de alarma. En tales sistemas, una persona puede presionar uno de la pluralidad de botones del llavero para dar instrucciones al sistema de alarma para cambiar el estado a un estado solicitado, teniendo como resultado que el llavero envíe una señal de RF indicativa del estado solicitado al procesador de señales. Tras recibir la señal, el procesador de señal procesa la señal, identifica el estado solicitado y da instrucciones de cambiar el estado del sistema de alarma al estado solicitado.

Sumario

Es un objeto de la presente invención proporcionar un sistema y método para detectar un intento de un desarme no autorizado del sistema de alarma.

Los anteriores y otros objetos se logran por las características de las reivindicaciones independientes. Otras formas de implementación son aparentes desde las reivindicaciones dependientes, la descripción y las figuras.

Los aspectos y las realizaciones de la presente invención se exponen en las reivindicaciones adjuntas. Estos y otros aspectos y realizaciones de la invención también se describen aquí.

De acuerdo con un primer aspecto de la invención, un sistema de alarma comprende al menos un transceptor de radiofrecuencia (RF) y al menos un procesador de señal, conectado eléctricamente al al menos un transceptor de RF. El al menos un transceptor RF se configura para: recibir una primera señal de RF de desarme desde un dispositivo de control de alarma; y durante un tiempo de retraso predeterminado tras recibir la primera señal de RF de desarme, transmitir al menos una señal de RF de engaño durante una o más franjas de tiempo de transmisión seleccionadas desde una pluralidad de franjas de tiempo consecutivas del tiempo de retraso predeterminado, y determinar si una o más de las señales de RF de recepción se reciben durante una o más franjas de tiempo de recepción seleccionadas de la pluralidad de franjas de tiempo consecutivas, las una o más franjas de tiempo de recepción intercaladas con las una o más franjas de tiempo de transmisión. El al menos un procesador de señal se configura para determinar una operación de sistemas de alarma de acuerdo con el análisis de las una o más señales de RF de recepción.

De acuerdo con un segundo aspecto de la invención, un método para un sistema de alarma comprende: recibir una primera señal de RF de desarme desde un dispositivo de control de alarma; durante un tiempo de retraso predeterminado tras recibir la primera señal de RF de desarme, transmitir al menos una señal de RF de engaño durante una o más franjas de tiempo de transmisión seleccionadas desde una pluralidad de franjas de tiempo consecutivas del tiempo de retraso predeterminado, y determinar si una o más señales de RF de recepción se reciben durante una o más franjas de tiempo de recepción seleccionadas de la pluralidad de franjas de tiempo consecutivas, las unas o más franjas de tiempo de recepción intercaladas con las una o más franjas de tiempo de transmisión; y determinar una operación del sistema de alarma de acuerdo con el análisis de las una o más señales de RF de recepción.

En referencia al primer y segundo aspecto, en una primera posible implementación del primer y segundo aspecto de la presente invención el análisis comprende: hacer coincidir al menos una de las una o más señales de RF de recepción con un patrón de señal de engaño predefinido; producir una auténtica indicación de detección de engaño para cada una de las una o más señales de RF de recepción que coinciden con el patrón de señal de engaño predefinido; y seleccionar la operación del sistema de alarma de acuerdo con la indicación de detección de engaño auténtica. Detectar una señal de engaño es suficiente para identificar una intrusión intentada.

En referencia al primer y segundo aspecto, en una segunda posible implementación del primer y segundo aspecto de la presente invención el análisis comprende: producir una falsa indicación de detección de engaño sometida a ninguna de las una o más señales de RF de recepción que se reciben durante las una o más franjas de tiempo de recepción o cada una de las una o más señales de RF de recepción que fallan al coincidir con el patrón de señal de engaño predefinido; y seleccionar la operación del sistema de alarma de acuerdo con la indicación de detección de engaño falsa. Cuando ninguna señal de RF se detecta durante las franjas de recepción, o cuando ninguna de las una o más de las señales de RF recibidas coinciden con el patrón de señal de engaño predefinido, ningún engaño se detecta.

En referencia al primer y segundo aspecto, o a la primera y segunda implementación del primer y segundo aspecto, en una tercera posible implementación del primer y segundo aspecto de la presente invención el al menos un procesador de señal se configura además para: determinar si la primera señal de RF de desarme es válida, sometida a no recibir ninguna de las una o más señales de RF de recepción o producir solo indicaciones de detección de engaño falsas; y recibir una segunda señal de RF de desarme desde el dispositivo de control de alarma después del tiempo de retraso predeterminado. Tras recibir la segunda señal de RF de desarme, la operación del sistema de alarma comprende al menos uno de: dar instrucciones del desarme del sistema de alarma, y transmitir una señal de RF de acuse de recibo al dispositivo de control de alarma mediante el al menos un transceptor de RF. Tras identificar una señal de desarme válida, también el reintento puede considerarse válido.

En referencia al primer y segundo aspecto, en una cuarta posible implementación del primer y segundo aspecto de la presente invención la franja de tiempo de transmisión se selecciona aleatoriamente mediante el procesador de señal tras recibir la primera señal de RF de desarme para transmitir al menos una señal de RF de engaño, y las franjas de tiempo de recepción comprenden todas de la pluralidad de franjas de tiempo consecutivas diferentes de las franjas de tiempo de transmisión. Seleccionar un patrón aleatorio de transmisión de franjas reduce la probabilidad de repetir la misma secuencia e incrementa la probabilidad de detectar una señal de engaño grabada en una de las franjas de recepción. Escuchar las señales recibidas durante todas las franjas de tiempo restantes incrementa la probabilidad de detectar una secuencia de engaño retransmitida.

En referencia al primer y segundo aspecto, en una quinta posible implementación del primer y segundo aspecto de la presente invención una cantidad de franjas de tiempo de transmisión está entre 15 % y 30 % de una cantidad de la pluralidad de franjas de tiempo consecutivas. Esta relación permite un equilibrio entre alta probabilidad de detectar un engaño y reducir los gastos del cambio frecuente entre transmisión y recepción.

En referencia al primer y segundo aspecto, en una sexta posible implementación del primer y segundo aspecto de la presente invención el tiempo de retraso predeterminado se divide en 25 franjas de tiempo consecutivas. Esta cantidad de franjas de tiempo consecutivas permite un equilibrio entre alta probabilidad de detectar un engaño y reducir los gastos del cambio frecuente entre transmisión y recepción.

En referencia al primer y segundo aspecto, en una séptima posible implementación del primer y segundo aspecto de la presente invención la al menos una señal de RF de recepción se protege por un código de detección de error que es una comprobación de redundancia cíclica de 16 bits. La protección de la al menos una señal de RF de engaño reduce la probabilidad de detectar falsamente el engaño. La comprobación de redundancia cíclica de 16 bits es fácil de implementar e introduce poca sobrecarga en el procesamiento y ancho de banda.

En referencia al primer y segundo aspecto, en una octava posible implementación del primer y segundo aspecto de la presente invención la al menos una señal de RF de engaño se codifica usando un método seleccionado del grupo de: ofuscación, o exclusivo con una palabra clave predefinida, y o exclusivo con una palabra clave aleatoria. El cifrado de la al menos una señal de RF de engaño reduce la probabilidad de que una parte no autorizada distinga entre la al menos una señal de RF de engaño y la señal de RF de desarme. La ofuscación y o exclusivo son fáciles de implementar e introducen poca sobrecarga en el procesamiento y ancho de banda.

En referencia al primer y segundo aspecto, en una novena posible implementación del primer y segundo aspecto de la presente invención la operación del sistema de alarma comprende al menos una operación seleccionada del grupo que comprende: notificar a un centro de control operativamente conectado a dicho al menos un procesador de señal de una intrusión intentada, sometida a producir al menos una auténtica indicación de detección de engaño y suministrar una corriente eléctrica a un dispositivo capaz de emitir una señal de audio o señal visual, conectado eléctricamente a dicho al menos un procesador de señal, sometido a producir al menos una auténtica indicación de detección de engaño.

Con referencia al primer y segundo aspecto, o a la primera implementación del primer y segundo aspecto, en una décima posible implementación del primer y segundo aspecto de la presente invención la al menos una señal de RF de engaño comprende al menos uno de: un identificador, un sello de tiempo y un número aleatorio, para uso al identificar un origen de una señal de RF de engaño grabada. Opcionalmente, el identificador consiste en 32 bits binarios, el sello de tiempo consiste en 32 bits binarios y el número aleatorio consiste en 8 bits binarios. Opcionalmente, la coincidencia del patrón de señal de engaño predefinido comprende detectar en la una señal de RF recibida al menos uno de: un identificador, un sello de tiempo y un número aleatorio.

En referencia al primer y segundo aspecto, o a la primera implementación del primer y segundo aspecto, en una decimoprimera posible implementación del primer y segundo aspecto de la presente invención el análisis comprende además: detectar un número de paquete en la primera señal de RF de desarme; comparar una diferencia entre el número de paquete y un número de paquete almacenado previamente con un número de umbral predefinido; y producir una auténtica indicación de detección de engaño cuando la diferencia es mayor que el número de umbral predefinido. Añadir un número de paquete a la señal de RF de desarme proporciona un medio adicional para detectar el reenvío de una señal grabada detectando un número de paquete repetido.

Otros sistemas, métodos, características y ventajas de la presente divulgación serán o se volverán aparentes para el experto tras examinar los siguientes dibujos y la descripción detallada. Se pretende que todos esos sistemas, métodos, características y ventajas adicionales se incluyan dentro de esta descripción, dentro del alcance de la presente divulgación, y queden protegidos por las reivindicaciones adjuntas.

A menos que se defina lo contrario, todos los términos científicos y/o técnicos usados en este caso tienen el mismo significado que se entiende comúnmente por un experto en la materia al que pertenece la invención. Aunque los métodos y materiales similares o equivalentes a los descritos aquí pueden usarse en la práctica o ensayo de realizaciones de la invención, los métodos y/o materiales ejemplares se describen a continuación. En caso de conflicto, la memoria descriptiva de patente, incluyendo definiciones, tendrá el control. Además, los materiales, métodos y ejemplos son solo ilustrativos y no pretenden ser necesariamente limitativos.

Breve descripción de las varias vistas de los dibujos

Algunas realizaciones de la invención en este caso se describen a modo de ejemplo únicamente en referencia a los dibujos adjuntos. En referencia específica ahora a los dibujos en detalle, se especifica que estos particulares mostrados son a modo de ejemplo y con fines de análisis ilustrativo de realizaciones de la invención. En este sentido, la descripción tomada con los dibujos hace que sea aparente para los expertos en la técnica como las realizaciones de la invención pueden practicarse.

En los dibujos:

la FIG. 1 es una ilustración esquemática de un sistema ejemplar de acuerdo con algunas realizaciones de la presente invención;
las FIGS. 2A, 2B, 2C, y 2D son ilustraciones esquemáticas de señales de RF ejemplares con respecto al tiempo, de acuerdo con algunas realizaciones de la presente invención;
la FIG. 3 es un diagrama de flujo que representa esquemáticamente un flujo opcional de operaciones para detectar un intento de intrusión usando transmisión y recepción intercaladas de una señal de engaño, de acuerdo con algunas realizaciones de la presente invención;
la FIG. 4 es un diagrama de flujo que representa esquemáticamente un flujo opcional de operaciones para detectar un intento de intrusión usando imperfecciones de señal de RF de una señal, de acuerdo con algunas realizaciones de la presente invención;
la FIG. 5 es un diagrama de flujo que representa esquemáticamente otro flujo opcional de operaciones para detectar un intento de intrusión usando imperfecciones de señal de RF de una señal, de acuerdo con algunas realizaciones de la presente invención;
la FIG. 6 es un diagrama de flujo que representa esquemáticamente un flujo opcional de operaciones para producir imperfecciones de señal de referencia, de acuerdo con algunas realizaciones de la presente invención; y
las FIGS. 7A y 7B son secuencias de tiempo que representan esquemáticamente un flujo opcional de operaciones para detectar un intento de intrusión usando una instrucción inválida, de acuerdo con algunas realizaciones de la presente invención.

Descripción detallada

La presente invención, en algunas realizaciones de la misma, se refiere a un sistema de alarma y más específicamente, pero no en exclusiva, a detectar un intento de desarme no autorizado de un sistema de alarma.

Tal como se usa aquí, el término “desarme” significa “dar instrucciones para cambiar a un estado deshabilitado o parcialmente activo” y el término “señal” significa “señal de RF”.

Los intentos de entrar en una instalación protegida por un sistema de alarma pueden incluir intentos de atravesar cualquier componente del sistema de alarma.

Una señal de RF típica puede detectarse y grabarse en un intervalo identificado de distancias desde un dispositivo que envía la señal de RF. En un sistema de alarma controlado usando una o más señales de radiofrecuencia (RF), una persona no autorizada a acceder a las instalaciones puede grabar una señal ilegítima enviada por un dispositivo de control de alarma dando instrucciones de desarme del sistema de alarma, y retransmitir la señal grabada en un momento posterior. Un sistema de alarma típico no puede distinguir entre la señal legítima original y la señal grabada, y tras recibir la señal grabada el procesador de la señal del sistema de alarma puede dar instrucciones de desarmar el sistema de alarma. Así, una señal grabada puede usarse para ganar acceso no autorizado a las instalaciones.

Las soluciones de autenticación usando señales cifradas o incluyendo información predefinida en una o más señales transmitidas por un dispositivo de control de alarma se limitan ya que requieren sustituir múltiples dispositivos de control de alarma existentes, por ejemplo sustituyendo llaveros existentes por dispositivos de control de alarma que soportan cifrado o información predefinida. Además, los dispositivos de control de alarma que soportan el cifrado o envían información predefinida pueden ser más caros que los dispositivos de control de alarma simples existentes, tal como llaveros existentes.

La presente invención, en algunas realizaciones de la misma, permite que un sistema de alarma distinga entre una señal legítima y la retransmisión de una señal grabada anteriormente, sin necesitar un dispositivo de control de alarma especialmente configurado, cambiando la manera en que opera el procesador de señal.

En algunas realizaciones de la presente invención, el procesador de señal, tras recibir una señal de desarme desde un dispositivo de control de alarma, envía una o más señales de engaño. Un intento de grabar la señal de desarme grabará las una o más señales de engaño también. Cuando se transmite la señal grabada, las una o más señales de engaño se transmiten también y pueden recibirse por el procesador de señal. En estas realizaciones, el procesador de señal transmite de forma intercambiable las una o más señales de engaño y comprueba la recepción de una o más otras señales. Cuando se determina que una o más de las otras señales son señales de engaño, el procesador de señal determina un intento de intrusión no autorizada.

En otras realizaciones de la presente invención, el procesador de señal analiza las imperfecciones de señal de RF de una señal de desarme recibida por imperfecciones. Una señal típica transmitida por un dispositivo de control de alarma comprende una secuencia de bits digitales codificados en una señal portadora analógica que comprende una pluralidad de componentes de señal sinusoidal. Cuando un transceptor de RF codifica bits digitales en una señal portadora analógica y transmite la señal de RF resultante, el transceptor introduce ruido en la señal transmitida, incluyendo al menos uno de una imperfección de frecuencia de una señal sinusoidal, una imperfección de fase de una señal sinusoidal y una imperfección de amplitud de la señal sinusoidal. Por ejemplo: desplazamiento de frecuencia portadora, ruido de fase, desequilibrio en fase y cuadratura (IQ) y no linealidad de señal (es decir, cambios no lineales en una resistencia de señal de salida en respuesta a una resistencia de señal de entrada). Tal ruido, mencionado como imperfecciones de señal de RF, es una imperfección de señal del transceptor de RF y puede cuantificarse, combinarse y normalizarse, terminando por ejemplo en un número entre 0 y 1. Dos transceptores de RF se caracterizan normalmente por imperfecciones de señal de RF diferentes distintivamente. Una señal de desarme grabada normalmente comprende una secuencia grabada de bits digitales. Cuando un dispositivo de control de alarma no autorizado transmite una señal de alarma grabada, el dispositivo de control de alarma no autorizado vuelve a codificar la secuencia grabada de bits digitales en una nueva señal portadora analógica. Las imperfecciones de señal de RF de la señal transmitida por el dispositivo de control de alarma no autorizado serán diferentes de las imperfecciones de señal de RF de la señal de desarme original, resultando en las imperfecciones de RF de la señal transmitida por el dispositivo de control de alarma no autorizado que son diferentes de las imperfecciones de RF de la señal de desarme original. En estas realizaciones, el procesador de señal compara las imperfecciones de RF de una señal de preámbulo recibida con un conjunto predeterminado de imperfecciones de RF asociadas con transmisores legítimos. Cuando las imperfecciones de RF de la señal de preámbulo recibida no cumplen con el conjunto predeterminado de imperfecciones de RF, el procesador de señal determina en estas realizaciones un intento de intrusión no autorizada.

En otras realizaciones de la presente invención, el dispositivo de control de alarma se configura para enviar una señal que indica un evento, y recibir una señal que incluye una identificación de una función a ejecutar por el dispositivo de control de alarma. Por ejemplo, el dispositivo de control de alarma puede ser un llavero, configurado para enviar una señal que indica un botón pulsado y una duración, por ejemplo “pulsación corta en el botón 1” y recibir una señal que incluye una codificación de una identificación de una función, por ejemplo “función 3”. Una posible función es activar un diodo emisor de luz (LED) durante un período de tiempo predeterminado. Opcionalmente, tras recibir una señal

que incluye una codificación de una identificación de una función no reconocida por el dispositivo de control de alarma, el dispositivo de control de alarma envía un mensaje de error que indica un error y la identificación de una función no reconocida. En estas realizaciones, el procesador de señal, tras recibir una señal de desarme desde un dispositivo de control de alarma, envía una señal de engaño que incluye un identificador seleccionado aleatoriamente de una función inválida. Un intento de grabar la señal de desarme grabará también la señal de engaño. Cuando se transmite la señal grabada, la señal de engaño se transmite también y puede recibirse por el procesador de señal. En estas realizaciones, después de transmitir una señal de engaño que incluye un identificador de función inválida, el procesador de señal comprueba la recepción de otra señal. Cuando otra señal se recibe, la señal recibida se procesa para extraer un identificador de función desconocido posible. Cuando el identificador de función desconocido se extrae, el identificador extraído se compara con el identificador de función inválida. Cuando el identificador extraído es distinto del identificador de función inválido, el procesador de señal determina en estas realizaciones un intento de intrusión no autorizada, ya que se asume que el identificador extraído es el resultado de una señal pregrabada.

Antes de explicar al menos una realización de la invención en detalle, debe entenderse que la invención no se limita necesariamente en su aplicación a los detalles de construcción y la disposición de los componentes y/o métodos expuestos en la siguiente descripción y/o ilustrados en los dibujos y/o en los Ejemplos. La invención es capaz de tener otras realizaciones o practicarse o llevarse a cabo de diversas maneras.

La presente invención puede ser un sistema, un método y/o un producto de programa informático. El producto de programa informático puede incluir un medio (o medios) de almacenamiento legible a ordenador con instrucciones de programa legibles a ordenador en el mismo para provocar que un procesador lleve a cabo aspectos de la presente invención.

El medio de almacenamiento legible a ordenador puede ser un dispositivo tangible que puede retener y almacenar instrucciones para uso por un dispositivo de ejecución de instrucción. El medio de almacenamiento legible a ordenador puede ser, por ejemplo, pero no se limita a, un dispositivo de almacenamiento electrónico, un dispositivo de almacenamiento magnético, un dispositivo de almacenamiento óptico, un dispositivo de almacenamiento electromagnético, un dispositivo de almacenamiento semiconductor o cualquier combinación adecuada de lo anterior.

Las instrucciones de programa legibles a ordenador descritas en este caso pueden descargarse a dispositivos de procesamiento/informáticos respectivos desde un medio de almacenamiento legible a ordenador o a un ordenador externo o dispositivo de almacenamiento externo mediante una red, por ejemplo, Internet, una red de área local, una red de área amplia y/o una red inalámbrica.

Las instrucciones de programa legibles a ordenador pueden ejecutarse por completo en el ordenador del usuario, parcialmente en el ordenador del usuario, como un paquete de software autónomo, parcialmente en el ordenador del usuario y parcialmente en un ordenador remoto o por completo en el ordenador remoto o servidor. En el último escenario, el ordenador remoto puede conectarse al ordenador del usuario a través de cualquier tipo de red, incluyendo una red de área local (LAN) o una red de área amplia (WAN) o la conexión puede realizarse a un ordenador externo (por ejemplo, mediante Internet usando un Proveedor de Servicios de Internet). En algunas realizaciones, la circuitería electrónica incluyendo, por ejemplo, circuitería analógica programable, matriz de puertas programables en campo (FPGA) o matrices lógicas programables (PLA) pueden ejecutar las instrucciones de programa legibles a ordenador utilizando información de estado de las instrucciones de programa legibles a ordenador para personalizar la circuitería electrónica, para realizar aspectos de la presente invención.

Los aspectos de la presente invención se describen en este caso en referencia a ilustraciones de diagrama de flujo y/o diagramas de bloques de métodos, aparatos (sistemas) y productos de programa informático de acuerdo con realizaciones de la invención. Se entenderá que cada bloque de las ilustraciones de diagramas de flujo y/o diagramas de bloques, y combinaciones de bloques en las ilustraciones de diagramas de flujo y/o diagramas de bloques, pueden implementarse por instrucciones de programa legibles a ordenador.

Los diagramas de bloques y diagramas de flujo en las Figuras ilustran la arquitectura, funcionalidad y operación de posibles implementaciones de sistemas, métodos y productos de programa informático de acuerdo con diversas realizaciones de la presente invención. En este sentido, cada bloque en el diagrama de flujo o diagramas de bloques puede representar un módulo, segmento o porción de instrucciones, que comprende una o más instrucciones ejecutables para implementar las funciones lógicas especificadas. En algunas implementaciones alternativas, las funciones mencionadas en el bloque pueden ocurrir fuera del orden mencionado en las figuras. Por ejemplo, dos bloques mostrados en sucesión pueden, de hecho, ejecutarse sustancialmente a la vez, o los bloques pueden a veces ejecutarse en el orden inverso, dependiendo de la funcionalidad implicada. También se aprecia que cada bloque de la ilustración de diagramas de bloques y/o diagrama de flujo y combinaciones de bloques en la ilustración de diagramas de bloques y/o de diagramas de flujo, puede implementarse por sistemas basados en hardware de fin especial que realizan las funciones o actos especificados o llevan a cabo combinaciones de hardware de fin especial e instrucciones informáticas.

Ahora se hace referencia a la FIG. 1 que muestra una ilustración esquemática del sistema ejemplar 100 de acuerdo con algunas realizaciones de la presente invención. En tales realizaciones, el sistema 100 comprende uno o más

sensores 111, para detectar movimiento dentro de las instalaciones, la presencia dentro de las instalaciones o intrusión en una abertura de las instalaciones. Uno o más sensores 110 pueden conectarse a un panel de control 106 que comprende un controlador de alarma 110 que comprende al menos un procesador de hardware. Opcionalmente, el controlador de alarma 110 se configura para dar instrucciones de la activación de los uno o más sensores y deshabilitar los uno o más sensores.

Además, en tales realizaciones el sistema 100 comprende un procesador de señal 101 conectado a un controlador de alarma 110 para controlar el sistema. El procesador de señal 101 puede conectarse eléctricamente al controlador de alarma 110. Opcionalmente, el procesador de señal 101 se conecta al controlador de alarma 110 mediante una red de comunicación digital, tal como Red de Área Local. Opcionalmente, el procesador de señal 101 se conecta eléctricamente al controlador de alarma 110.

Opcionalmente, el procesador de señal 101 se conecta eléctricamente a un transceptor de RF 102, para comunicarse con uno o más dispositivos de control de alarma 103 tal como llaveros. Opcionalmente, el procesador de señal 101 comprende al menos un procesador de hardware. En tales realizaciones el transceptor de RF 102 recibe una o más señales de RF desde el dispositivo de control de alarma 103. Opcionalmente, cada una de las una o más señales de RF codifica una secuencia de bits digitales en una señal portadora analógica. Opcionalmente, una o más de las señales de RF son un mensaje de desarme, enviado desde el dispositivo de control de alarma 103 a un procesador de señal 101 para dar instrucciones de desarmar el sistema de alarma 100. Opcionalmente, el procesador de señal 101 procesa el mensaje de desarme para determinar si el mensaje es un mensaje válido recibido desde un dispositivo de control de alarma autorizado, o un intento de intrusión no autorizado. Tras determinar un mensaje de desarme válido, el procesador de señal 101 puede dar instrucciones de desarmar el sistema de alarma 100. Opcionalmente, el procesador de señal 101 da instrucciones al controlador de alarma 110 de desarmar el sistema.

En algunas realizaciones, el procesador de señal 101 se conecta eléctricamente a uno o más dispositivos de alarma 105 capaces de emitir una señal de audio tal como un sonido de alarma, y/o una señal visual tal como una luz intermitente, para atraer la atención de una persona suficientemente cerca a uno o más dispositivos de alarma 105 para apreciar la señal de alarma o señal visual. Opcionalmente, tras detectar un intento de intrusión, el procesador de señal 101 acciona una corriente eléctrica a uno o más dispositivos de alarma 105 para emitir la señal de audio o visual. En algunas realizaciones, el procesador de señal 101 se conecta a uno o más centros de control 104, que comprenden al menos un procesador de hardware. Opcionalmente, tras detectar un intento de intrusión, el procesador de señal 101 notifica al centro de control 104 la detección del intento de intrusión. Después de recibir la notificación de la detección del intento de intrusión, el centro de control 104 puede realizar una o más acciones tal como llamar a una persona designada, grabar un evento en un registro de eventos, etc.

En algunas realizaciones, el procesador de señal 101 se conecta eléctricamente a un almacenamiento digital no volátil 112 tal como un disco duro o una memoria programable borrable eléctricamente, con el fin de almacenar datos de referencia usados para determinar la validez del mensaje recibido.

Para determinar si un mensaje recibido es válido, el sistema 100 puede implementar uno o más de los siguientes métodos.

Un posible método para detectar un intento de intrusión usa transmisión y recepción intercaladas de una señal de engaño.

La referencia se hace ahora también a la FIG. 2A, que muestra una ilustración esquemática de una señal de desarme de RF ejemplar transmitida por un dispositivo de control de alarma 103 a un procesador de señal 101, de acuerdo con algunas realizaciones de la presente invención. Siguiendo la línea de tiempo 210, en el tiempo 211 el dispositivo de control de alarma 103 transmite en tales realizaciones un primer mensaje de desarme 201. Opcionalmente, el tiempo 212 indica el tiempo en el que el dispositivo de control de alarma 103 completó la transmisión del mensaje de desarme 201. Opcionalmente, después de un tiempo de retraso predeterminado tras el tiempo 212, si el dispositivo de control de alarma 103 no recibe una señal de acuse de recibo del procesador de señal 101, el dispositivo de control de alarma 103 transmite un segundo mensaje de desarme 202 en el tiempo 214.

Tras recibir un mensaje de desarme, en algunas realizaciones de la presente invención el procesador de señal 101 transmite una señal de engaño. La referencia se hace ahora también a la FIG. 2B, que muestra una ilustración esquemática de una posible señal de RF de engaño transmitida por el procesador de señal 101 mediante un transceptor de RF 102, de acuerdo con algunas realizaciones de la presente invención. En tales realizaciones, el tiempo de retraso predeterminado se divide en una pluralidad de franjas de tiempo consecutivas. Un ejemplo no limitante de una cantidad de franjas de tiempo es 25 franjas de tiempo. Opcionalmente, el tiempo 213 indica el tiempo más temprano en el que el transceptor de RF 102 que recibe el mensaje de desarme 201 puede comenzar a transmitir. Opcionalmente, el procesador de señal 101 selecciona un grupo de franjas de tiempo de transmisión desde la pluralidad de franjas de tiempo consecutivas y transmite una o más secuencias de engaño 220 transmitiendo en cada una de las franjas de tiempo de transmisión una secuencia de engaño. Una grabadora que graba las señales transmitidas al procesador de señal 101 grabará tanto el mensaje de desarme 201 como las una o más secuencias de engaño 220. La referencia se hace ahora también a la FIG. 2C, que muestra una ilustración esquemática de una

posible señal de RF grabada, de acuerdo con algunas realizaciones de la presente invención. En tales realizaciones, la señal grabada 230 comprende un mensaje de desarme 201, y las una o más secuencias de engaño 220 transmitidas por el procesador de señal 101.

Opcionalmente, el grupo de franjas de transmisión se selecciona aleatoriamente por el procesador de señal 101 tras recibir un mensaje de desarme, que comprende menos franjas que la pluralidad de franjas de tiempo consecutivas. Por ejemplo, la cantidad de franjas de transmisión está entre 15 % y 30 % de la cantidad de franjas de la pluralidad de franjas de tiempo consecutivas. Por ejemplo, la cantidad de franjas de transmisión es el 25 % de la cantidad de franjas en la pluralidad de franjas de tiempo consecutivas. Por ejemplo, cuando el tiempo de retraso predeterminado se divide en 25 franjas de tiempo, la cantidad de franjas de tiempo de transmisión puede ser 5.

En algunas realizaciones, un dispositivo de control de alarma no autorizado que transmite una señal grabada transmite el mensaje de desarme originalmente transmitido por el dispositivo de control de alarma autorizado, seguido por las una o más secuencias de desarme como se transmitieron previamente por el procesador de señal.

Ahora se hace referencia además a la FIG. 2D, que muestra una ilustración esquemática de una posible señal de RF grabada retransmitida, en comparación con una nueva señal de engaño, de acuerdo con algunas realizaciones de la presente invención. En tales realizaciones, un dispositivo de control de alarma 105 transmite en el tiempo 241 una señal grabada 250, que comprende una señal de desarme 201 originalmente transmitida por un dispositivo de control de alarma autorizado. Opcionalmente, la transmisión de la señal de desarme 201 termina en el tiempo 242. Tras recibir el mensaje de desarme 201, el procesador de señal 101 selecciona un nuevo grupo de franjas de transmisión desde una pluralidad de franjas de tiempo consecutivas entre el tiempo 243 y el tiempo 244, y transmite por el receptor de RF 102 una o más señales de engaño 260. El nuevo grupo de franjas de transmisión puede ser diferente del grupo de franjas de transmisión en la señal grabada. Opcionalmente, el transceptor RF 102 escucha las señales recibidas en un grupo de franjas de tiempo de recepción seleccionado de la pluralidad de franjas de tiempo consecutivas de manera que las franjas de tiempo de recepción son diferentes del nuevo grupo de franjas de tiempo de transmisión y se intercalan con el nuevo grupo de franjas de tiempo de transmisión. En algunas realizaciones las franjas de tiempo de recepción son todas de la pluralidad de franjas de tiempo consecutivas no en las nuevas franjas de tiempo de transmisión. Cuando las franjas de tiempo de transmisión se seleccionan aleatoriamente, existe una probabilidad mayor que cero de que el nuevo grupo de franjas de tiempo de transmisión sea diferente del grupo de franjas de tiempo en la señal grabada. Dependiendo del número de franjas de tiempo y el número de franjas de tiempo de transmisión, la probabilidad puede superar 0,99. Como resultado, el procesador de señal 101 opcionalmente detecta una o más secuencias de engaño grabadas durante las franjas de tiempo de recepción, por ejemplo en la franja 262. Opcionalmente, una o más franjas de tiempo están tanto en el nuevo grupo de franjas de tiempo de transmisión como en el grupo de franjas de tiempo de transmisión en la señal grabada, por ejemplo en la franja 261. En tales franjas, el procesador de señal 101 no puede detectar una señal de engaño, ya que el transceptor 102 está transmitiendo.

Detectar una señal de engaño en una franja de tiempo de recepción indica una alta probabilidad de que la señal de desarme sea una señal grabada retransmitida por un dispositivo de control de alarma no autorizado. Dependiendo de la cantidad de franjas de tiempo en la pluralidad de franjas de tiempo consecutivas y la cantidad de franjas de tiempo de transmisión, no detectar ninguna señal de engaño en cualquiera de las franjas de tiempo de recepción indica una alta probabilidad de que la señal de desarme se transmitió por un dispositivo de control de alarma autorizado. Por ejemplo, cuando la pluralidad de franjas de tiempo consecutivas comprende 25 franjas de tiempo y el grupo de franjas de tiempo de transmisión comprende 5 franjas de tiempo, la probabilidad de repetir el mismo grupo exacto de franjas de tiempo es menor de 1 en 50 000. Usar menos franjas de tiempo en la pluralidad de franjas de tiempo consecutivas incrementa la probabilidad de repetir el mismo grupo exacto de franjas de tiempo. Una mayor cantidad de franjas de tiempo en la pluralidad de franjas de tiempo consecutivas o una mayor cantidad de franjas de tiempo de transmisión incrementa la seguridad reduciendo la probabilidad de repetir un mismo grupo exacto de franjas de tiempo, pero además puede incrementar el consumo de potencia debido a una conmutación más frecuente del transceptor de RF entre transmisión y recepción.

A continuación se encuentra un método implementado por el sistema 100 en algunas realizaciones de la presente invención, para detectar un intento de intrusión usando transmisión y recepción intercaladas de una señal de engaño.

La referencia se hace ahora además a la FIG. 3, que muestra un diagrama de flujo que representa esquemáticamente un flujo opcional de operaciones 300 para detectar un intento de intrusión usando transmisión y recepción intercaladas de una señal de engaño, de acuerdo con algunas realizaciones de la presente invención.

En tales realizaciones, un transceptor de RF 102 conectable eléctricamente a un procesador de señal 101 recibe en 301 una primera señal de RF de desarme desde un dispositivo de control de alarma 103. Opcionalmente, después de transmitir el primer mensaje de RF de desarme, el dispositivo de control de alarma 103 espera un acuse de recibo del procesador de señal 101 durante un tiempo de retraso predeterminado. Opcionalmente, el procesador de señal 101 divide el tiempo de retraso predeterminado de una pluralidad de franjas de tiempo consecutivas, por ejemplo 25 franjas de tiempo. Durante el tiempo de retraso predeterminado, opcionalmente el procesador de señal 101 transmite 302 una o más señales de RF de engaño durante las franjas de tiempo de transmisión seleccionadas de la pluralidad de franjas de tiempo consecutivas. Opcionalmente, cada una de las una o más señales de RF de engaño comprende al menos

uno de un identificador, un sello de tiempo y un número aleatorio. Un identificador puede usarse para identificar el origen de la señal de RF de engaño, y en particular una señal de RF grabada. Un sello de tiempo puede usarse para identificar un tiempo original de una señal de RF de engaño grabada. Un número aleatorio puede usarse para detectar una señal de RF de engaño repetida, que tiene el mismo número aleatorio. Un sello de tiempo y un identificador pueden consistir cada uno en 32 bits digitales. Un número aleatorio puede consistir en 8 bits digitales. Opcionalmente, cada una de las una o más señales de RF de engaño comprende un número de paquete en una secuencia de números de paquete. El número de paquete puede consistir en un número de 8 bits digitales. Cuando el número de paquetes consiste en 8 bits digitales, el número de paquete es un número en un módulo de secuencia 256.

Además, durante el tiempo de retraso predeterminado, el procesador de señal 101 intercepta opcionalmente en 303 una pluralidad de señales de RF durante las franjas de tiempo de recepción seleccionadas de la pluralidad de franjas de tiempo consecutivas e intercaladas con las franjas de tiempo de transmisión. Cuando una o más señales de RF de recepción se detectan en las franjas de tiempo de recepción, el receptor de RF 102 envía opcionalmente las una o más señales de RF al procesador de señal 101. Opcionalmente, el procesador de señal 101 recibe las una o más señales de RF y analiza la primera señal de RF de desarme y las una o más señales de RF para producir al menos una indicación de detección de engaño. En algunas realizaciones, analizar las una o más señales de RF comprende hacer coincidir en 304 al menos una de las una o más señales de RF con un patrón de señal de engaño predefinido. En realizaciones donde las una o más secuencias de engaño comprenden al menos uno de un identificador, un sello de tiempo y un número aleatorio, hacer coincidir una de las señales de RF con el patrón de señal de engaño predefinido comprende detectar en la una señal de RF al menos uno de un identificador, un sello de tiempo y un número aleatorio. Cuando una de las señales de RF coincide con el patrón de señal de engaño predefinido, el procesador de señal 101 produce en 305 una auténtica indicación de detección de engaño. En realizaciones donde el primer mensaje de RF de desarme comprende un número de paquete, el procesador de señal 101 puede almacenar al menos un número de paquete recibido. En tales realizaciones, analizar el primer mensaje de RF de desarme comprende detectar un número de paquete en el primer mensaje de RF de desarme y comparar una diferencia entre el número de paquete almacenado y el número de paquete detectado con un número de umbral predefinido. Cuando la diferencia es mayor que el número de umbral predefinido, el procesador de señal 101 produce opcionalmente una auténtica indicación de detección de engaño.

En 314, el procesador de señal 101 determina opcionalmente una operación de sistema de alarma de acuerdo con la al menos una indicación de detección de engaño. Los ejemplos de una operación de sistema de alarma son procesar un mensaje, enviar una señal de acuse de recibo, dar instrucciones de desarmar el sistema de alarma, hacer sonar una alarma y notificar al centro de control. Cuando al menos una auténtica indicación de detección de engaño se produce, el procesador de señal 101 determina opcionalmente un intento de intrusión en 308. Opcionalmente, el procesador de señal 101 notifica a continuación al centro de control 104 en 309. Opcionalmente, en 310 el procesador de señal 101 suministra una corriente eléctrica a uno o más dispositivos de alarma 105 capaces de emitir una señal de audio o señal visual.

Cuando ninguna indicación de detección de engaño auténtica se produce, el procesador de señal 101 determina opcionalmente una primera señal de RF de desarme válida. Opcionalmente, el procesador de señal 101 determina una primera señal de RF de desarme válida cuando ninguna señal de RF se recibe en las franjas de tiempo de recepción. En algunas realizaciones, después del tiempo de retraso predefinido el dispositivo de control de alarma 103 envía una segunda señal de RF de desarme. Opcionalmente, el procesador de señal 101 recibe la segunda señal de desarme mediante el transceptor de RF 102 en 311 tras determinar una primera señal de RF de desarme válida, y en 312 opcionalmente envía al dispositivo de control de alarma 103 una señal de RF de acuse de recibo. Opcionalmente, el procesador de señal 101 da instrucciones de desarmar el sistema de alarma en 313.

En algunas realizaciones, la al menos una señal de RF de engaño se protege por un código de detección de error. Opcionalmente, el código de detección de error es una comprobación de redundancia cíclica de 16 bits. En algunas realizaciones, la al menos una señal de RF de engaño se codifica. Opcionalmente, la al menos una señal de RF de engaño se codifica usando ofuscación. Opcionalmente, la al menos una señal de RF de engaño se codifica usando o exclusivo con una palabra clave predefinida o con una palabra clave aleatoria.

Hasta un número predeterminado de señales de RF recibidas durante una o más de las franjas de tiempo de recepción y no reconocidas como señales de RF de engaño pueden descartarse e ignorarse por el procesador de señal 101.

Otro método posible para detectar un intento de intrusión usa imperfecciones de RF de una señal. A continuación está un método opcional implementado por el sistema en algunas realizaciones de la presente invención, para detectar un intento de intrusión usando imperfecciones de RF de una señal.

La referencia se hace ahora además a la FIG. 4, que muestra un diagrama de flujo que representa esquemáticamente un flujo opcional de operaciones 400 para detectar un intento de intrusión usando imperfecciones de RF de una señal, de acuerdo con algunas realizaciones de la presente invención. En algunas realizaciones, una señal transmitida por un dispositivo de control de alarma comprende una secuencia de bits digitales codificados en una señal portadora analógica. Opcionalmente, la señal comprende un preámbulo y/o una contraseña antes de un mensaje. Opcionalmente, un transceptor de RF 102 recibe en 401 una señal de RF de preámbulo desde un dispositivo de control

de alarma 103. La señal de RF de preámbulo comprende una secuencia de bits digitales de preámbulo codificados en una señal portadora de preámbulo analógica. Opcionalmente, el transceptor de RF 102 envía la señal de RF de preámbulo recibida a un procesador de señal 101 y en 402 el procesador de señal 101 analiza la señal de RF de preámbulo para determinar una pluralidad de imperfecciones de preámbulo de la señal portadora de preámbulo analógica. Los ejemplos de imperfecciones de preámbulo son un desplazamiento de una frecuencia de la señal portadora de preámbulo analógica, un ruido de fase en la señal portadora de preámbulo analógica, un desequilibrio IQ en la señal portadora de preámbulo analógica y una no linealidad de la señal portadora de preámbulo analógica. Por ejemplo, un nivel de imprecisión de señal sinusoidal en los senos que conforman la señal portadora de preámbulo analógica (es decir, un desplazamiento de una frecuencia de la señal portadora de preámbulo analógica) puede expresarse como un intervalo normalizado de números. Por ejemplo, un subintervalo entre 0 y 1, por ejemplo 0,7-0,72. En 403, el procesador de señal opcionalmente compara la pluralidad de imperfecciones de preámbulo con una pluralidad de imperfecciones de preámbulos de referencia para determinar el cumplimiento del preámbulo. En algunas realizaciones el procesador de señal 101 usa un correlacionador que tiene un índice de muestreo de 16 bits por segundo para comparar la pluralidad de imperfecciones de preámbulo con la pluralidad de imperfecciones de preámbulo de referencia. En 404, el procesador de señal 101 opcionalmente selecciona una operación de sistema de alarma que funciona de acuerdo con el cumplimiento de preámbulo. Cuando la pluralidad de imperfecciones de preámbulo no cumple con la pluralidad de imperfecciones de preámbulo de referencia, el procesador de señal 101 determina opcionalmente un intento de intrusión en 407. Opcionalmente, el procesador de señal 101 a continuación notifica al centro de control 104 en 410. Opcionalmente, en 411, el procesador de señal 101 suministra una corriente eléctrica a uno o más dispositivos de alarma 105 capaces de emitir una señal de audio o señal visual.

Cuando la pluralidad de imperfecciones de señal de preámbulo cumple con la pluralidad de referencia de imperfecciones de señal de preámbulo, el procesador de señal 101 determina opcionalmente un mensaje válido. Cuando un mensaje se recibe en 408 tras determinar un mensaje válido, el procesador de señal 101 en 409 procesa opcionalmente el mensaje. Cuando el mensaje es un mensaje de desarme, el procesador de señal 101 da instrucciones opcionalmente de desarmar el sistema de alarma, por ejemplo, dando instrucciones al controlador de alarma 110.

Opcionalmente, el transceptor de RF 102 recibe una palabra de sincronización (palabra sinc) después del preámbulo. La referencia se hace ahora además a la FIG. 5 que muestra un diagrama de flujo que representa esquemáticamente otro flujo opcional de operaciones 500 para detectar un intento de intrusión usando imperfecciones de señal de RF de una señal, de acuerdo con algunas realizaciones de la presente invención. En tales realizaciones, tras recibir la señal de RF de preámbulo, el procesador de señal 101 recibe por el transceptor de RF 102 una señal de RF de palabra sinc en 501. La señal de RF de palabra sinc comprende una secuencia de bits digitales de palabras sinc codificados en una señal portadora de palabra sinc analógica. Opcionalmente, en 502 el procesador de señal 101 analiza la señal de red de palabra sinc para determinar una pluralidad de imperfecciones de señal de palabra sinc de la señal portadora de palabra sinc analógica. Los ejemplos de imperfecciones de señal de palabra sinc son un desplazamiento de una frecuencia de la señal portadora de palabra sinc analógica, un ruido de fase en la señal portadora de palabra sinc analógica, un desequilibrio IQ en la señal portadora de palabra sinc analógica y no linealidad de la señal portadora de palabra sinc analógica. Por ejemplo, un nivel de imprecisión de señal sinusoidal en los senos que conforman la señal portadora de palabra sinc analógica (es decir, un desplazamiento de la frecuencia de la señal portadora de contraseña analógica) puede expresarse como un intervalo. Por ejemplo, un subintervalo entre 0 y 1, por ejemplo 0,7-0,72. En 506, el procesador de señal 101 opcionalmente compara la pluralidad de imperfecciones de señal de palabra sinc con una pluralidad de imperfecciones de señal de palabra sinc de referencia para determinar el cumplimiento de palabra sinc. En algunas realizaciones, el procesador de señal 101 usa un correlacionador que tiene un índice de muestreo de 16 bits por segundo para comparar la pluralidad de imperfecciones de señal de palabra sinc con la pluralidad de imperfecciones de señal de palabra sinc de referencia. En 503, el procesador de señal 101 selecciona opcionalmente una operación de sistema de alarma que funciona de acuerdo con el cumplimiento de palabra sinc. Cuando la pluralidad de imperfecciones de señal de palabra sinc no cumple con la pluralidad de imperfecciones de señal de palabra sinc de referencia, el procesador de señal 101 determina opcionalmente un intento de intrusión en 407. Opcionalmente, el procesador de señal 101 a continuación notifica al centro de control 104 en 410. Opcionalmente, en 401 el procesador de señal 101 suministra una corriente eléctrica a uno o más dispositivos de alarma 105 capaces de emitir una señal de audio o señal visual.

Cuando la pluralidad de imperfecciones de señal de palabra sinc cumple con la pluralidad de referencia de imperfecciones de señal de palabra sinc, el procesador de señal 101 determina opcionalmente un mensaje válido. Cuando un mensaje válido se recibe en 408 tras determinar un mensaje válido, el procesador de señal 101 en 409 procesa opcionalmente el mensaje. Cuando el mensaje es un mensaje de desarme, el procesador de señal 101 da instrucciones opcionalmente de desarmar el sistema de alarma, por ejemplo dando instrucciones al controlador de alarma 110.

En algunas otras realizaciones, el procesador de señal 101 determina un mensaje válido solo cuando uno del cumplimiento de palabra sinc y el cumplimiento de preámbulo es cierto.

En algunas realizaciones, las imperfecciones de señal de referencia se producen analizando una señal de referencia transmitida por un dispositivo de control de alarma autorizado. La referencia se hace ahora a la FIG. 6, que muestra

un diagrama de flujo que representa esquemáticamente un flujo opcional de operaciones 600 para producir imperfecciones de señal de referencia, de acuerdo con algunas realizaciones de la presente invención. En tales realizaciones, el procesador de señal 101 puede recibir en 601 por el transceptor de RF 102 una señal de RF de referencia, codificando una secuencia de bits digitales de referencia en una señal portadora de referencia analógica. El procesador de señal 101 procesa opcionalmente la señal portadora de referencia analógica en 602 para obtener una pluralidad de imperfecciones de señal de preámbulo de referencia y en 603 almacena opcionalmente la pluralidad de imperfecciones de señal de preámbulo de referencia en un almacenamiento no volátil 112. De manera similar, para producir una pluralidad de imperfecciones de señal de palabra sinc, el procesador de señal 101 procesa opcionalmente la señal portadora de referencia analógica en 602 para obtener una pluralidad de imperfecciones de señal de preámbulo de palabra sinc, y en 603 opcionalmente almacena la pluralidad de imperfecciones de señal de palabra sinc de referencia en el almacenamiento no volátil 112.

Otro método posible para detectar un intento de intrusión usa instrucciones de dispositivo de control de alarma no soportadas. A continuación se encuentra un método opcional implementado por el sistema en algunas realizaciones de la presente invención, para detectar un intento de intrusión usando instrucciones de dispositivos de control de alarma no soportadas.

Ahora se hace referencia además a las FIGS. 7A y 7B, que muestran secuencias de tiempo que representan esquemáticamente un flujo opcional de operaciones para detectar un intento de intrusión usando una instrucción no soportada, de acuerdo con algunas realizaciones de la presente invención. En tales realizaciones el dispositivo de control de alarma tiene un conjunto predefinido de instrucciones soportadas. Una instrucción no soportada es una instrucción que no está en el conjunto predefinido de instrucciones soportadas. Cuando el dispositivo de control de alarma recibe una señal desde el procesador de señal que da instrucciones de una instrucción no soportada, el dispositivo de control de alarma transmite opcionalmente al procesador de señal un mensaje de señal de RF de error que incluye una indicación de la instrucción no soportada. Este protocolo se usa en algunas realizaciones para crear una señal de engaño.

La referencia se hace ahora además a la FIG. 7A, que muestra una secuencia de tiempo que representa esquemáticamente un flujo opcional de operaciones para detectar un intento de intrusión usando una instrucción no soportada con respecto a un dispositivo de control de alarma autorizado, de acuerdo con algunas realizaciones de la presente invención. En tales realizaciones, el transceptor de RF 702 recibe en 710 una primera señal de RF de desarme desde un dispositivo de control de alarma 701, y transmite en 711 una señal de RF de engaño que comprende una instrucción no soportada X seleccionada desde un grupo de instrucciones predefinidas conocidas como no soportadas por el dispositivo de control de alarma 701. Opcionalmente, la instrucción no soportada X se selecciona aleatoriamente desde el grupo de instrucciones no soportadas predefinidas. Cuando el dispositivo de control de alarma 701 se autoriza, el dispositivo de control de alarma transmite opcionalmente en 712 una respuesta de RF de error que comprende la instrucción no soportada X recibida desde el transceptor de RF 702. El transceptor de RF envía opcionalmente la respuesta de RF de error al procesador de señal 703 en 713. Opcionalmente, el procesador de señal 703 recibe la respuesta de RF de error y extrae en 714 la instrucción no soportada devuelta. En 715, el procesador de señal 703 compara opcionalmente la instrucción no soportada devuelta con la instrucción no soportada X. A continuación, el procesador de señal 703 selecciona opcionalmente una operación de sistema de alarma para enviar de acuerdo con el cumplimiento de instrucción no soportada. Cuando la instrucción no soportada devuelta cumple con X, por ejemplo es igual a X, en 716 el procesador de señal 703 determina opcionalmente un mensaje de desarme válido. Opcionalmente, en 717 el procesador de señal 703 envía al dispositivo de control de alarma 701 mediante el transceptor de RF 702 una señal de RF de respuesta que comprende una instrucción soportada seleccionada del conjunto predefinido del dispositivo de control de alarma de instrucciones soportadas. Opcionalmente, el procesador de señal 703 da instrucciones de desarmar el sistema de alarma, por ejemplo dando instrucciones al controlador de alarma.

Una secuencia de señales que incluye un mensaje de desarme y una señal de respuesta de RF que indica una instrucción errónea puede grabarse y transmitirse por un dispositivo de control de alarma no autorizado. La referencia se hace ahora además a la FIG. 7B, que muestra una secuencia de tiempo que representa esquemáticamente un flujo opcional de operaciones para detectar un intento de intrusión usando una instrucción no soportada con respecto a un dispositivo de control de alarma no autorizado, de acuerdo con algunas realizaciones de la presente invención. En tales realizaciones, en respuesta a una primera señal de RF de desarme grabada en 710, el procesador de señal 703 transmite en 721 una señal de RF de engaño que comprende otra instrucción no soportada Y seleccionada de un grupo de instrucciones predefinidas conocidas como no soportadas por el dispositivo de control de alarma 701. Opcionalmente, la instrucción no soportada Y se selecciona aleatoriamente del grupo de instrucciones no soportadas predefinidas. Cuando el dispositivo de control de alarma 701 no está autorizado, el dispositivo de control de alarma transmite opcionalmente en 712 una respuesta de RF de error grabada que comprende la instrucción no soportada grabada X. El transceptor de RF envía opcionalmente la respuesta de RF de error al procesador de señal 703 en 713. Opcionalmente, el procesador de señal 703 recibe la respuesta de RF de error y extrae en 714 la instrucción no soportada devuelta. En 715, el procesador de señal 703 compara opcionalmente la instrucción no soportada devuelta con la instrucción no soportada Y. A continuación, el procesador de señal 703 selecciona opcionalmente una operación de sistema de alarma para enviar de acuerdo con el cumplimiento de instrucción no soportada. Cuando la instrucción no soportada devuelta (X) no cumple con Y, por ejemplo es diferente de Y, en 724 el procesador de señal 703

determina opcionalmente un intento de intrusión. Opcionalmente, el procesador de señal a continuación notifica al centro de control. Opcionalmente, el procesador de señal suministra una corriente eléctrica a uno o más dispositivos de alarma capaces de emitir una señal de audio o una señal visual.

Normalmente, un dispositivo de control de alarma soporta solo varias funciones, normalmente menos de 100. Cuando la instrucción no soportada se representa por una palabra digital de 16 bits y una instrucción no soportada transmitida por el transceptor al dispositivo de control de alarma se selecciona aleatoriamente, la probabilidad de seleccionar la misma instrucción no soportada grabada está cerca de 2^16. Comparar una indicación de instrucción no soportada recibida con una indicación de instrucción no soportada transmitida tiene una alta probabilidad de detectar una señal de RF de error grabada.

Un sistema de alarma posible comprende al menos un transceptor de radiofrecuencia (RF) configurado para recibir una señal de RF de preámbulo desde un dispositivo de control de alarma, la señal de RF de preámbulo que comprende una secuencia de bits digitales de preámbulo codificados en una señal portadora de preámbulo analógica; y al menos un procesador de señal conectado eléctricamente al al menos un transceptor de RF, configurado para: analizar la señal de RF de preámbulo para determinar una pluralidad de imperfecciones de señal de preámbulo de la señal portadora de preámbulo analógica, las imperfecciones de señal de preámbulo que comprenden al menos uno de una imperfección de frecuencia de una señal sinusoidal, una imperfección de amplitud de la señal sinusoidal y una imperfección de fase de la señal sinusoidal; comparar la pluralidad de imperfecciones de señal de preámbulo con una pluralidad de imperfecciones de señal de preámbulo de referencia para determinar un cumplimiento de preámbulo; recibir mediante el al menos un transceptor de RF una señal de RF de mensaje desde el dispositivo de control de alarma, la señal de RF de mensaje que comprende una secuencia de bits digitales de mensaje codificados en una señal portadora de mensaje analógica; y realizar una operación de sistema de alarma de acuerdo con el cumplimiento de preámbulo.

Opcionalmente, el al menos un procesador de señal se configura además para determinar un intento de intrusión, sometido a al menos una de la pluralidad de imperfecciones de señal de preámbulo que fallan al cumplir con la pluralidad de imperfecciones de señal de preámbulo de referencia.

Opcionalmente, el al menos un procesador de señal se configura además para determinar un mensaje válido sometido a la pluralidad de imperfecciones de señal de preámbulo que cumplen con la pluralidad de imperfecciones de señal de preámbulo de referencia; y en el que la operación de sistema de alarma comprende procesar la señal de RF de mensaje.

Opcionalmente, la pluralidad de imperfecciones de señal de preámbulo de referencia comprende al menos una característica de preámbulo seleccionada del grupo de: un desplazamiento de frecuencia portadora, un ruido de fase, un desequilibrio en fase y cuadratura (desequilibrio IQ) y una no linealidad de señal.

Opcionalmente, el al menos un procesador de señal se configura además para: recibir mediante el al menos un transceptor de RF después de la señal de preámbulo una señal de RF de palabra de sincronización (palabra sinc) desde el dispositivo de control de alarma, la señal de RF de palabra sinc que comprende una secuencia de bits digitales de palabra sinc codificados en una señal portadora de palabra sinc analógica; analizar la señal portadora de palabra sinc analógica para determinar una pluralidad de imperfecciones de señal de palabra sinc de la señal de palabra sinc, las imperfecciones de señal de palabra sinc que comprenden al menos uno de una imperfección de frecuencia de la señal sinusoidal, imperfección de amplitud de la señal sinusoidal y una imperfección de fase de la señal sinusoidal; comparar la pluralidad de imperfecciones de señal de palabra sinc con una pluralidad de imperfecciones de señal de palabra sinc de referencia para determinar un cumplimiento de palabra sinc; y realizar la operación del sistema de alarma de acuerdo con el cumplimiento de preámbulo y el cumplimiento de palabra sinc.

Opcionalmente, el al menos un procesador de señal se configura además para determinar un intento de intrusión, sometido a al menos uno de la pluralidad de imperfecciones de señal de palabra sinc que fallan al cumplir con la pluralidad de imperfecciones de señal de palabra sinc de referencia, o al menos una de la pluralidad de imperfecciones de señal que fallan al cumplir con la pluralidad de imperfecciones de señal de referencia.

Opcionalmente, el al menos un procesador de señal se configura además para determinar un mensaje válido sometido a la pluralidad de imperfecciones de señal de preámbulo que cumplen con la pluralidad de imperfecciones de señal de preámbulo de referencia y la pluralidad de imperfecciones de señal de palabra sinc que cumplen con la pluralidad de imperfecciones de señal de palabra sinc de referencia, y la operación del sistema de alarma comprende procesar la señal de RF de mensaje.

Opcionalmente, la pluralidad de imperfecciones de señal de palabra sinc de referencia comprende al menos una característica de palabra sinc seleccionada del grupo de: un desplazamiento de frecuencia portadora, un ruido de fase, un desequilibrio IQ y una no linealidad de señal.

Opcionalmente, la operación del sistema de alarma comprende notificar al centro de control que comprende al menos un procesador de hardware después de determinarse la intrusión intentada.

Opcionalmente, sistema de alarma comprende además un dispositivo capaz de emitir una señal de audio o señal visual, eléctricamente conectado al al menos un procesador de señal; y la operación del sistema de alarma comprende suministrar una corriente eléctrica al dispositivo después de determinarse la intrusión intentada.

Opcionalmente, el sistema de alarma comprende además un almacenamiento digital no volátil acoplado eléctricamente con el al menos un procesador de señal; y el al menos un procesador de señal se configura además para: recibir por el al menos un transceptor de RF una señal de RF de referencia, codificar una secuencia de bits digitales de referencia en una señal portadora de referencia analógica; procesar la señal portadora de referencia analógica para obtener la pluralidad de imperfecciones de señal de preámbulo de referencia; y almacenar las imperfecciones de señal de preámbulo de referencia en el almacenamiento digital no volátil.

Opcionalmente, la comparación se hace usando un correlacionador con un índice de muestreo de 16 bits por segundo.

Un método posible para un sistema de alarma comprende: recibir una señal de RF de preámbulo desde un dispositivo de control de alarma, la señal de RF de preámbulo que comprende una secuencia de bits digitales de preámbulo codificados en una señal portadora de preámbulo analógica; analizar la señal de RF de preámbulo para determinar una pluralidad de imperfecciones de señal de preámbulo de la señal portadora de preámbulo analógica, las imperfecciones de señal de preámbulo que comprenden al menos uno de una imperfección de frecuencia de una señal sinusoidal, una imperfección de amplitud de una señal sinusoidal y una imperfección de fase de la señal sinusoidal; comparar la pluralidad de imperfecciones de señal de preámbulo con una pluralidad de imperfecciones de señal de preámbulo de referencia para determinar un cumplimiento de preámbulo; recibir mediante el al menos un transceptor de RF una señal de RF de mensaje desde el dispositivo de control de alarma, la señal de referencia de mensaje que comprende una secuencia de bits digitales de mensaje codificados en una señal portadora de mensaje analógica; y realizar una operación de sistema de alarma de acuerdo con el cumplimiento de preámbulo.

Un posible sistema de alarma, comprende al menos un transceptor de radiofrecuencia (RF) configurado para: recibir una primera señal de RF de desarme desde un dispositivo de control de alarma; transmitir, después de recibir la primera señal de RF de desarme, una señal de RF de engaño al dispositivo de control de alarma, la señal de RF de engaño que comprende una instrucción no soportada seleccionada del grupo de instrucciones predefinidas no soportadas por el dispositivo de control de alarma; y recibir una respuesta de RF de error desde dicho dispositivo de control de alarma, la respuesta de RF de error que comprende una indicación de una instrucción no soportada devuelta; y al menos un procesador de señal conectado eléctricamente al al menos un transceptor de RF, configurado para: recibir la respuesta de RF de error desde el transceptor de RF; extraer la instrucción no soportada devuelta desde la respuesta de RF de error; comparar la instrucción no soportada devuelta con la instrucción no soportada para determinar un cumplimiento; y enviar una operación del sistema de alarma de acuerdo con el cumplimiento.

Opcionalmente, el al menos un procesador de señal se configura además para determinar un intento de intrusión, sometido a la instrucción no soportada devuelta que difiere de la instrucción no soportada.

Opcionalmente, el al menos un procesador de señal se configura además para determinar un mensaje de desarme válido sometido a la instrucción no soportada devuelta que es igual a la instrucción no soportada; y la operación del sistema de alarma comprende al menos uno de un grupo de: dar instrucciones del desarme de dicho sistema de alarma y transmitir mediante dicho al menos un transceptor de RF una señal de RF de respuesta que comprende una instrucción soportada.

Opcionalmente, la operación del sistema de alarma comprende notificar al centro de control que comprende al menos un procesador de hardware después de detectarse la intrusión intentada.
Opcionalmente, el sistema de alarma comprende además un dispositivo capaz de emitir una señal de audio o señal visual, conectado eléctricamente al al menos un procesador de señal; y la operación del sistema de alarma comprende suministrar una corriente eléctrica al dispositivo después de detectarse la intrusión intentada.

Opcionalmente, la instrucción no soportada se selecciona aleatoriamente del grupo de instrucciones predefinidas; y la instrucción no soportada se representa como una palabra digital de 16 bits.

Un método posible para un sistema de alarma comprende: recibir una primera señal de RF de desarme desde un dispositivo de control de alarma; transmitir, después de recibir la primera señal de RF de desarme, una señal de RF de engaño al dispositivo de control de alarma, la señal de RF de engaño que comprende una instrucción no soportada seleccionada del grupo de instrucciones predefinidas no soportadas por el dispositivo de control de alarma; recibir una respuesta de RF de error desde el dispositivo de control de alarma, la respuesta de RF de error que comprende una indicación de una instrucción no soportada devuelta; extraer la instrucción no soportada devuelta desde la respuesta de RF de error; comparar la instrucción no soportada devuelta con la instrucción no soportada para determinar un cumplimiento; y enviar una operación del sistema de alarma de acuerdo con el cumplimiento.

Las descripciones de las diversas realizaciones de la presente invención se han presentado con fines de ilustración, pero no pretenden ser exhaustivas o limitarse a las realizaciones divulgadas. Muchas modificaciones y variaciones

serán aparentes para los expertos en la materia sin apartarse del alcance y espíritu de las realizaciones descritas. La terminología usada en este caso se eligió para explicar mejor los principios de las realizaciones, la aplicación práctica o mejora técnica sobre tecnologías encontradas en el mercado, o para permitir a otros expertos en la materia entender las realizaciones aquí divulgadas.

Se espera que durante la vida de la patente que madura de esta solicitud muchos dispositivos de control de alarma relevantes se desarrollen y el alcance del término “dispositivo de control de alarma” pretenda incluir todas esas nuevas tecnologías a priori.

Tal como se usa en este caso el término “aproximadamente” se refiere a ± 10 %.

Los términos “comprende”, “que comprende”, “incluye”, “que incluye”, “que tiene” y sus conjugados significan “incluyendo pero sin limitarse a”. Este término abarca los términos “que consiste en” y “que consiste esencialmente en”.

La frase “que consiste esencialmente en” significa que la composición o método puede incluir ingredientes y/o etapas adicionales, pero solo si los ingredientes y/o etapas adicionales no alteran materialmente las características básicas y nuevas de la composición o método reivindicado.

Tal como se usa en este caso, las formas singulares “uno”, “una” y “el” incluyen referencias en plural a menos que el contexto indique claramente lo contrario. Por ejemplo, el término “un compuesto” o “al menos un compuesto” puede incluir una pluralidad de compuestos, incluyendo mezclas de los mismos.

La palabra “ejemplar” se usa en este caso para significar “que sirve como un ejemplo, caso o ilustración”. Cualquier realización descrita como “ejemplar” no necesita interpretarse necesariamente como preferente o ventajosa sobre otras realizaciones y/o para excluir la incorporación de características desde otras realizaciones.

La palabra “opcionalmente” se usa en este caso para significar “que se proporciona en algunas realizaciones y no se proporciona en otras realizaciones”. Cualquier realización particular de la invención puede incluir una pluralidad de características “opcionales” a menos que tales características entren en conflicto.

A través de esta solicitud, diversas realizaciones de la invención pueden presentarse en un formato de intervalo. Debería entenderse que esta descripción en formato de intervalo es únicamente por conveniencia y brevedad y no debería interpretarse como una limitación inflexible del alcance de la invención. Por consiguiente, la descripción de un intervalo debería considerarse como que ha divulgado específicamente todos los posibles subintervalos así como valores numéricos individuales dentro de ese intervalo. Por ejemplo, la descripción de un intervalo tal como de 1 a 6 debería considerarse como que ha divulgado específicamente subintervalos tal como de 1 a 3, de 1 a 4, de 1 a 5, de 2 a 4, de 2 a 6, de 3 a 6, etc., así como también números individuales dentro del intervalo, por ejemplo, 1, 2, 3, 4, 5 y 6. Esto se aplica independientemente de la amplitud del intervalo.

Siempre que un intervalo numérico se indique en este caso, pretende incluir cualquier número mencionado (fraccionario o integral) dentro del intervalo indicado. Las frases “variando/que varía entre” un primer número indicado y un segundo número indicado y “variando/que varía desde” un primer número indicado “a” un segundo número indicado se usan de manera intercambiable en este caso y pretenden incluir el primer y segundo número indicado y todos los números fraccionarios e integrales entre medias.

Se apreciará que algunas características de la invención que, por claridad, se describen en el contexto de realizaciones separadas, también puede proporcionarse en combinación en una única realización. Al contrario, diversas características de la invención, que por brevedad, se describen en el contexto de una única realización, también pueden proporcionarse por separado o en cualquier combinación adecuada o como sea adecuado en otra realización cualquiera descrita de la invención. Algunas características descritas en el contexto de diversas realizaciones no pretenden considerarse características esenciales de esas realizaciones, a menos que la realización sea inoperativa sin esos elementos.

Todas las publicaciones, patentes y solicitudes de patente mencionadas en esta memoria descriptiva se incorporan por tanto en su totalidad por referencia en la memoria descriptiva, en la misma extensión como si cada publicación individual, patente o solicitud de patente se indicara específicamente e individualmente como incorporada en este caso por referencia. Además, la mención o identificación de cualquier referencia en esta solicitud no deberá interpretarse como admisión de que tal referencia está disponible como técnica anterior en la presente invención. En la extensión en que los encabezamientos de sección se usan, estos no deberían interpretarse como necesariamente limitantes.

Se entenderá que la invención se ha descrito antes solo a modo de ejemplo, y las modificaciones de los detalles pueden realizarse dentro del alcance de la invención.

Cada característica divulgada en esta descripción, y (donde sea apropiado) las reivindicaciones y dibujos puede proporcionarse independientemente o en cualquier combinación apropiada.

Los números de referencia que aparecen en las reivindicaciones son solo a modo de ilustración y no deberían tener un efecto limitante en el alcance de las reivindicaciones.

REIVINDICACIONES

1. Un sistema de alarma (100) que comprende:

al menos un transceptor de radiofrecuencia (RF) (102) configurado para:

recibir una primera señal de RF de desarme (201) desde un dispositivo de control de alarma (103);
durante un tiempo de retraso predeterminado después de recibir dicha primera señal de RF de desarme, transmitir al menos una señal de RF de engaño (220) durante una o más franjas de tiempo de transmisión seleccionadas de una pluralidad de franjas de tiempo consecutivas de dicho tiempo de retraso predeterminado, y determinar si una o más señales de RF de recepción (250) se reciben durante una o más franjas de tiempo de recepción seleccionadas de dicha pluralidad de franjas de tiempo consecutivas, dichas una o más franjas de tiempo de recepción intercaladas con dichas una o más franjas de tiempo de transmisión; y

al menos un procesador de señal (101), eléctricamente conectado a dicho al menos un transceptor de RF, configurado para:
determinar una operación de sistema de alarma de acuerdo con el análisis de dichas una o más señales de RF de recepción.

2. El sistema (100) de la reivindicación 1, en el que dicho análisis comprende:

hacer coincidir al menos una de dichas señales de RF de recepción (250) con un patrón de señal de engaño predefinido;
producir una auténtica indicación de detección de engaño para cada una de dichas una o más señales de RF de recepción que coinciden con dicho patrón de señal de engaño predefinido; y
seleccionar dicha operación de sistema de alarma de acuerdo con dicha auténtica indicación de detección de engaño.

3. El sistema (100) de la reivindicación 1 o 2, en el que dicho análisis comprende:

producir una falsa indicación de detección de engaño sometida a ninguna de dichas una o más señales de RF de recepción (250) que se reciben durante dichas una o más franjas de tiempo de recepción o cada una de dichas una o más señales de RF de recepción que fallan al coincidir con dicho patrón de señal de engaño predefinido; y
seleccionar dicha operación de sistema de alarma de acuerdo con dicha falsa indicación de detección de engaño.

4. El sistema (100) de cualquier reivindicación anterior, en el que dicho al menos un procesador de señal (101) se configura además para:

determinar si dicha primera señal de RF de desarme (201) es válida, sometida a no recibir ninguna de dichas una o más señales de RF de recepción (250) o producir solo una falsa indicación de detección de engaño; y
recibir una segunda señal de RF de desarme (202) desde dicho dispositivo de control de alarma (103) después de dicho tiempo de retraso predeterminado;
en el que, tras recibir dicha segunda señal de RF de desarme, dicha operación de sistema de alarma comprende al menos uno de: dar instrucciones de desarmar dicho sistema de alarma, y transmitir una señal de RF de acuse de recibo a dicho dispositivo de control de alarma mediante dicho al menos un transceptor de RF (102).

5. El sistema (100) de cualquier reivindicación anterior, en el que dichas franjas de tiempo de transmisión se seleccionan aleatoriamente por dicho procesador de señal (101) tras recibir dicha primera señal de RF de desarme (201) para transmitir dicha al menos una señal de RF de engaño (220); y
en el que dichas franjas de tiempo de recepción comprenden todas de dicha pluralidad de franjas de tiempo consecutivas diferentes de dichas franjas de tiempo de transmisión.

6. El sistema (100) de cualquier reivindicación anterior, en el que una cantidad de dichas franjas de tiempo de transmisión está entre 15 % y 30 % de una cantidad de dicha pluralidad de franjas de tiempo consecutivas.

7. El sistema (100) de cualquier reivindicación anterior, en el que dicho tiempo de retraso predeterminado se divide en 25 franjas de tiempo consecutivas.

8. El sistema (100) de cualquier reivindicación anterior, en el que al menos una señal de RF de engaño (220) comprende al menos uno de: un identificador, un sello de tiempo y un número aleatorio, para el uso al identificar un origen de una señal de RF de engaño grabada.

9. El sistema (100) de la reivindicación 8, en el que dicho identificador consiste en 32 bits binarios, en el que dicho sello de tiempo consiste en 32 bits binarios, y en el que dicho número aleatorio consiste en 8 bits binarios.

10. El sistema (100) de la reivindicación 8 o 9, en el que dicha coincidencia de dicho patrón de señal de engaño predefinido comprende detectar en dicha una señal de RF de recepción (250) al menos uno de: un identificador, un

sello de tiempo y un número aleatorio.

11. El sistema (100) de cualquier reivindicación anterior, en el que dicha al menos una señal de RF de engaño (220) está protegida por un código de detección de error que es una comprobación de redundancia cíclica de 16 bits.

12. El sistema (100) de cualquier reivindicación anterior, en el que dicha al menos una señal de RF de engaño (220) se codifica usando un método seleccionado del grupo de: ofuscación, o exclusivo con una palabra clave predefinida y o exclusivo con una palabra clave aleatoria.

13. El sistema (100) de cualquier reivindicación anterior, en el que dicho análisis comprende además:

detectar un número de paquete en dicha primera señal de RF de desarme (201);
comparar una diferencia entre dicho número de paquete y un número de paquete almacenado previamente con un número de umbral predefinido; y
producir una auténtica indicación de detección de engaño cuando dicha diferencia es mayor que dicho número de umbral predefinido.

14. El sistema (100) de cualquier reivindicación anterior, en el que dicha operación de sistema de alarma comprende al menos una operación seleccionada del grupo que comprende: notificar a un centro de control (104) operativamente conectado a dicho al menos un procesador de señal (101) de una intrusión intentada, sometida a producir al menos una auténtica indicación de detección de engaño y suministrar una corriente eléctrica a un dispositivo (105) capaz de emitir una señal de audio o señal visual, eléctricamente conectado a dicho al menos un procesador de señal (101), sometido a producir al menos una auténtica indicación de detección de engaño.

15. Un método para un sistema de alarma (100), que comprende:

recibir una primera señal de RF de desarme (201) desde un dispositivo de control de alarma (103);
durante un tiempo de retraso predeterminado tras recibir dicha primera señal de RF de desarme, transmitir al menos una señal de RF de engaño (220) durante una o más franjas de tiempo de transmisión seleccionadas desde una pluralidad de franjas de tiempo consecutivas de dicho tiempo de retraso predeterminado, y determinar si una o más señales de RF de recepción (250) se reciben durante una o más franjas de tiempo de recepción seleccionadas de dicha pluralidad de franjas de tiempo consecutivas, dichas una o más franjas de tiempo de recepción intercaladas con dichas una o más franjas de tiempo de transmisión; y
determinar una operación de sistema de alarma de acuerdo con el análisis de dichas una o más señales de RF de recepción.

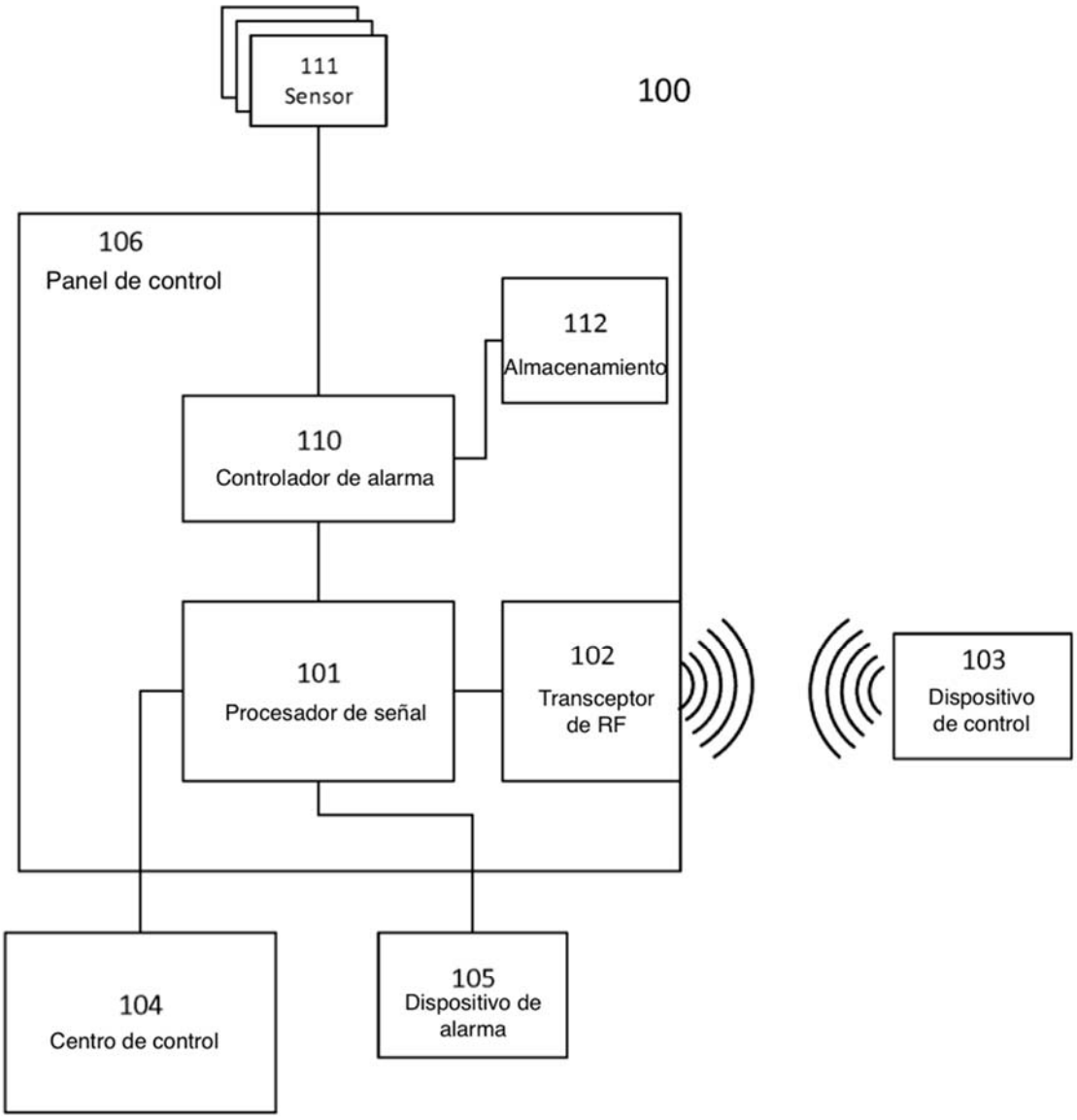

111
Sensor
100
106
Panel de control
112
Almacenamiento
110
Controlador de alarma
101
Procesador de señal
102
Transceptor de RF
103
Dispositivo de control
104
Centro de control
105
Dispositivo de alarma

FIG. 1

FIG. 2A

FIG. 2B

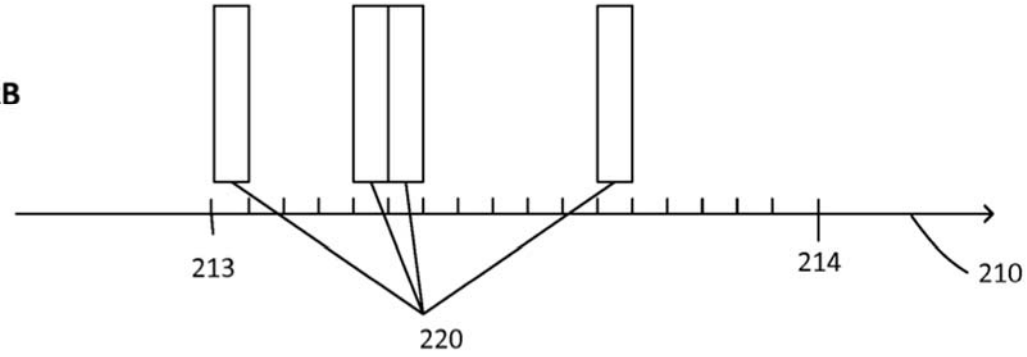
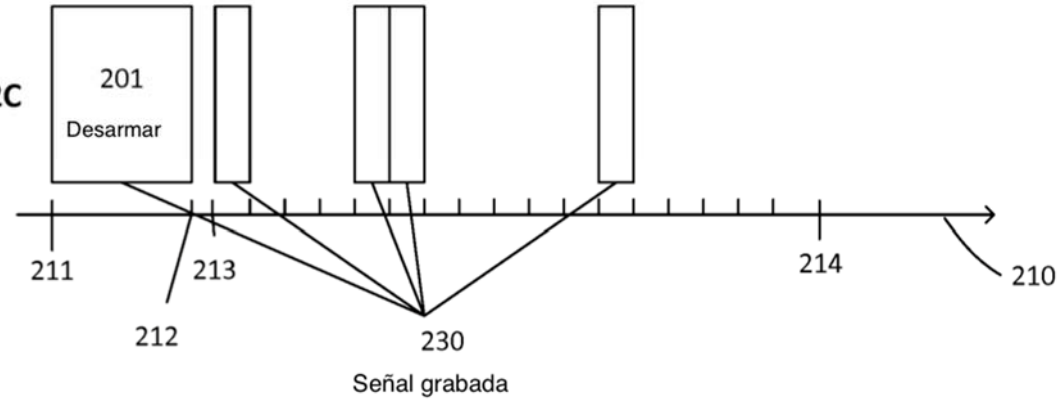


FIG. 2C



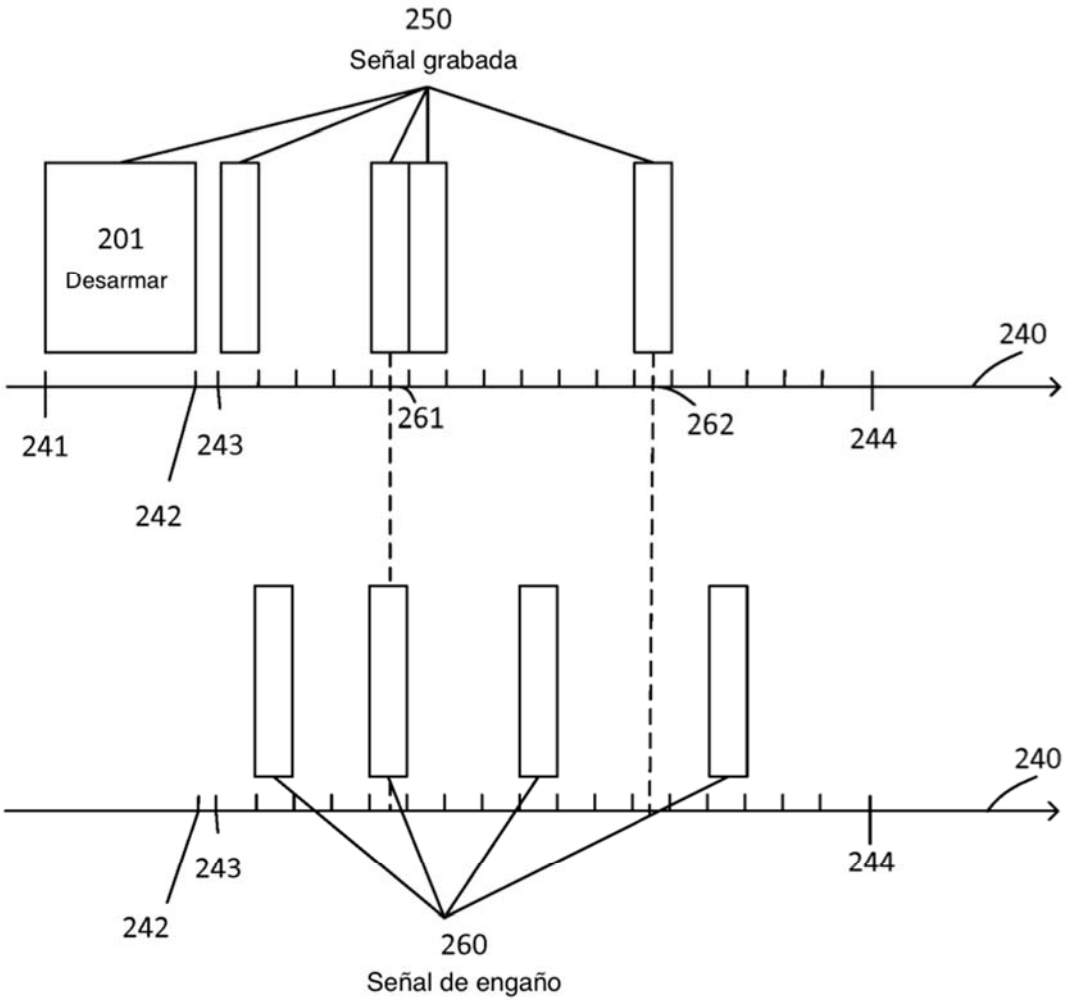

250
Señal grabada
201
Desarmar
240
241
242
243
261
262
244
240
243
242
244
260
Señal de engaño

FIG. 2D

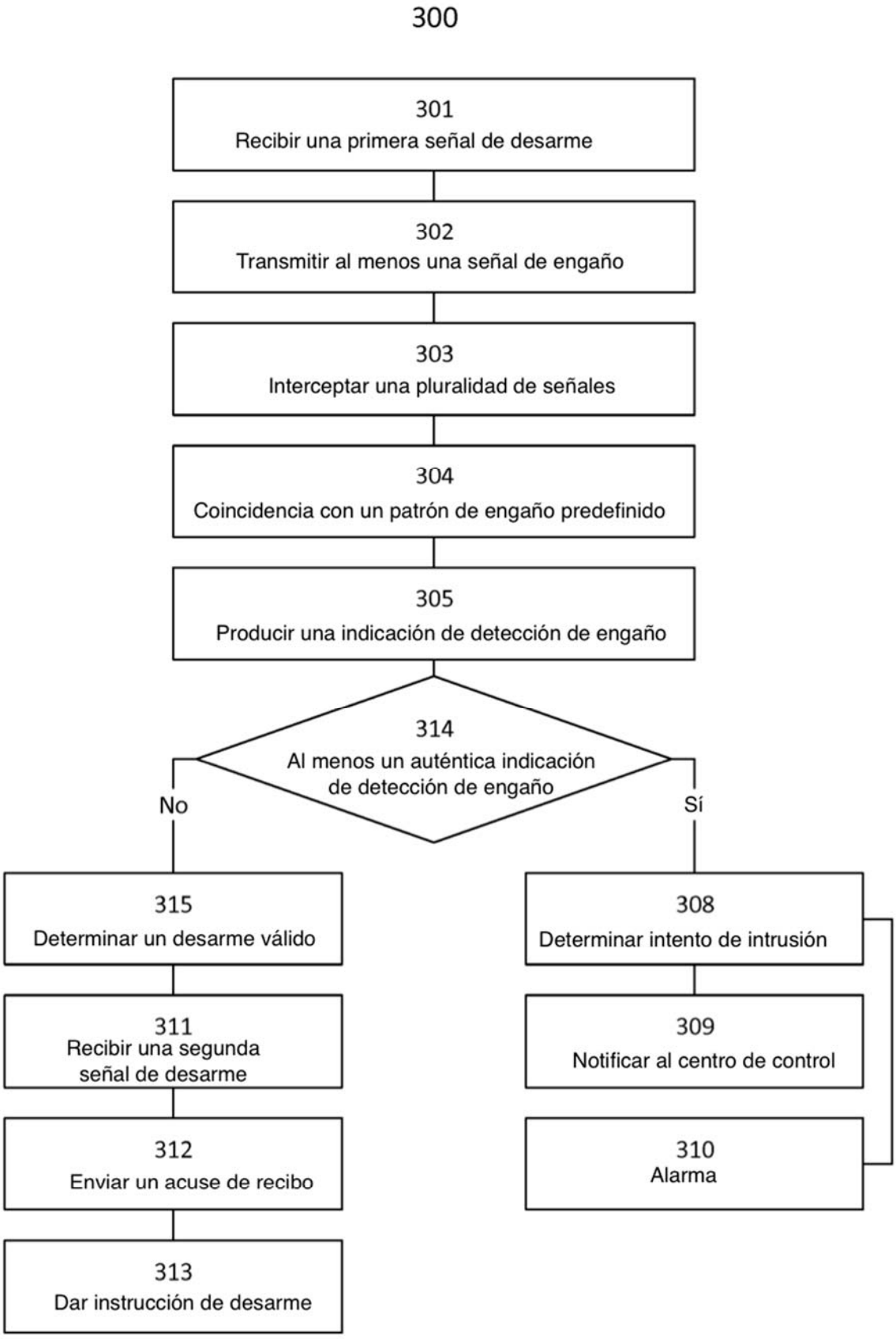

300
301
Recibir una primera señal de desarme
302
Transmitir al menos una señal de engaño
303
Interceptar una pluralidad de señales
304
Coincidencia con un patrón de engaño predefinido
305
Producir una indicación de detección de engaño
314
Al menos un auténtica indicación de detección de engaño
No
Sí
315
Determinar un desarme válido
311
Recibir una segunda señal de desarme
312
Enviar un acuse de recibo
313
Dar instrucción de desarme
308
Determinar intento de intrusión
309
Notificar al centro de control
310
Alarma

FIG. 3

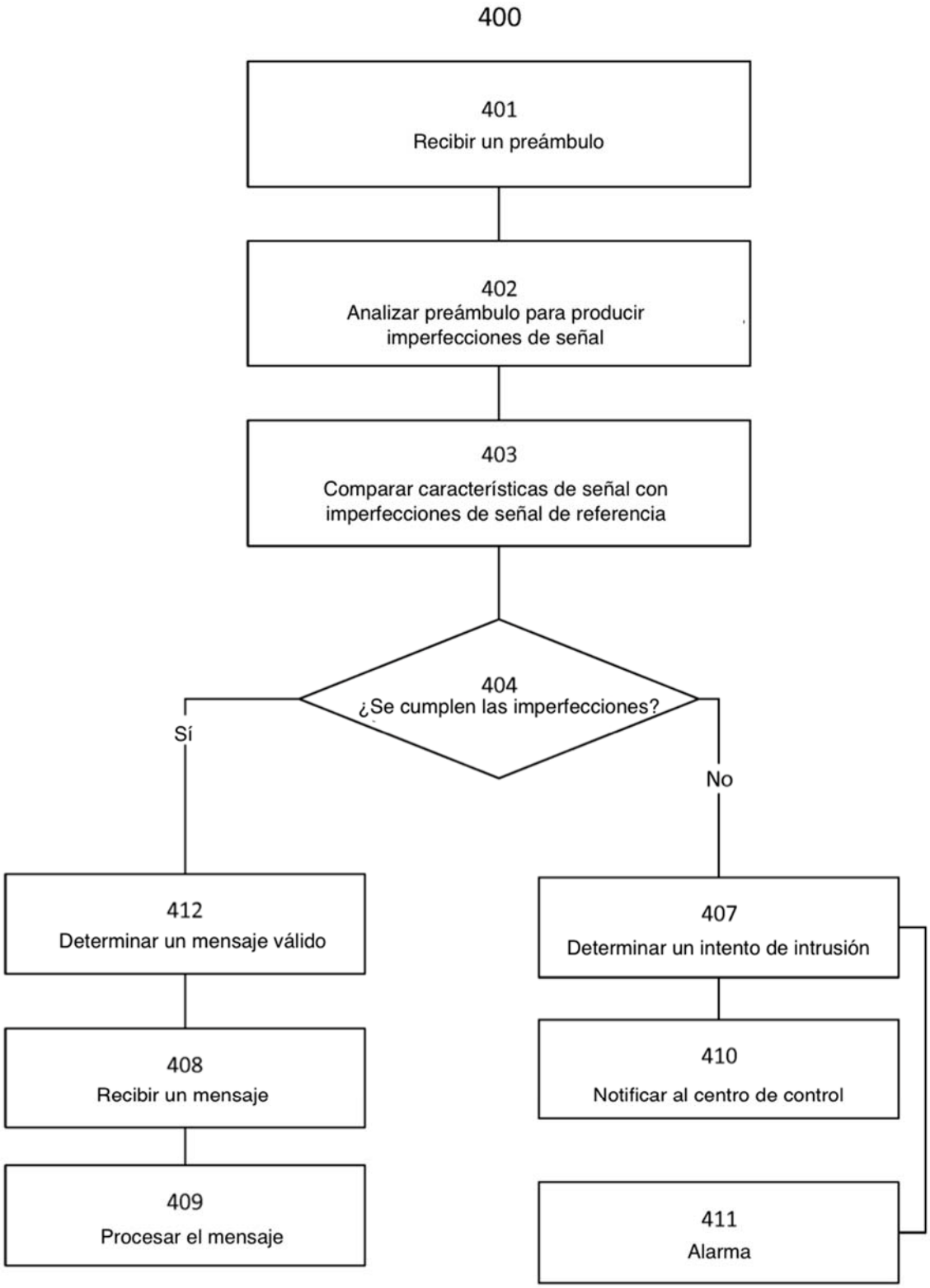

400
401
Recibir un preámbulo
402
Analizar preámbulo para producir imperfecciones de señal
403
Comparar características de señal con imperfecciones de señal de referencia
404
¿Se cumplen las imperfecciones?
Sí
No
412
Determinar un mensaje válido
408
Recibir un mensaje
409
Procesar el mensaje
407
Determinar un intento de intrusión
410
Notificar al centro de control
411
Alarma

FIG. 4

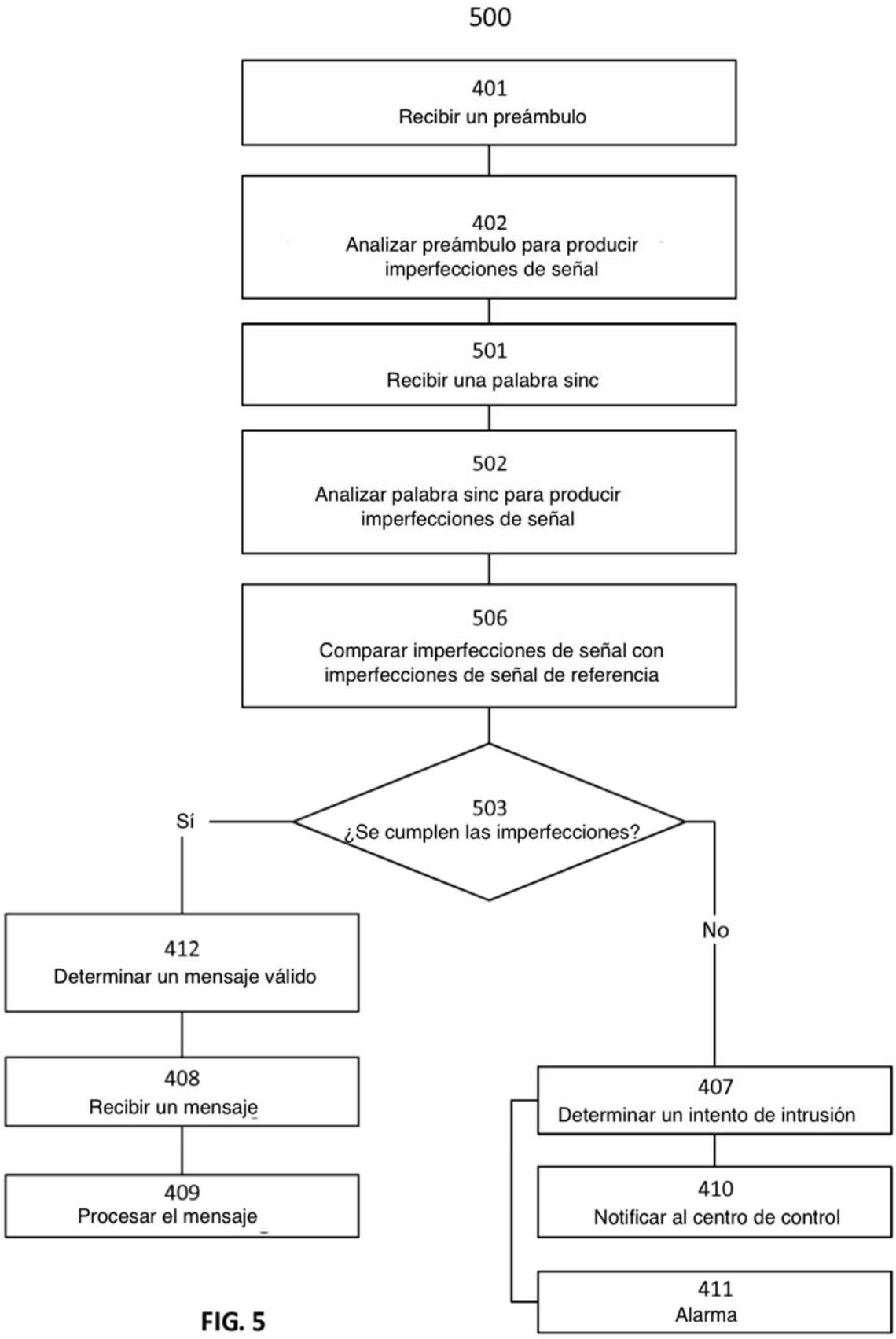

500
401
Recibir un preámbulo
402
Analizar preámbulo para producir imperfecciones de señal
501
Recibir una palabra sinc
502
Analizar palabra sinc para producir imperfecciones de señal
506
Comparar imperfecciones de señal con imperfecciones de señal de referencia
503
¿Se cumplen las imperfecciones?
Sí
No
412
Determinar un mensaje válido
408
Recibir un mensaje
409
Procesar el mensaje
407
Determinar un intento de intrusión
410
Notificar al centro de control
411
Alarma

FIG. 5

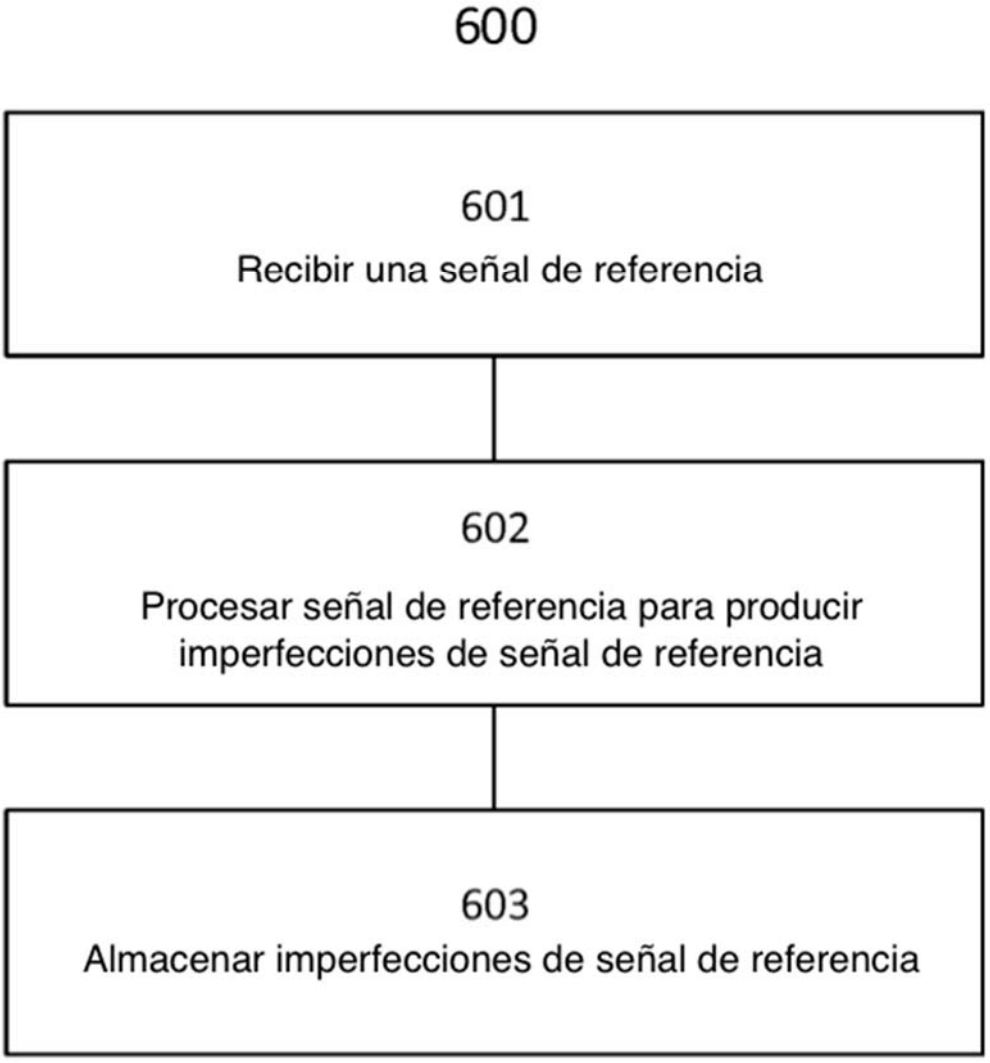

600
601
Recibir una señal de referencia
602
Procesar señal de referencia para producir imperfecciones de señal de referencia
603
Almacenar imperfecciones de señal de referencia

FIG. 6

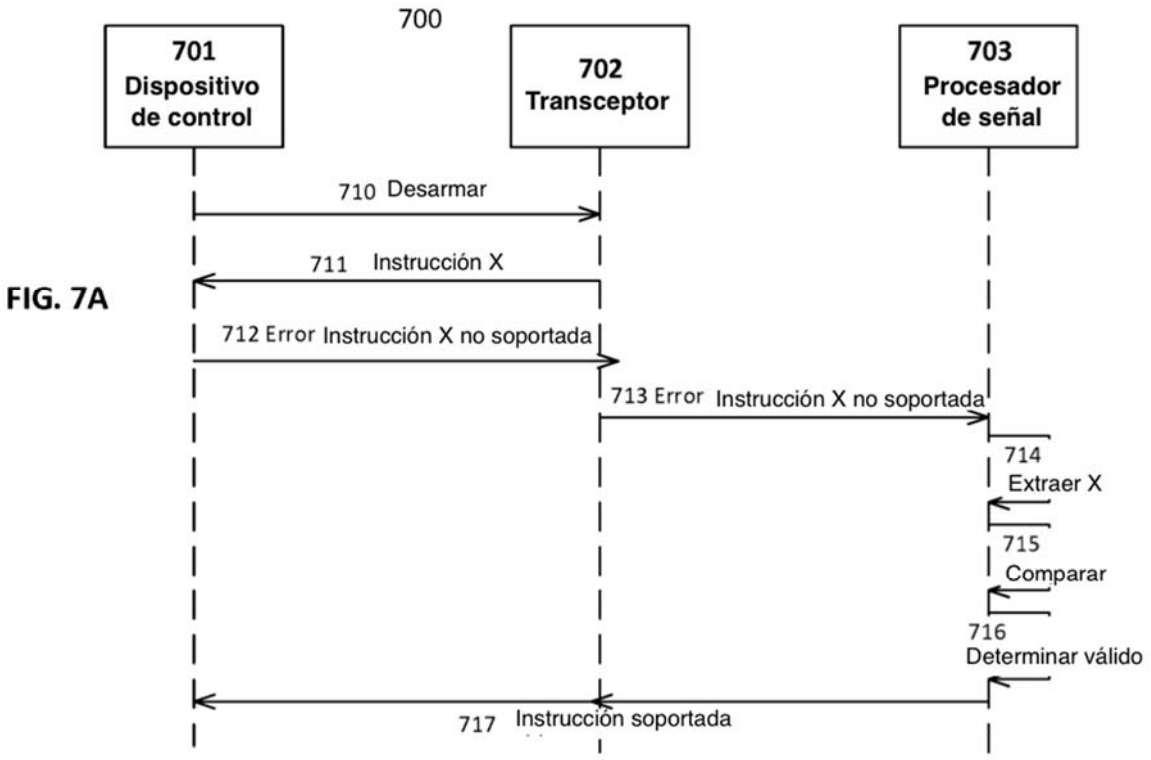

700
701 Dispositivo de control
702 Transceptor
703 Procesador de señal
710 Desarmar
711 Instrucción X
712 Error Instrucción X no soportada
713 Error Instrucción X no soportada
714 Extraer X
715 Comparar
716 Determinar válido
717 Instrucción soportada

FIG. 7A

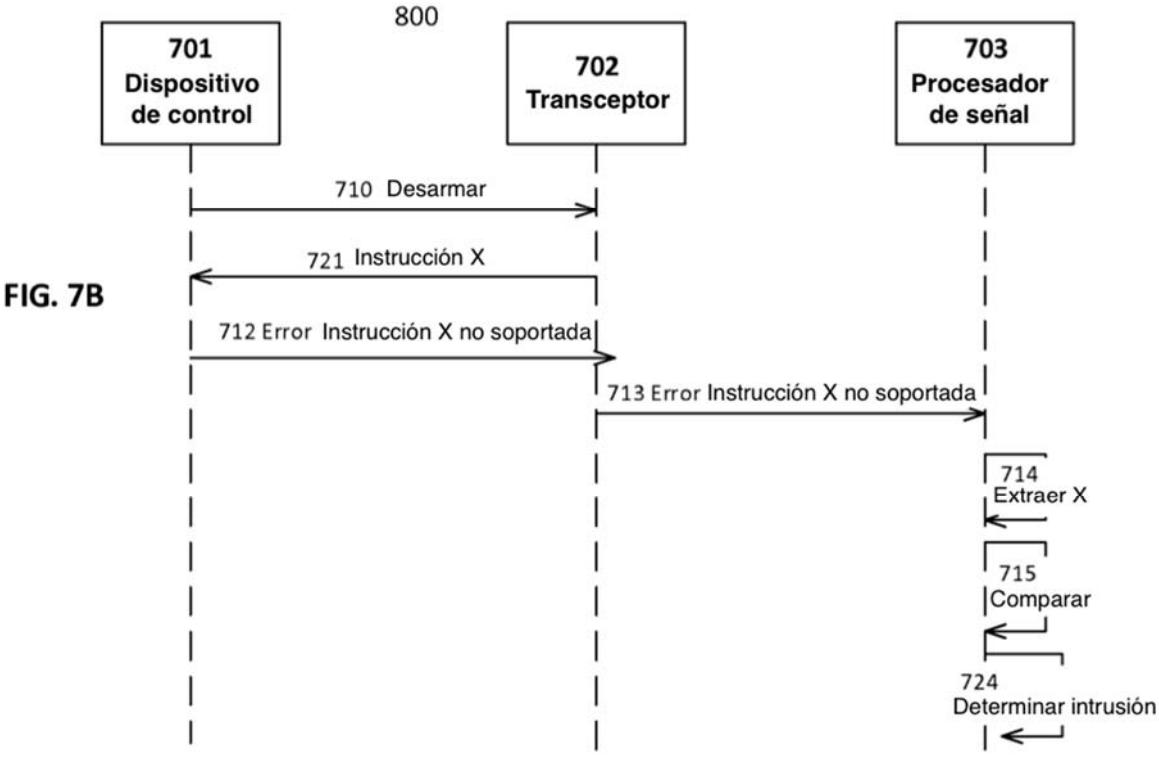

800
701 Dispositivo de control
702 Transceptor
703 Procesador de señal
710 Desarmar
721 Instrucción X
712 Error Instrucción X no soportada
713 Error Instrucción X no soportada
714 Extraer X
715 Comparar
724 Determinar intrusión

FIG. 7B