(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 691 531**

(51) Int. CI.:

G08B 25/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.02.2016 E 16155077 (7)**

(97) Fecha y número de publicación de la concesión europea: **05.09.2018 EP 3059719**

(54) Título: **Sistema de alarma basado en la nube con supervisión y notificación de alarmas**

(30) Prioridad:

17.02.2015 US 201514623698

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.11.2018

(73) Titular/es:

HONEYWELL INTERNATIONAL INC. (100.0%)
115 Tabor Road, M/S 4D3, P.O. Box 377
Morris Plains, NJ 07950, US

(72) Inventor/es:

PROBIN, ROBERT JOHN y
LEGRIS, LAURENT

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Sistema de alarma basado en la nube con supervisión y notificación de alarmas

Campo

Esta solicitud se refiere a sistemas de seguridad y, más en particular, a sistemas de seguridad en áreas pequeñas.

Antecedentes

Se conocen sistemas para proteger a personas y bienes en áreas protegidas. Tales sistemas se basan normalmente en el uso de uno o más sensores que detectan amenazas en el área protegida.

Las amenazas contra las personas y bienes pueden deberse a diferentes causas. Por ejemplo, un incendio puede matar o herir a personas que han quedado atrapadas por el incendio en su hogar. Asimismo, el monóxido de carbono de un incendio puede matar a personas mientras duermen.

Por otro lado, un intruso no autorizado, tal como un ladrón, puede suponer una amenaza para los bienes dentro del área. Se sabe que los intrusos hieren o matan a las personas que viven en el área.

En el caso de los intrusos, pueden colocarse sensores en diferentes áreas según el respectivo uso de tales áreas. Por ejemplo, si hay personas presentes en algunos tramos de un día normal y no en otros momentos, entonces los sensores pueden colocarse a lo largo de una periferia del espacio para ofrecer protección cuando el espacio está ocupado, mientras que sensores adicionales pueden estar ubicados en el interior del espacio y usarse cuando el espacio no está ocupado.

En la mayoría de los casos, los detectores de amenazas están conectados a un panel de control local. En caso de que se detecte una amenaza a través de los sensores, el panel de control puede hacer sonar una alarma local audible. El panel de control también puede enviar una señal a una estación de vigilancia central.

Aunque los sistemas de seguridad convencionales funcionan bien, a veces son excesivamente complejos y caros. Por consiguiente, existe la necesidad de mejores procedimientos y aparatos para proteger áreas seguras.

La publicación de solicitud de patente estadounidense n.º US 2015/015401A1 describe un procedimiento para recibir una condición detectada, compararla con un umbral e iniciar acciones en función de si se supera el umbral.

Resumen de la invención

La presente invención está definida por las reivindicaciones adjuntas.

Breve descripción de los dibujos

La FIG. 1 ilustra un diagrama de bloques de un sistema de seguridad según la presente invención.

Descripción detallada

Aunque las formas de realización dadas a conocer pueden adoptar muchas formas diferentes, formas de realización específicas de las mismas se muestran en los dibujos y se describirán en detalle en el presente documento teniendo en cuenta que la presente divulgación debe considerarse una ejemplificación de los principios de las mismas, así como el mejor modo de llevar a la práctica las mismas, y no pretende limitar la solicitud o reivindicaciones a la forma de realización específica ilustrada.

La FIG. 1 es un diagrama de bloques de un sistema de seguridad 10 mostrado en términos generales según una forma de realización ilustrada. El sistema puede incluir uno o más sensores de amenazas 12, 14 que detectan amenazas en un área geográfica protegida 16.

Las amenazas a la seguridad y/o la estabilidad dentro del área protegida pueden deberse a cualquiera de una pluralidad de causas diferentes. Por ejemplo, al menos algunos de los sensores pueden ser detectores de intrusión implementados como interruptores de límite colocados en las puertas y/o ventanas que permiten el acceso a y la salida del área protegida. Otros de los sensores pueden ser sensores de movimiento (p.ej., detectores de infrarrojos pasivos (PIR), cámaras de televisión con detección de movimiento, etc.) colocados en el interior del espacio. Otros sensores pueden ser detectores de gas o de incendios.

Una o más aplicaciones en la nube 34, 36 pueden supervisar los sensores. Tras la activación de uno de los sensores, la aplicación en la nube puede enviar un mensaje de alarma a una estación de vigilancia central 28. La estación de vigilancia central puede responder pidiendo la ayuda adecuada (por ejemplo, policía, bomberos, etc.).

La aplicación en la nube también puede enviar el mensaje de alarma a un dispositivo inalámbrico portátil 32 llevado por un usuario humano. El usuario humano es un ocupante autorizado del área protegida.

Los sensores son dispositivos inalámbricos que se comunican con la aplicación en la nube a través de un sistema de comunicación accesible públicamente basado en el uso de una red de área extensa de baja potencia (LPWAN) 30 que incluye una estación base asociada 24. La estación base y la aplicación en la nube pueden, a su vez, comunicarse a través de Internet 26.

La red LPWAN puede estar definida por una pluralidad de dispositivos de baja potencia 18, 20, 22 de acuerdo con la utilización de cualquiera de una pluralidad de tecnologías (p.ej., Semtech LoRa, módulos celulares diseñados para aplicaciones de máquina a máquina (M2M), Weightless (http://www.neul.com/neul/?page_id=3318), Sigfox, POPS, Air Lynx (http://air-lynx.com/wal-overview-uk/), etc.). Como se sabe, los sistemas LPWAN tienen un alcance relativamente largo, proporcionan una conectividad de muy bajo coste, tienen una larga duración de batería y solo se necesitan ocasionalmente para enviar y recibir mensajes.

En general, las aplicaciones en la nube 34, 36 son programas de ordenador cargados desde un medio legible por ordenador no transitorio (memoria) 38, que se ejecutan en uno o más aparatos de procesador (es decir, un procesador en la nube) 40. Tal y como se usa en el presente documento, la referencia a una etapa realizada por una aplicación en la nube también hace referencia al procesador que ejecutó esa etapa.

Las aplicaciones en la nube y los procesadores en la nube no tienen relación geográfica con el área geográfica protegida. Como se sabe, una aplicación en la nube se ejecuta normalmente en un procesador en la nube accesible públicamente, a menudo pagando una pequeña tarifa o sin coste alguno.

Las áreas geográficas protegidas pueden tener solamente un único o solamente un pequeño número de sensores. Los sensores pueden ser alimentados por batería.

Cada sensor incluye un elemento de detección que detecta un parámetro de amenaza (p.ej., intrusión, incendios, etc.). Los sensores también incluyen un sistema de circuitos de control (p.ej., un procesador y programas de ordenador asociados) que compara el parámetro detectado con uno o más valores de umbral y notifica eventos a la aplicación en la nube a través de un transceptor inalámbrico correspondiente.

Al detectar una amenaza, un sensor comienza a buscar un dispositivo LPWAN cercano que forma parte de una red LPWAN local. Al detectar un dispositivo cercano, el sensor selecciona el dispositivo y genera un mensaje de alarma para transferirlo a la aplicación en la nube. El mensaje puede incluir una dirección IP de la aplicación en la nube, un identificador del sensor, un identificador del área protegida (p.ej., dirección, número de cuenta, etc.) y el instante de tiempo.

El dispositivo LPWAN seleccionado recibe el mensaje de alarma y lo transfiere a la estación base. El dispositivo seleccionado puede enviar el mensaje directamente o a través de otro(s) dispositivo(s) LPWAN de baja potencia. Este puede ser el caso porque el dispositivo LPWAN seleccionado puede estar demasiado lejos de la estación base para enviar el mensaje directamente. En cambio, el otro dispositivo LPWAN funciona como un retransmisor para recibir y retransmitir el mensaje a la estación base. En una forma de realización, el dispositivo LPWAN puede incorporarse a una parte del sensor.

La estación base recibe el mensaje y reenvía el mensaje a través de Internet a la aplicación en la nube. La aplicación en la nube puede recibir y autenticar el mensaje haciendo referencia a un archivo de referencia 42. La autenticación puede estar basada en un número de serie electrónico del sensor, un número de cuenta o comparando cualquier otra característica del mensaje de alarma con un contenido del archivo de referencia.

Tras autenticar el mensaje de alarma, la aplicación en la nube puede enviar un mensaje de alarma correspondiente a la estación de vigilancia central. Al igual que el mensaje procedente del sensor, el mensaje de alarma puede incluir un identificador del sensor, la ubicación, el tipo de amenaza detectada y el instante de tiempo.

Además de o como alternativa a enviar el mensaje de alarma a la estación de vigilancia central, la aplicación en la nube también puede enviar un mensaje de alarma al dispositivo portátil del usuario humano. El mensaje de alarma enviado al usuario puede incluir un identificador del sensor, la ubicación, el tipo de amenaza detectada y el instante de tiempo. El mensaje puede mostrarse automáticamente en una pantalla del dispositivo portátil.

En otra forma de realización, la aplicación en la nube puede ejecutarse en la estación base local. En este caso, el mensaje de alarma al usuario humano puede originarse en la estación base local.

En otra forma de realización, el sistema de alarma puede dar servicio a una pluralidad de áreas geográficas protegidas independientes 16, 44 pertenecientes a entidades completamente independientes. En este caso, una pasarela regional 48 puede utilizarse para reducir los requisitos de procesamiento de datos de la aplicación en la nube. En este caso, mensajes duplicados de los mismos sensores o de múltiples sensores en la misma área

protegida o áreas protegidas cercanas pueden dividirse o consolidarse de otra manera. Como alternativa, la gestión de fallos puede realizarse en la pasarela. Asimismo, el procesamiento de comandos de usuario y el análisis de alarmas pueden gestionarse en la pasarela en vez de en la nube.

El uso de la tecnología LPWAN para conectar los sensores a aplicaciones en la nube tiene diversos beneficios. Por ejemplo, el uso de una LPWAN proporciona una solución de bajo coste que es de gran utilidad en sistemas más pequeños (p.ej., domicilios, pequeños comercios, etc.) y, especialmente, cuando no se requieren trayectorias de comunicación de respaldo.

El sistema consigue beneficios adicionales al reducir la complejidad de los equipos en el área protegida. El sistema elimina el coste de proporcionar encaminadores/pasarelas en el área protegida junto con la necesidad de energía de reserva para dar soporte a encaminadores/pasarelas que de otro modo se necesitarían en el área protegida.

Algunas tecnologías LPWAN permiten la comunicación de igual a igual, así como comunicaciones a larga distancia. La característica de igual a igual evita puntos negros asociados a sensores colocados demasiado lejos de una estación base mediante la realización de un salto local para mensajes procedentes de un primer dispositivo (nodo) dirigidos hacia otro nodo local (sensor/accionador) que utiliza la misma tecnología de transceptor inalámbrico.

Los nodos de un sistema LPWAN reducen el uso de energía entre transmisores al usar, preferentemente, modos con mejor intensidad de señal para conectarse progresivamente con estaciones base a larga distancia. Los nodos igualan la duración de la batería de nodo en todos los nodos del sistema comunicándose a menor potencia con nodos cercanos (que tienen una mayor reserva de energía) y permitiendo que los nodos cercanos envíen las transmisiones de larga distancia (mayor potencia) a la estación base.

Un sistema de seguridad basado en tecnología LPWAN también hace que el sistema sea robusto contra ataques energéticos que tienen como fin inhabilitar el sistema. El sistema también es resistente a los ataques dirigidos al sistema de comunicación. Por ejemplo, muchos sistemas de seguridad de diseños anteriores han requerido múltiples trayectorias de comunicación independientes con el fin de proporcionar robustez frente a fallos o sabotaje de una o más trayectorias de comunicación. Sin embargo, el sistema de la FIG. 1 incluye una pluralidad de características que obvian estos problemas. Por ejemplo, es probable que cada dispositivo LPWAN esté dentro del alcance de más de una estación base a "larga distancia", y esto puede proporcionar una ruta alternativa. Si un dispositivo LPWAN específico sólo tiene una estación base a "larga distancia", otros dispositivos de baja potencia pueden tener múltiples rutas que salen de este sistema y que entran en los nodos de otro sistema LPWAN, y sus nodos locales pueden proporcionar una trayectoria temporal para la obtención de una señal de entrada y de salida.

Dependiendo del procedimiento de comunicación inalámbrica elegido, pueden utilizarse múltiples canales o espectros ensanchados para evitar atascos. Si un nodo es inaccesible, no inhabilita todo el sistema como lo haría con una sola trayectoria basada en un único encaminador/pasarela.

El sistema de la FIG. 1 también podría implementar trayectorias de respaldo adicionales. Por ejemplo, uno o más de los nodos de baja potencia puede tener un enlace de comunicación de respaldo totalmente independiente (p.ej., una línea alquilada, una conexión de banda ancha ADSL de hilos de cobre, una conexión de banda ancha de fibra óptica, etc.). Otros nodos de sistema pueden comunicarse con este nodo en caso de un fallo en todas las conexiones de comunicación inalámbrica de larga distancia. Esto es una posible actualización del sistema de la FIG. 1, en lugar de una parte obligatoria del sistema básico como en los sistemas de la técnica anterior. Debido a la robustez y la diversidad de las trayectorias de comunicación, la aplicación de servidor/en la nube asociada a la aplicación de panel sabe muy rápidamente que los dispositivos en un emplazamiento están teniendo dificultades de comunicación y puede adoptar las medidas adecuadas.

En general, el sistema de la FIG. 1 incluye un sensor de alarma inalámbrico que detecta una amenaza en un área geográfica protegida, donde una aplicación en la nube que supervisa la asociación con la aplicación de panel sabe muy rápidamente que los dispositivos de un emplazamiento están teniendo dificultades de comunicación y puede adoptar las medidas adecuadas.

En general, el sistema de la FIG. 1 incluye un sensor de alarma inalámbrico que detecta una amenaza en un área geográfica protegida, una aplicación en la nube que supervisa el sensor de alarma y notifica amenazas detectadas por el sensor de alarma dentro del área protegida a un usuario humano del área protegida y un sistema de comunicación inalámbrica accesible públicamente definido por una pluralidad de dispositivos de comunicación de potencia relativamente baja y una estación base local, donde el sensor de alarma detecta un dispositivo cercano de la pluralidad de dispositivos de comunicación de baja potencia y se conecta de manera inalámbrica a la aplicación en la nube a través del dispositivo de comunicación cercano de baja potencia y la estación base local.

Como alternativa, el sistema incluye un sensor inalámbrico que detecta amenazas en un área geográfica protegida, una aplicación en la nube que supervisa el sensor y notifica amenazas detectadas por el sensor dentro del área protegida a un usuario humano del área protegida y al menos un dispositivo de comunicación inalámbrica, de potencia relativamente baja y accesible públicamente, y una estación base local, donde el sensor inalámbrico

detecta el al menos un dispositivo de comunicación de baja potencia y se conecta a la aplicación en la nube mediante el al menos un dispositivo de comunicación de baja potencia y la estación base local.

Como alternativa, el sistema incluye un sensor de alarma inalámbrico que detecta una amenaza en un área geográfica protegida, una aplicación en la nube que supervisa el sensor de alarma y notifica amenazas detectadas por el sensor de alarma dentro del área protegida a un usuario humano del área protegida, un sistema de comunicación inalámbrica accesible públicamente definido por una pluralidad de dispositivos de comunicación de potencia relativamente baja y una estación base local, donde el sensor de alarma detecta un dispositivo cercano de la pluralidad de dispositivos de comunicación de baja potencia y se conecta de manera inalámbrica a la aplicación en la nube a través del dispositivo de comunicación cercano y la estación base local y un enlace de comunicación de respaldo que acopla el sensor de alarma inalámbrico a la aplicación en la nube, donde el enlace de comunicación de respaldo incluye al menos uno de una línea alquilada, una línea de abonado digital y un cable de fibra óptica.

REIVINDICACIONES

1. Un aparato, que comprende:

un sensor de alarma inalámbrico (12) que detecta una amenaza en un área geográfica protegida;
una aplicación en la nube (34) que supervisa el sensor de alarma inalámbrico y notifica la amenaza detectada por el sensor de alarma inalámbrico en el área geográfica protegida a un usuario humano asociado al área geográfica protegida; y
un sistema de comunicación inalámbrica accesible públicamente definido por una pluralidad de dispositivos de comunicación de potencia baja (32) y una estación base local (24),
donde el sistema de comunicación inalámbrica accesible públicamente comprende una red de área extensa de baja potencia (LPWAN) (30),
donde, después de que el sensor de alarma inalámbrico detecte la amenaza en el área geográfica protegida, el sensor de alarma inalámbrico busca uno de la pluralidad de dispositivos de comunicación de baja potencia,
donde el sensor de alarma inalámbrico detecta el uno de la pluralidad de dispositivos de comunicación de baja potencia y se conecta de manera inalámbrica a la aplicación en la nube a través del uno de la pluralidad de dispositivos de comunicación de baja potencia y la estación base local, y
donde la LPWAN utiliza cualquier tecnología de un grupo que consiste en Semtech, LoRa, módulos celulares diseñados para aplicaciones de máquina a máquina, Weightless, Sigfox, POPS y Air Lynx.

2. El aparato según la reivindicación 1, que comprende además una pasarela (48) que procesa señales procedentes del sensor de alarma inalámbrico y reenvía las señales al usuario humano.

3. El aparato según la reivindicación 2, en el que la pasarela (48) comprende una pasarela regional que procesa otras señales procedentes de otros sensores de alarma (12, 14) que protegen otras áreas geográficas protegidas (16, 44) y notifica otras amenazas a otros usuarios humanos.

4. El aparato según la reivindicación 2, que comprende además una aplicación en la nube independiente (34) que supervisa los otros sensores de alarma (12, 14) y notifica las otras amenazas a los otros usuarios humanos.

5. El aparato según la reivindicación 2, en el que la pasarela (48) comprende aplicaciones independientes (34, 36) que dividen la detección y la notificación para diferentes áreas geográficas protegidas (16, 44).

6. El aparato según la reivindicación 1, en el que el sensor de alarma inalámbrico (12) comprende uno o más de un sensor de intrusión y un sensor de incendios.

7. El aparato según la reivindicación 1, que comprende además un procesador (40) que notifica la amenaza a una estación de vigilancia central (28).

8. El aparato según la reivindicación 1, que comprende además un dispositivo inalámbrico portátil (32) que recibe la amenaza notificada por la aplicación en la nube.

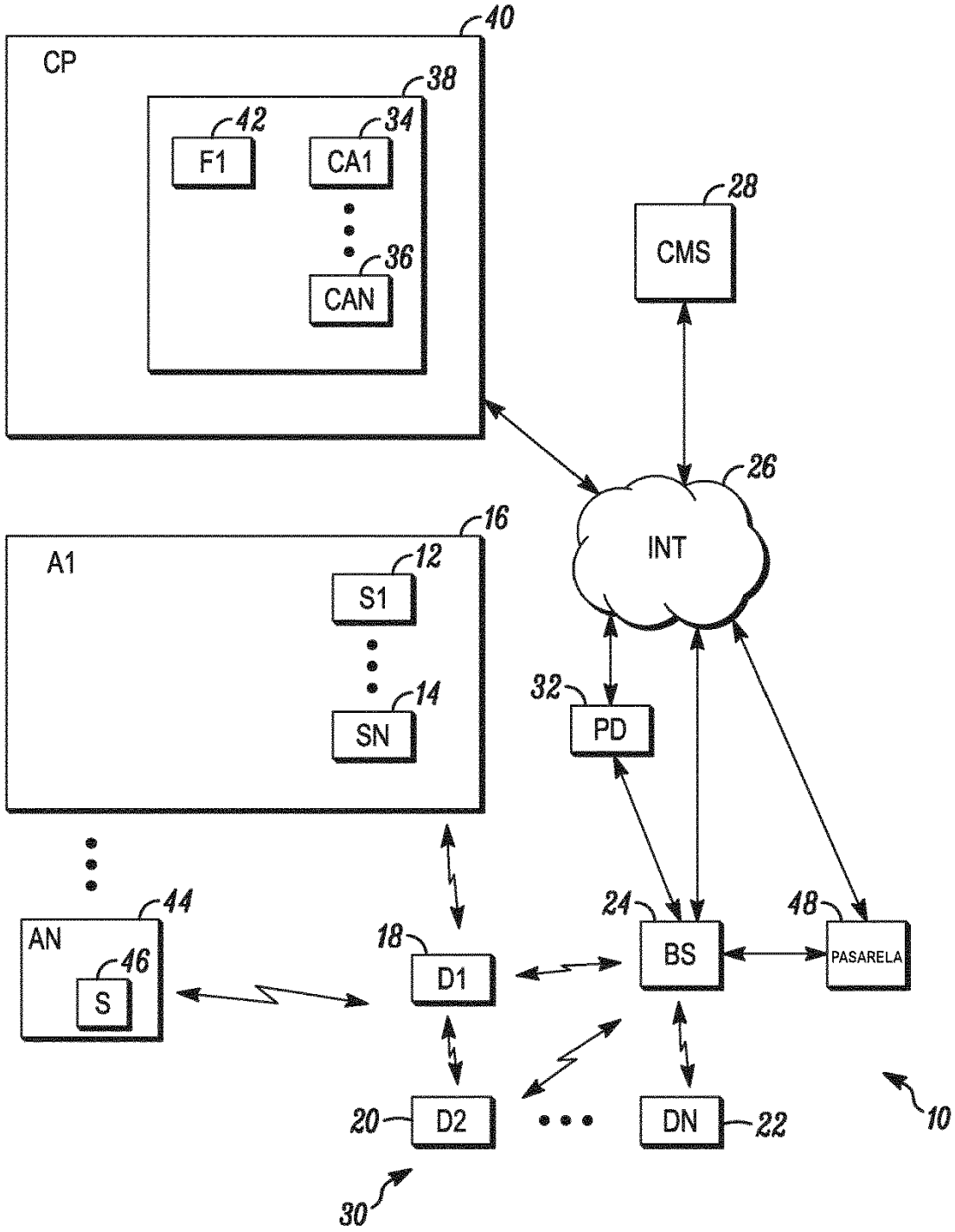
CP
40
38
42
F1
34
CA1
36
CAN
28
CMS
26
INT
16
A1
12
S1
14
SN
32
PD
44
AN
46
S
18
D1
24
BS
48
PASARELA
20
D2
DN
22
10
30

FIG. 1