(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 732 196**

(51) Int. CI.:

G08B 25/10 (2006.01)
H04W 4/16 (2009.01)
H04L 29/08 (2006.01)
G08B 25/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.08.2017 E 17185613 (1)**

(97) Fecha y número de publicación de la concesión europea: **15.05.2019 EP 3282432**

(54) Título: **Sistema de seguridad distribuido por dispositivos inteligentes**

(30) Prioridad:

10.08.2016 US 201615233462

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.11.2019

(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 J.;
CRISP, MARTIN y
BROWN, WILLIAM J.

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Sistema de seguridad distribuido por dispositivos inteligentes

Antecedentes de la invención

La presente descripción se refiere a dispositivos inteligentes y sistemas de seguridad. El documento US2015/339912 describe sistemas, métodos y software para monitorizar y controlar un sistema de seguridad para una estructura que comprende la recepción de datos de sensores desde al menos un primer periférico, los datos de sensor asociados con al menos una de actividad dentro y actividad fuera de una estructura; determinar un evento crítico basado en parte en los datos de sensor; crear una alerta basada en parte en el evento crítico; obtener preferencias de usuario asociadas con al menos uno de un usuario y una unidad base; determinar una respuesta basada en parte en las preferencias de alerta y de usuario; y activar al menos uno de un segundo periférico y un servicio basado en parte en la respuesta. El documento US2016/149720 describe un sistema de monitorización de casas que incluye al menos un sensor que detecta un evento predeterminado, un dispositivo maestro que se comunica con el sensor y se conecta a una red telefónica fija para realizar llamadas a otros teléfonos fijos, y un terminal de teléfono móvil que incluye una unidad de visualización/entrada, que realiza una comunicación inalámbrica con el dispositivo maestro utilizando un enrutador inalámbrico, y se conecta a otros teléfonos móviles a través de una red de teléfono móvil.

Compendio

La invención se establece de acuerdo con las reivindicaciones anejas. La descripción revela un sistema de seguridad que incorpora uno o más sensores y uno o más dispositivos inteligentes conectados entre sí por Internet, otra red o medios de comunicación. Uno o más dispositivos inteligentes pueden tener una aplicación de alarma (app) que permite a un usuario conectar y desconectar una alarma, monitorizar un cambio de estado de un evento, tener acceso a la información de vídeo asociada con el evento, realizar acciones remotas o locales relacionadas con el evento, y mucho más. El procesamiento puede ser más que mover el procesamiento a un dispositivo inteligente. El control del núcleo puede residir en más de un dispositivo, y por lo tanto da como resultado una robustez del sistema completo.

Breve descripción de los dibujos

La Figura 1 es un diagrama de un sistema de alarma de aplicación telefónica;

la Figura 2 es un diagrama que indica un ajuste del presente sistema;

la Figura 3 es un diagrama que indica una intrusión en el sistema;

la Figura 4 es un diagrama de una vista general lógica de un ejemplo del presente sistema;

la Figura 5 es un diagrama de un ejemplo del sistema como el de la Figura 4, pero con una delineación de dispositivos in situ y dispositivos externos;

la Figura 6 es un diagrama de una vista general física de un ejemplo del presente sistema;

la Figura 7 es un diagrama de una vista del dispositivo inteligente del presente sistema sin comunicación de sensor o salida; y

la Figura 8 es un diagrama de la vista del dispositivo inteligente, que incorpora un servidor opcional, pero sin comunicación de sensor o salida.

Descripción

El presente sistema y procedimiento pueden incorporar uno o más procesadores, ordenadores, controladores, interfaces de usuario, conexiones inalámbricas y/o por cable, y/o similares, en una implementación mostrada en la presente.

Esta descripción puede proporcionar uno o más ejemplos ilustrativos y específicos o formas de implementar el sistema y el enfoque actuales. Puede haber muchos otros ejemplos o formas de implementar el sistema y el enfoque.

Los aspectos del sistema o del enfoque pueden describirse como símbolos en el dibujo. Los símbolos pueden tener virtualmente cualquier forma (p.ej., un bloque) y pueden indicar hardware, objetos, componentes, actividades, estados, etapas, procedimientos y otros elementos.

Para sistemas automonitorizados de bajo coste (posiblemente sistemas autoinstalados "por uno mismo"), algunas soluciones pueden utilizar un panel de control local (que también podría ser una pasarela) y servidores (autónomos o en una nube) además de aplicaciones de usuario en teléfonos móviles y ordenadores de sobremesa y PC. Sin embargo,

puede haber una oportunidad para un modelo centrado en el usuario que aproveche los avances tecnológicos en las zonas de dispositivos conectados a Internet (como los sensores de intrusión), los avances en conectividad y los avances en la potencia de procesamiento de dispositivos inteligentes portátiles tales como teléfonos inteligentes. La presente solución tiene un menor coste inicial y reduce el hardware que necesita ser instalado y soportado in situ.

Un dispositivo inteligente puede ser un dispositivo electrónico conectado a otros dispositivos o redes a través de diferentes protocolos, que puede funcionar hasta cierto punto de forma interactiva y autónoma. Los ejemplos de dispositivos inteligentes pueden incluir teléfonos inteligentes, tabléfono y tabletas, relojes inteligentes, bandas inteligentes y cadenas de llaves inteligentes.

Un ejemplo de un dispositivo inteligente puede ser un teléfono inteligente que es un teléfono móvil con un sistema operativo móvil avanzado, que combina características de un sistema operativo de ordenador personal con otras características útiles para uso móvil o portátil. Los teléfonos inteligentes pueden combinar las características de un teléfono móvil, como la capacidad de recibir y hacer llamadas telefónicas, con las características de otros dispositivos móviles digitales. Otras características pueden incluir un asistente digital personal (PDA) para realizar citas en un calendario, navegador web, reproductor multimedia, videojuegos, unidad de navegación GPS, cámara digital, cámara de vídeo digital, etc. Un teléfono inteligente puede acceder a Internet y ejecutar componentes de software de terceros (p.ej., aplicaciones). Pueden tener una interfaz gráfica de usuario en color con pantalla táctil que a menudo cubre el setenta por ciento o más de la superficie frontal con una pantalla LCD, OLED, AMOLED, LED o similar.

El presente enfoque puede simplificar la implementación de sistemas de bajo coste y automonitorizados reduciendo el número de elementos físicos in situ. Un sistema en su forma básica puede ser un sensor conectado a Internet (u otra red) y una aplicación ejecutándose en un dispositivo inteligente conectado a Internet (o conectado a otra red) (p.ej., un teléfono móvil).

En una forma, el sensor puede estar compuesto por un sensor estándar, una conexión a Internet (u otra red) y quizás algún procesamiento adicional básico (p.ej., conocer el estado establecido del sistema).

Una aplicación de dispositivo inteligente puede permitir al usuario conectar y desconectar un sistema de alarma, permanecer constantemente en contacto con cualquier sensor de un sistema predeterminado, monitoriza cualquier cambio en el estado sobre el que deba actuar el usuario (p.ej., un evento de intrusión, un incendio o un apagón), permitir que el usuario tenga acceso a las señales de vídeo/audio asociadas y tomar alguna medida de forma remota ya sea de forma automática o activada por el usuario, p.ej., llamar a un timbre, llamar a los servicios de emergencia, llamar a la policía, transmitir un mensaje a un sitio, grabar imágenes y realizar acciones similares.

El presente sistema puede ser escalable sobre la base de una serie de sensores conectados a Internet (u otra red) y una serie de dispositivos inteligentes (usuarios) que se añaden al sistema. Una característica de la presente solución puede ser la capacidad de cada uno de los componentes del sistema (ya sean sensores o dispositivos inteligentes) de sincronizarse continuamente con los demás sensores y dispositivos para garantizar que el sistema siga siendo robusto y que exista cierta redundancia en el procesamiento de las alarmas, p.ej., que cada una de las aplicaciones sea capaz de activar una acción remota, que posteriormente se comunicaría a los demás dispositivos.

Un ejemplo de una presente solución puede ser un sistema de alarma con componentes clave. En primer lugar, puede haber uno o más sensores de intrusión conectados a Internet (u otra red) (p.ej., movimiento, puerta abierta, rotura de cristales, etc.) y otros dispositivos relacionados con la seguridad, como una cámara de vídeo conectada a Internet, dispositivos de audio, etc. Estos dispositivos pueden contener suficiente funcionalidad para que puedan formar una red local en la que cada dispositivo contenga información actualizada del sistema, p.ej., el estado establecido del sistema y los detalles de prácticamente todos los usuarios asociados.

Puede haber una o varias aplicaciones ejecutándose en uno o más teléfonos inteligentes o equivalentes. Cada aplicación puede ser capaz de ejecutar el procesamiento de alarma, es decir, monitorizar los mensajes de uno o más sensores y notificar a uno o más usuarios cuando se activa un evento. Se puede permitir que uno o más usuarios tomen medidas. Puede haber sincronización con otras aplicaciones conectadas al sistema.

Algunos teléfonos o dispositivos inteligentes pueden tener control sobre el sistema (actuando de este modo como un dispositivo principal); otros pueden ser solo auxiliares cuando no se pueda acceder a los teléfonos/dispositivos inteligentes principales.

El control puede ser como en la "lógica del sistema de control" más que un simple control utilizado en el sentido de "elemento de ajuste de la interfaz de usuario". En los controles de temperatura de las habitaciones, esto puede ser una diferencia entre un módulo lógico de caldera real y el selector de control de la habitación. Es decir, "control" puede entenderse en el sentido de la inteligencia o la lógica del sistema no necesariamente en el sitio en un "panel de control"

(como puede ser típico con sistemas de robo/intrusión y acceso) sino en realidad en algo que, hasta ahora, solo se ha utilizado como un "dispositivo de IU" para sistemas de seguridad, tales como un teléfono inteligente o una tableta.

Como se muestra en la presente, uno también puede ir más allá de simplemente mover este procesamiento a un solo dispositivo inteligente. Se muestra cómo este control del núcleo puede residir en más de un dispositivo, y por lo tanto crear la robustez del sistema completo.

El presente sistema puede ser un sistema de alarma en una "aplicación móvil". Puede utilizar un dispositivo inteligente portátil (como un teléfono) para ejecutar el sistema. También puede ejecutarse en un dispositivo portátil, u otro dispositivo móvil o reubicable (p.ej., como un ordenador portátil o un ordenador de enchufe).

Los sensores pueden comunicarse con una aplicación móvil. Las Figuras 4 y 5 pueden mostrar un ejemplo de la vista general del sistema (vista lógica), una vista teórica y una vista sin optimizaciones.

Las características clave pueden incorporar principalmente un sistema de automonitorización. Se puede añadir la monitorización profesional en una base temporal o de respaldo o, dependiendo de la decisión de negocio, de suministrar la monitorización.

Las capacidades del sistema pueden incorporar un conjunto de "dispositivos del sitio" compuestos por uno o más sensores (in situ), cero o más salidas (in situ), cero o más dispositivos distintos (in situ), y uno o más dispositivos inteligentes u otros equivalentes (dispositivos en cualquier lugar). En los diagramas de las Figuras que aquí se mencionan, esto puede mostrarse, por ejemplo, como un " teléfono inteligente" o una "tableta". Los dispositivos inteligentes pueden gestionar uno o más sitios.

La Figura 6 es un diagrama de un ejemplo de una vista general del sistema (vista física). La Figura 7 es un diagrama de una vista del dispositivo inteligente, que ignora la comunicación de sensor/salida.

La Figura 8 es un diagrama de una vista del dispositivo inteligente, que incluye un servidor opcional, pero que ignora la comunicación de sensor/salida. Pueden observarse dispositivos principales y dispositivos auxiliares. Los dispositivos inteligentes pueden dividirse en dos tipos, es decir, dispositivos principales y dispositivos auxiliares.

Un dispositivo principal puede ser un procesador principal de información. Puede ser "preferido" por los dispositivos del sitio como un primer dispositivo para enviar información de señal. El dispositivo principal puede tener una autoridad para determinar un orden de eventos cuando exista un conflicto.

Las responsabilidades del dispositivo principal ("lo que hace") puede incorporar la monitorización de eventos desde los sensores, permitiendo a los usuarios con suficientes derechos de acceso para alterar la configuración del sistema y añadir dispositivos auxiliares.

Un dispositivo auxiliar puede proporcionar respaldo cuando no están disponibles los dispositivos principales. Las responsabilidades del dispositivo auxiliar pueden ser las mismas que aquellas de los dispositivos principales, excepto que no puede proporcionar una autoridad sobre el orden de los eventos (en presencia de un dispositivo principal) y no puede tener control de administrador sobre ninguna configuración del sistema.

Los problemas comerciales de algunos sistemas pueden involucrar a un sector significativo de propietarios de viviendas que encajan dentro de una o más de las siguientes categorías (con respecto a los sistemas de alarma). Algunos propietarios de viviendas pueden tener un nivel de miedo a usar un sistema en el que "se les da 30 segundos para desactivar el sistema y si no lo hacen, se producirá una situación caótica". Algunos propietarios de viviendas pueden no querer pagar una tarifa elevada para instalar un sistema (preferirían un sistema realizado por ellos mismos o al menos poder instalarlo en menos de una hora). Es posible que algunos no quieran pagar tarifas elevadas mensuales para poseer y ejecutar un sistema. Algunos pueden querer automonitorizar el sistema si fuera posible. Algunos propietarios de viviendas pueden ver un sistema de alarma como una compra a regañadientes. Algunos propietarios no están familiarizados con las interfaces de usuario. Algunos ya tienen varios dispositivos electrónicos en su posesión y no quieren más (especialmente si tienen que aprender a usarlos). Algunos propietarios pueden ver los productos encendidos permanentemente como un desperdicio de energía. Las alarmas antirrobo se pueden ver como artículos de baja tecnología.

Se pueden observar los problemas técnicos. Existe la necesidad de proporcionar las siguientes soluciones técnicas. El sistema debe tener un equipo fácil de instalar en un entorno DIY, ser fácil de mantener, tener un bajo coste, poder reutilizar el equipo estándar que ya está disponible en el hogar, tener una interfaz de usuario que sea familiar y a la vez se perciba como de alta tecnología (p.ej., un teléfono inteligente), ser sencillo (o al menos que transmita familiaridad) en relación con el acceso a una serie de características (p.ej., un sistema operativo estándar de un teléfono inteligente (SO)), etc.

Cualquier dispositivo con alimentación principal puede ser retirado del sistema. Los sistemas de alarma pueden estar "permanentemente encendidos". Puede haber una integración del sistema de alarma en otro producto ya activo.

Las características del presente sistema pueden incorporar el hardware que almacena y ejecuta el sistema, el firmware o el software que se encuentra en un teléfono inteligente (o un dispositivo equivalente), y la reutilización de la tecnología existente de los usuarios finales, que ya es familiar y es "tecnología reciente", y la redundancia de la unidad principal de procesamiento puede incorporarse en el diseño de todo el sistema y, por tanto, eliminar una debilidad actual del sistema de intrusión a un coste mínimo.

Las características adicionales indicadas en el sistema pueden involucrar prácticamente a todos los usuarios, zonas, manipulaciones indebidas, etc., los datos que se transfieren a través de una o múltiples rutas de comunicación desde el sitio de instalación a una aplicación móvil limitada o sin control del sistema realmente ubicado en el sitio de instalación, todo el firmware/software relacionado con el sistema ubicado en la aplicación móvil, el firmware/software del sistema que se actualiza según el método establecido para la aplicación móvil, las aplicaciones que se descargan desde el sitio web de una empresa o desde tiendas de aplicaciones de terceros existentes, los periféricos comunes a través de todas las líneas de productos (p.ej., sensores, módulos de comunicación, módulos de interfaz de usuario, fuentes de alimentación, etc.), solo se requiere que el almacén del fabricante realice un conjunto común de periféricos, el instalador solo necesita llevar un conjunto común de periféricos, se puede considerar como un enfoque más ecológico de la seguridad y se vende como tal (menos módulos de encendido permanente en el sistema propio), y un usuario puede tener el control total del sistema y, por lo tanto, puede desactivar el sistema antes de entrar en la casa (eliminando parte del miedo a usar el sistema).

Los tipos de sensores de ejemplo pueden incorporar detectores de movimiento (PIR, sensores de ventana/puerta) y cámaras de vídeo con detección de movimiento incorporada.

Los dispositivos pueden optimizar las comunicaciones entre dispositivos inteligentes (teléfonos, tabletas, etc.) y los dispositivos in situ.

El presente sistema puede ser un sistema distribuido, pero debe ser capaz de combinar actualizaciones de múltiples fuentes y destinos con (como máximo) (n*m) + (n* (n-1)/2) rutas de comunicación en un historial lineal sin interacción humana, donde m es un número de dispositivos del sitio (sensores/salidas), n es el número de dispositivos inteligentes.

Se pueden utilizar marcas de tiempo para ayudar al presente enfoque. El tiempo entre los dispositivos se puede sincronizar con técnicas informáticas. El número de conexiones puede excluir la optimización de las comunicaciones iniciales que van al nodo principal. Todos los eventos de un dispositivo de un solo sitio también pueden tener un recuento monotono, y la reconstrucción del historial puede que solo tenga que ocurrir en dispositivos inteligentes. Los dispositivos del sitio no necesariamente necesitan una orden para funcionar.

El sistema puede tener características adicionales. Un "servidor de mensajes" puede ser una adición al presente sistema principal. Puede ayudar a que los datos que se obtienen de los teléfonos que no pueden recibir conexiones entrantes se puedan registrar periódicamente con el servidor de mensajes para recibir mensajes. El servidor de mensajes también puede implementar un servicio "push" para proveer datos a un teléfono. Los datos pueden ser enrutados desde sensores a múltiples lugares. El servidor puede ser solo un transporte de datos, y por lo tanto no necesita lógica en el sentido de que puede ser efectivamente solo un enrutador especialista.

Puede ser totalmente posible que todos (o algunos de) los sensores puedan implementar un servidor push, sin la necesidad de un servidor independiente. Un rastreador de sistemas puede proporcionar un servicio que permite encontrar rápidamente los sistemas autorizados. No se requiere necesariamente el rastreador una vez que se establece una conexión entre el sistema local y el teléfono. El rastreador puede permitir el acceso a Internet o a los servidores basados en la Red o a una nube.

Una aplicación principal y una aplicación auxiliar pueden ser características del presente sistema. Una aplicación auxiliar temporal puede dar a alguien un acceso temporal de confianza y (opcionalmente) hacer que su dispositivo también pueda ejecutar el sistema.

El servicio de apoyo en la nube puede ser un auxiliar. Si no están localizables todos los dispositivos, el servicio puede actuar como un sistema de emergencia. Puede ser un servicio facturado por día, mes, de pago único o cuota recurrente, dependiendo de los requisitos actuales del negocio.

Los sensores pueden tener un estado establecido. Opcionalmente, puede haber sensores que tengan un estado (armado) establecido. El estado establecido puede ser solo para evitar transmisiones innecesarias cuando se desconecta. Los teléfonos del sistema que se comunican entre sí para conectarse/desconectarse pueden evitarse. Los sensores no necesitan necesariamente un almacenamiento permanente.

El sensor principal puede hacer alguna coordinación en el sitio. Puede tener un almacenamiento adicional, y actuar como pasarela de comunicación o enrutador si fuese necesario.

Se pueden señalar los enrutadores. Un enrutador de sitio local puede ser efectivamente una implementación de detalles que sea transparente para el sistema. Algunos tipos de enrutadores de sitios locales pueden ser de interés. Uno de ellos puede ser un enrutador de pasarela local (es decir, un enrutador entre redes) que enruta los paquetes IP a un destino. Este puede ser un enrutador de aplicaciones. Puede recibir mensajes a partir de protocolos enrutables que no sean de Internet y traducirlos. Puede recibir mensajes de múltiples sensores y actuar como un dispositivo multidifusión, enviando mensajes únicos a múltiples dispositivos inteligentes.

Una multidifusión por Internet (IPv4) puede estar bloqueada o no necesariamente configurada en muchos lugares. Otra multidifusión por Internet puede ser más fácil debido a las direcciones de multidifusión IPv6 basadas en prefijos de unidifusión. Se desconoce si se bloqueará una multidifusión.

Un caso práctico puede incorporar un sistema de seguridad (intrusión/robo), domótica, control de entretenimiento audiovisual, acceso, vídeo, control de la calefacción del hogar, control interno de la temperatura, iluminación, timbre/puerta/videoportero, alimentación de peces, monitorización, monitorización interna y externa de la temperatura, y monitorización externa (jardín/terreno).

Un ejemplo de automonitorización puede ser cuando un usuario configura un sistema, se produce un evento (se activa el sensor), se envía una notificación a un usuario y un usuario interactúa con el sistema para verificar el estado (un enlace a todo lo que hay en la aplicación) por vídeo, por audio, o por otros sensores inteligentes, o el usuario llama a un vecino u otros usuarios.

Un usuario puede responder de forma remota con una activación dependiendo del resultado de una verificación (un enlace a todo está en la aplicación), por ejemplo, llamar a un timbre, encender las luces, responder con audio, llamar a la policía, capturar un vídeo, desconectar el sistema, o ignorar el evento (por ejemplo, una falsa alarma).

La Figura 1 es un diagrama de una alarma de aplicación telefónica. Un dispositivo 41 inteligente (maestro), un dispositivo 42 inteligente, un dispositivo 43 inteligente y un dispositivo 44 inteligente pueden conectarse a una aplicación de alarma de intrusión del dispositivo inteligente mostrada por el símbolo 45 que se encuentra dentro del sistema de alarma de aplicación móvil como se indica con el símbolo 46. Dentro de la aplicación de alarma de intrusión del dispositivo inteligente del símbolo 45 pueden estar los símbolos 51, 52, 53, 54, 55 y 56 que representan el inicio de sesión, la gestión de usuarios, las aplicaciones de sincronización, los dispositivos de sincronización, el estado de cambio y la automonitorización 56, respectivamente.

La aplicación de alarma de intrusión del dispositivo inteligente en el símbolo 45 puede conectarse a enrutadores de Internet (u otra red) en el símbolo 57, que pueden estar conectados a, por ejemplo, un enrutador local en un símbolo 58 en un área dispositivos locales dentro de un símbolo 60. La aplicación en el símbolo 45 también puede estar conectada a una ruta secundaria, como un radio celular, en el símbolo 59. La ruta secundaria del símbolo 59 puede conectarse al primero y segundo sensor representado por los símbolos 61 y 62, respectivamente, y a un dispositivo de advertencia representado por el símbolo 63. Los sensores y el dispositivo de advertencia pueden estar situados dentro del área dispositivos locales del símbolo 60, que a su vez es parte del sistema de alarma de aplicación móvil del símbolo 46. Puede haber más o menos sensores que incluyan más o menos dispositivos de advertencia en el área dispositivos locales. Los sensores y el dispositivo de advertencia de los símbolos 61, 62 y 63, respectivamente, pueden estar conectados al enrutador local en el símbolo 58.

La Figura 2 es un diagrama que indica un ajuste del presente sistema. Un ejemplo de ajuste puede ser el armado del sistema. Un dispositivo 21 inteligente (p.ej., un teléfono móvil) puede enviar una señal o mensaje que indica que se ha armado el sistema y que se puede enviar a una aplicación 22 de alarma de intrusión del dispositivo inteligente. La aplicación 22 puede ser registrada en el símbolo 23. A continuación, el sistema puede configurarse en el símbolo 24. Se puede configurar un estado para que los dispositivos del sistema sean armados en el símbolo 25. El estado de un dispositivo puede configurarse como armado a través de una ruta de transferencia de datos en el símbolo 26. La ruta 26 puede estar conectada con dispositivos in situ en el símbolo 27 Por ejemplo, puede haber un estado de dispositivo configurado como armado para el sensor 28, el sensor 29 y el sensor 30.

La Figura 3 es un diagrama que indica una intrusión en el sistema. Un intruso 31 puede activar un sensor de sistema 32 dentro de un dispositivo local dentro del símbolo 33 que está dentro de la activación de la alarma como se indica en el símbolo 34. Tras la activación del sensor 32 del sistema por el intruso 31, se puede activar un dispositivo 35 de advertencia con una señal del sensor 32 del sistema. Además, se puede informar de una activación del sensor con una señal del sensor 32 del sistema a través de una ruta de transferencia de datos como se indica en el símbolo 36 a una aplicación 37 de alarma de intrusión del dispositivo inteligente. Un mensaje de alarma en la aplicación 37 puede ser recibido y gestionado en el símbolo 38 que es el resultado de la señal de la ruta 36 de transferencia de datos. Una señal

puede proceder del símbolo 38 que recibió y gestionó el mensaje de alarma, e ir a alertar a un usuario en el símbolo 39 dentro de la aplicación de alarma de intrusión del dispositivo inteligente indicada en el símbolo 37.

La Figura 4 es un diagrama de un ejemplo 61 del presente sistema. El ejemplo 61 es una vista general lógica del sistema, que puede ser teórica sin optimizaciones. El ejemplo 61 puede tener sensores 62 y 63 conectados a los teléfonos inteligentes 64 y 65. Puede haber otro dispositivo conectado a los teléfonos inteligentes 64 y 65. También se puede conectar una salida a los teléfonos 64 y 65. Los sensores pueden considerarse también como detectores. Los teléfonos inteligentes 64 y 65 pueden estar conectados entre sí. Esta conexión puede considerarse como comunicación entre dispositivo inteligentes.

La Figura 5 es un diagrama del ejemplo 61, como el de la Figura 4, pero con una delineación de dispositivos 68 in situ y dispositivos 69 externos. Los dispositivos 68 in situ pueden incorporar sensores 62 y 63, la salida 67 y uno o más dispositivos 66. Los dispositivos 69 externos pueden incorporar teléfonos inteligentes 64 y 65.

La Figura 6 es un diagrama de un ejemplo 71 del presente sistema. El ejemplo 71 es una vista general del sistema, que puede ser física. Los sensores 62, 63 y 74 pueden estar conectados a un enrutador 75 de sitio local. La salida 67 puede estar conectada al enrutador 75. Por otra parte, los sensores 62, 63 y 74 podrían ser Wi-Fi o cualquier otra conexión con cable o inalámbrica. El enrutador 75 de sitio local puede conectarse a uno o más enrutadores 76 de Internet (u otra red). Los teléfonos inteligentes 64, 65 y 77 pueden conectarse a los enrutadores 76 de Internet (u otra red). Además, puede haber una ruta secundaria, como la radio celular, que conecta los sensores 62, 63 y 74, y la salida 67 a uno o más enrutadores 76 de Internet. Puede haber comunicación entre dispositivos inteligentes entre los teléfonos inteligentes 64, 65 y 77.

La Figura 7 es un diagrama de un ejemplo 81 desde una perspectiva de un dispositivo inteligente en el que se ignora la comunicación de sensor y de salida. Un teléfono 82 inteligente puede ser un dispositivo principal conectado a las tabletas 83 y 84 que pueden considerarse como dispositivos auxiliares. Las conexiones entre el teléfono 82 inteligente y las tabletas 83 y 84 pueden considerarse como una comunicación optimizada. El teléfono 82 inteligente, como el dispositivo principal, puede conectarse a teléfonos inteligentes, que pueden considerarse como dispositivos auxiliares.

La Figura 8 es un diagrama de un ejemplo 91 a partir de una perspectiva de dispositivos inteligentes en los que se ignora la comunicación de sensor y de salida. El ejemplo 91 puede incorporar un servidor 92 opcional. El teléfono 82 inteligente, como dispositivo principal, puede conectarse a las tabletas 83 y 84, que pueden tener una comunicación optimizada. El teléfono 82 inteligente también puede conectarse a los teléfonos inteligentes 85 y 86.

REIVINDICACIONES

1. Un método para proporcionar seguridad para un entorno que comprende:

conectar uno o más sensores (28, 29, 30, 32, 35, 61, 62, 63, 66, 67, 74) en un lugar tanto a un enrutador de sitio local como a Internet u otra red (26, 36, 57, 58, 59, 75, 76);

conectar uno o más dispositivos móviles (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) a Internet u otra red (26, 36, 57, 58, 59, 75, 76); y

ejecutar una aplicación inteligente (22, 45) en uno o más dispositivos móviles (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86)) para gestionar un sistema de alarma (27, 37, 46), en el que todo el firmware y/o software del sistema de alarma se almacena en la aplicación inteligente (22, 45); y

en el que el sistema de alarma (27, 37, 46) comprende:

el uno o más sensores (28, 29, 30, 32, 35, 61, 62, 63, 66, 67, 74) en los que cada uno de ellos tenga capacidad de conexión a Internet; y

el uno o más dispositivos móviles (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) tienen una conexión con uno o más sensores a través de Internet u otra red (26, 36, 57, 58, 59, 75, 76) de manera que la aplicación inteligente y uno o más sensores se sincronicen continuamente entre sí; y

en el que el sistema de alarma (27, 37, 46) puede configurarse o desarmarse a través de uno o más dispositivos móviles (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) y la aplicación inteligente (22, 45).

2. El método de la reivindicación 1, en el que:

un cambio en el estado es uno o más artículos en un grupo que comprende una intrusión, un incendio, un apagón, un robo, una rotura de vidrio, una explosión, un movimiento de un objeto y un sonido; y

el cambio en el estado resulta en una acción a través de uno o más dispositivos móviles o se selecciona automáticamente de un grupo que comprende la grabación de información de vídeo y audio del cambio de estado, la llamada a un timbre, la llamada a los servicios de salud de emergencia, la llamada a un departamento de bomberos, la llamada a un departamento de policía y la transmisión de un mensaje a un sitio del cambio de estado.

3. El método de la reivindicación 1, que comprende, además:

conectar uno o más dispositivos móviles adicionales (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) a Internet u otra red (26, 36, 57, 58, 59, 75, 76); y

en el que:

el uno o más dispositivos móviles adicionales tienen una o más aplicaciones de alarma inteligentes (22, 45), respectivamente, para gestionar el sistema de alarma (27, 37, 46);

algunos de los uno o más sensores (28, 29, 30, 32, 35, 61, 62, 63, 66, 67, 74) en el entorno, el dispositivo móvil y los uno o más dispositivos móviles adicionales (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) se sincronizan continuamente con algunos de los otros uno o más sensores y el uno o más dispositivos móviles (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) para proporcionar cierta redundancia al procesar el cambio en el estado;

cada aplicación de alarma inteligente (22,45) puede activar una acción remota en respuesta a un cambio en el estado del entorno que está siendo monitorizado, que se comunica a otro o más dispositivos móviles; y

la acción remota es para eliminar, rehabilitar, reducir y prevenir los efectos nocivos del cambio en el estado del entorno.

4. Un sistema de seguridad distribuido que comprende:

uno o más sensores (28, 29, 30, 32, 35, 61, 62, 63, 66, 67, 74) conectados a un enrutador de sitio local y a Internet u otra red (26, 36, 57, 58, 59, 75, 76), donde cada uno del uno o más sensores tiene capacidades de conectividad de Internet; y

al menos un dispositivo (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) inteligente conectado a Internet u otra red (26, 36, 57, 58, 59, 75, 76); y

en el que:

el por lo menos un dispositivo (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) inteligente ejecuta una aplicación de alarma (app) (22, 45) y en donde todo el firmware y/o software del sistema de seguridad (27, 37, 46) se almacena dentro de la aplicación de alarma; y

al menos un dispositivo (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) inteligente con la aplicación de alarma (22, 45) permite al usuario configurar y desconectar un sistema de alarma, monitorizar uno o más sensores, monitorizar un cambio en el estado de un evento, tener acceso a las señales de vídeo y audio asociadas con el evento y tomar acciones remotas o locales con respecto al evento; y

la aplicación inteligente y el uno o más sensores se sincronizan continuamente.

5. El sistema de la reivindicación 4, en el que:

el sistema (27, 37, 46) es escalable en base a un número de uno o más sensores (28, 29, 30, 32, 35, 61, 62, 63, 66, 67, 74) y un número de dispositivos (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) inteligentes;

cada uno de los uno o más sensores (28, 29, 30, 32, 35, 61, 62, 63, 66, 67, 74) y al menos un dispositivo (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) inteligente se sincronizan de manera continua con otros sensores y otros dispositivos inteligentes en el sistema (27, 37, 46) para su redundancia en el procesamiento;

cada dispositivo (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) inteligente con la aplicación (22, 45) puede activar una acción remota que se comunica a otro uno o más dispositivos inteligentes;

uno o más de los uno o más sensores (28, 29, 30, 32, 35, 61, 62, 63, 66, 67, 74) es un sensor de intrusión; y

cada dispositivo (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) inteligente tiene información actualizada sobre el sistema de alarma (27, 37, 46).

6. El sistema de la reivindicación 4, en el que:

un dispositivo (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) inteligente que tiene control sobre el sistema (27, 37, 46) es un dispositivo principal; y

un dispositivo inteligente (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) que tiene control sobre el sistema porque no se puede acceder a un dispositivo principal, es un dispositivo auxiliar; o

un sensor del uno o más sensores (28, 29, 30, 32, 35, 61, 62, 63, 66, 67, 74) puede comunicarse con la aplicación de alarma (22, 45) de al menos un dispositivo (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) inteligente a través de Internet u otra red (26, 36, 57, 58, 59, 75, 76); o

el sistema es un sistema (27, 37, 46) automonitorizado.

7. El sistema de la reivindicación 4, en el que:

al menos un dispositivo (21, 41, 42, 43, 44, 64, 65, 77, 82, 83, 84, 85, 86) inteligente es un dispositivo principal o un dispositivo auxiliar;

el dispositivo principal monitoriza los eventos de los sensores, permite a los usuarios con suficientes derechos de acceso para alterar una configuración del sistema (27, 37, 46), y añade dispositivos auxiliares;

un dispositivo auxiliar proporciona un respaldo en ausencia de un dispositivo principal; y

el respaldo comprende actividades como las del dispositivo principal excepto la determinación del orden de los eventos en presencia del dispositivo principal, y el control administrativo sobre la configuración del sistema (27, 37, 46).

FIG. 1

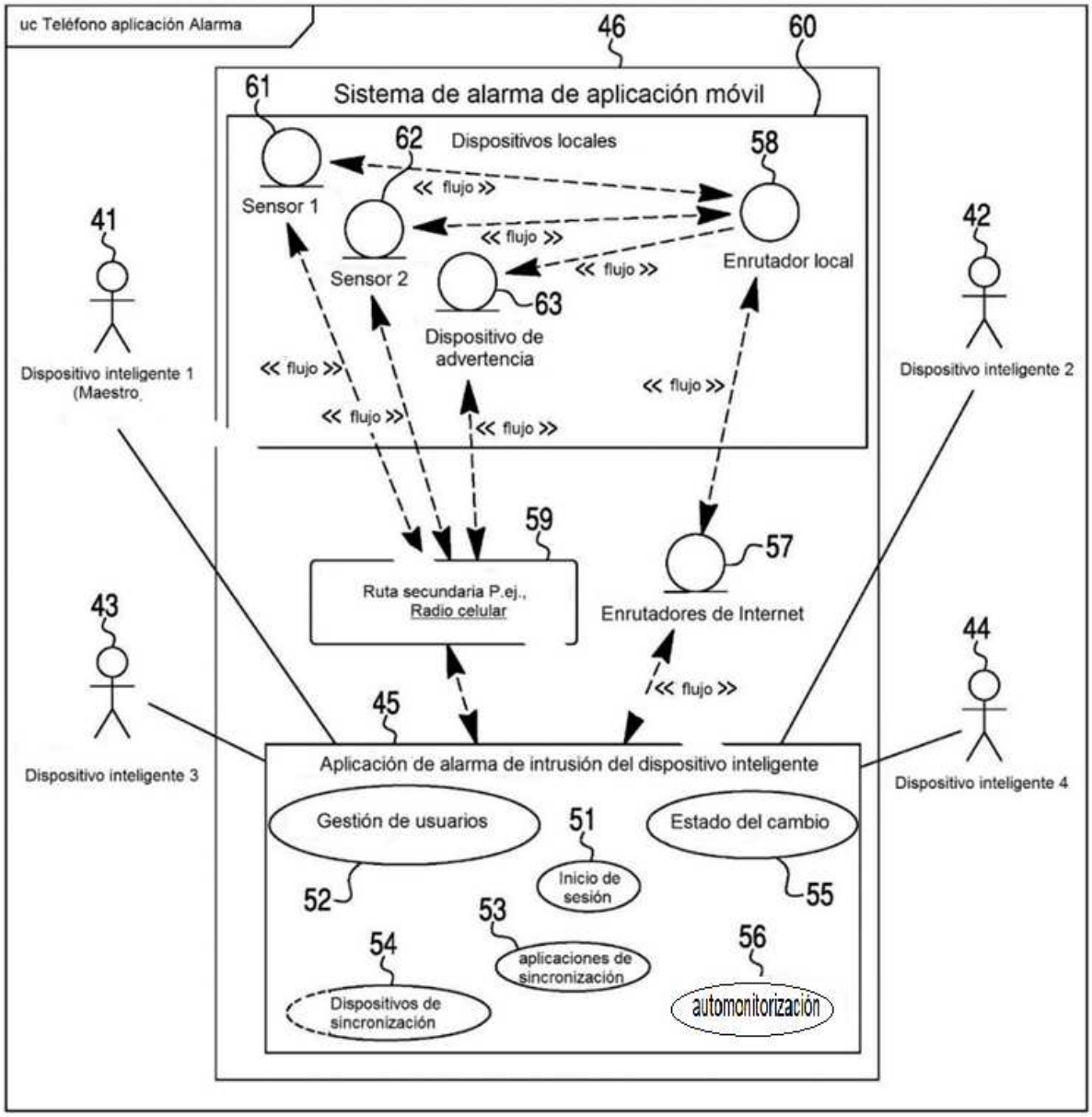

uc Teléfono aplicación Alarma
46
60
61
Sistema de alarma de aplicación móvil
62
Dispositivos locales
58
Sensor 1
<< flujo >>
Sensor 2
Enrutador local
63
Dispositivo de advertencia
41
Dispositivo inteligente 1 (Maestro
42
Dispositivo inteligente 2
59
57
Ruta secundaria P.ej., Radio celular
Enrutadores de Internet
43
44
45
Dispositivo inteligente 3
Dispositivo inteligente 4
Aplicación de alarma de intrusión del dispositivo inteligente
Gestión de usuarios
51
Estado del cambio
Inicio de sesión
52
55
53
54
56
aplicaciones de sincronización
Dispositivos de sincronización
automonitorización

FIG. 2

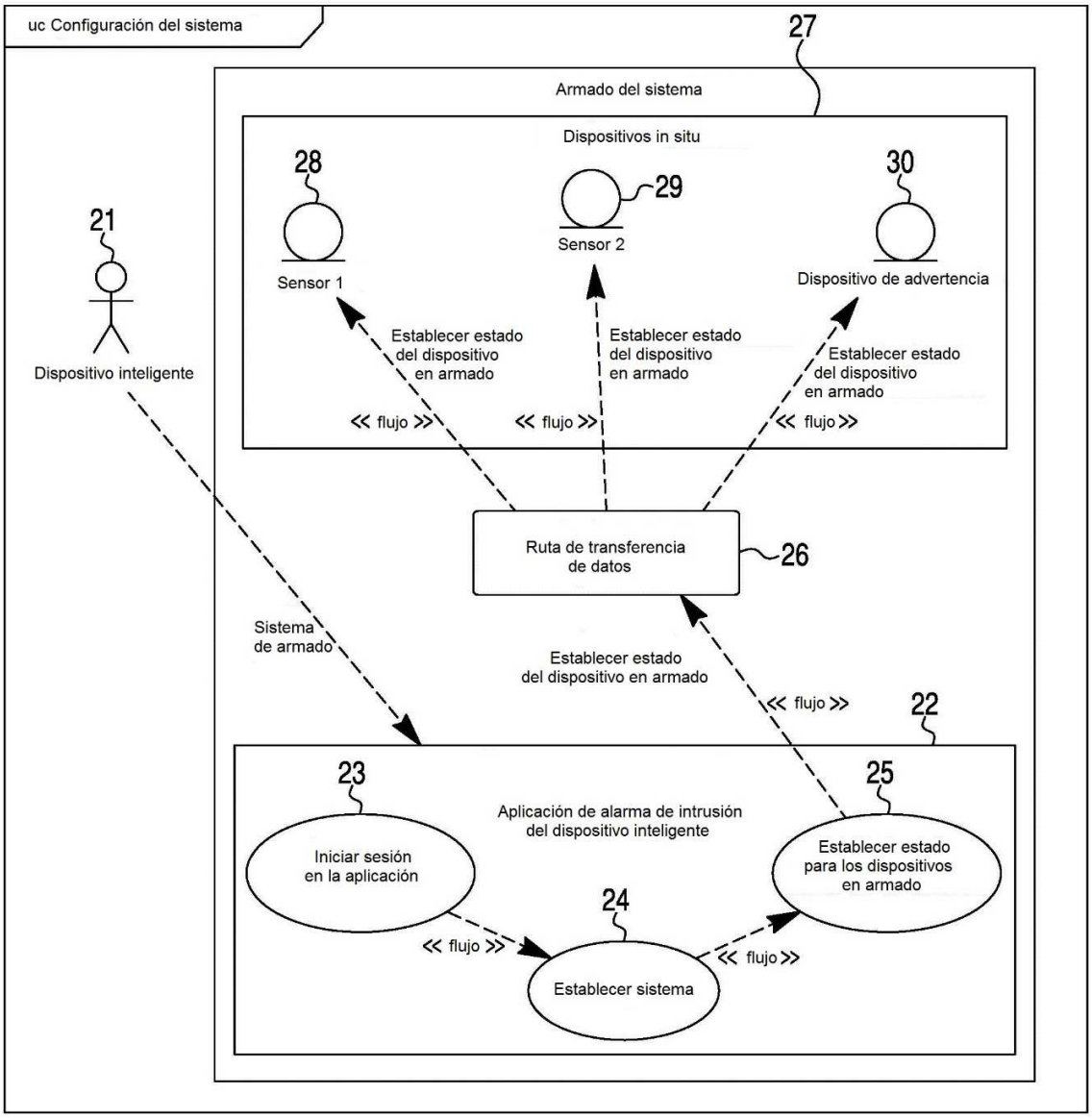

uc Configuración del sistema
27
Armado del sistema
Dispositivos in situ
28
29
30
21
Sensor 1
Sensor 2
Dispositivo de advertencia
Dispositivo inteligente
Establecer estado del dispositivo en armado
Establecer estado del dispositivo en armado
Establecer estado del dispositivo en armado
<< flujo >>
<< flujo >>
<< flujo >>
Ruta de transferencia de datos
26
Sistema de armado
Establecer estado del dispositivo en armado
<< flujo >>
22
23
25
Aplicación de alarma de intrusión del dispositivo inteligente
Iniciar sesión en la aplicación
Establecer estado para los dispositivos en armado
24
<< flujo >>
<< flujo >>
Establecer sistema

FIG. 3

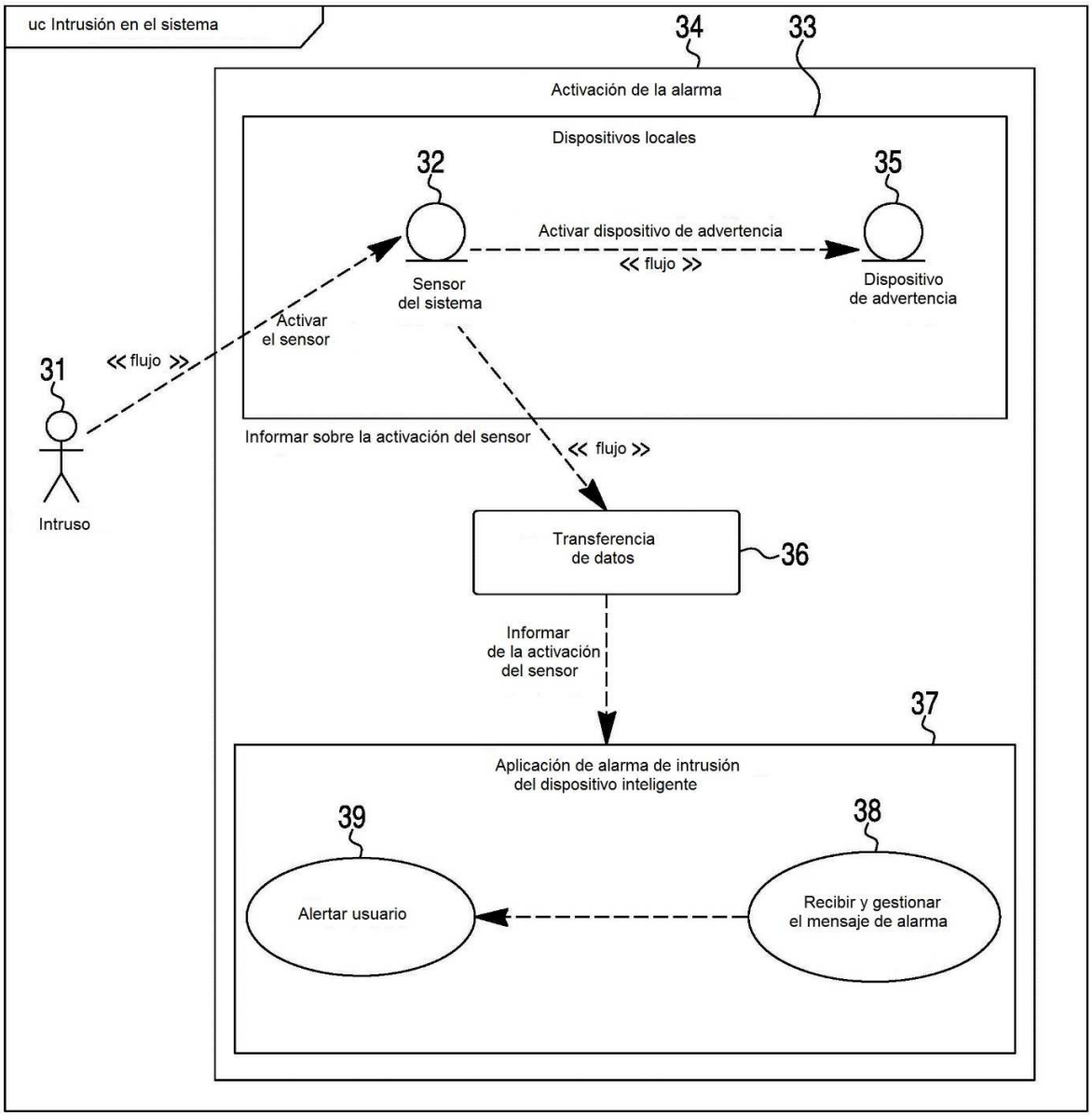

uc Intrusión en el sistema
34
33
Activación de la alarma
Dispositivos locales
32
35
Activar dispositivo de advertencia
<< flujo >>
Sensor
del sistema
Dispositivo
de advertencia
Activar
el sensor
31
<< flujo >>
Informar sobre la activación del sensor
<< flujo >>
Intruso
Transferencia
de datos
36
Informar
de la activación
del sensor
37
Aplicación de alarma de intrusión
del dispositivo inteligente
39
38
Alertar usuario
Recibir y gestionar
el mensaje de alarma

FIG. 4

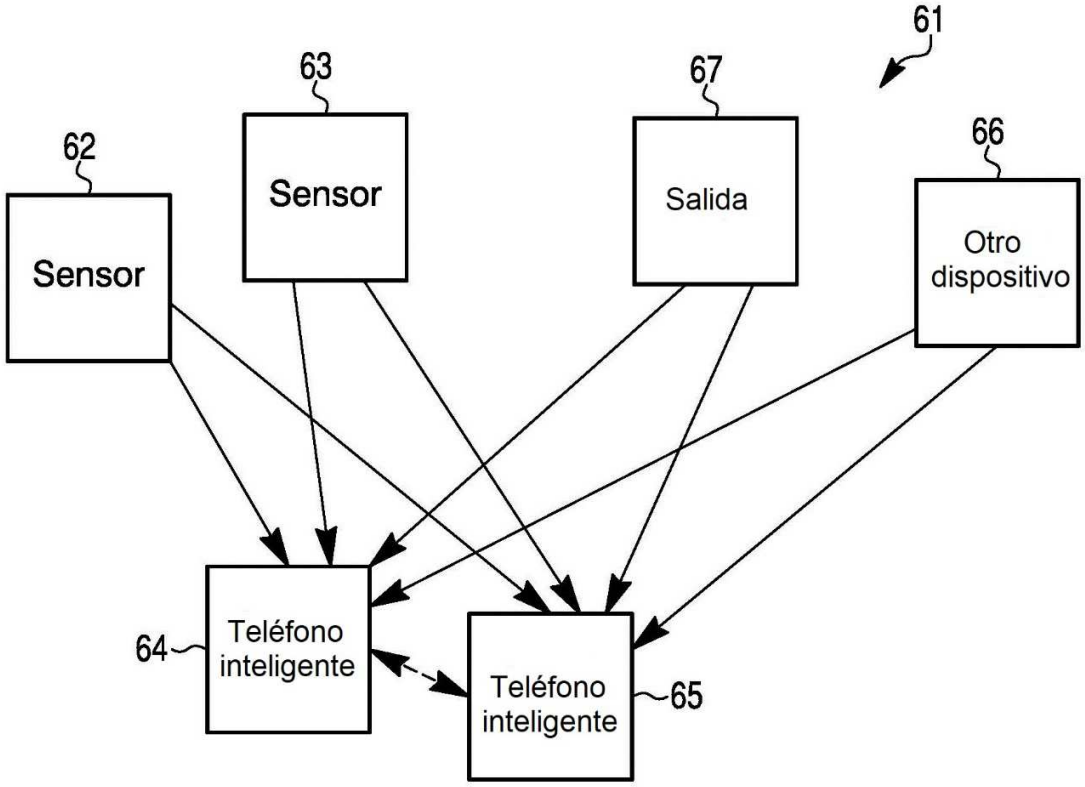

61
63
67
62
Sensor
Sensor
Salida
66
Otro dispositivo
64
Teléfono inteligente
Teléfono inteligente
65

FIG. 5

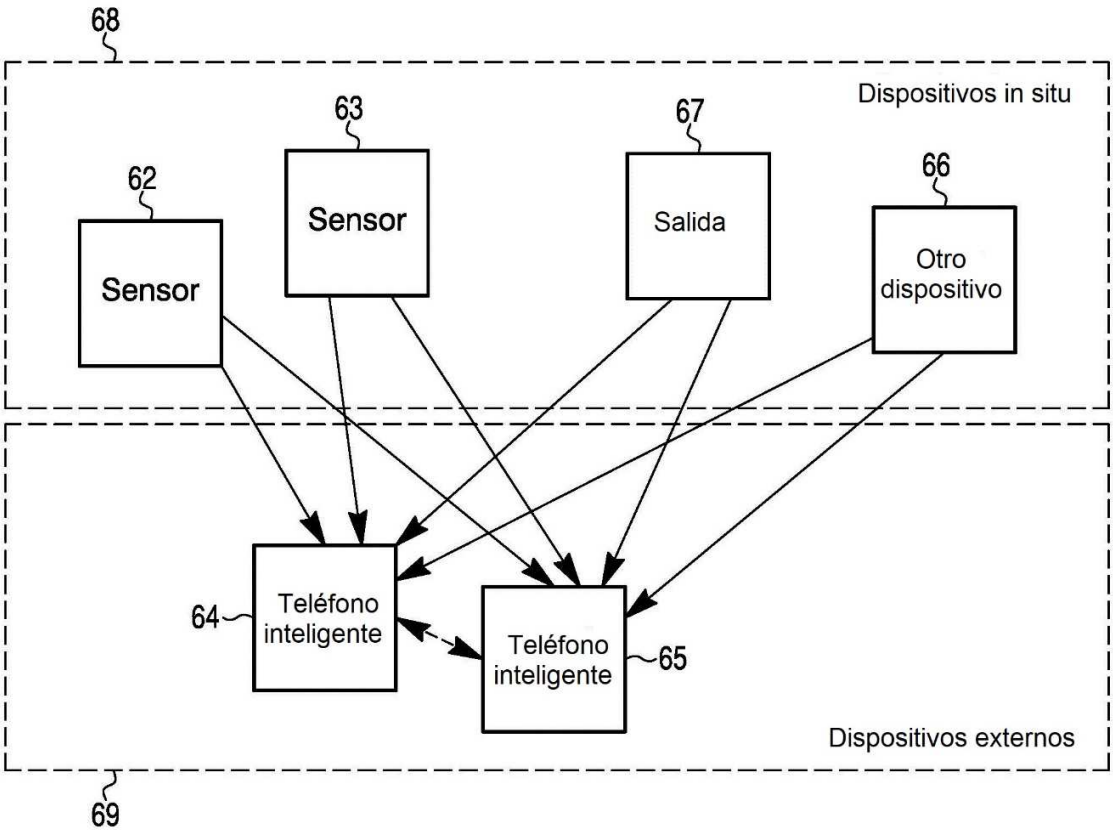

68
Dispositivos in situ
63
67
62
66
Sensor
Sensor
Salida
Otro dispositivo
64
Teléfono inteligente
Teléfono inteligente
65
Dispositivos externos
69

FIG. 6

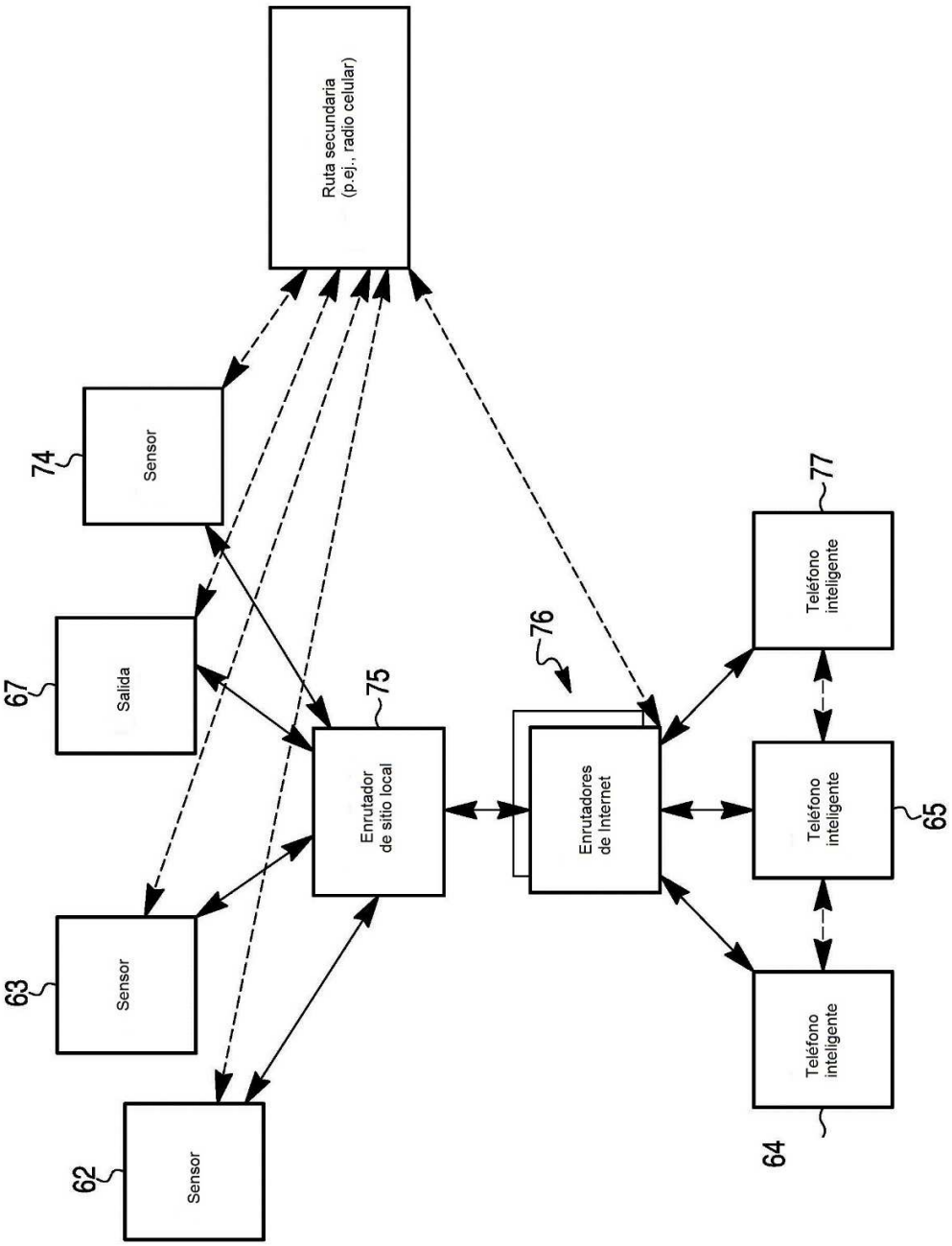

Ruta secundaria
(p.ej., radio celular)
74
Sensor
67
Salida
63
Sensor
62
Sensor
75
Enrutador
de sitio local
76
Enrutadores
de Internet
77
Teléfono
inteligente
Teléfono
inteligente
65
Teléfono
inteligente
64

FIG. 7

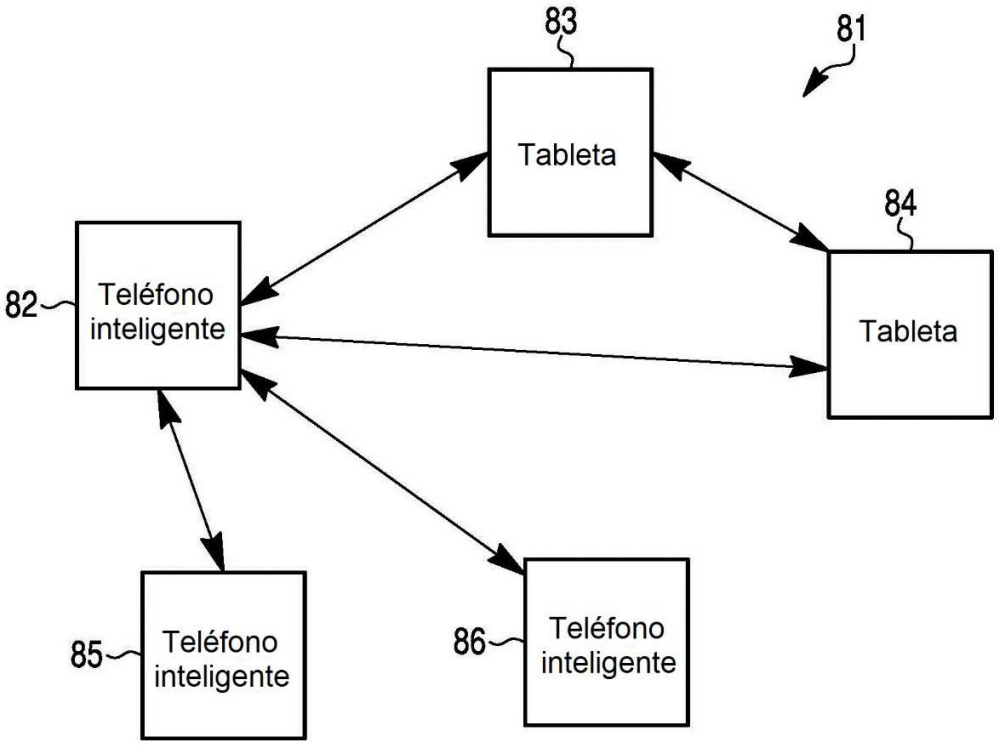
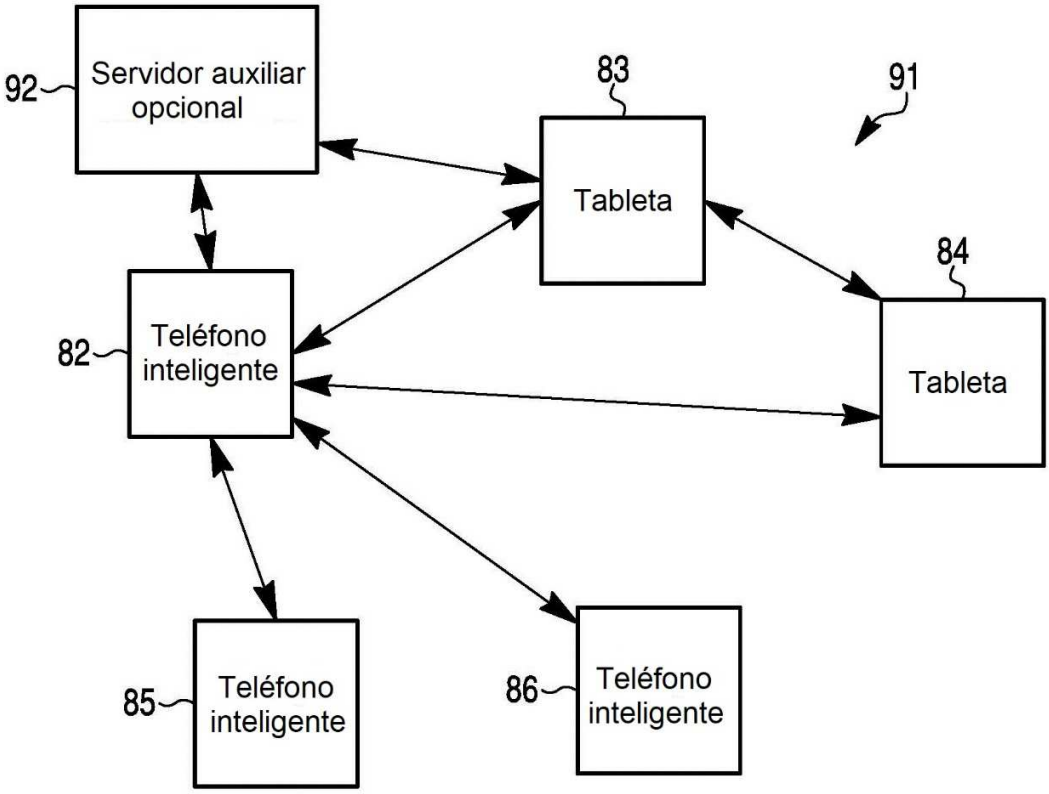

83
81
Tableta
84
82
Teléfono inteligente
Tableta
85
Teléfono inteligente
86
Teléfono inteligente

FIG. 8


92
Servidor auxiliar opcional
83
91
Tableta
84
82
Teléfono inteligente
Tableta
85
Teléfono inteligente
86
Teléfono inteligente