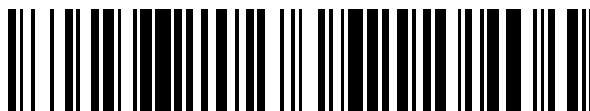


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 675 736**

51 Int. Cl.:

G08B 25/00 (2006.01)

G08B 25/10 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **23.06.2016 E 16176070 (7)**

97 Fecha y número de publicación de la concesión europea: **16.05.2018 EP 3115980**

54 Título: **Algoritmo de selección de canal adaptativo y automatizado sobre la base del menor ruido y de la menor densidad de la red de sensores inalámbricos en la proximidad**

30 Prioridad:

09.07.2015 US 201514794935

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

12.07.2018

73 Titular/es:

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

72 Inventor/es:

**BEEMA, VISHNU VARDHAN REDDY y
SURESH, SANDEEP**

74 Agente/Representante:

LEHMANN NOVO, María Isabel

ES 2 675 736 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Algoritmo de selección de canal adaptativo y automatizado sobre la base del menor ruido y de la menor densidad de la red de sensores inalámbricos en la proximidad

5

CAMPO DE LA INVENCION

Esta solicitud se refiere a sistemas de seguridad y más en particular, a interferencias entre sistemas de seguridad inalámbricos.

10

ANTECEDENTES DE LA INVENCION

Es conocido que existen sistemas destinados a proteger a las personas y los bienes dentro de zonas aseguradas. Dichos sistemas suelen estar basados en el uso de uno o más sensores inalámbricos que detectan amenazas dentro de la zona asegurada.

15

Las amenazas a personas y activos se pueden originar a partir de cualquiera de varias fuentes diferentes. A modo de ejemplo, un incendio puede causar la muerte, o lesionar, a los ocupantes que quedaron atrapados por un incendio en una vivienda. De modo similar, el monóxido de carbono procedente de un incendio puede matar a las personas mientras duermen.

20

Como alternativa, un intruso no autorizado, según un ladrón, puede presentar una amenaza a los bienes dentro de la zona. Además, se tiene conocimiento de que los intrusos lesionan o causan la muerte a personas que viven dentro de la zona.

25

En el caso de intrusos, los sensores se pueden colocar en diferentes zonas, en función de los respectivos usos respectivos de dichas zonas. A modo de ejemplo, si las personas están presentes durante algunas partes de un día normal y no en otras ocasiones, los sensores se pueden colocar a lo largo de la periferia del espacio con el fin de proporcionar protección cuando el espacio está ocupado, mientras que sensores adicionales pueden colocarse en el interior del espacio y utilizarse cuando el espacio no está ocupado.

30

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

35

Los documentos de patente números US2007/038743A1 y US2015/097689A1 dan a conocer sistemas y métodos para comunicaciones o redes inalámbricas.

Mientras que los sistemas de seguridad convencionales, que utilizan sensores inalámbricos funcionan bien, a veces son difíciles de configurar. En consecuencia, existe la necesidad de mejores métodos y aparatos para configurar tales sistemas.

40

La presente invención, en sus diversos aspectos, es según se establece en las reivindicaciones adjuntas.

45

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 ilustra un diagrama de bloques de un sistema de automatización de conformidad con la presente; y

La Figura 2 es un diagrama de flujo de un método de conformidad con las formas de realización descritas.

50

DESCRIPCIÓN DETALLADA

Mientras que las formas de realización aquí dadas a conocer pueden tomar muchas formas diferentes, las formas de realización específicas de las mismas se ilustran en los dibujos y se describen aquí, en detalle, con el entendimiento de que la presente idea inventiva se debe considerar como un ejemplo de los principios de la misma, así como el mejor modo de su puesta en práctica, y no pretende limitar la aplicación o las reivindicaciones a la forma de realización específica ilustrada.

55

La Figura 1 representa un sistema de automatización 10 (a modo de ejemplo, un sistema de seguridad) que se muestra, en general, de conformidad con una forma de realización ilustrada. Incluido dentro del sistema de seguridad pueden existir varios sensores 12, 14, utilizados para detectar amenazas dentro de una zona geográfica asegurada 16 del sistema. Las amenazas pueden originarse a partir de cualquiera de varias fuentes diferentes. A modo de ejemplo, un intruso puede representar una amenaza para personas y/o bienes dentro de una vivienda o negocio. De modo similar, una fuga de gas o incendio puede amenazar la seguridad de esas mismas personas y/o bienes.

60

En consecuencia, los sensores pueden estar incorporados en cualquiera de una serie de formas diferentes. A modo

65

de ejemplo, al menos algunos de los sensores pueden ser interruptores colocados en las puertas y ventanas que proporcionan entrada y salida de la zona asegurada. Otros sensores pueden ser sensores de infrarrojos pasivos (PIR), situados dentro de la zona asegurada para detectar intrusos que han podido eludir los sensores a lo largo de la periferia de la zona asegurada. Otros sensores adicionales pueden ser detectores de humo y/o fuego.

5 Un panel de control o controlador 18 está asociado, además, con la zona asegurada. El panel de control puede estar situado dentro de la zona asegurada según se ilustra en la Figura 1, o situada de forma distante.

10 El panel de control puede supervisar los sensores para activación. A la activación de uno de los sensores, el panel de control puede componer un mensaje de alarma y enviarlo a una estación central de supervisión 20. La estación central de supervisión puede responder realizando una llamada a la ayuda adecuada (a modo de ejemplo, policía, departamento de bomberos, etc.).

15 El sistema de seguridad se puede controlar por un usuario humano a través de una interfaz de usuario 22. En la interfaz de usuario se puede incluir una pantalla 24 y un teclado 26.

20 Situada dentro del panel de control, la interfaz de usuario, y cada uno de los sensores, puede ser uno o más aparatos de procesamiento (procesadores) 28, 30, operando, cada uno de ellos, bajo el control de uno o más programas informáticos 32, 34 cargados desde un soporte legible por ordenador no transitorio (memoria) 36. Según aquí se utiliza, la referencia a una etapa puesta en práctica mediante un sistema informático, es también una referencia al procesador que ejecuta dicha etapa.

25 El sistema de seguridad puede activarse y desactivarse a través de la interfaz de usuario. En este sentido, un usuario autorizado puede introducir un número de identificación personal (PIN) y una instrucción a través del teclado. La instrucción puede ser una instrucción de activación, una activación a distancia y/o una orden de desactivación.

30 Un procesador de estado puede supervisar la interfaz de usuario para la entrada procedente del usuario humano. A la detección de un PIN, el procesador de estado puede comparar el PIN introducido con los PIN de usuarios autorizados. Si el PIN introducido coincide con el PIN de un usuario autorizado entonces, el procesador de estado ejecuta la instrucción. Si no es así, se puede ignorar la entrada o se genera un mensaje de error.

35 En el estado activado, un procesador de alarma supervisa cada uno de los sensores para activación. A la detección de la activación de uno de los sensores, el procesador de alarma compone y envía un mensaje de alarma a la estación central de supervisión. El mensaje de alarma puede incluir un identificador del sistema (a modo de ejemplo, número de cuenta, dirección postal, etc.), un identificador del sensor y el momento de la activación.

40 En general, los sensores ilustrados en la Figura 1 son dispositivos inalámbricos que se comunican, cada uno, con el panel de control, en uno o más canales de radiofrecuencia (RF). En consecuencia, se proporciona, en apoyo de dicha comunicación inalámbrica, un transceptor de radiofrecuencia 38 localizado dentro del panel de control y cada uno de los sensores.

45 A modo de ejemplo, el panel de control puede incluir uno o más procesadores de comunicación que definen una súper-trama de RF para la comunicación entre el panel de control y los sensores. La súper-trama, a su vez, puede definirse por varias ranuras de acceso múltiple por división de tiempo (TDMA) que tienen lugar durante un período de tiempo predeterminado. Algunas de las ranuras se pueden reservar para ser utilizadas por los sensores bajo un protocolo 6LowPan/IPv6 /IoT.

50 La súper-trama puede incluir una ranura reservada para una baliza, y ranuras reservadas para el intercambio de mensajes entre los sensores y el panel de control bajo un protocolo IEEE 802.15.4 y/o 6LowPAN. La baliza puede identificar un punto de inicio de la súper-trama e incorporar una diversidad de campos de datos que definen, cada uno, aspectos respectivos de la súper-trama.

55 Cada sensor del sistema de la Figura 1 puede tener una dirección corta y una dirección IPv6 (6LowPan) y un identificador MAC (MAC ID). El sistema de direccionamiento facilita el acceso a los sensores por cualquier otro dispositivo compatible con IPv6, según se describe en varias publicaciones de Internet de Things (IoT). Lo que antecede permite que los sensores estén dispuestos por respectivos procesadores en redes en estrella o árbol.

60 El estado del panel de control (a modo de ejemplo, activado, desactivado, en condición anómala, etc.) puede transmitirse como parte de la carga útil de la baliza. Si es necesario, se puede transmitir, además, un indicador detallado del estado del panel, dentro de las respectivas ranuras bajo los protocolos 6LowPAN/802.15.4. Las ranuras de control de la baliza se pueden utilizar, además, para enviar mensajes de demanda desde el panel de control a dispositivos finales (a modo de ejemplo, sensores, etc.) sobre la base de las direcciones IEEE802.15.4 de los dispositivos finales.

65 Bajo una forma de realización ilustrada, la frecuencia de canal, utilizada como un canal de operación principal por el sistema, para intercambiar información entre el panel de control y los sensores a través de la súper-trama, se

- 5 selecciona automáticamente por un sistema de selección de canal en funcionamiento desde dentro del panel de control. El sistema de selección de canal selecciona un canal de RF en función de una serie de etapas específicas. En primer lugar, un procesador de detección del sistema de selección de canal escanea activamente un espectro predeterminado (por ejemplo, un conjunto de canales contiguos) para puntos de acceso de otros sistemas de automatización en funcionamiento en uno o más de dichos canales escaneados. El escaneo activo, en esta situación operativa, significa la recepción y decodificación de identificadores de red de área personal (PAN-IDs) desde otros puntos de acceso en cada canal escaneado, con el fin de determinar el número de puntos de acceso que son operativos en ese canal.
- 10 Sobre la base del número de puntos de acceso identificados por el escaneo activo, el sistema de selección de canal puede funcionar mediante varios métodos diferentes. De conformidad con la presente invención, el procesador de detección identifica, en primer lugar, los canales escaneados con el menor número relativo de puntos de acceso en funcionamiento en ese canal. Si solamente existe un canal que cumple este criterio entonces, el procesador de detección, o un procesador de selección relacionado, selecciona este canal. Por otro lado, si existe más de un canal que cumple este criterio (es decir, dos o más canales con cero puntos de acceso, o dos o más canales con el mismo número de puntos de acceso) entonces, el procesador de detección (o un procesador relacionado), efectúa un escaneo de energía sobre estos canales. En este caso, el escaneo de energía identifica el canal con la menor cantidad de energía y el menor número de puntos de acceso próximos en funcionamiento en este canal. En este caso, el canal con la menor energía es seleccionado por el procesador de detección, o el procesador de selección relacionado.
- 15 Una vez que se ha seleccionado una frecuencia de canal, el procesador de detección, o procesador de configuración, realiza otro escaneo activo del canal seleccionado. En este caso, el segundo escaneo activo es para identificar los PAN-IDs de cualquier otro punto de acceso que opere en este canal. Lo que antecede es parte de un proceso utilizado por el sistema para seleccionar su propio PAN-ID único. En este caso, el identificador PAN-ID único del sistema se selecciona, de forma aleatoria, sobre la base de los PAN-IDs identificados.
- 20 Una vez que se han seleccionado la frecuencia del canal y el identificador PAN-ID, entonces un procesador de baliza puede comenzar a transmitir una baliza en beneficio de los sensores inalámbricos próximos, dentro de la zona asegurada. Los sensores detectan la baliza y se registran, automáticamente, ya sea directamente con el panel de control o a través de otros sensores en una relación principal-secundario.
- 25 En general, el sistema de la Figura 1 resuelve una serie de problemas no abordados por sistemas anteriores. A modo de ejemplo, según las normas IEEE 802.15.4, la selección de canales del coordinador/maestro se basa en el canal con menos ruido. Lo que antecede tiene el inconveniente de que, en un entorno ruidoso (ruido generado por otras tecnologías que utilizan 2,4 GHz, según WiFi o ZigBee, etc.), el maestro captará los canales que no se solapen de conformidad con las normas del canal 11 y el canal 25 solamente. Con otras redes de automatización habilitadas con baliza de alta potencia en el mismo canal (11 o 25), en un entorno ruidoso de apartamentos/hogares situados en la proximidad, lo que antecede causará que una baliza interfiera con la otra y se solapen, además, las ranuras entre los sistemas, teniendo como resultado la pérdida de alarmas/mensajes.
- 30 Bajo la norma IEEE802.15.4, se debe realizar un escaneo de energía en todos los canales. El canal es seleccionado sobre la base de la menor energía. Una vez que se selecciona un canal, se realiza un escaneo activo para seleccionar el identificador PAN-ID único.
- 35 Los canales WiFi coexisten con dispositivos IEEE802.15.4. Debido a la alta energía de los dispositivos WiFi, la mayoría de los puntos de acceso basados en IEEE802.15.4 seleccionarán canales de interferencia no WiFi.
- 40 En un sistema habilitado para baliza, con varios puntos de acceso de IEEE802.15.4 en funcionamiento en el mismo canal de radiofrecuencia, se producirán numerosas colisiones y una gran interferencia entre balizas. Debido a esta situación operativa, es difícil inscribir dispositivos y más tarde, resulta difícil mantener el sincronismo entre los dispositivos registrados y la baliza.
- 45 El sistema de la Figura 1 resuelve muchos de estos problemas. El proceso (algoritmos) del sistema de la Figura 1 se ejecuta de forma completamente automática. No es necesario que el usuario intervenga o introduzca ningún parámetro específico.
- 50 El sistema proporciona una interferencia mínima o nula. Existe una distribución uniforme de puntos de acceso y sensores a través de los canales 11-25, lo que resulta en interferencia mínima/cero entre los sensores en los mismos canales. Pueden existir hasta 15 próximos sin un canal superpuesto, lo que es más que suficiente para una instalación práctica/escenario operativo de realización.
- 55 No existen mensajes perdidos. Debido a la no superposición de canales y a la ausencia de interferencias entre los sistemas próximos, no desaparecen alarmas ni ningún otro mensaje crítico.
- 60 Existe un menor tiempo de registro. Debido a la interferencia mínima/cero, se evitan los intentos de detección por parte de los sensores, lo que resulta en una inscripción más rápida y, por lo tanto, un tiempo de inscripción reducido.
- 65

Se realiza la detección automática y se evitan canales WiFi. El sistema detecta, automáticamente, la existencia de tráfico WiFi en un canal específico, y evita que esos canales sean utilizados por el sistema.

5 El sistema proporciona el mejor compromiso entre canales ruidosos y densamente utilizados. Mejora, además, la vida útil de la batería. Debido a la interferencia reducida de otros sistemas en el mismo canal, los sensores son capaces de transmitir alarmas en el primer intento y, en la mayoría de los casos, eliminar reintentos.

10 La secuencia de etapas que sigue el sistema se puede resumir de la siguiente manera, de modo que existan puntos de acceso mínimos por canal. En primer lugar, el sistema realiza un escaneo activo en todos los canales. Al hacerlo, el sistema conoce la cantidad de puntos de acceso/identificadores PAN-IDs ya presentes en el canal. Si existe un canal con cero o con menos puntos de acceso que los otros canales, en ese caso, el sistema selecciona ese canal. Si existe más de un canal con 0 puntos de acceso, o con el mismo número de puntos de acceso, entonces, el sistema realiza un escaneo de energía en esos canales. Esto ayudará a seleccionar un canal con la menor cantidad de energía y el menor número de puntos de acceso. Por último, el sistema realiza un segundo escaneo activo en el canal seleccionado. Lo que antecede se realiza con el fin de seleccionar el identificador PAN-ID único, distinto de los PAN-IDs próximos. Una vez que se selecciona el identificador PAN-ID, el sistema comienza a balizar en el canal seleccionado.

20 En general, el sistema incluye un panel de control de un sistema de automatización que protege una zona geográfica asegurada, mediante el escaneo activo de cada uno de entre una pluralidad de canales de radiofrecuencia de un espectro de radiofrecuencia predeterminado para otros puntos de acceso en funcionamiento bajo un formato IEEE802.15.4, identificando el panel de control al menos dos de entre la pluralidad de canales con un número relativo menor de los otros puntos de acceso en funcionamiento bajo el formato IEEE802.15.4, poniendo en práctica, el panel de control, un escaneo de energía en cada uno de los al menos dos canales identificados, seleccionando, el panel de control, uno de los al menos dos canales con la energía relativa más baja y estableciendo, el panel de control, una conexión inalámbrica con cada uno de una pluralidad de sensores inalámbricos dentro de la zona asegurada, en el canal seleccionado, en el formato IEEE802.15.4.

30 Como alternativa, el sistema incluye un sistema de automatización que protege una zona geográfica asegurada, un procesador del sistema de automatización que escanea, activamente, cada uno de entre una pluralidad de canales de radiofrecuencia de un espectro de radiofrecuencia predeterminado para otros puntos de acceso próximos en funcionamiento bajo un formato IEEE802.15.4, un procesador del sistema de automatización que identifica al menos dos de la pluralidad de canales con un número relativo más bajo que los otros puntos de acceso próximos en funcionamiento bajo el formato IEEE802.15.4, un procesador del sistema de automatización que realiza un escaneo de energía sobre cada uno de los al menos dos canales identificados, y un procesador del sistema de automatización que selecciona uno de los al menos dos canales con la energía relativa más baja.

40 Como alternativa, el sistema incluye a) un panel de control de un sistema de automatización que protege una zona geográfica asegurada escaneando, activamente, cada uno de entre una pluralidad de canales de radiofrecuencia de un espectro de radiofrecuencia predeterminado para otros puntos de acceso en funcionamiento bajo un formato IEEE802.15.4, b) el panel de control que identifica uno o más canales de radiofrecuencia escaneados activamente que tienen un número relativo menor de puntos de acceso en funcionamiento en uno o más canales, c) si los canales identificados de entre los uno o más canales, incluyen solamente un canal, entonces se salta a la etapa e, d) si los canales identificados, de entre los uno o más canales incluyen más de un canal, entonces, se salta a la etapa f, e) el panel de control selecciona un canal de radiofrecuencia y salta a la etapa h, f) el panel de control realiza un escaneo de energía en cada uno de los más de un canal identificado, g) el panel de control selecciona uno de los más de un canal con la energía relativa más baja y h) el panel de control establece una conexión inalámbrica con cada uno de una pluralidad de sensores inalámbricos dentro de la zona asegurada en el canal seleccionado en el formato IEEE802.15.4.

50 A partir de lo que antecede, ha de observarse que se pueden ponerse en práctica numerosas variaciones y modificaciones sin desviarse del alcance de la presente invención. Conviene señalar que no se pretende o debe inferirse ninguna limitación con respecto al aparato específico ilustrado en este documento. Por supuesto, se pretende cubrir mediante las reivindicaciones adjuntas todas las modificaciones que caigan dentro del alcance de las reivindicaciones. Además, los flujos lógicos, representados en las figuras, no requieren el orden particular ilustrado, o el orden secuencial, para conseguir resultados deseables. Se pueden proporcionar otras etapas, o se pueden eliminar etapas, a partir de los flujos descritos, y se pueden añadir otros componentes, o eliminarlos de las formas de realización descritas.

60

REIVINDICACIONES

1. Un método que comprende:

5 un panel de control (18) de un sistema de automatización (10) que protege una zona geográfica asegurada (16), mediante el escaneo, de forma activa, de cada uno de entre una pluralidad de canales de radiofrecuencia de un espectro de radiofrecuencia predeterminado para puntos de acceso de otros sistemas de automatización en funcionamiento bajo un formato IEEE802.15.4;
10 el panel de control (18) que recibe y decodifica identificadores personales de red para cualquiera de los puntos de acceso;

el panel de control determina un número de puntos de acceso en funcionamiento en cada uno de la pluralidad de canales de radiofrecuencia sobre la base de los identificadores personales de red;

15 el panel de control que identifica canales de radiofrecuencia identificados de la pluralidad de canales de radiofrecuencia, en los que un número de puntos de acceso en funcionamiento es el más pequeño;

el panel de control selecciona uno de los canales de radiofrecuencia identificados sobre la base de una serie de canales de radiofrecuencia identificados y una energía relativa más baja de los canales de radiofrecuencia identificados, se recibe desde un escaneo de energía en cada uno de los canales de radiofrecuencia identificados cuando el número de los canales de radiofrecuencia identificados es mayor que uno;

20 el panel de control realiza un escaneo activo de uno de los canales de radiofrecuencia identificados, para identificar los identificadores personales de red para cualquiera de los puntos de acceso en funcionamiento en uno de los canales de radiofrecuencia identificados;

25 el panel de control selecciona, de forma aleatoria, un identificador personal de red único para el sistema de automatización basado en los identificadores personales de red para cualquiera de los puntos de acceso en funcionamiento en uno de los canales de radiofrecuencia identificados a partir del escaneo activo; y

30 el panel de control establece una conexión inalámbrica con cada uno de una pluralidad de sensores inalámbricos (12) dentro de la zona geográfica asegurada (16) en uno de los canales de radiofrecuencia identificados en el formato IEEE802.15.4.

35 2. El método según la reivindicación 1, en donde el establecimiento de la conexión inalámbrica incluye la definición de una súper-trama en uno de los canales de radiofrecuencia identificados.

40 3. El método según la reivindicación 2, que comprende, además, el panel de control (18) que transmite una baliza que define la súper-trama.

4. El método según la reivindicación 1, en donde el establecimiento de la conexión inalámbrica con cada uno de la pluralidad de sensores inalámbricos (12) comprende, además, establecer una red de malla entre el panel de control (18) y la pluralidad de sensores inalámbricos.

45 5. El método según la reivindicación 1, en donde el sistema de automatización (10) incluye un sistema de seguridad.

6. El método según la reivindicación 1 que comprende, además, al menos parte de la pluralidad de sensores inalámbricos (12) que detectan amenazas dentro de la zona geográfica asegurada (16).

50 7. El método según la reivindicación 6, que comprende, además, un procesador (28) del panel de control (18) que informa sobre las amenazas detectadas a una estación central de supervisión (20).

8. Un aparato que comprende:

55 un sistema de automatización (10) que protege una zona geográfica asegurada (16); y

un procesador (28), del sistema de automatización (10), que escanea activamente cada uno de una pluralidad de canales de radiofrecuencia de un espectro de radiofrecuencia predeterminado para puntos de acceso próximos de otros sistemas de automatización en funcionamiento bajo un formato IEEE802.15.4,

60 en donde el procesador (28) del sistema de automatización (10) recibe y decodifica identificadores personales de red para cualquiera de los puntos de acceso y determina un número de puntos de acceso en funcionamiento en cada uno de la pluralidad de canales de radiofrecuencia en función de los identificadores personales de red,

65 en donde el procesador del sistema de automatización identifica canales de radiofrecuencia identificados de la pluralidad de canales de radiofrecuencia en los que el número de puntos de acceso en funcionamiento es el más

pequeño,

5 en donde el procesador del sistema de automatización selecciona uno de los canales de radiofrecuencia identificados, en función del número de canales de radiofrecuencia identificados, y la energía relativa más baja de los canales de radiofrecuencia identificados, que se recibe desde un escaneo de energía en cada uno de los canales de radiofrecuencia identificados, que se realiza cuando el número de canales de radiofrecuencia identificados es mayor que uno,

10 en donde el procesador del sistema de automatización realiza un escaneo activo de uno de los canales de radiofrecuencia identificados, con el fin de identificar los identificadores personales de red para cualquiera de los puntos de acceso en funcionamiento en uno de los canales de radiofrecuencia identificados, y

15 en donde el procesador del sistema de automatización selecciona, de forma aleatoria, un identificador personal de red único para el sistema de automatización, sobre la base de los identificadores personales de red para cualquiera de los puntos de acceso en funcionamiento en uno de los canales de radiofrecuencia identificados, que se identifican a partir del escaneo activo.

20 9. El aparato según la reivindicación 8 que comprende, además, una pluralidad de sensores (12) que detecta amenazas dentro de la zona geográfica asegurada (16).

10. El aparato según la reivindicación 9 en donde el procesador (28) del sistema de automatización (10) establece una conexión inalámbrica con cada uno de entre la pluralidad de sensores (12) dentro de la zona geográfica asegurada (16) en uno de los canales de radiofrecuencia identificados bajo el formato IEEE802.15.4.

25 11. El aparato según la reivindicación 10, en donde el procesador (28) del sistema de automatización (10) establece una red de malla entre un panel de control (18) y la pluralidad de sensores (12).

30

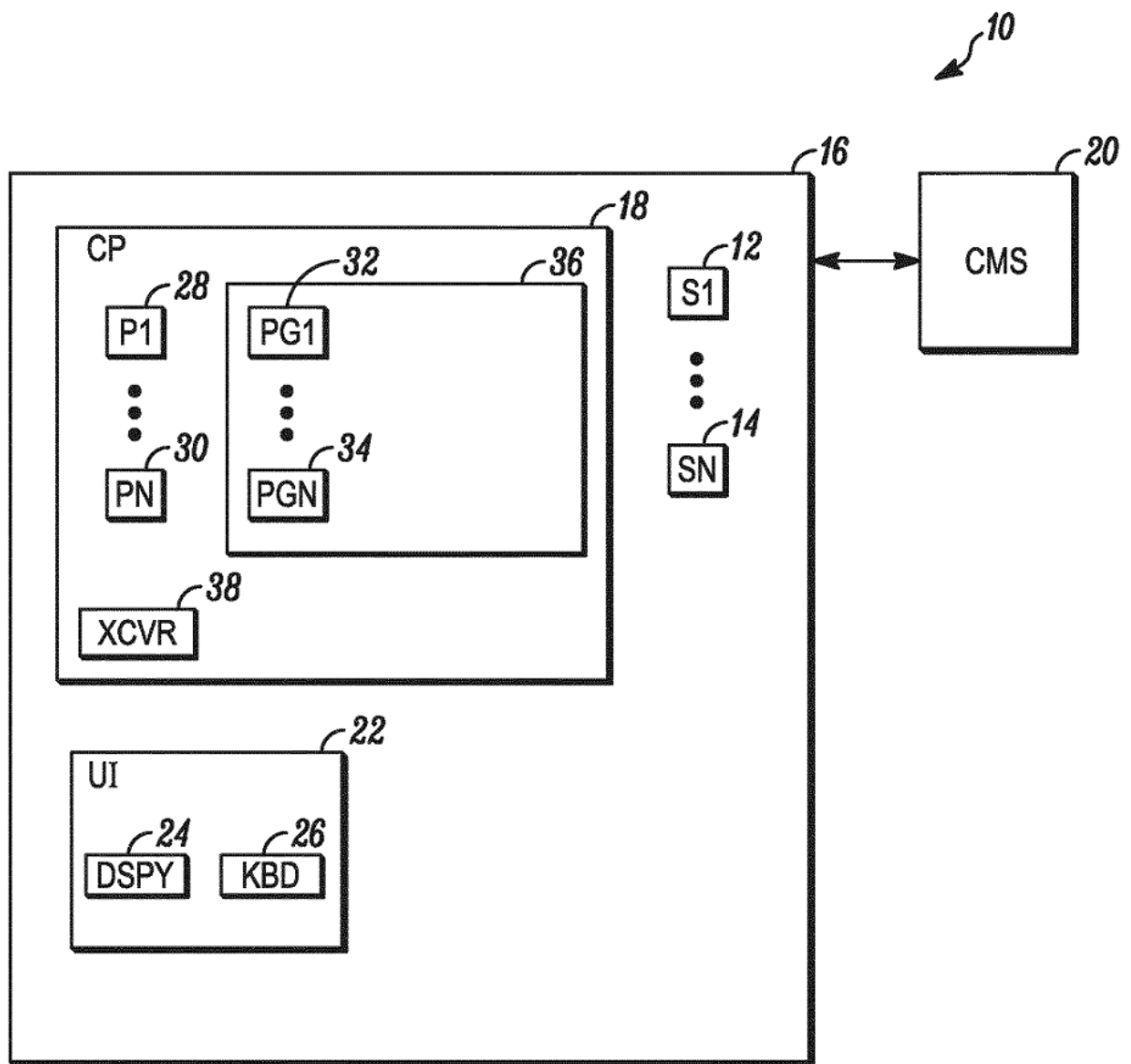


FIG. 1

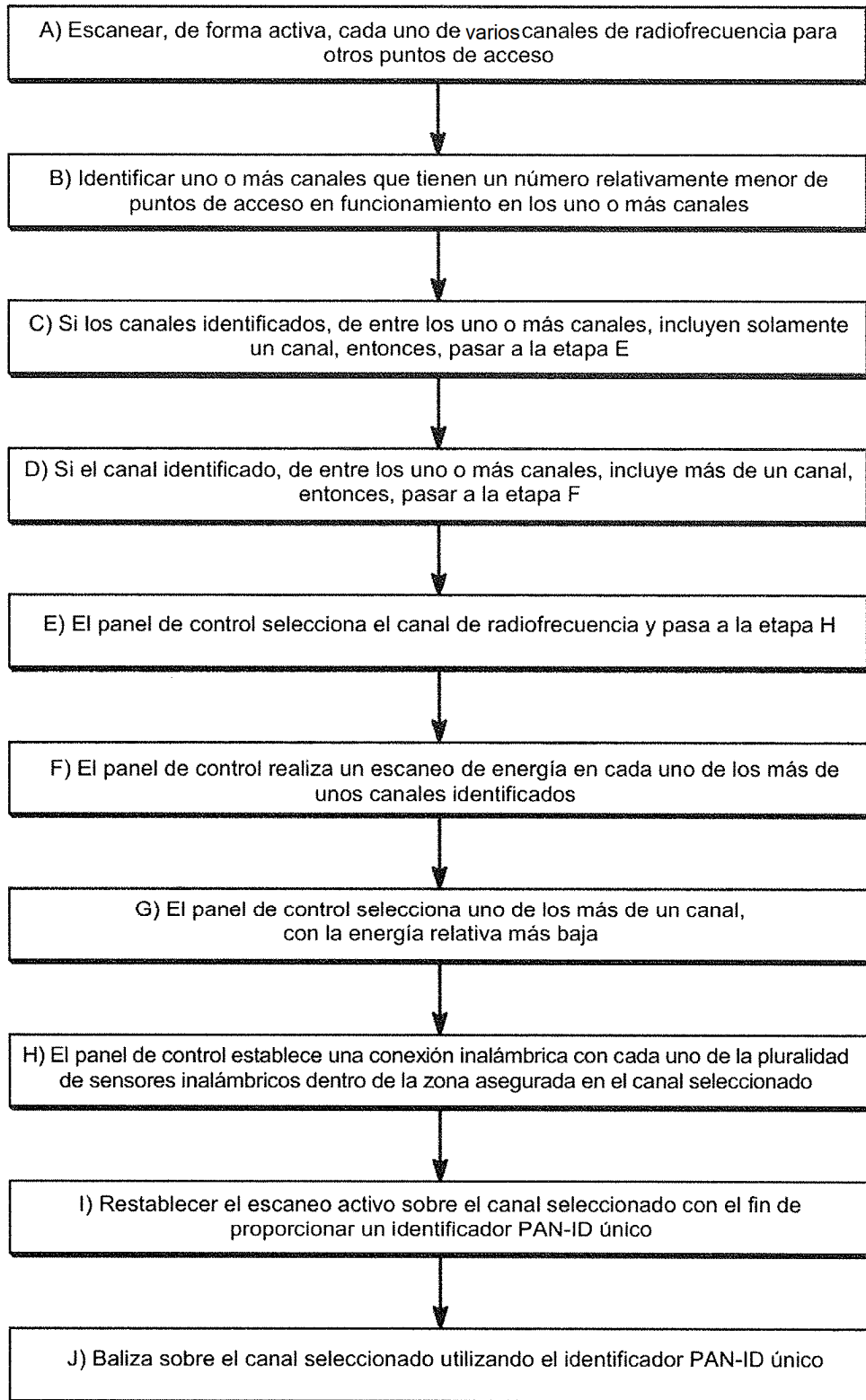


FIG. 2