(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 691 959**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04W 12/04 (2009.01)
H04W 84/18 (2009.01)
H04L 29/08 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.11.2013 E 13193579 (3)**

(97) Fecha y número de publicación de la concesión europea: **12.09.2018 EP 2747470**

(54) Título: **Autenticación y seguridad de datos para redes inalámbricas 6LoWPAN**

(30) Prioridad:

18.12.2012 US 201213719057

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.11.2018

(73) Titular/es:

HONEYWELL INTERNATIONAL INC. (100.0%)
115 Tabor Road
Morris Plains, NJ 07950, US

(72) Inventor/es:

SCHMIT, THOMAS PAUL y
SHRIVASTAVA, ABHISHEK

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Autenticación y seguridad de datos para redes inalámbricas 6LoWPAN.

Campo

El campo está relacionado con sistemas de seguridad y, más en particular, con sistemas de seguridad inalámbricos.

Antecedentes

Los sistemas de seguridad son bien conocidos. Dichos sistemas comprenden típicamente un área asegurada protegida por uno o más sensores. El área asegurada puede incluir algún tipo de barrera física (por ejemplo, una pared, una valla, etc.) emplazada alrededor del área asegurada con uno o más accesos (por ejemplo, puertas, ventanas, etc.) que permiten que las personas autorizadas entren en o salgan del área asegurada. Los sensores se pueden proporcionar en forma de interruptores de frontera dispuestos para detectar la apertura de los accesos por parte de intrusos. Los sensores también se pueden proporcionar en forma de detectores de movimiento que detectan el desplazamiento en una parte del área asegurada.

Los sensores pueden estar conectados a un panel de alarma local. En caso de detección de un intruso, el panel de alarma puede activar una alarma acústica local. El panel de alarma también puede enviarle un mensaje de alarma a una estación central de monitorización.

Los sensores pueden estar conectados al panel de alarma de forma inalámbrica. En este caso, cada uno de los sensores (así como el panel de alarma) está equipado con un transceptor de radiofrecuencia independiente. Dicho transceptor opera usualmente a un nivel bajo de potencia que no requiere una licencia de la FCC.

En la mayor parte de los casos, el intercambio inalámbrico entre los transceptores se cifra para evitar la subversión del sistema de seguridad. Normalmente, esto requiere el uso de métodos secretos de codificación. Sin embargo, esto hace que la configuración de los sensores inalámbricos resulte laboriosa en el tiempo y costosa. En consecuencia, existe la necesidad de métodos mejores para configurar dichos sistemas.

El documento de KIM K Y OTROS: "Commissioning in 6LoWPAN (Puesta en servicio en redes 6LoWPAN) draft-6lowpan-commissioning-02.txt; draft-daniel-6lowpan-commissioning-02.txt", 15 de julio de 2008 (2008-07-15), 20080715, XP015055411, ISSN: 0000-0004, divulga técnicas para la puesta en servicio en una 6LoWPAN. El proceso de puesta en servicio define el procedimiento de inicio ejecutado por cualquier dispositivo de la 6LoWPAN. Se define un procedimiento de inicio que debe ser seguido por un dispositivo 6LoWPAN en cualquier red abierta o asegurada.

El documento US2007186105A1 divulga métodos y equipos de autenticación inalámbrica, en los que un primer dispositivo de procesamiento (por ejemplo, un token (testigo) de autenticación inalámbrica o una etiqueta RFID) transmite información en una red inalámbrica de tal forma que emula las comunicaciones estándar de un punto de acceso de la red inalámbrica, aunque el primer dispositivo de procesamiento no esté configurado para operar como un punto de acceso real de la red inalámbrica. Un segundo dispositivo de procesamiento (por ejemplo, un ordenador u otra estación de la red inalámbrica) recibe la información transmitida y, a partir de la misma, puede determinar que la información tiene su origen en un punto de acceso emulado en lugar de un punto de acceso real.

En el documento US6314521 B1 se divulga otra solución de la técnica anterior.

Resumen de la invención

La presente invención se define por las reivindicaciones adjuntas.

Breve descripción de los dibujos

La FIG. 1 es un diagrama de bloques de un sistema de seguridad que se muestra en líneas generales de acuerdo con el modo de realización que se ilustra; y

la FIG. 2 es una red inalámbrica del sistema de la FIG. 1.

Descripción detallada del modo de realización ilustrado

Aunque los modos de realización pueden adoptar muchas formas diferentes, en los dibujos se ilustran los modos de realización específicos de las mismas y se describirán en la presente solicitud en detalle, en el bien entendido de que la presente divulgación se debe considerar como una ejemplificación de los principios de la misma, así como el mejor modo de llevarla a la práctica. No se pretende limitar el modo de realización específico ilustrado.

La FIG. 1 es un diagrama de bloques de un sistema 10 de seguridad que muestra en líneas generales de acuerdo con el modo de realización que se ilustra. En el sistema 10 de seguridad se incluye un grupo 14 de sensores 16, 18

que se utilizan para proteger un área asegurada 12. Los sensores 16, 18, a su vez, pueden estar conectados a un panel 20 de alarma que monitoriza el estado de cada uno de los sensores 16, 18.

Los sensores 16, 18 se pueden basar en una cualquiera de una serie de tecnologías diferentes. Por ejemplo, los sensores 16, 18 pueden incluir uno o más interruptores de frontera conectados a una puerta o ventana que permita la entrada en o la salida del área asegurada 12.

Alternativamente, los sensores 16, 18 pueden incluir uno o más dispositivos de detección de movimiento mediante técnicas de detección de infrarrojos o procesamiento de imágenes. Por ejemplo, en un modo de realización, el uno o más dispositivos 16, 18 pueden ser dispositivos PIR. Alternativamente, el uno o más dispositivos pueden ser cámaras con un procesador que compara imágenes sucesivas con el fin de detectar el movimiento de personas u objetos a través del campo de visión de cada una de las cámaras.

Como una alternativa adicional, los sensores 16, 18 pueden incluir uno o más dispositivos de detección de fuego o gas. Cuando los sensores detectan fuego, los dispositivos 16, 18 se pueden basar en uno cualquiera de una serie de métodos de detección diferentes (por ejemplo, detección de monóxido de carbono, detección de humo, etc.).

Cada uno de los dispositivos 16, 18 puede estar conectado al panel 20 de alarma de forma inalámbrica. A este respecto, uno o más transceptores inalámbricos 22 en el panel 20 de alarma pueden estar conectados a un transceptor 24 respectivo en cada uno de los sensores 16, 18.

El panel 20 de alarma puede incluir uno o más equipos de procesamiento (procesadores) 26, 28 que monitorizan los sensores 16, 18. Cada uno de los sensores 16, 18 también puede incluir uno o más procesadores 26, 28. Los procesadores 26, 28 pueden actuar bajo el control de uno o más programas 30, 32 para ordenador cargados desde un medio no transitorio legible por ordenador (memoria) 34. Tal como se aplica en la presente solicitud, la referencia a un paso ejecutado por uno de los programas 30, 32 es también una referencia al procesador 26, 28 que ejecuta dicho paso.

En general, el panel 20 de alarma se puede controlar a través de una interfaz 36 de usuario. Un usuario puede armar o desarmar el sistema 10 y el panel 20 a través de un teclado 40 de la interfaz de usuario. El estado del panel 20 de alarma se puede mostrar en una pantalla 38.

Una vez armado, un procesador 26, 28 de sensores puede monitorizar el estado de cada uno de los sensores 16, 18. Al detectarse la activación de uno de los sensores 16, 18, el procesador de sensores puede transferir una notificación de la activación a un procesador 26, 28 de alarmas. El procesador de alarmas, en respuesta, puede enviarle un mensaje de alarma a una estación central 42 de monitorización. La estación central de monitorización puede responder llamando al departamento de bomberos o policía, en función del tipo de alarma.

La FIG. 2 representa una red 128 de comunicación inalámbrica que incluye un grupo 14 de sensores 16, 18 (etiquetados como 100-126 en la FIG. 2) y un transceptor 22. Por conveniencia, los sensores 100-126 de la FIG. 2 se utilizarán para explicar el sistema de comunicación que interconecta los sensores 100-126 entre sí y con el panel 20 de alarma a través del transceptor 22.

En general, los sensores 100-126 intercambian paquetes entre sí y con el transceptor 22 mediante la versión 6 del Protocolo de Internet (IPv6). Con ciertas excepciones, la red de comunicación de la FIG. 2 se organiza a sí misma en una jerarquía de comunicación mediante el protocolo de Redes Inalámbricas de Área Personal de Baja potencia basadas en IPv6 (6LoWPAN). Una excepción es el uso de una clave secreta o un conjunto de claves secretas que se describirá con más detalle más adelante.

La red inalámbrica de la FIG. 2 incluye una serie de sensores que gestionan la coordinación de la comunicación entre los otros sensores (sensores coordinadores 100, 102, 118, 120) y una serie de sensores al final de las respectivas cadenas de comunicación (sensores finales 104, 106, 108, 110, 116, 122, 124, 126). El sistema de la FIG. 2 también incluye un sensor que enruta la comunicación entre los sensores (sensor enrutador 112).

Los transceptores 22, 24 de los sensores 100-126 y el panel 20 de alarma pueden operar en el rango de frecuencias desde 2405 a 2480 MHz. Los transceptores pueden operar en 16 canales diferentes dentro de este rango de frecuencias.

Cada uno de los sensores 100-126 se puede suministrar con una clave secreta 128 o un conjunto 130 de claves secretas 128 y una dirección de sistema del panel 20 de alarma. Cada uno de los sensores 100-126 también puede disponer de su propia y única dirección IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) o una dirección MAC (Control de Acceso al Medio). Las claves secretas 128, la dirección de sistema del panel 20 y la dirección IEEE o MAC se pueden suministrar mediante una conexión física directa con un dispositivo de programación durante el proceso de fabricación con el fin de garantizar la seguridad de los sensores 100-126.

Para componer una red inalámbrica, a cada uno de los sensores coordinadores se les pueden proporcionar los detalles de los sensores que se unirán potencialmente a la red. Un sensor válido se puede identificar mediante la dirección IEEE o MAC y una clave única de puesta en servicio. A este respecto, la clave de puesta en servicio se

compone de forma independiente en cada uno de los sensores 100-126 mediante un procesador 24, 26 de cifrado de los sensores 100-126. A este respecto, la clave de puesta en servicio se compone cifrando la dirección IEEE o MAC con la clave secreta.

Para componer una red, como parte del proceso que permite que un sensor final se una a un sensor coordinador, cada uno de los sensores finales puede enviarle a un sensor coordinador respectivo un mensaje de registro. El mensaje de registro incluye la dirección IEEE o MAC del sensor final y la clave de puesta en servicio del sensor final. El sensor coordinador recibe el mensaje de registro y autentica al sensor final haciendo uso de su propia copia independiente de la clave secreta para descifrar la clave de puesta en servicio en un procesador de descifrado, recuperando de ese modo la dirección IEEE o MAC del sensor final. Sin embargo, como la dirección IEEE o MAC que incluía el mensaje de solicitud de registro recibido originalmente estaba en un formato no cifrado, se puede utilizar un procesador de comparación del sensor coordinador para comparar simplemente la dirección IEEE o MAC recuperada con la dirección IEEE o MAC no cifrada recibida originalmente como parte del mensaje de registro. Cuando la dirección IEEE o MAC recuperada y la recibida originalmente coinciden, el sensor final se ha autenticado. De forma análoga, cada sensor 100-126 puede autenticar cualquier transmisión desde cualquier otro sensor 100-126. Se puede utilizar un proceso similar por parte del panel de alarma para autenticar las transmisiones desde los sensores 100-126 y por parte de los sensores para autenticar las transmisiones desde el panel de alarma.

Volviendo ahora a la red inalámbrica, en general, se proporcionará una explicación de cómo los sensores 100-126 se organizan a sí mismos en la red inalámbrica. Para simplificar la explicación, ésta se basará fundamentalmente en un solo sensor coordinador y unos solos sensores finales. Se puede utilizar un proceso similar por parte de los sensores coordinadores para unirse a otros sensores coordinadores y al panel 20 de alarma.

Por ejemplo, tras el inicio, los sensores coordinadores comienzan inmediatamente a buscar un canal de radio apropiado. A este respecto, el sensor coordinador buscará, identificará y adoptará para su uso el canal de radiofrecuencia en el que se detecte la menor actividad.

El sensor coordinador puede asignarle a la red un identificador (id) único de Red de Área Personal (PAN). El identificador de la PAN se puede almacenar en una memoria del sensor durante el proceso de fabricación o se puede basar en la clave secreta 128. El sensor coordinador puede escuchar los id de PAN de otras redes vecinas con el fin de verificar que el identificador de la PAN es único. Si no lo es, el sensor coordinador puede incrementar el identificador hasta que encuentre un valor único.

El sensor coordinador puede pasar a continuación al "modo puesta en servicio", en el que el sensor coordinador puede unirse a otros sensores. A continuación, el sensor coordinador escucha el canal adoptado a la espera de solicitudes de registro de otros sensores (sensores enrutadores y sensores finales) para unirse a la red.

Tras el inicio, los sensores finales (y los sensores enrutadores) exploran en modo de puesta en servicio los canales disponibles para identificar canales con sensores coordinadores. El sensor final (y los sensores enrutadores) transmiten solicitudes de señales de baliza a través de los canales identificados y esperan señales de baliza de los sensores coordinadores a los que el sensor se puede unir. A este respecto, los sensores finales (y los sensores enrutadores) pueden detectar uno o más sensores coordinadores a los que los sensores finales (y los sensores enrutadores) se pueden unir en una relación padre-hijo.

Los sensores finales se pueden unir al sensor coordinador en una red en estrella o en árbol. En una red en estrella, un sensor enrutador asumirá simplemente el papel de cualquier otro sensor final.

Inicialmente, el sensor coordinador puede ser el único padre potencial de un nuevo sensor final. Sin embargo, una vez que la red se ha formado parcialmente, el sensor extremo de unión puede detectar los sensores coordinadores y uno o más sensores enrutadores de la misma red. En este caso, el sensor final puede utilizar un conjunto secuencial de reglas para elegir su padre. La primera elección se puede basar en la potencia de la señal, de tal modo que se selecciona en primer lugar el padre con la mayor potencia de señal. A continuación, se considera el número de hijos de cada padre, de tal modo que se da preferencia al padre con el menor número de hijos. Por último, se considera la profundidad del árbol, de tal modo que se da preferencia al padre más alto en el árbol. Estas reglas son utilizadas en orden inverso por parte de cualquier sensor que opere como sensor enrutador.

A continuación, el sensor final le envía al padre seleccionado un mensaje de registro como una petición de unión, solicitando unirse a la red inalámbrica a través de él. El sensor coordinador puede rechazar inicialmente la petición de unión pendiente de verificar (mediante la dirección IEEE o MAC y la clave de puesta en servicio) que el sensor final está autorizado para registrarse en el sistema. Tras el rechazo inicial, el sensor final puede volver a enviarle la solicitud de registro al mismo padre potencial, cifrando esta vez la solicitud con la clave de puesta en servicio del sensor. Si el sensor es validado satisfactoriamente por el padre potencial y se puede descifrar la solicitud de registro con la clave secreta, se acepta la petición.

A continuación, el sensor final le envía un mensaje de establecimiento de ruta al sensor coordinador. El sensor coordinador responde con una confirmación de incorporación del sensor a la red. Este intercambio de mensajes da lugar a que se agregue un conjunto de entradas para el sensor final a las tablas de enrutamiento entre el sensor final y el sensor coordinador.

En general, cualquier paquete enviado por un sensor a través de la red 128 puede contener dos direcciones para fines de enrutamiento, incluyendo una primera dirección del sensor de destino y una segunda dirección del sensor de salto siguiente. La segunda dirección es modificada tras cada salto por el sensor receptor a medida que el paquete se propaga a través de la red, y se convierte en la misma dirección del sensor de destino para el último salto.

En respuesta a la recepción del mensaje de ruta establecida, el sensor coordinador puede reenviarle una clave de seguridad de red (clave en tiempo de ejecución) al sensor final. La clave de seguridad de red puede basarse en la clave secreta o puede ser una clave seleccionada del conjunto de claves secretas.

Una vez que los sensores 100-126 se han organizado entre sí en una red 128 de comunicación inalámbrica, un procesador 26, 28 de monitorización respectivo en cada uno de los sensores 100-126 puede monitorizar los cambios en un elemento de detección. Cuando se detecta un cambio por encima de un valor umbral, el procesador 100, 126 puede componer y enviarle un paquete a un procesador 26, 28 correspondiente en el panel de alarma notificándole al panel de alarma el cambio. En ciertos casos el paquete puede ser transmitido directamente al panel 20 (por ejemplo, el sensor coordinador 100) o puede ser recibido y retransmitido por otros sensores (por ejemplo, el sensor 106 le transmite el paquete al sensor 100 y el sensor 100 le retransmite el paquete al panel 20 de alarma.

El sistema 10 y, en particular, la red inalámbrica del sistema 10 ofrece una serie de ventajas sobre los sistemas convencionales. Por ejemplo, el ahorro de la clave secreta en los sensores 100-126 permite que el sistema se pueda configurar sin necesidad de que un técnico experimentado introduzca las contraseñas u otros datos de cifrado. Como cada uno de los sensores 100-126 tiene la clave secreta almacenada en su memoria, cada sistema 10 puede identificar de forma inequívoca a cualquier otro miembro de su red de sensores 100-126.

Además, la presencia de la clave secreta almacenada en la memoria de cada uno de los dispositivos 100-126 permite cambiar periódicamente (o inmediatamente tras la instalación) la clave secreta sin comprometer la seguridad. En este caso, cualquier nueva clave secreta simplemente puede ser cifrada mediante la clave secreta almacenada originalmente y transferida a través de la interfaz aérea sin pérdida de seguridad.

Alternativamente, cuando se ha almacenado en la memoria un conjunto de claves secretas, la clave secreta se puede seleccionar de dicho conjunto de claves secretas de forma secuencial o aleatoria para un período predeterminado de tiempo.

Una vez transcurrido el período de tiempo predeterminado, se puede utilizar la siguiente clave secreta del conjunto durante otro período de tiempo.

A partir de lo anterior, se observará que se pueden efectuar numerosas variaciones y modificaciones. Se debe entender que no se pretende ni debe deducirse ninguna limitación en relación con el equipo específico que se ilustra en la presente solicitud. Sí se pretende, desde luego, amparar mediante las reivindicaciones adjuntas todas aquellas modificaciones como incluidas en el alcance de las reivindicaciones.

REIVINDICACIONES

1. Un método para configurar un sistema (10) de seguridad que tiene una pluralidad de sensores (16, 18; 100-126) utilizado para proteger un área asegurada (12), comprendiendo dicho método:

un sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro de la pluralidad de sensores (16, 18; 100-126) que tiene una clave secreta (128) y una dirección IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) o una dirección MAC (Control de Acceso al Medio);

el sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro compone automáticamente una clave de puesta en servicio cifrando la dirección IEEE o la dirección MAC con la clave secreta, en donde el sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro opera bajo el protocolo de operación de Red de Área Personal Inalámbrica de Baja potencia sobre la versión 6 del Protocolo de Internet, 6LoWPAN, en una red inalámbrica (128);

el sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro compone una solicitud de registro que incluye un formato no cifrado de la dirección IEEE o la dirección MAC y la clave de puesta en servicio;

un sensor coordinador (100, 102, 118, 120) de la pluralidad de sensores (16, 18; 100-126) que opera bajo el protocolo de operación 6LoWPAN en la red inalámbrica recibe la solicitud de registro del sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro, en donde el sensor coordinador (100, 102, 118, 120) dispone de una copia independiente de la clave secreta;

el sensor coordinador (100, 102, 118, 120) descifra la clave de puesta en servicio mediante la copia independiente de la clave secreta con el fin de obtener en formato descifrado la dirección IEEE o la dirección MAC para el sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro;

el sensor coordinador (100, 102, 118, 120) compara el formato descifrado de la dirección IEEE o la dirección MAC con el formato no cifrado de la dirección IEEE o la dirección MAC con el fin de determinar si el formato descifrado de la dirección IEEE o la dirección MAC descifrada coincide con el formato no cifrado de la dirección IEEE o la dirección MAC;

el sensor coordinador (100, 102, 118, 120) autentica automáticamente el sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro mediante la solicitud de registro y la copia independiente de la clave secreta cuando el formato descifrado de la dirección IEEE o la dirección MAC descifrada coincide con el formato no cifrado de la dirección IEEE o la dirección MAC;

el sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro se une al sensor coordinador de la red inalámbrica (128) bajo el protocolo de operación 6LoWPAN, en donde la dirección IEEE o la dirección MAC y la clave secreta se proporcionan a través de una conexión física directa con un dispositivo de programación durante el proceso de fabricación con el fin de garantizar la seguridad de la pluralidad de sensores (16, 18; 100-126);

el sensor coordinador (100, 102, 118, 120) crea una nueva clave secreta después de autenticar el sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro;

el sensor coordinador (100, 102, 118, 120) cifra la nueva clave secreta mediante la clave secreta; y

el sensor coordinador (100, 102, 118, 120) le transmite la nueva clave secreta cifrada al sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro, en donde:

la clave secreta se selecciona de forma secuencial o aleatoria a partir de un conjunto de claves secretas para un período de tiempo predeterminado.

2. El método como el de la reivindicación 1, que comprende además almacenar la clave de puesta en servicio y la dirección IEEE o la dirección MAC en una lista de la pluralidad de sensores (16, 18; 100-126) registrados en el sensor coordinador (100, 102, 118, 120).

3. El método como el de la reivindicación 1, que comprende además almacenar el conjunto (130) de claves secretas en una memoria del sensor coordinador durante el proceso de fabricación del sensor coordinador (100, 102, 118, 120).

4. Un sistema (10) de seguridad, que comprende:

una pluralidad de sensores (16, 18; 100-126) utilizados para proteger un área asegurada (12);

un sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro de la pluralidad de sensores (16, 18; 100-126) que opera bajo un protocolo de operación de Red de Área Personal Inalámbrica de Baja potencia sobre la versión 6 del Protocolo de Internet, 6LoWPAN, en una red inalámbrica (128), en donde el sensor (104, 106, 108, 110, 116, 122,

124, 126) de registro tiene una clave secreta y una dirección IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) o una dirección MAC (Control de Acceso al Medio), en donde el sensor de registro compone automáticamente una clave de puesta en servicio cifrando la dirección IEEE o la dirección MAC con la clave secreta, y en donde el sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro compone y transmite de forma inalámbrica una solicitud de registro que incluye un formato no cifrado de la dirección IEEE o la dirección MAC y la clave de puesta en servicio;

un sensor de siguiente salto de la pluralidad de sensores que operan bajo el protocolo de operación 6LoWPAN en la red inalámbrica (128); y

un sensor coordinador (100, 102, 118, 120) de la pluralidad de sensores (16, 18; 100-126) que operan bajo el protocolo de operación 6LoWPAN en la red inalámbrica (128),

en donde el sensor coordinador (16, 18; 100-126) recibe la solicitud de registro del sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro,

en donde el sensor coordinador (100, 102, 118, 120) dispone de una copia independiente de la clave secreta,

en donde el sensor coordinador descifra la clave de puesta en servicio mediante la copia independiente de la clave secreta con el fin de obtener en formato descifrado la dirección IEEE o la dirección MAC para el sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro, compara el formato descifrado de la dirección IEEE o la dirección MAC con el formato no cifrado de la dirección IEEE o la dirección MAC con el fin de determinar si el formato descifrado de la dirección IEEE o la dirección MAC coincide con el formato no cifrado de la dirección IEEE o la dirección MAC, autentica automáticamente el sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro mediante la solicitud de registro y la copia independiente de la clave secreta cuando el formato descifrado de la dirección IEEE o la dirección MAC coincide con el formato no cifrado de la dirección IEEE o la dirección MAC, crea una nueva clave secreta después de autenticar el sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro, cifra la nueva clave secreta utilizando la clave secreta, y le transmite la nueva clave secreta cifrada al sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro,

en donde el sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro se une al sensor coordinador (100, 102, 118, 120) de la red inalámbrica bajo el protocolo de operación 6LoWPAN, y

en donde la dirección IEEE o la dirección MAC y la clave secreta se proporcionan mediante una conexión física directa con un dispositivo de programación durante el proceso de fabricación con el fin de garantizar la seguridad de la pluralidad de sensores (16, 18; 100-126),

en donde la clave secreta se selecciona secuencial o aleatoriamente a partir de un conjunto de claves secretas para un período de tiempo predeterminado.

5. Un sistema de seguridad como el de la reivindicación 4, que comprende además un procesador de claves que selecciona la clave secreta a partir del conjunto de claves secretas para la creación de la clave de puesta en servicio.

6. Un sistema de seguridad como el de la reivindicación 4, que comprende además un procesador de claves de red que selecciona una clave secreta a partir del conjunto de claves secretas y cifra una nueva clave secreta con la clave secreta.

7. Un sistema de seguridad como el de la reivindicación 4, en donde el sensor (104, 106, 108, 110, 116, 122, 124, 126) de registro comprende además una pluralidad de sensores hijo, y en donde cada uno de la pluralidad de sensores hijo se registra en el sensor coordinador (100, 102, 118, 120).

8. Un sistema de seguridad como el de la reivindicación 4, que comprende además un sensor enrutador (112) que se registra en el sensor coordinador (100, 102, 118, 120).

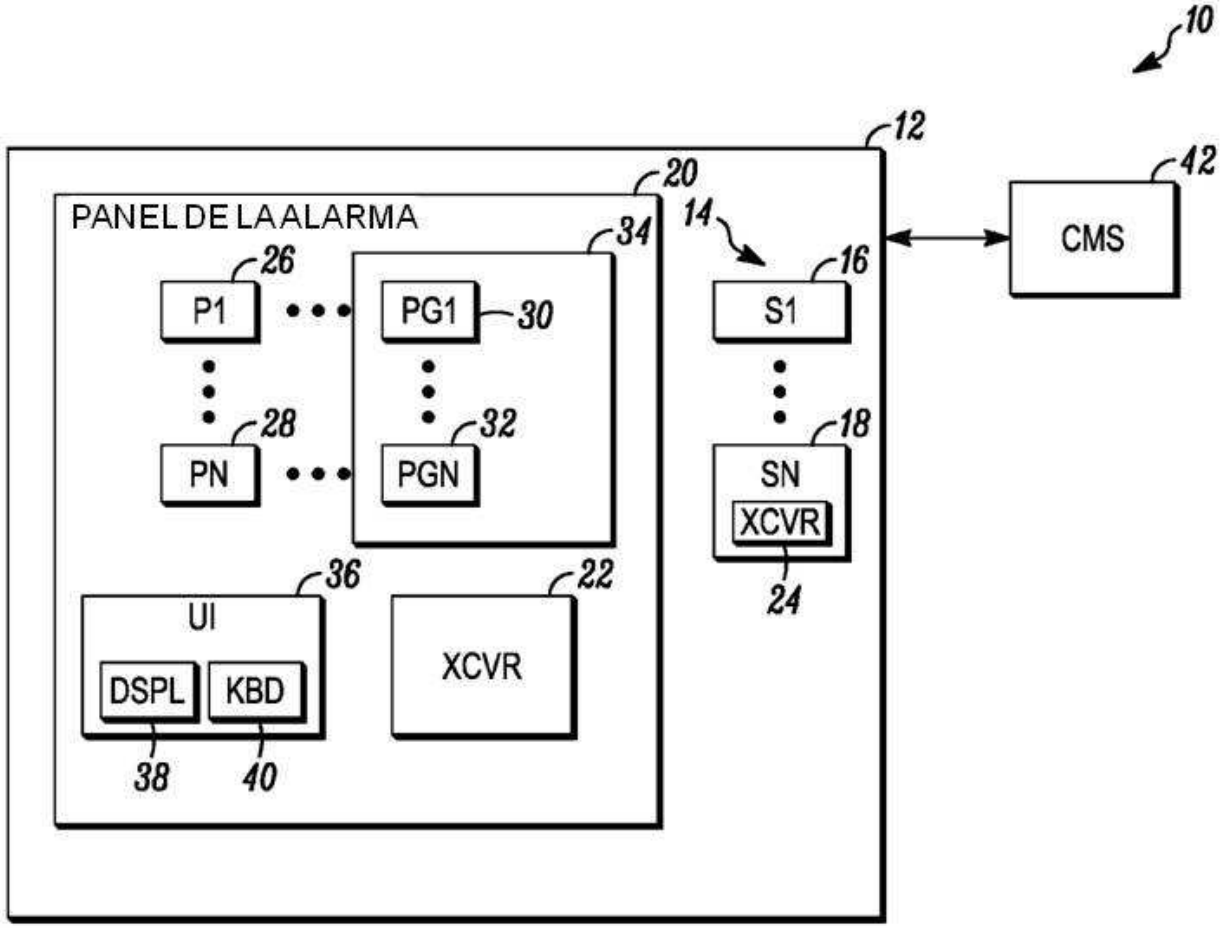
10
12
20
PANEL DE LA ALARMA
34
14
42
CMS
26
P1
PG1
30
16
S1
28
PN
32
PGN
18
SN
XCVR
24
36
UI
DSPL
KBD
38
40
22
XCVR

FIG. 1

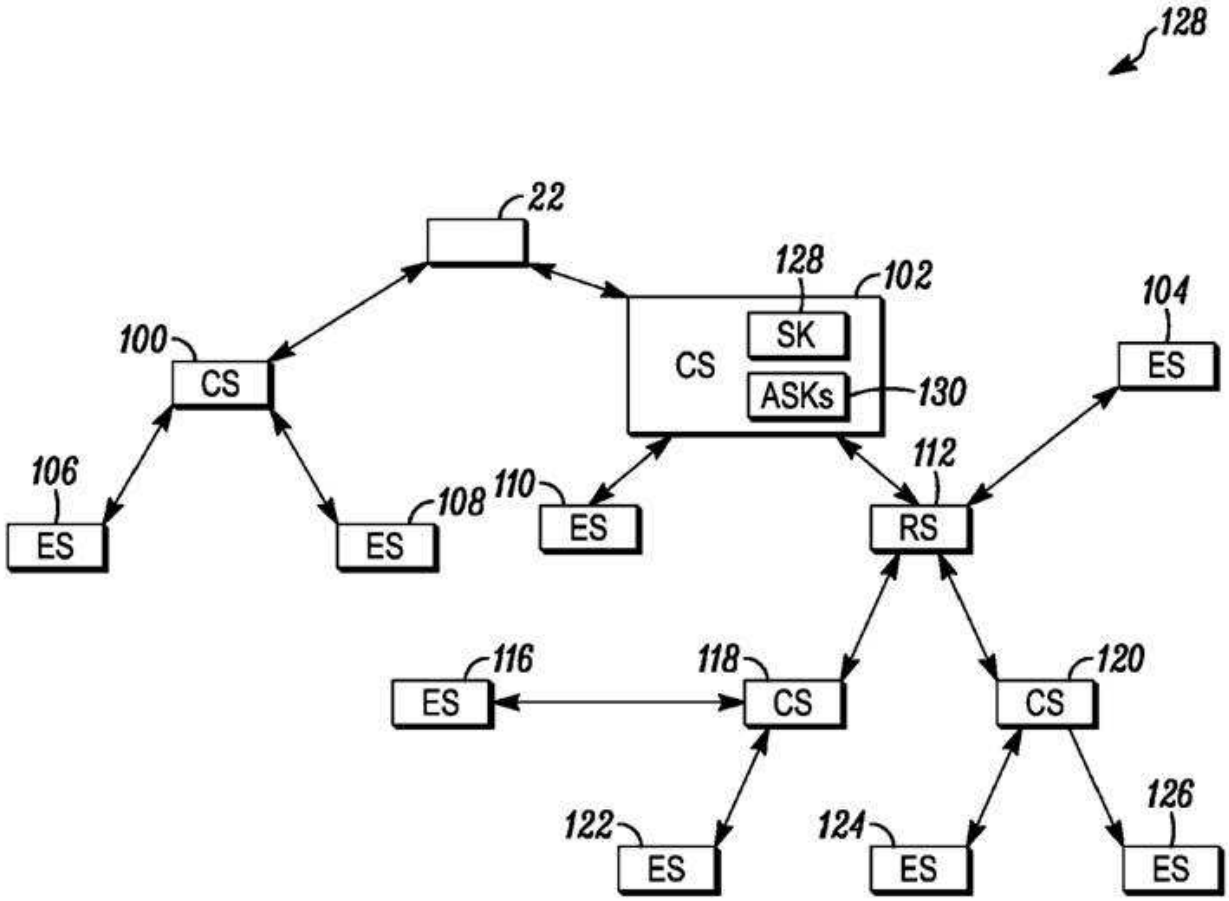
128
22
128
102
104
100
CS
SK
CS
ES
ASKs
130
106
112
110
108
ES
ES
ES
RS
116
118
120
ES
CS
CS
122
124
126
ES
ES
ES

FIG. 2