(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 511 017**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.03.2003 E 12156949 (5)**

(97) Fecha y número de publicación de la concesión europea: **10.09.2014 EP 2475147**

(54) Título: **Red de área local**

(30) Prioridad:

**08.03.2002 US 362865 P**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**22.10.2014**

(73) Titular/es:

**CERTICOM CORP. (100.0%)**
**4701 Tahoe Boulevard, Tahoe A, 6th Floor**
**Mississauga, Ontario L4W 0B5, CA**

(72) Inventor/es:

**STRUIK, MARINUS y**
**VANSTONE, SCOTT A**

(74) Agente/Representante:

**DE ELZABURU MÁRQUEZ, Alberto**

## DESCRIPCIÓN

Red de área local

CAMPO DE LA INVENCIÓN

Esta invención se refiere a redes de comunicaciones, más en particular se refiere a seguridad dentro de esas redes.

DESCRIPCIÓN DE LA TÉCNICA ANTERIOR

Uno de los desarrollos recientes más significativo en tecnologías inalámbricas es la aparición de las redes de área personal inalámbricas. Las redes de área personal inalámbricas, WPANs® usan frecuencias de radio para transmitir tanto voz como datos, y están especificadas mediante estándares tales como el estándar IEEE 802.15 o 802.3 del Instituto de la Asociación de Estándares de Ingenieros Eléctricos y Electrónicos (IEEE-SA), entre otras especificaciones. La especificación 802.15 es ideal para enlazar ordenadores portátiles, teléfonos móviles, asistentes digitales personales (PDAs), cámaras digitales, y otros dispositivos portátiles para realizar negocios en el domicilio, en la carretera o en la oficina.

Estas redes inalámbricas están formadas por un número de dispositivos que se incorporan y salen de la red de una manera ad hoc, con lo que tales redes se conocen como redes ad hoc o picorredes. Así, el conjunto de dispositivos conectados a la red ad hoc en cualquier momento dado puede fluctuar, y por tanto la topología de la red es dinámica. Resulta deseable controlar el acceso a la red y proporcionar un mecanismo para establecer y mantener la seguridad. Tradicionalmente, la seguridad se establece usando un dispositivo central o un controlador de picorred (PNC) que controla el acceso y distribuye claves dentro de la red. Un inconveniente de este esquema es que se necesita que cada miembro de la red confíe en el PNC.

La admisión en la picorred se basa en el resultado de los protocolos siguientes entre el dispositivo potencial que se incorpora y el PNC de la picorred. El dispositivo que se incorpora y el PNC participan en un protocolo de autenticación mutua de entidad en base a técnicas de clave pública o de clave simétrica. La verdadera identidad de dispositivo tanto del dispositivo que se incorpora como del PNC se determina usando este protocolo. También se puede deducir una clave de enlace en base a claves auténticas de ambas partes. Otro protocolo incluye el uso de técnicas de autorización entre ambos dispositivos, en base a listas de control de acceso (ACLs). Las Listas de Control de Acceso pueden ser actualizadas dinámicamente, de forma similar a la funcionalidad de PDA, donde se adopta una determinación de si una entidad se añade o se retira de la ACL a la entrada. Esta determinación puede ser usada por un operador, tal como un operador humano. Para dispositivos que carecen de interfaz de usuario, este mecanismo de actualización puede ser invocado mediante un período de inscripción abierta seguido de una etapa de bloqueo, por ejemplo, que puede ser confirmada por medio de un pulsador o mediante un simple reseteo de la lista completa. Esto puede hacerse accionando un botón de reseteo o de reinicialización del dispositivo.

Por tanto, los dispositivos de la picorred dependen por completo de información proporcionada por el PNC con respecto a cuáles de los dispositivos han sido admitidos en la picorred, puesto que la admisión se basa en la comunicación entre el PNC y un dispositivo de incorporación solamente. Si, no obstante, una lista inapropiada de dispositivos, DeviceList, de la picorred ha sido distribuida por el PNC, ya sea por error o de forma malintencionada, la seguridad de la red se pone en peligro. Cada dispositivo tiene una dirección de lado corto, tal como un ID local de 8 bits, y una dirección de lado largo, tal como un ID de dispositivo global de 48 bits. Por ejemplo, en una picorred en la que todos los dispositivos comparten una clave de difusión común, la lista de dispositivos admitidos en la picorred es L: = ID de dispositivo local de 8 bits, ID de dispositivo global de 48 bits), entonces el fallo en la obtención de la lista completa y auténtica de dispositivos admitidos tiene las siguientes consecuencias:

Escenario de “*Mosca en la pared*”:

Si un dispositivo obtiene una lista incompleta L’c (L’ ≠ L) de dispositivos admitidos, todos los dispositivos del conjunto complementario L/L’ “son invisibles” para el dispositivo. Por ello, el dispositivo podría pensar erróneamente que está compartiendo información segura solamente con dispositivos de la lista L’, mientras que realmente está compartiendo sin saberlo con otros dispositivos del conjunto L también. Esto viola, obviamente, la práctica de seguridad de sonido.

Escenario “*Cuadro de conmutación”*

Si el enlace entre el ID de dispositivo local y el ID de dispositivo global se recibe incorrectamente, por ejemplo si se intercambian 2 entradas, un dispositivo podría dirigir información al dispositivo inapropiado y comprometer así la pretendida seguridad. Esta propiedad también se mantiene en otros entornos en los que una parte generadora de clave no comparte información completa y auténtica sobre la composición del propio grupo de compartición de clave con los otros miembros de ese grupo. Por lo tanto, estos escenarios presentan un modelo de seguridad en el que existe una confianza total o un modelo de seguridad en el que un dispositivo no confía en ningún otro dispositivo, aunque no obstante es posible un modelo hibrido de esos dos modelos.

El documento de Venkatraman L. et al., “Un nuevo esquema de autenticación para redes ad hoc”, Departamento de Ingeniería Eléctrica y de Computación y Ciencia de Computación, vol. 3, del 23 de septiembre de 2000, páginas 1268-1273, describe un método para establecer y mantener seguridad distribuida entre una pluralidad de dispositivos en una red ad hoc, donde a uno de dichos dispositivos se ha asignado una función de control para controlar el acceso mediante otros dispositivos a dicha red, los dispositivos se autentican por sí mismos periódicamente con dichos otros dispositivos con el fin de determinar el estado de dichos otros dispositivos, y se organizan por sí mismos según una pluralidad de grupos de confianza, teniendo cada grupo una clave de grupo para su distribución dentro de dicho grupo de confianza; no obstante, los dispositivos no generan las propias claves, y no se realiza ningún acuerdo de clave para establecer un canal de comunicación seguro.

El documento de S. Jacobs y M.S. Corson, “Arquitectura de Autenticación de Manet”, proyecto de Internet, publicado en Marzo de 1999, describe un sistema de seguridad distribuida para una pluralidad de dispositivos en una red de comunicación, siendo cada uno de dichos dispositivos responsable de generar, distribuir y controlar su propia clave para el acceso a dicha red de comunicación, y usar dichas claves para establecer una red segura, siendo cada miembro del dispositivo en dicha red de comunicación comprobado periódicamente por otros dispositivos, con el fin de establecer a cuales de los dispositivos se les permite el acceso a dicha red de comunicación y a dicha red segura. No describe ningún protocolo de desafío y respuesta para realizar autenticación entre los diferentes dispositivos.

La solicitud de patente internacional WO 01/31836 A2 describe un sistema para gestionar un grupo de dispositivos de confianza en una red ad hoc.

Por lo tanto, un objeto de la presente invención consiste en mitigar u obviar al menos una de las desventajas mencionadas anteriormente.

SUMARIO DE LA INVENCIÓN

Según un aspecto, la invención proporciona un método según la reivindicación 1, y un gestor de seguridad según la reivindicación 10.

Según otro aspecto, se describe un método de establecimiento y mantenimiento de seguridad distribuida entre un primer interlocutor y otro interlocutor, siendo los interlocutores miembros de diferentes redes ad hoc y formando un grupo de interlocutores de comunicación, teniendo el método las etapas de:
asociar un primer interlocutor y el otro interlocutor con direcciones de dispositivo únicas;
controlar el acceso a las diferentes redes ad hoc;
disponer en cada una de las redes ad hoc una puerta de enlace y transferir tráfico entre los interlocutores a través de las puertas de enlace;
generar en el primer interlocutor una clave pública para su distribución al otro interlocutor;
autenticarse por sí mismo el primer interlocutor periódicamente con el otro interlocutor, con el fin de determinar el estado del otro interlocutor;
determinar una clave de grupo para su distribución a los interlocutores conforme a la etapa de control de acceso;
asociar un nivel de confianza a cada interlocutor; usando cada uno de los interlocutores la clave pública y la clave de grupo para realizar un acuerdo de clave con el fin de establecer comunicación segura dentro del grupo;
con lo que el primer interlocutor es responsable de su propia seguridad mediante generación y distribución de sus propias claves al otro interlocutor.

Según otro aspecto, se describe un método de establecimiento y mantenimiento de seguridad distribuida entre un primer interlocutor y otro interlocutor, siendo dichos interlocutores miembros de diferentes redes ad hoc, y formando un grupo de interlocutores comunicantes, teniendo el método las etapas de:
asociar dicho primer interlocutor y dicho segundo interlocutor con una dirección de dispositivo única;
controlar el acceso a dichas diferentes redes ad hoc;
teniendo cada red ad hoc una puerta de enlace y transfiriendo tráfico entre dichos interlocutores a través de las citadas puertas de enlace;
generando dicho primer interlocutor una clave pública para su distribución a dicho otro interlocutor;
autenticándose dicho primer interlocutor a sí mismo periódicamente con dicho otro interlocutor con el fin de determinar el estado de dicho otro interlocutor;
determinar una clave de grupo para su distribución a dichos interlocutores conforme a dicha etapa de control de acceso;
asociar un nivel de confianza a cada uno de dichos interlocutores;
utilizando cada uno de dichos interlocutores la citada clave pública y dicha clave de grupo para realizar un acuerdo clave a efectos de establecer comunicación segura con dicho grupo;
en donde cada uno de dichos interlocutores es responsable de su propia seguridad con la generación y distribución de sus propias claves a dichos otros dispositivos.

Con preferencia, dicha etapa de transferir tráfico incluye una etapa adicional de asociar cada uno de dichos interlocutores con un enrutador para almacenar información de enrutamiento que tiene instrucciones para enrutar tráfico desde dicho primer interlocutor hasta dicho otro interlocutor.

Con preferencia, dichos enrutadores preguntan unos a otros periódicamente con el fin de actualizar y mantener dicha información de enrutamiento.

Con preferencia, dicha etapa de determinar dicho estado de dicho otro interlocutor incluye una etapa adicional de usar un protocolo de desafío y respuesta para establecer si dicho otro interlocutor está autorizado para acceder a dicha red ad hoc diferente que tiene dicho primer interlocutor, conforme a dicha función de control.

Según otro aspecto más, se describe un sistema de seguridad distribuida para una pluralidad de dispositivos de una red, siendo cada uno de los dispositivos responsable de generar, distribuir y controlar sus propias claves para el acceso a la red, y usar las claves para establecer una red de confianza, siendo cada miembro del dispositivo en la red comprobado periódicamente mediante otros dispositivos usando un protocolo de desafío y respuesta para establecer los dispositivos a los que se les permite el acceso a la red y a la red de confianza.

Según otro aspecto más, se describe un sistema de seguridad distribuida para una pluralidad de dispositivos en una red de comunicación, siendo cada uno de dichos dispositivos responsable de generar, distribuir y controlar sus propias claves para el acceso a dicha red de comunicación, y usar dichas claves para establecer una red de confianza, siendo cada miembro del dispositivo en dicha red de comunicación comprobado periódicamente por medio de otros dispositivos usando un protocolo de desafío y respuesta para establecer los dispositivos a los que se les permite el acceso a dicha red de comunicación y a dicha red de confianza.

Con preferencia, cada dispositivo incluye un gestor de seguridad que tiene las funciones de generar dichas claves y distribuir dichas claves a dispositivos seleccionados en la citada red de confianza.

Con preferencia, dicha red de confianza está asociada a un nivel de confianza.

Con preferencia, dicho gestor de seguridad determina una fuente de dichas claves de tal modo que dichas claves provenientes de un dispositivo dentro de la citada red de confianza pueden ser usadas para encriptación y desencriptación de datos, y dichas claves provenientes de un dispositivo excluido de la citada red de confianza pueden ser usadas para la desencriptación de dichos datos.

Con preferencia, dicho gestor de seguridad renuncia a desencriptar dichos datos cuando las citadas claves provienen de un dispositivo excluido de la citada red de confianza.

Con preferencia, el resultado de dicha comprobación periódica se registra por medio de dicho gestor de seguridad con el fin de mantener y actualizar una lista de miembros, y ajustar dicho nivel de confianza apropiadamente.

Con preferencia, se pueden establecer diferentes redes de confianza dentro de la citada red en base a diferentes niveles de confianza.

Con preferencia, dicha red de comunicación incluye una pluralidad de redes ad hoc, y dicho sistema de seguridad distribuida se establece entre dispositivos en diferentes redes ad hoc.

Con preferencia, cada una de las redes ad hoc incluye un controlador para controlar el acceso a cada una de dichas redes ad hoc, teniendo cada red ad hoc una puerta de enlace para transferir tráfico entre ellas, y un dispositivo que tiene un enrutador para almacenar información de enrutamiento que tiene instrucciones para enrutar tráfico desde dicho dispositivo hasta otro dispositivo a través de las citadas puertas de enlace y de otros enrutadores.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Estas y otras características de las realizaciones preferidas de la invención resultarán más evidentes en la descripción detallada que sigue en la que se hace referencia a los dibujos anexos, en los que:

La Figura 1 es una red de comunicación;
La Figura 2 es una estructura de grupo para un modelo de seguridad que tiene diferentes niveles de confianza;
La Figura 3 es una estructura de grupo para un modelo de seguridad que tiene diferentes niveles de confianza;
La Figura 4 es una estructura de grupo para un modelo de seguridad que tiene diferentes niveles de confianza;
La Figura 5 es una estructura de grupo para un modelo de seguridad que tiene diferentes niveles de confianza;
La Figura 6 muestra la comunicación entre picorredes;
La Figura 7 muestra un diagrama de flujo que delimita etapas para establecer comunicación segura entre dispositivos de diferentes picorredes, y
La Figura 8 muestra comunicación segura entre picorredes.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES PREFERIDAS

En primer lugar se hace referencia a la Figura 1, la cual muestra una visión general de un sistema 10 de seguridad distribuida que tiene una pluralidad de dispositivos de comunicación 11, 12, 14, 16 en una red de comunicación 18, según una realización preferida. La red de comunicación 18 puede ser una red de área personal inalámbrica (WPAN™) tal como una picorred, en la que los dispositivos 11, 12, 14, 16 se conectan entre sí de una manera ad hoc. Los dispositivos 11, 12, 14, 16 pueden ser dispositivos de computación portátiles y móviles tal como PCs, Asistentes Digitales Personales (PDAs), periféricos, teléfonos celulares, radiobuscadores, electrónica de consumo, y otros dispositivos portátiles. Se comprenderá que tales dispositivos 11, 12, 14, 16 incluyen información de direccionamiento para facilitar la comunicación dentro de la red 18. La información de direccionamiento incluye un ID de dispositivo local, que tiene 8 bits por ejemplo, y un ID de dispositivo, tal como una Dirección IEEE MAC que incluye 48 bits. Por lo tanto, con la incorporación de un dispositivo 11, 12, 14, 16 a la red, se le asigna un ID local no utilizado. En general, un dispositivo 11 actuará como maestro o controlador de red picorred (PNC), y los otros dispositivos 12, 14, 16 actúan como esclavos durante el intervalo de conexión de la picorred 18. El PNC 11 establece una señal de reloj, un patrón de salto determinado por el ID del dispositivo, y asigna tiempo para las conexiones entre todos los dispositivos 11, 12, 14, 16. Así, cada picorred 18 incluye un único patrón de salto/ID, y el PNC 11 proporciona a los esclavos 12, 14, 16 la señal de reloj y un ID de dispositivo local, el cual se utiliza opcionalmente junto con la Dirección IEEE MAC, para formar la picorred 18.

El PNC 11 activa un controlador de acceso 20 usando los IDs de los dispositivos y opcionalmente una lista de control de acceso de tal modo que los dispositivos 12, 14, 16 que hayan sido autenticados positivamente y hayan sido autorizados, sean admitidos en la picorred 18. El PNC 11 incluye también un controlador 22 de tráfico para regular flujos de datos dentro de la red 18. Esto puede hacerse asignando ranuras de tiempo a cada dispositivo 11, 12, 14, 16 para distribución de mensajes. Cada uno de los dispositivos 11, 12, 14, 16 incluye una función 24 de gestor de seguridad. La función 24 de gestor de seguridad genera claves para comunicar con otros dispositivos 11, 12, 14, 16 dentro de la red 18, y distribuye esas claves hasta miembros 11, 12, 14, 16 de dispositivo seleccionados de la red 18. Cada dispositivo 11, 12, 14 ó 16 incluye un transceptor 25 para establecer un canal de comunicación con otros dispositivos 11, 12, 14, 16. Cuando se distribuye una clave, la función 24 de gestor de seguridad indica también a los otros dispositivos 11, 12, 14, 16 de la red 18 los otros dispositivos 11, 12, 14, 16 a los que se está distribuyendo la clave. De ese modo, no hay dependencia alguna sobre los otros dispositivos 11, 12, 14, 16 en cuanto a funcionalidad de confianza, puesto que cada dispositivo 11, 12, 14 ó 16 necesita solamente confiar en sí mismo, para formar un régimen de seguridad distribuido.

De ese modo, la función 24 de gestor de seguridad puede establecer un conjunto de confianza, o TrustList, que indique en cuál de los dispositivos 11, 12, 14, 16 de la red está dispuesto a confiar el gestor 24 de seguridad de ese dispositivo 11, 12, 14 ó 16 particular. La función 24 de gestor de seguridad puede atribuir también niveles diferentes de confianza a cada uno de los conjuntos de confianza establecidos. De esa forma, se puede establecer el equivalente de una red 18 centralizada donde un dispositivo 11, 12, 14 ó 16 confía en cualquier otro dispositivo 11, 12, 14 ó 16; o se proporciona una red 18 completamente descentralizada donde un dispositivo 11, 12, 14, ó 16 no confía en ningún otro dispositivo 11, 12, 14, ó 16, sino en sí mismo.

De forma similar, el gestor 24 de seguridad que recibe una clave desde otro dispositivo 11, 12, 14, 16 puede determinar su fuente y asignar a esa clave un nivel de confianza que determine las funciones para las que una clave podrá ser usada. Así, el gestor 24 de seguridad puede determinar si la clave proviene de una parte 11, 12, 14 ó 16 de confianza, y si la clave puede ser usada tanto para desencriptar mensajes recibidos desde esa parte 11, 12, 14 ó 16 de confianza como para encriptar mensajes enviados a esa parte 11, 12, 14 ó 16 de confianza. Alternativamente, la función 24 de gestor de seguridad puede determinar que la clave se origina en una parte 11, 12, 14 ó 16 que no es de confianza en sí mismo, y permitir solamente que la clave sea usada a efectos de descodificación. Sin embargo, el dispositivo 11, 12, 14 ó 16 puede elegir ignorar los datos, en vez de realizar el esfuerzo de tener que desencriptar los datos en primer lugar. Esta opción puede ser usada para hacer frente a las comunicaciones no solicitadas o “correo basura”.

El gestor 24 de seguridad incluye también métodos de determinación de cuáles de los dispositivos 11, 12, 14 ó 16 están actualmente activos en la red 18. Esos métodos incluyen las funciones de cada dispositivo 11, 12, 14 ó 16 de re-autenticarse a sí mismo con cada una de sus partes 11, 12, 14 ó 16 que comparten clave en un instante predeterminado. Un método de ese tipo incluye las etapas de realizar periódicamente una “operación heartbeat” en forma de protocolo de desafío y respuesta para determinar cuáles de los dispositivos están actualmente incluidos en la red 18, y ajustar los grupos y niveles de confianza adecuadamente. Así, cada dispositivo 11, 12, 14 ó 16 puede actualizar dinámicamente su propia TrustList para reflejar cambios en las relaciones de confianza. Para los dispositivos 11, 12, 14 ó 16 que carezcan de una interfaz de usuario, se puede invocar este mecanismo de actualización mediante un período de inscripción abierta seguido de una etapa de bloqueo, confirmada posiblemente por medio de un pulsador, o puede ser un simple reseteo de la lista completa, por ejemplo presionando un pulsador de reseteo o de reinicialización en el dispositivo 11, 12, 14 ó 16. Además, algunos de los cambios podrían ser invocados por medio de una tercera entidad que realice una gestión de confianza remota o delegada para ese

dispositivo.

Haciendo ahora referencia a la Figura 2, a efectos de describir el modelo de seguridad distribuida, a título de ejemplo, supóngase que el PNC 11 permite el acceso a dispositivos A, B, C, D, E, F, G, H, con lo que el DeviceSet: = {A, B, C, D, E, F, G, H}. Sin embargo, si el dispositivo A solamente confía en los dispositivos A, B, C, entonces TrustSet (A): = {A, B, C}, es decir el Grupo 1. También, el dispositivo A puede participar en otros grupos que tengan un conjunto de confianza diferente, tal como el Grupo 2, que tiene solamente el dispositivo D. Así, la función 24 de gestor de seguridad del dispositivo A detecta el Grupo 1 y el Grupo 2 con diferentes miembros constituyentes y con diferentes niveles de confianza. Por ejemplo, en el Grupo 1, si el dispositivo C es la fuente clave, y puesto que el dispositivo C es parte del TrustSet (A), esta clave se distribuye por medio del dispositivo C, lo que se utiliza para ambas codificación/descodificación permitidas como C, y el dispositivo A solamente acepta claves transferidas a si mismo por dispositivos DEV $\in$ TrustSet (A), a efectos de codificación y descodificación. En el Grupo 2, puesto que el dispositivo D no forma parte de TrustSet (A), entonces A acepta una clave procedente del dispositivo D, y de cualesquiera otros dispositivos E, F, G y H, que no sean parte de TrustSet (A), a efectos de descodificación solamente. Por consiguiente, si el dispositivo A desea comunicar con miembros del Grupo 2, el dispositivo A genera una nueva clave de grupo para formar un nuevo grupo, el Grupo 3, y el dispositivo A distribuye la nueva clave de grupo a los miembros del Grupo 2', es decir el dispositivo D. Por lo tanto, los grupos que están entonces bajo el control del gestor de seguridad del dispositivo A serán entonces el Grupo 1, el Grupo 2, según se ha mencionado anteriormente, y el Grupo 3, según se muestra en la Figura 3.

La flexibilidad de los gestores 24 de seguridad de los dispositivos A, B, C, D, E, F, G, H, permite que se mimeticen diferentes estructuras de red. Por ejemplo, usando la notación que antecede, si DeviceSet: = {A, B, C, D, E, F, G, H} y TrustSet (A): = Universe, entonces el dispositivo A puede ser considerado como un dispositivo altruista que proporciona una estructura equivalente a un modelo centralizado. A la inversa, si TrustSet (D): = {D}, entonces el dispositivo D es un dispositivo egocéntrico, y es una estructura equivalente a un modelo completamente descentralizado. Entonces, viendo la Figura 4, el dispositivo A participa en los Grupos 1, 2 y 3, teniendo todos los grupos relaciones de confianza diferentes. Por ejemplo, en el Grupo 1 que tiene los dispositivos A, B y C, si la fuente clave es el dispositivo C, entonces esta clave de grupo se utiliza para encriptación y desencriptación, puesto que el dispositivo A confía en todos los dispositivos B, C, D, E, F, G y H, lo que incluye por supuesto la fuente clave C. Sin embargo, en el Grupo 2 que tiene los dispositivos A, D y G, siendo la fuente clave el dispositivo G, una vez más el dispositivo A utiliza esta clave de grupo para encriptación y desencriptación, mientras que el dispositivo D la usa para desencriptación solamente puesto que éste no confía en ningún otro de los dispositivos A, B, C, E, F, G o H. En el Grupo 3 que tiene los dispositivos D y E, siendo la fuente clave el dispositivo E, el dispositivo D utiliza la clave de grupo para desencriptación solamente puesto que éste no confía en el dispositivo E. Puesto que el dispositivo A no está incluido en el Grupo 3, éste no recibe la clave.

En la Figura 5, donde un dispositivo F está oculto de los otros miembros en la red 18, el grupo 2 no incluye entonces la lista completa de dispositivos miembro A, D, G y H. Por lo tanto, el dispositivo D no puede comunicar con el dispositivo F puesto que la operación heartbeat indicará que el dispositivo D no está vivo. Puesto que la dirección de 8 bits o la dirección de 48 bits de un dispositivo no está disponible, no hay comunicación entre D y el dispositivo F. Por lo tanto, el dispositivo D utiliza las claves de grupo para desencriptación solamente.

Así, esas estructuras de grupo diferentes según se muestra en las Figuras 2, 3, 4 y 5 pueden ser establecidas dentro de la misma red 18 usando un esquema de gestión de seguridad descentralizada o distribuida que tiene la capacidad de establecer diferentes niveles de confianza por dispositivo. Esto puede ser usado según un número de formas, tal como admisión de dispositivos A, B, C, D, E, F, G y H, tal como PDAs en una picorred 18 en base a diferentes modelos de suscripción. Por ejemplo, un modelo de suscripción puede incluir cargar una tasa por tiempo de uso/tasa por ancho de banda, mientras que otro modelo puede estar basado en cargos por contenido. En este ejemplo, los modelos pueden ser implementados en una edificación, tal como un aeropuerto o un club de fitness, donde la red 18 incluye un PNC 11 fijo en un techo y el PNC 11 realiza multidifusión a los dispositivos de abono solamente, o los modelos pueden ser implementados entre dispositivos individuales. Así, separando el papel del gestor 24 de seguridad del correspondiente al PNC 11, son posibles modelos de cargo que hacen diferencia entre coste por tiempo de uso/coste por ancho de banda y coste por contenido/suscripción, de modo que estos modelos de cargo podrían estar operados por diferentes entidades A, B, C, D, E, F, G o H, u otra entidad intermedia.

Se apreciará por lo tanto que se proporciona una red 18 versátil, y además la retirada de un dispositivo A, B, C, D, E, F, G o H de la red 18 no requiere el restablecimiento de todas las claves de la red 18 dado que los dispositivos A, B, C, D, E, F, G o H individuales controlan la distribución de las claves. La Figura 6 muestra la comunicación entre un dispositivo A de la picorred 1 con otro dispositivo B de la picorred 2, donde $Z_1$ y $Z_2$ son miembros de la picorred 1 y de la picorred 2, respectivamente. $Z_1$ y $Z_2$ incluyen transceptores 25 para establecer un canal de comunicación o canal 26 de retransmisión entre la picorred 1 y la picorred 2. Así, $Z_1$ escucha todo el tráfico y envía todo el tráfico destinado al dispositivo B a $Z_2$ a través del canal 26 de retransmisión. Tras la recepción del tráfico reenviado por $Z_1$, $Z_2$ difunde además este tráfico a B. $Z_1$ y $Z_2$ incluyen funcionalidad WPAN y pueden actuar como agentes de retransmisión de datos solamente, y por lo tanto no pueden procesar datos. La picorred 1 y la picorred 2 incluyen $PNC_1$ y $PNC_2$ respetivos y por lo tanto los dispositivos A y B solamente necesitan $PNC_1$ y $PNC_2$, respectivamente,

para la asignación de ranuras de tiemplo, y la función de protección del contenido se realiza mediante el gestor 24 de seguridad de cada dispositivo A, B.

Con el fin de facilitar la comunicación entre los dispositivos A y B, en diferentes picorredes 1 y 2, el dispositivo A está asociado a un enrutador 28 que almacena información relacionada con otros dispositivos en su picorred 1, y que enruta información que tiene instrucciones sobre cómo enrutar tráfico desde el dispositivo A hasta otros dispositivos, tal como el dispositivo B. De manera correspondiente, el dispositivo B está también asociado a un enrutador 30 que tiene funcionalidades similares. Así, el dispositivo A o B está asociado a un enrutador y estos enrutadores 28, 30 consultan, cada uno de ellos al otro periódicamente, a efectos de actualizar la información de enrutador, debido a la naturaleza dinámica de las redes 18 ad hoc.

Con referencia a la Figura 7 y a la Figura 8, con el fin de establecer una comunicación segura entre el dispositivo A y el B, el dispositivo A realiza las etapas de adquirir la dirección estática completa del dispositivo B o el ID del dispositivo, y una clave pública o clave simétrica con el fin de realizar una conformidad de clave, en la etapa 110. En la siguiente etapa 112, la conformidad de clave genera una clave de autenticación para una comunicación posterior. Un dispositivo A recibe una respuesta, en un momento predeterminado, que prueba la posesión de la clave pública de grupo, en la etapa 114, después de lo cual el dispositivo A genera un nuevo conjunto de claves de grupo y transporta estas claves al dispositivo B, en la etapa 116. El dispositivo B puede a continuación acusar recibo de las claves de grupo en la etapa 118. De ese modo, los dispositivos A y B requieren cada uno la clave pública auténtica del otro y el ID de dispositivo completo de cada uno de los otros a efectos de autenticación y establecimiento de un canal 26 seguro, puesto que las diferentes picorredes pueden usar diferentes direcciones de dirección de lado corto para cada dispositivo A o B. Por lo tanto, el dispositivo A y el dispositivo B forman un grupo de confianza y se establece un canal seguro si el dispositivo B confía en cualquiera de los enrutadores intermedios, mientras que en otro caso el dispositivo B crea sus propias claves con el fin de establecer un canal 26 seguro.

Aunque la invención ha sido descrita con referencia a determinadas realizaciones específicas, diversas modificaciones de la misma resultarán evidentes para los expertos en la materia sin apartarse del alcance de la invención según se define en las reivindicaciones anexas.

Lo que sigue son aspectos particularmente preferidos según la presente descripción:

Cláusula número 1. Un método de un dispositivo de comunicaciones que permite comunicaciones con otros dispositivos en una red ad hoc, comprendiendo la red ad hoc una pluralidad de dispositivos, comprendiendo el método:

asociar un nivel de confianza a cada uno de la pluralidad de dispositivos, y
tras la obtención de una clave, el dispositivo de comunicaciones asigna un nivel de confianza para la clave basada en el nivel de confianza asociado a una fuente para la clave, en donde el nivel de confianza para la clave determina funciones para las que se usara la clave por parte del dispositivo de comunicaciones en comunicación con un grupo de dispositivos que hayan obtenido la clave.

Cláusula número 2. El método según la cláusula número 1, en donde dicha obtención comprende: generar y distribuir la clave al grupo de dispositivos para comunicar con los mismos, o recibir la clave desde otro dispositivo del grupo de dispositivos.

Cláusula número 3. El método según la cláusula número 1 o la cláusula número 2, que comprende además establecer un conjunto de confianza que comprende dispositivos que son de confianza.

Cláusula número 4. El método según una cualquiera de las cláusulas número 1 a 3, en donde la red ad hoc comprende un dispositivo maestro configurado para activar un controlador de acceso que usa identificadores de los otros dispositivos.

Cláusula número 5. El método según la cláusula número 4, en donde el dispositivo maestro usa una lista de control de acceso para admitir solamente los otros dispositivos que han sido autenticados positivamente en la red ad hoc.

Cláusula número 6. El método según la cláusula número 4 o la cláusula número 5, en donde el dispositivo maestro comprende además un controlador de tráfico para regular flujos de datos dentro de la red ad hoc.

Cláusula número 7. El método según la cláusula número 6, en donde el dispositivo maestro asigna una ranura de tiempo a cada uno de los otros dispositivos para distribución de mensaje.

Cláusula número 8. El método según una cualquiera de las cláusulas número 1 a 7, en donde el nivel de confianza para la clave indica si la clave puede ser usada tanto para encriptar como para desencriptar mensajes enviados desde, y recibidos por, el dispositivo de comunicaciones, o solamente para desencriptar

mensajes recibidos por el dispositivo de comunicaciones.

Cláusula número 9. El método según una cualquiera de las cláusulas número 1 a 8, que comprende además que el dispositivo de comunicaciones determine cuáles de los otros dispositivos están actualmente activos en la red ad hoc.

Cláusula número 10. El método según la cláusula número 9, en donde la determinación comprende re-autenticar cada uno de los otros dispositivos en un momento predeterminado.

Cláusula número 11. El método según la cláusula número 10, en donde la re-autenticación comprende ejecutar un protocolo de desafío y respuesta respecto a cada uno de los otros dispositivos, para determinar cuáles de los otros dispositivos están actualmente incluidos en la red ad hoc.

Cláusula número 12. Un dispositivo de comunicaciones configurado para ejecutar el método según una cualquiera de las cláusulas número 1 a 11.

Cláusula número 13. Un método para mantener la seguridad entre una pluralidad de dispositivos en una red ad hoc, comprendiendo dicho método las etapas de:

determinar en uno de dicha pluralidad de dispositivos, que éste ha sido designado como dispositivo maestro;
mantener en dicho dispositivo maestro una lista de control de acceso perteneciente a cuáles de los dispositivos forman actualmente parte de dicha red ad hoc;
recibir en dicho dispositivo maestro, desde cada uno de dichos otros de la citada pluralidad de dispositivos, una comunicación periódica que indique cuáles de los dispositivos están actualmente en la citada red ad hoc, y
proporcionar con dicho dispositivo maestro al otro de la citada pluralidad de dispositivos, información indicativa de cuáles de los dispositivos están presentes.

Cláusula número 14. Un método para facilitar comunicación entre un primer dispositivo situado en una primera red ad hoc y un segundo dispositivo situado en una segunda red ad hoc, comprendiendo dicho método:

un primer agente de retransmisión que escucha el tráfico en dicha primera red ad hoc, y
enviar con dicho primer agente de retransmisión tráfico destinado a dicho segundo dispositivo para un segundo agente de retransmisión en la citada segunda red ad hoc a través de un canal de retransmisión establecido entre ambos, para reenvío adicional mediante el segundo agente de retransmisión hasta dicho segundo dispositivo;
en donde dicho primer agente de retransmisión cuestiona periódicamente a dicho segundo agente de retransmisión y recibe peticiones periódicas desde dicho segundo agente de retransmisión para habilitar información perteneciente a sus redes ad hoc respectivas que van a ser actualizadas.

**REIVINDICACIONES**

1.- Un método, mediante un gestor de seguridad en una primera red ad hoc, para facilitar comunicación (26) entre un primer dispositivo situado en la primera red ad hoc y un segundo dispositivo situado en una segunda red ad hoc, comprendiendo dicho método:

autenticar el primer dispositivo;
enviar al primer dispositivo una primera clave de grupo;
recibir, a través de un primer y un segundo agentes de retransmisión, una consulta de autenticación desde el segundo dispositivo, en donde el primer agente de retransmisión está en dicha primera red ad hoc y el segundo agente de retransmisión está en dicha segunda red ad hoc, y
enviar al segundo dispositivo la primera clave de grupo.

2.- El método de la reivindicación 1, en donde el primer agente de retransmisión incluye un enrutador.

3.- El método de la reivindicación 1, en donde una primera pluralidad de dispositivos en la primera red ad hoc comunican entre sí en base a la primera clave de grupo, y una segunda pluralidad de dispositivos en la segunda red ad hoc comunican entre sí en base a una segunda clave de grupo.

4.- El método de la reivindicación 1, en donde el primer agente de retransmisión actúa solamente como agente de retransmisión de datos en la primera red ad hoc, y el segundo agente de retransmisión actúa solamente como agente de retransmisión de datos en la segunda red ad hoc.

5.- El método de la reivindicación 1, en donde dicho primer agente de retransmisión interroga periódicamente a dicho segundo agente de retransmisión y recibe consultas periódicas desde dicho segundo agente de retransmisión para facilitar información perteneciente a sus redes ad hoc respectivas que van a ser actualizadas, y en donde las consultas periódicas son enviadas a intervalos predeterminados.

6.- El método de la reivindicación 1, en donde el primer agente de retransmisión y el segundo agente de retransmisión incluyen transceptores que establecen un canal de retransmisión.

7.- El método de la reivindicación 1, en donde, tras la recepción de tráfico destinado al segundo dispositivo, el segundo agente de retransmisión transmite el tráfico al segundo dispositivo.

8.- El método de la reivindicación 1, en donde la primera red ad hoc incluye un primer controlador que asigna ranuras de tiempo para comunicación en la primera red ad hoc, y la segunda red ad hoc incluye un segundo controlador que asigna ranuras de tiempo para comunicación en la segunda red ad hoc.

9.- El método de la reivindicación 1, en donde la consulta de autenticación incluye una clave creada por el segundo dispositivo.

10.- Un gestor de seguridad en una primera red ad hoc configurado para realizar operaciones que faciliten comunicación (26) entre un primer dispositivo situado en la primera red ad hoc y un segundo dispositivo situado en una segunda red ad hoc, en donde las operaciones comprenden:

autenticar el primer dispositivo;
enviar al primer dispositivo una primera clave de grupo;
recibir, a través de un primer y un segundo agentes de retransmisión, una consulta de autenticación desde el segundo dispositivo, en donde el primer agente de retransmisión está en la primera red ad hoc y el segundo agente de retransmisión está en dicha segunda red ad hoc, y
enviar al segundo dispositivo la primera clave de grupo.

11.- El gestor de seguridad de la reivindicación 10, en donde dicho primer agente de retransmisión interroga periódicamente a dicho segundo agente de retransmisión y recibe consultas periódicas desde dicho segundo agente de retransmisión para que facilite información perteneciente a sus redes ad hoc respectivas que van a ser actualizadas, y en donde las consultas periódicas son enviadas a intervalos predeterminados.

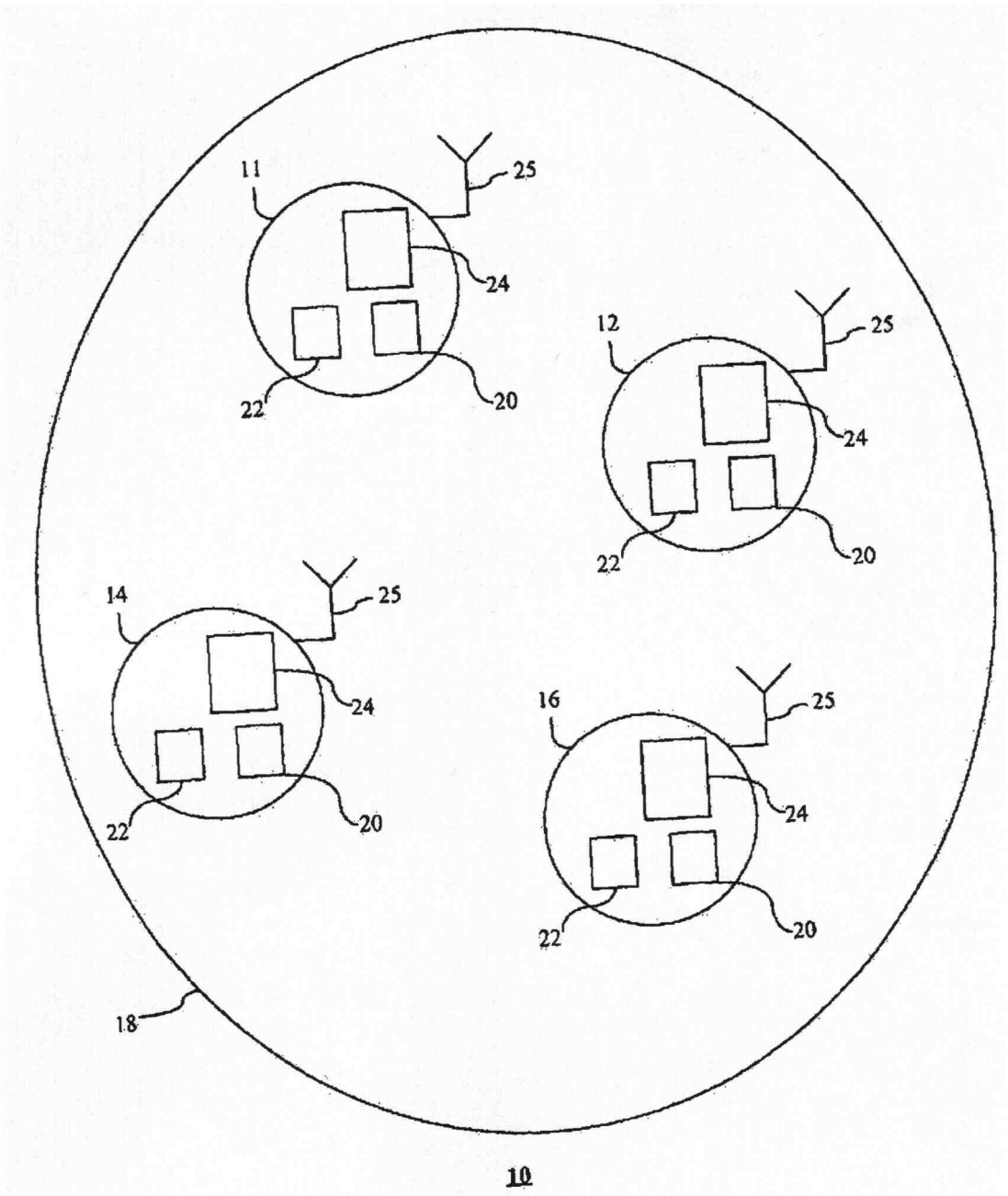


Figura 1

| | A B C D E F G H | | |
|---|---|---|---|
| Grupo 1' | x x x | Fuente Clave: C | codificación/descodificación permitida |
| Grupo 2' | x x | Fuente Clave: D | descodificación solamente |

Figura 2

| | A B C D E F G H | | |
|---|---|---|---|
| Grupo 1' | x x x | Fuente Clave: C | codificación/descodificación |
| Grupo 2' | x x | Fuente Clave: D | descodificación |
| Grupo 3' | x x | Fuente Clave: A | codificación/descodificación |

Figura 3

| | A B C D E F G H | | A | D |
|---|---|---|---|---|
| Grupo 1' | x x x | Fuente Clave: C | codificación/descodificación | |
| Grupo 2' | x x x | Fuente Clave: G | codificación/descodificación | descodificación |
| Grupo 3' | x x | Fuente Clave: E | | descodificación |

Figura 4

| | A B C D E F G H | | A | D |
|---|---|---|---|---|
| Grupo 1 | x x x | Fuente Clave: C | codificación/descodificación | |
| Grupo 2 | x x $ x | Fuente Clave: G | codificación/descodificación | descodificación |
| Grupo 3' | x x | Fuente Clave: E | | descodificación |

$: Nodo oculto ("mosca en la pared)

Figura 5

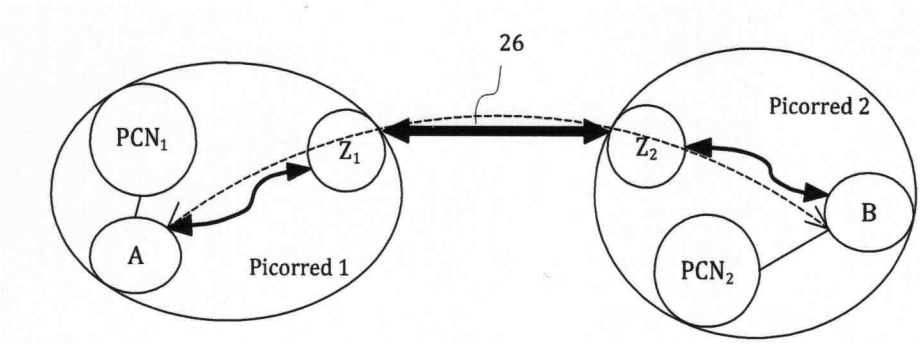


Figura 6

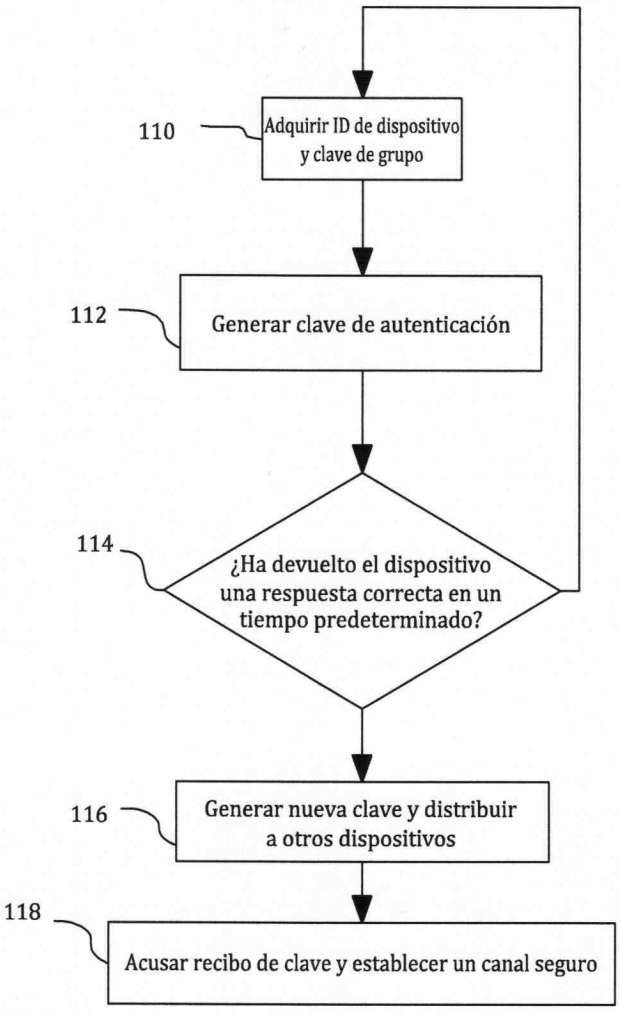


Figura 7

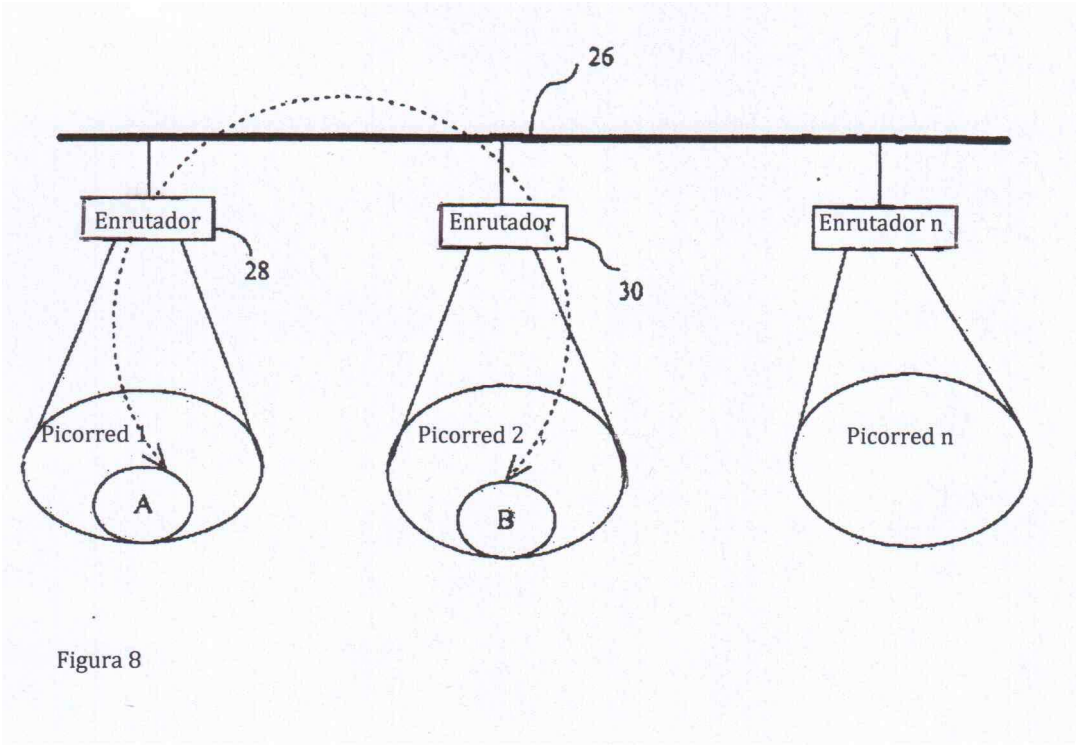
26
Enrutador
28
Enrutador
30
Enrutador n
Picorred 1
A
Picorred 2
B
Picorred n

Figura 8