(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 346 251**

(51) Int. Cl.:
H04L 29/06 (2006.01)
H04L 12/56 (2006.01)
H04L 12/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07106581 .7**
(96) Fecha de presentación : **20.04.2007**
(97) Número de publicación de la solicitud: **1983715**
(97) Fecha de publicación de la solicitud: **22.10.2008**

(54) Título: **Configuración de red inalámbrica.**

(73) Titular/es:
VALTION TEKNILLINEN TUTKIMUSKESKUS
Vuorimiehentie 3
02150 Espoo, FI

(45) Fecha de publicación de la mención BOPI:
13.10.2010

(72) Inventor/es: **Latvakoski, Juhani y**
Vaisanen, Teemu

(45) Fecha de la publicación del folleto de la patente:
13.10.2010

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Configuración de red inalámbrica.

Ámbito

La invención se refiere a un aparato, un programa informático y un método para la configuración de redes inalámbricas.

Antecedentes

El problema para un nodo de ordenador que funciona en una red inalámbrica dinámica es que se desconoce la fiabilidad de los otros nodos, es difícil confiar en los otros nodos: ¿se puede entregar información valiosa a un nodo de destino mediante los nodos vecinos? Y, en consecuencia, si un nodo vecino transmite información/datos al nodo de ordenador, ¿debe recibirse y retransmitirse?

Este encaminamiento puede provocar problemas, debido a que la carga de tráfico a encaminar se puede transmitir maliciosamente con el fin de impedir el funcionamiento de la red mediante la simple sobrecarga de la red. Los usuarios/nodos no deseados pueden transmitir información errónea a la red sólo para provocar problemas en algún lugar de la red. Además, cualquier retransmisión de mensajes utiliza la potencia del nodo del ordenador, lo que consume una valiosa carga de la batería si el nodo de ordenador es un dispositivo inalámbrico. Si el nodo del ordenador es un router inalámbrico, es problemático permitir el libre encaminamiento para todos los demás nodos, ya que esto puede provocar problemas significativos con la seguridad y el uso de recursos de encaminamiento. El concepto del router móvil inalámbrico ("múltiples saltos": "multihop") no es factible, a menos que se encuentre una solución para los problemas descritos.

Existen múltiples algoritmos de encaminamiento *ad hoc* disponibles, pero ninguno de ellos proporcionan un encaminamiento *ad hoc* seguro en un dominio inalámbrico, ya que la autenticación fiable de los nodos y los usuarios no se resuelve de manera satisfactoria y porque las soluciones de la técnica anterior requieren el uso de certificación o servidores de terceros. Además, algunas de las soluciones hacen un encaminamiento seguro pero no la conexión de extremo a extremo.

Documentos pertinentes de la técnica anterior que se ocupan de los protocolos de encaminamiento en redes *ad hoc* y que se encuentran con los problemas mencionados anteriormente son los siguientes: "Model Based Protocol Fusion for MANET-lnternet Integration", (Fusión de Protocolos Basado en Modelos para Integración de Internet-MANET(Mobile *Ad hoc* NETworking: redes móbiles *ad hoc*)), C. JELGER, C. TSCHUDIN; "HIP Applications" (Aplicaciones HIP) S.TARKOMA, W. ZHOU, MIIKA KOMU; y "Trust-Based Route Selection in Dynamic Source Routing" (Selección de Ruta Basada en la Confianza en Encaminamiento de Fuentes Dinámicas) CHRISTIAN D. JENSEN Y OTROS.

Breve descripción

La presente invención tiene por objeto proporcionar un aparato, programa informático y método mejorados.

Según un aspecto de la presente invención, se proporciona un aparato según se especifica en la reivindicación 1.

Según otro aspecto de la presente invención, se proporciona un programa informático según se especifica en la reivindicación 27.

Según otro aspecto de la presente invención, se proporciona un método de ordenador según se especifica en la reivindicación 14.

Lista de los dibujos

A continuación se describen realizaciones de la presente invención, solamente a modo de ejemplo, haciendo referencia a los dibujos que se acompañan, en los que

Las figuras 1, 2 y 3 ilustran un entorno de red y su funcionamiento;

La figura 4 ilustra un intercambio básico HIP;

La figura 5 ilustra una estructura simplificada del aparato;

Las figuras 6 y 7 ilustran la integración de SAODV (Simplified Ad-hoc On-demand Distance Vector: Vector a Distancia Simplificado Bajo Demanda Ad-hoc) y HIP (Host Identity Protocol: Protocolo de Identidad de Anfitrión);

La figura 8 ilustra un método; y

Las figuras 9, 10 y 11 ilustran varias estructuras de mensaje de respuesta de rutas y solicitudes de ruta.

Descripción de realizaciones

La figura 5 ilustra una estructura simplificada de un aparato. El aparato puede ser un nodo de computación. El nodo de computación puede colocarse de manera fija. El nodo de computación fijo puede ser un router o un ordenador de servidor, por ejemplo. El nodo de computación también puede ser móvil. El nodo de computación móvil puede ser un dispositivo portátil de comunicaciones inalámbricas móviles que funciona con o sin un módulo de identificación de usuario (SIM), incluyendo pero no limitado a los siguientes tipos de dispositivos: un teléfono móvil, un teléfono inteligente (smartphone), un asistente digital personal (PDA) o un microteléfono.

El aparato puede ser implementado como un dispositivo de computación electrónica digital, que puede comprender una memoria de trabajo (RAM), una unidad de procesamiento central (CPU) y un reloj de sistema. La CPU puede comprender un conjunto de registros, una unidad de lógica aritmética y una unidad de control. La unidad de control se controla mediante una secuencia de instrucciones de programa transferidas a la CPU desde la RAM. La unidad de control puede contener varias microinstrucciones para operaciones básicas. La implementación de microinstrucciones puede variar, dependiendo del diseño de la CPU. Las instrucciones de programa pueden codificarse mediante un lenguaje de programación, que puede ser un lenguaje de programación de alto nivel, como C, Java, etc., o un lenguaje de programación de bajo nivel, como un lenguaje máquina o ensamblador. El dispositivo electrónico de computación digital también puede tener un sistema operativo, que puede proporcionar servicios de sistema a un programa informático escrito con las instrucciones de programa.

El aparato comprende un transmisor-receptor 500 configurado para comunicarse de forma inalámbrica con otros aparatos. Una conexión inalámbrica puede implementarse con el transmisor-receptor inalámbrico 500 que funciona de acuerdo con el estándar GSM (Sistema Global para Comunicaciones Móviles), GPRS (Servicio General de Paquetes vía Radio), WCDMA (Acceso Múltiple Por División De Código De Banda Ancha), WLAN (Red Inalámbrica de Área Local) o Bluetooth®, o cualquier otro medio adecuado de comunicación inalámbrica estándar o no estándar.

Además, el aparato comprende un módulo de interfaz 504 configurado para introducir un identificador de auto-certificación del aparato. El identificador de auto-certificación se refiere a un identificador que puede verificarse sin consultar o confiando en un tercero, tal como una autoridad de certificación externa. El identificador de auto-certificación puede ser una cadena gestionada de forma manual, y su asociación a una clave pública se puede verificar matemáticamente. Tales identidades de los aparatos se pueden aplicar para permitir el descubrimiento de ruta y configuración de red seguros. Un usuario puede utilizar el mismo identificador de auto-certificación en diferentes aparatos.

El módulo de interfaz 504 puede configurarse para obtener el identificador de auto-certificación del aparato a partir de una memoria 506. La memoria 506 puede ser una parte interna del aparato, o una parte externa que se comunica mediante medios con cables o inalámbricos con el módulo de interfaz 504. La memoria 506 puede ser un dispositivo portátil pequeño que contiene el identificador de auto-certificación. La portabilidad de la memoria 506 hace que sea fácil utilizar el mismo identificador de auto-certificación en distintos aparatos del usuario. Además, la memoria 506 puede contener parámetros de configuración de sistema de la persona que está empezando a utilizar el aparato que está unido a la red. Estos parámetros se pueden utilizar como punto de partida para la configuración de red. La memoria 506 puede ser una memoria flash USB (Universal Serial Bus), o algún otro tipo portátil de memoria.

El aparato también comprende un módulo de procesamiento 502, acoplado con el transmisor-receptor inalámbrico 500 y el módulo de interfaz 504. El módulo de procesamiento 502 se configura para realizar un proceso de autenticación utilizando el identificador de auto-certificación del aparato con otros aparatos en el alcance del transmisor-receptor 500. El módulo de procesamiento también se configura para añadir rutas a esos otros aparatos que pasaron el proceso de autenticación. Las rutas se pueden añadir a una tabla de encaminamiento 510.

El módulo de interfaz 504 puede configurarse para introducir información en los identificadores de auto-certificación de otros aparatos amistosos. “Amistoso” en esta memoria se refiere otros aparatos en los que se puede confiar, es decir aparatos que se consideran seguros para fines de encaminamiento y/o de comunicación. El aparato y los otros aparatos amistosos pueden pertenecer al mismo grupo en el que los aparatos confían entre sí. La información en los identificadores de auto-certificación de los otros aparatos amistosos puede residir en la memoria 506, y puede ser en forma de una lista. La lista puede actualizarse periódicamente o cuando sea necesario con el fin de mantenerla actualizada, es decir, otros aparatos amistosos pueden añadirse o retirarse de la lista. La actualización se puede realizar con cualquier mecanismo apropiado, tal como transferencia de datos inalámbricos. El módulo de procesamiento 502 puede configurarse para utilizar la información en los identificadores de auto-certificación de los otros aparatos amistosos en el proceso de autenticación. El módulo de procesamiento 502 puede comprobar si el identificador de auto-certificación transmitido por el otro aparato pertenece a otro aparato amistoso utilizando la información en los identificadores de auto-certificación de los aparatos de otros amistosos.

Una realización proporciona un programa informático que comprende instrucciones de programa que, una vez cargadas en el aparato, constituyen los módulos anteriores 502, 504.

El programa informático puede estar en forma de código fuente, forma de código de objetos o en alguna forma intermedia, y puede almacenarse en algún tipo de soporte, que puede ser de cualquier entidad o dispositivo capaz

de llevar el programa. Estos soportes incluyen unos medios de grabación, memoria de ordenador, memoria de sólo lectura, señal portadora eléctrica, señal de telecomunicaciones y paquete de distribución de software, por ejemplo. Dependiendo de la potencia de procesamiento necesaria, el programa informático puede ejecutarse en un solo ordenador digital electrónico o puede distribuirse entre varios ordenadores.

Los módulos 502, 504 también se pueden implementar como uno o más circuitos integrados, tales como circuitos integrados de aplicación específica ASIC. Otras realizaciones de hardware (equipo físico) también son factibles, tales como un circuito construido de componentes lógicos independientes. También es factible un híbrido de estas diferentes implementaciones. Cuando se seleccione el método de implementación, un experto en la materia tendrá en cuenta los requisitos establecidos para el tamaño y el consumo de energía del aparato, la capacidad de procesamiento necesaria, los costes de producción y volúmenes de producción, por ejemplo.

Un ejemplo de un entorno de red se ilustra en las figuras 1, 2 y 3. En este ejemplo AODV ó SAODV se utilizan como algoritmos de encaminamiento, pero la invención no se limita a los mismos, ya que también se pueden utilizar otros algoritmos de encaminamiento adecuados.

Se puede utilizar una etiqueta de identidad de anfitrión (HIT) como identificador de auto-certificación cuando se utiliza IP versión 6, tanto en AODV como en SAODV. HIT puede ser una representación de 128 bits para una identidad de anfitrión (Host Identity). Se pueden crear mediante la adopción de un cálculo de clave criptográfica (cryptographic hash) sobre el correspondiente identificador de anfitrión. Hay dos ventajas por utilizar un cálculo de clave en vez de usar el identificador de anfitrión en los protocolos. En primer lugar, su longitud fija hace más fácil la codificación del protocolo y también permite una mejor gestión de los costes de tamaño de paquete. En segundo lugar, presenta la identidad en un formato compatible con el protocolo independiente de los algoritmos criptográficos usados.

Se puede utilizar un identificador local de alcance (LSI: Local Scope Identifier) como identificador de auto-certificación cuando se utiliza IP versión 4 en AODV. LSI puede ser una representación localizada de 32 bits para una identidad de anfitrión (Host Identity). El propósito de un LSI es facilitar el uso de identidades de anfitrión en los protocolos existentes y API. La ventaja del LSI sobre el HIT es su tamaño.

La memoria 110, 112, 114, 116, 118 puede contener el identificador de auto-certificación y posiblemente también los parámetros de configuración del sistema de la persona que utiliza el nodo de ordenador 100, 102, 104, 106, 108. La memoria 110, 112, 114, 116, 118 puede contener también las identidades de otros miembros del grupo. Para facilitar la consulta, cada nodo 100, 102, 104, 106, 108 tiene como referencia una letra (A, B, C, D y E).

Cuando el nodo A se activa, lee su propio identificador de auto-certificación de la memoria de 110, y entonces empieza a unirse a la red *ad hoc* dinámica, por ejemplo, de acuerdo con el protocolo de encaminamiento AODV o SAODV.

TABLA 1

El mensaje de Hola del nodo A

□Tipo	Origen	HIT de origen
HOLA	IPv6 de A	HIT de A

Cuando el nodo A se está uniendo a la red, puede transmitir un “hola A” como un mensaje de multidifusión al entorno que le rodea. El mensaje “hola A” puede contener, además de los elementos habituales de información de protocolo de encaminamiento *ad hoc*, también el HIT etiqueta de identificador de anfitrión de origen y la dirección de origen de Protocolo de Internet versión 6 (IPv6) del nodo A como se muestra en la Tabla 1. El HIT de origen se incluye para permitir la identificación de nodos y usuarios, y la IPv6 de origen se utiliza para la elaboración y actualización de las tablas de encaminamiento.

El módulo de procesamiento 502 puede configurarse para colocar el identificador de auto-certificación del aparato 100 en el mensaje de hola, y para la multidifusión del mensaje de hola a los otros aparatos 102, 104 en el alcance del transmisor-receptor inalámbrico 500 como parte del proceso de autenticación. El módulo de procesamiento 502 también puede configurarse para colocar una dirección de protocolo de internet del aparato 100 en el mensaje de hola.

Los nodos B y C están supervisando el canal de multidifusión y reciben los mensajes “hola A”. El HIT que se recibe en el mensaje “hola A” se utiliza para identificar al remitente de acuerdo a las siguientes reglas:

1. Si el nodo receptor (nodo B y/o el nodo C en este caso) sabe el HIT del nodo A, y sabe que el HIT pertenece al grupo permitido (= nodo A es un amigo), el nodo añade la dirección IPv6 actual recibida del nodo A a su tabla de encaminamiento como se ilustra en la Tabla 2.

2. Si el nodo receptor (nodo B y/o el nodo C en este caso) no tiene conocimiento del HIT del nodo A, el nodo no añade la dirección IPv6 de A a la tabla de encaminamiento, ya que no está seguro acerca de su amistad.

3. El HIT aplicado puede ser una etiqueta de identidad de anfitrión del nodo o una etiqueta de identidad del anfitrión del grupo (HIT del grupo).

TABLA 2

La tabla de encaminamiento en los nodos B y C

□Destino	Siguiente
IPv6 de A	IPv6 de A

Los nodos B y C también se están uniendo a la red, también envían un mensaje “hola B”, que se ilustra en la Tabla 3, y un mensaje “hola C”, que se ilustra en la Tabla 4, como un mensaje de multidifusión para el entorno que los rodea.

TABLA 3

El mensaje de hola del nodo B

□Tipo	Origen	HIT de origen
HOLA	IPv6 de B	HIT de B

TABLA 4

El mensaje de hola del nodo C

□Tipo	Origen	HIT de origen
HOLA	IPv6 de C	HIT de C

El nodo A recibe los mensajes de hola de los nodos B y C. A continuación, el nodo A actualiza su tabla de encaminamiento de acuerdo con las reglas previamente definidas. La tabla resultante de encaminamiento del nodo A se ilustra en la tabla 5.

TABLA 5

La tabla de encaminamiento del nodo A

□Destino	Siguiente
IPv6 de B	IPv6 de B
IPv6 de C	IPv6 de C

Cuando se inicia la configuración de la red, el nodo A es conocedor de los HIT configurados previamente del nodo B y del nodo C. Durante el nuevo procedimiento de hola, encuentra las direcciones IPv6 del nodo B y del nodo C. Como resultado, puede construir la tabla de asignaciones de dirección IPv6-HIT visualizada en la tabla 6. La tabla de asignaciones de dirección IPv6-HIT también se construye en los nodos B y C.

TABLA 6

Tabla de asignaciones de dirección IPv6/HIT en el nodo A

□dirección IPv6	HIT
IPv6 de B	HIT de B
IPv6 de C	HIT de C

El módulo de procesamiento 502 puede configurarse para mantener una tabla de asignaciones 512 que incluye pares de identificador de auto-certificación/dirección de protocolo de internet de los otros aparatos, y para eliminar esos otros aparatos que no pasen el proceso de autenticación de la tabla de asignación 512. Además, los identificadores de auto-certificación que pasan el proceso de autenticación también pueden añadirse a la tabla de encaminamiento.

Por último, los nodos D y E también se unirán a la red por multidifusión de mensajes "hola D" y "hola E". Los mensajes de hola 130, 132, 134, 136, 138, 140 se intercambian de este modo entre todos los nodos adyacentes. Las tablas de encaminamiento completadas 120, 122, 124, 126, 128 de cada nodo A, B, C, D y E también se ilustran en la figura 1.

Si el nodo vecino es un amigo, puede ejecutarse el intercambio básico HIP para crear la seguridad de que los extremos poseen la clave privada correspondiente a sus HI (identificador de anfitrión), que son las claves públicas. El intercambio básico HIP se ilustra en la figura 4 y la Tabla 7. El módulo de procesamiento 502 puede configurarse para utilizar un intercambio básico de protocolo de identidad de anfitrión como parte del proceso de autenticación.

El intercambio básico HIP crea un par de Asociaciones de Seguridad (SA) por encapsulado de carga útil (ESP) de Seguridad de Protocolo de Internet (IPsec), una en cada sentido.

TABLA 7

Mensajes de intercambio básico HIP

□		I —>	Directorio: consulta R
		I <—	Directorio: devuelve HI/HIT y dirección de R
410	I1	I —> R	Hola, aquí está mi I1, permítenos hablar con HIP
412	R1	R—> I	De acuerdo, aquí está mi R1, maneja esta cookie HIP
414	I2	I —> R	Computando, aquí está mi contador 12
416	R2	R —> I	De acuerdo, permítenos terminar el HIP con mi R2
418		I <—> R	Datos protegidos ESP

El intercambio básico HIP se conoce en la tecnología, que se revisa en breve a continuación. Un mensaje I1 que contiene el HIT del iniciador 400 comienza 410 el intercambio básico HIP. El contestador 402 ha formado partes de mensajes R1 de antemano, y cuando recibe el mensaje I1, selecciona un R1 computado previamente, lo completa y lo envía 412 al iniciador 400. El mensaje R1 incluye un puzle, una puesta en marcha Diffie-Hellman, la HI pública del receptor en texto claro, una clave de Diffie-Hellman y otros parámetros de Diffie-Hellman.

Cuando el iniciador 400 recibe el mensaje R1, calcula la respuesta al puzle, calcula una clave de sesión y envía 414 un mensaje I2 al contestador. Esta parte utiliza la mayor potencia de procesamiento y hace los ataques DoS (Denegación de Servicio) más difíciles en el HIP, debido a que el intercambio básico HIP tiene más potencia de procesamiento desde el iniciador 400 que el contestador 402 y el contestador 402 utiliza poco cálculo antes del mensaje I2. El mensaje I2 incluye la respuesta al puzle, los parámetros de Diffie-Hellman, la HI pública del iniciador, SPI (Indice de Parámetros de Seguridad: Security Parameter Index) y HI cifrados con la clave de sesión.

Cuando el contestador 402 recibe el mensaje I2, comprueba que el puzle se resuelve correctamente, calcula la clave de sesión, autentica al iniciador y realiza el estado de sesión. Luego, envía 416 un mensaje R2 que incluye el SPI y la firma del contestador. La firma hace posible que el iniciador 400 termine la autenticación.

El HIP no cambia la forma de los paquetes IPv4 ó IPv6. Los paquetes 418 se cifran con ESP y son similares a paquetes normales protegidos con ESP IPsec. ESP permite que el nodo receptor valide y confirme que realmente han sido enviados por otro nodo conocido sin preocuparse de la direcciones de origen y destino de los paquetes. Se conectan SA a las claves públicas y el destino sólo se utiliza para el encaminamiento. El origen sólo es necesario durante el intercambio básico y cuando se actualizan las direcciones IP.

Después de que el intercambio básico HIP se ha realizado entre los nodos A-B y A-C, el resultado se interpreta de acuerdo a las siguientes reglas:

1. Si el intercambio básico HIP tiene éxito, se crea el túnel de IPsec SA y IPsec ESP entre los HIT de A y B, y entre los HIT de A y C.

2. Si el intercambio básico HIP no tiene éxito, el nodo A probablemente no es el A correcto, y los nodos B y C eliminan la información del nodo A de sus tablas de encaminamiento y las tablas de asignaciones de dirección IPv6-HIT.

Como resultado de la configuración de la red, cada nodo de la red *ad hoc* tiene la tabla de asignaciones de dirección IPv6-HIT (como la Tabla 6) en su memoria. Basándose en esta tabla, el nodo conoce fácilmente los nodos vecinos amistosos, en el que el nodo puede confiar en el sentido de que pertenecen al grupo permitido. La fiabilidad está garantizada por la aplicación de identidades criptográficas junto con el protocolo HIP.

A continuación, haciendo referencia a la figura 2, se explica un mecanismo de descubrimiento de ruta. El punto de partida para el descubrimiento de ruta es la ejecución de la configuración de la red, que se ha descrito anteriormente. Como resultado de la configuración de la red, existen túneles seguros IPsec entre nodos vecinos, es decir, A-B, A-C, B-C, B-D, C-D y D-E.

El módulo de procesamiento 502 puede configurarse para buscar por lo menos una ruta a partir de la tabla de encaminamiento 510, y para la unidifusión de una solicitud de ruta cifrada incluyendo un identificador de auto-certificación de un aparato de destino a través de por lo menos una ruta.

El módulo de procesamiento 502 también puede configurarse para colocar el identificador de auto-certificación del aparato en la solicitud de ruta.

El descubrimiento de ruta se inicia mediante el nodo A que desea comunicarse con el nodo E. El nodo A conoce el HIT del nodo E de destino, pero no su dirección IPv6 actual y la ruta al nodo E. Para encontrar la ruta al nodo E, el nodo A envía una solicitud de ruta modificada (RREQ) 200, mensaje 202 a todos los nodos vecinos fiables, que se encuentran en la tabla de asignación de dirección IPv6-HIT. Esto significa que el RREQ se envía al grupo de nodos vecinos fiables, pero no a todos los nodos vecinos posibles. La estructura del mensaje RREQ puede modificarse respecto la estructura del mensaje AODV RREQ. La novedad en la estructura del mensaje RREQ modificada es la indicación del origen y el destino como HIT. Otra diferencia esencial en comparación con AODV es que RREQ se envía al grupo de los nodos vecinos por los túneles IPSec entre el remitente y el nodo vecino receptor. En el AODV estándar, el RREQ se envía por multidifusión a todos los nodos vecinos.

Cuando un nodo recibe el mensaje RREQ, comprueba los HIT de origen y de destino mediante las siguientes reglas:

1. Si el HIT de destino es el HIT del nodo receptor, es decir, el nodo de destino E recibe el mensaje RREQ, entonces el nodo E comprueba si el nodo A es un nodo amistoso mediante la comparación del HIT de A con los configurados previamente almacenados en la clave.

    a. Si el nodo de origen A es un nodo amistoso, entonces el nodo E almacena la dirección IPv6 del nodo A en su tabla de encaminamiento, actualiza la tabla de asignación de dirección IPv6-HIT temporalmente, y comienza el proceso de respuesta de ruta.

    b. Si el nodo de origen A no es un nodo amistoso, entonces el nodo E envía un mensaje de error de router (RERR) con un código de error correspondiente, devuelto opcionalmente al origen.

2. Si los HIT de destino y de origen indican que son nodos amistosos, entonces el mensaje RREQ se envía hacia delante al grupo confiable de nodos vecinos, que están en la tabla de asignaciones de dirección IPv6-HIT como se describió anteriormente.

3. Si bien el destino o el origen no son nodos fiables, entonces el mensaje RREQ no se envía hacia adelante, y opcionalmente se devuelve un mensaje RERR con un código de error correspondiente al nodo de origen.

Como se ilustra en la figura 2, el nodo B transmite los mensajes RREQ a los nodos C y D. Nodo C rechaza 220 el mensaje RREQ 206 del nodo B, ya que el nodo C ya ha recibido el mensaje RREQ 202 desde el nodo A. El nodo C transmite el mensaje RREQ 208 al nodo D, pero el nodo D rechaza 222 el mensaje RREQ del C ya que el nodo D ya ha recibido el mensaje RREQ 204 desde el nodo B. Por último, el nodo D transmite el mensaje RREQ 210 al nodo E.

El proceso de respuesta de ruta se ilustra en la figura 3. El nodo de destino E responde mediante el envío 300 de un mensaje de respuesta de ruta (RREP), con el fin de indicar que se ha descubierto la ruta entre los nodos A y E. El módulo de procesamiento 502 puede configurarse para recibir una respuesta cifrada de ruta a través de la por lo menos una ruta, y añade una ruta al aparato de destino, incluyendo la dirección del otro aparato que ha transmitido la respuesta de ruta, en la tabla de encaminamiento 510. Cabe señalar que RREQ, RREP y RERR se envían por unidifusión a través de túneles seguros. La solicitud de ruta, la respuesta de ruta y los mensajes de error de ruta se refieren a un mecanismo general para encontrar rutas, es decir no deben entenderse como restringidos solamente a AODV.

El módulo de procesamiento 502 también se puede configurar para medir el tiempo para emitir por unidifusión la solicitud de ruta, posiblemente con un reloj 514, y añadir una ruta al aparato de destino, incluyendo una dirección de un servidor de encaminamiento de una red estática, en la tabla de encaminamiento, si no se recibe una respuesta cifrada de ruta en un período de tiempo predeterminado después de la unidifusión de la solicitud de ruta. El servidor de encaminamiento puede ser un denominado servidor de encuentro (rendezvous server).

El mensaje RREP se envía 302, 304, 306, 308 de vuelta a través de las rutas de acuerdo al último campo de salto por los canales protegidos con ESP entre los nodos vecinos. La diferencia esencial en comparación con AODV es que el mensaje RREP se envía al último nodo de salto por los túneles IPsec entre el remitente y el nodo vecino receptor. En la norma AODV, los mensajes RREP no están protegidos en absoluto. Cuando el nodo A recibe el mensaje RREP, actualiza la tabla de asignaciones de dirección IPv6-HIT con la dirección IPv6 del nodo E.

El módulo de procesamiento 502 puede configurarse para realizar un proceso de autenticación utilizando el identificador de auto-certificación del aparato con el aparato de destino a través de la ruta al aparato de destino.

A continuación, el nodo A ejecuta el intercambio básico HIP con el nodo E, y sigue las siguientes reglas:

1. Si el intercambio básico HIP tiene éxito, se crea el túnel IPsec ESP y IPsec SA entre los HIT del nodo A y el nodo E. Después de esto, la comunicación entre el nodo A y el nodo E puede continuar de un modo seguro.

2. Si el intercambio básico HIP no tiene éxito, entonces el nodo A elimina el nodo E de su tabla de asignaciones de dirección IPv6-HIT y la tabla de encaminamiento. Y el nodo E hace lo mismo con el nodo A, ya que no hay ninguna relación de confianza entre los nodos A y E.

Después de los procesos exitosos de descubrimiento de ruta y de configuración de red, el tráfico de usuario puede enviarse entre los nodos de origen y de destino (A y E en este caso) de manera segura. El módulo de procesamiento 502 puede configurarse para el intercambio de datos cifrados con el aparato de destino a través de la ruta al aparato de destino. Como se ilustra en la figura 5, el aparato puede incluir aplicaciones 508 que necesitan intercambiar datos a través de la conexión creada segura, en nuestro ejemplo la ruta es A-B-D-E.

Con la funcionalidad descrita anteriormente, un nodo de ordenador en la red *ad hoc* sabe cuáles de los nodos vecinos son fiables. Si el nodo no tiene una conexión directa con el nodo de destino, encuentra la ruta a la misma a través de una cadena fiable de nodos y establece un canal seguro de extremo a extremo de comunicación con él. Un nodo de ordenador que trabaja como un router móvil sólo encamina el tráfico de los nodos amistosos. La posibilidad de que nodos de mal comportamiento perturben el funcionamiento de la red se elimina o reduce de manera significativa. Se ahorra batería del nodo de ordenador, porque sólo se encamina tráfico de los nodos amistosos. La solución reduce la carga de la red de ordenadores. La escalabilidad de la solución es mejor en comparación con el encaminamiento tradicional *ad hoc* basado en AODV.

A continuación, se describirá un método haciendo referencia a la figura 8. El método se refiere al encaminamiento y configuración de redes inalámbricas. El método comienza en 800.

En 802, un identificador de auto-certificación del aparato se introduce en el aparato.

En 804, el aparato realiza un proceso de autenticación utilizando el identificador de auto-certificación del aparato con otros aparatos dentro del alcance de comunicación inalámbrica del aparato.

En 806, las rutas a esos otros aparatos que pasaron el proceso de autenticación se añaden a una tabla de encaminamiento.

La parte de configuración de red básica del método termina en 808. Las realizaciones mencionadas anteriormente del aparato se pueden aplicar al método igualmente, con el fin de añadir realizaciones, como se describe en las reivindicaciones adjuntas, a la parte de configuración de red del método, así como a la parte de encaminamiento del método.

A continuación, con referencia a las figuras 6 y 7, se describirán algunas realizaciones adicionales de la invención. Cuando un nodo se enciende, comienza a enviar continuamente paquetes de hola a una dirección IPv6 de difusión global. Un nodo tiene un archivo de configuración para determinar amigos. Este archivo enumera todos los HIT amistosos y se lee cada vez que se procesa un mensaje SAODV. Como se explicó anteriormente, el archivo de configuración

puede ser actualizado con el fin de mantener la lista de amigos actualizada. Si el nodo que envía mensajes de hola con un HIT no amistoso desea iniciar una negociación, el nodo receptor compara el HIT recibido con su lista e ignora este mensaje y todos los siguientes mensajes enviados por este nodo.

La figura 6 muestra un paso a paso detallado de ejecución del procedimiento de hola. El número de hola (no_of_hello) es un contador que cada nodo tiene como una variable estática y se incrementa en uno cada vez que un nodo envía un mensaje de hola. La necesidad de esta variable surge de la necesidad de un acuerdo mutuo de los cuales uno de los nodos debe comenzar el intercambio básico HIP. Este procedimiento se asegura de que el nodo que ha estado más tiempo en la red no tiene que iniciar el intercambio básico porque el establecimiento de comunicación HIP se construye de manera que siempre es computacionalmente más difícil para el iniciador completar el establecimiento de comunicación. De esta manera, se pueden evitar fácilmente el tipo de ataques de denegación de servicio cuando el iniciador tiene que resolver los puzles que necesitan potencia de CPU para resolver.

La figura 7 ofrece una explicación de pseudo-código de acuerdo del iniciador para el intercambio básico HIP. Después de un exitoso intercambio de mensajes de hola y ejecución de intercambios básicos, la red se ha configurado. Cuando se compara con un SAODV normal, las tablas de encaminamiento también pueden tener información de encaminamiento acerca de los HIT de nodo, además de direcciones IPv6 normales. Este cambio es necesario para el encaminamiento por unidifusión de mensajes SAODV utilizando HIT.

Como SAODV es un protocolo reactivo, envía paquetes bajo demanda y encuentra la ruta mediante la inundación de la red con paquetes RREQ. El envío se realiza normalmente mediante el uso de una dirección de difusión global que escucha cada nodo. Este mismo método se utiliza también para el envío de mensajes de hola.

Esta manera insegura de encaminamiento por multidifusión de paquetes a todo el mundo se ha transformado en un modelo de unidifusión que se aprovecha de las conexiones disponibles HIP entre los nodos. La lógica de funcionamiento básico es que si un paquete está destinado a un nodo en el que una ruta no se conoce, un se envía RREQ a todos los nodos vecinos. Si el destino es uno de los vecinos, envían hacia atrás un paquete RREP, y se puede establecer una ruta entre los nodos. Sin embargo, si el destino no es un vecino, envían el RREQ a todos sus vecinos excepto al nodo del que viene el paquete. De esta manera la red se inundada y finalmente se encuentra el destino.

Suponiendo que se tiene una red inalámbrica *ad hoc* de la figura 1. Ahora, si el nodo A desea enviar datos al nodo D, primero debe encontrar una ruta hacia el nodo D con RREQ.

Los nodos de la red *ad hoc* pueden ser capaces también de conectarse a anfitriones que se encuentran en una red estática y también en sentido contrario. El enlace con la red estática se proporciona mediante nodos de pasarela opcionales. Estos anfitriones tienen una conexión normal a la red *ad hoc*, pero también rutas estáticas a otras redes.

Cuando un nodo envía un paquete cuyo destino está en una red estática, este paquete puede diferenciarse de los otros paquetes mediante el prefijo de red de la dirección IPv6 de destino. Cuando una pasarela recibe un RREQ cuyo destino prefijo pertenece a una red estática, responderá con un RREP. El RREP tendrá como remitente la dirección que estaba en el destino del RREQ y el HIT de originen será una dirección nula. Con este mecanismo, los nodos de la red *ad hoc* obtendrán acceso a la red estática cuando se consideran las direcciones IPv6.

Sin embargo, si el destino buscado es un HIT, el funcionamiento de la pasarela es diferente. Como no conoce los HIT de los nodos de la red estática y por lo tanto no sabe si el HIT buscado está en la red estática, no puede responder con un RREP que contiene el HIT de destino del RREQ. En su lugar, solo remite el RREQ como lo hace con otros RREQ.

El problema se resuelve utilizando un temporizador en el nodo emisor original. Cuando envía un RREQ en busca de un determinado HIT, añade una nueva entrada a una tabla denominada rreq-list. Esta entrada contiene un identificador (id) para el RREQ (rreq_id), el HIT buscado y se inicia un temporizador cuando se envía el RREQ. Cuando el temporizador está en marcha, los RREQ se retransmiten en la red, pero debido a que el HIT buscado pertenece a un anfitrión, que se encuentra en la red estática, el RREP no se envía nunca. Esta es una señal para el remitente y cuando el tiempo se acaba, se ejecuta una función que asignará el HIT a la dirección IPv6 del servidor de encuentro (RVS). Ahora, todo lo que el remitente tiene que hacer es encontrar una ruta a la dirección IPv6 del RVS y entonces iniciar el intercambio básico HIP con el propietario del HIT que el remitente estaba tratando de alcanzar.

Si el RVS retransmite el HIT a un nodo que se encuentra en una red estática diferente al RVS, hay un problema cuando el nodo de las redes *ad hoc* debe enviar atrás el paquete I2 de intercambio básico HIP. La tabla de encaminamiento del nodo no tiene una entrada para la nueva red, por lo que el núcleo no procesará en absoluto el paquete.

Para superar esto, se añade una función al código de pasarela de manera que mantiene una tabla que tiene conocimiento de qué nodos de diferentes redes estáticas han enviado paquetes a qué nodos de la red *ad hoc*. Si la pasarela observa, mientras reenvían paquetes a un nodo, que el remitente del paquete pertenece a una nueva red para el destino, en primer lugar enviará un RREQ al destino y sustituirá su propia dirección con la dirección original del remitente. Esto tiene el efecto de que una vez que el destino recibe el RREQ, añade el origen del paquete a sus tablas de encaminamiento y esto permite al nodo de redes *ad hoc* hacer un intercambio básico HIP con un nodo de una red estática desconocida sin ninguna configuración manual.

Si la conexión se inicia desde una red estática, se utilizan dos enfoques diferentes. El primer enfoque se utiliza cuando un nodo de la red estática quiere enviar un paquete IPv6 a uno de los nodos de la red *ad hoc*. Cuando el paquete llega a un nodo de pasarela, enviará un RREQ al anfitrión de destino. Esto se hace por dos razones. En primer lugar, si la pasarela no conoce la ruta hacia el destino en la red *ad hoc*, debe encontrarla antes de reenviar el paquete al siguiente nodo de salto apropiado. En segundo lugar, si el destino no ha recibido ningún paquete de esta red antes, de nuevo se debe enviar un RREQ con el fin de añadir una ruta al destino que alberga las tablas de encaminamiento. Si estas dos condiciones se cumplen, el nodo de pasarela puede reenviar libremente el paquete hacia el nodo de destino.

El segundo enfoque se utiliza cuando un nodo de redes estáticas necesita establecer una conexión con un nodo que pertenece a una red *ad hoc* utilizando HIT. Esto requiere que el nodo contestador se haya registrado previamente en la RVS. Además, el iniciador debe asignar el HIT del contestador al RVS, porque los HIT no se pueden encaminar en la red estática. Después de la asignación, el I1 se redirige hacia el destino y se realizan los mismos procedimientos de pasarela de la misma manera como se explicó anteriormente.

Se envían paquetes RREP como tráfico en unidifusión en SAODV de manera que no hay necesidad de modificar ese comportamiento. Sin embargo, esos paquetes fueron entregados de manera insegura de manera que se alteró el camino predeterminado del SAODV para manejar los RREP. Ahora se envían con un HIT siempre en el campo de destino. A continuación se describen ejemplos de formatos de mensaje para HOLA, RREQ y RREP.

El formato del mensaje de HOLA (*HELLO*) puede ser como sigue:

```
Hello->pkt_type          = HELLO;
Hello->no_reply          = no_reply_n;
Hello->hit               = local_hit;
Hello->no_of_hello       = no_of_hello;

typedef struct {//multicast
u_int8_t                 pkt_type;
u_int8_t                 no_reply;
in6_addr_t               hit;
u_int32_t                no_of_hello;
} Chello;
```

El formato del mensaje RREQ puede ser como sigue:

```
rreq->pkt_type           = RREQ;
rreq->dest_ipaddr        = dest_ipaddr;
rreq->source_ipaddr      = own_ipaddr;
rreq->source_hit         = own_hit;
rreq->last_ipv6          = own_ipaddr;
rreq->rreq_id            = no_of _rreq ;
rreq->hop_count          = RREQ_HOP_COUNT ;
rreq->seq_no             = own_rreq_seq_no;
```

```
typedef struct { //unicast
u_int8_t            pkt_type ;
in6_addr_t          dest_ipaddr;
in6_addr_t          source_ipaddr;
in6_addr_t          source_hit;
in6_addr_t          last_ipv6;
u_int8_t            seq_no;
u_int8_t            hop_count;
u_int32_t           rreq_id; } Crreq;
```

El formato del mensaje RREP puede ser como sigue:

```
rrep->pkt__type          = RREP;
rrep->source_ipaddr      = own_ipaddr;
rrep->source_hit         = own_hit;
rrep->last_ipv6          = own_ipaddr;
rrep->dest_ipaddr        = dest_ipaddr;
rrep->seq_num            = seq_num;
rrep->rreq_id            = rreq_id;
```

```
typedef struct { //unicast
u_int8_t            pkt_type;
in6_addr_t          source_ipaddr ;
in6_addr_t          source_hit;
in6_addr_t          dest_ipaddr ;
in6_addr_t          last_ipv6;
u_int 8_t           seq_num;
u_int32_t           rreq_id;
} Crrep;
```

En la figura 9 se ilustra adicionalmente cómo pueden formarse un mensaje RREQ 900 especial y un mensaje RREP 902 especial cuando se integra SAODV con HIP. Los campos del mensaje RREQ 900 se explican a continuación.

HIT o dirección IP de destino: La dirección IP o el HIT del destino para el que se desea una ruta.

Dirección IP del originador: La dirección IP del nodo que originó el RREQ.

HIT del originador: El HIT del nodo que originó el RREQ.

Última Dirección IP: La última dirección IP lleva la dirección IPv6 del último anfitrión que ha procesado este mensaje. Es necesaria porque cuando el RREQ se envía por la conexión de HIP, el receptor ve el paquete que viene de un HIT y no de una dirección IPv6.

ID RREQ: ID RREQ se añade para permitir las conexiones a las redes estáticas. Cuando un nodo envía un RREQ en busca de un determinado HIT, añade una nueva entrada a una tabla denominada rreq-list. Esta entrada contiene un identificador para el RREQ (rreq_id), el HIT buscado y se inicia un temporizador cuando se envía el RREQ. Cuando el temporizador está en marcha, los RREQ se reenvían en la red, pero debido a que el HIT buscado pertenece a un anfitrión que se encuentra en la red estática, el RREP no se envía nunca.

Cuenta de saltos: El número de saltos desde la Dirección IP del originador al nodo que maneja la solicitud.

Número de secuencia del originador: El número de secuencia actual a utilizar en la entrada de la ruta que apunta hacia el originador del RREQ.

Los campos del mensaje RREQ 902 se explican a continuación.

Dirección IP del originador: La dirección IP del nodo que originó el RREQ para el que se suministra la ruta.

HIT del originador: El HIT del nodo que originó el RREQ.

Última Dirección IP: La última dirección IP lleva la dirección IPv6 del último anfitrión que ha procesado el mensaje.

HIT o dirección IP de destino: La dirección IP o el HIT del destino para el cual se suministra una ruta.

Número de secuencia del destino: El número de secuencia de destino asociado con la ruta.

ID RREQ: ID RREQ se añade para permitir las conexiones a las redes estáticas.

Obsérvese que el campo de salto siguiente antiguo de SAODV se ha caído ya que no tiene ningún uso más porque el siguiente salto se comprueba cada vez en la propia tabla de encaminamiento del SAODV cuando se envía o reenvía un paquete.

La figura 10 ilustra otros formatos posibles para el mensaje RREQ 1000 y el mensaje RREP 1002 cuando se integra AODV con HIP en un entorno IP versión 6. Los campos nuevos o modificados en texto en negrita: ID RREQ, HIT de destino, HIT de originador y última dirección IP.

La figura 11 ilustra otros formatos posibles para el mensaje RREQ 1100 y el mensaje RREP 1102 cuando se integra AODV con HIP en un entorno IP versión 4. Los campos nuevos o modificados en texto en negrita: ID RREQ, LSI de destino, LSI de originador y última dirección IP. Aunque la invención se ha descrito anteriormente con referencia a un ejemplo de acuerdo a los dibujos adjuntos, es evidente que la invención no se limita al mismo sino que se puede modificar de varias maneras dentro del alcance de las reivindicaciones anexas.

REIVINDICACIONES

1. Un aparato que comprende:

un transmisor-receptor (500) configurado para comunicarse de forma inalámbrica con otros aparatos;

un módulo de interfaz (504) configurado para introducir un identificador de auto-certificación del aparato, el identificador de auto-certificación se refiere a un identificador que puede verificarse sin consultar o confiar en un tercero; y

un módulo de procesamiento (502), acoplado con el transmisor-receptor inalámbrico (500) y el módulo de interfaz (504), configurado para realizar un proceso de autenticación que utiliza el identificador de auto-certificación del aparato con otros aparatos dentro del alcance del transmisor-receptor (500);

caracterizado porque el módulo de procesamiento (502) también se configura para añadir rutas a esos otros aparatos que hayan pasado el proceso de autenticación a una tabla de encaminamiento (510), para buscar por lo menos una ruta desde la tabla de encaminamiento (510), y para la unidifusión de una solicitud de ruta cifrada que incluye un identificador de auto-certificación de un aparato de destino a través de la por lo menos una ruta.

2. El aparato de la reivindicación 1, en el que el módulo de interfaz (504) se configura además para introducir información en identificadores de auto-certificación de otros aparatos amistosos, y el módulo de procesamiento (502) también se configura para utilizar la información en los identificadores de auto-certificación de los otros aparatos amistosos en el proceso de autenticación.

3. El aparato de la reivindicación 1 ó 2, en el que el módulo de procesamiento (502) se configura además para colocar el identificador de auto-certificación del aparato en un mensaje de hola, y para la multidifusión del mensaje de hola a los otros aparatos en el alcance del transmisor-receptor inalámbrico (500) como parte del proceso de autenticación.

4. El aparato de la reivindicación 3, en el que el módulo de procesamiento (502) se configura además para colocar una dirección de protocolo de internet del aparato en el mensaje de hola.

5. El aparato según cualquier reivindicación anterior, en el que el módulo de procesamiento (502) se configura además para mantener una tabla de asignaciones (512) que incluye pares de identificador de auto-certificación/dirección de protocolo de internet de los otros aparatos, y para eliminar esos otros aparatos que no pasen el proceso de autenticación de la tabla de asignación (512).

6. El aparato según cualquier reivindicación anterior, en el que el módulo de procesamiento (502) se configura además para recibir una respuesta cifrada de ruta a través de por lo menos una ruta, y añadir una ruta al aparato de destino, incluyendo la dirección del otro aparato que ha transmitido la respuesta de ruta, a la tabla de encaminamiento (510).

7. El aparato según cualquier reivindicación anterior de 1 a 5, en el que el módulo de procesamiento (502) se configura además para medir el tiempo de la unidifusión de la solicitud de ruta, y si no se recibe una respuesta cifrada de ruta en un período de tiempo predeterminado después de la unidifusión de la solicitud de ruta, añadir una ruta al aparato de destino, incluyendo una dirección de un servidor de encaminamiento de una red estática, a la tabla de encaminamiento (510).

8. El aparato según cualquier reivindicación anterior de 1 a 5, en el que el módulo de procesamiento (502) se configura además para colocar el identificador de auto-certificación del aparato en la solicitud de ruta.

9. El aparato según cualquier reivindicación anterior, en el que el módulo de procesamiento (502) se configura además para realizar un proceso de autenticación utilizando el identificador de auto-certificación del aparato con el aparato de destino a través de la ruta al aparato de destino.

10. El aparato de la reivindicación 9, en el que el módulo de procesamiento (502) se configura además para el intercambio de datos cifrados con el aparato de destino a través de la ruta hacia el aparato de destino.

11. El aparato según cualquier reivindicación anterior, en el que el módulo de procesamiento (502) se configura además para funcionar en un entorno de red dinámica.

12. El aparato según cualquier reivindicación anterior, en el que el módulo de procesamiento (502) se configura además para utilizar una etiqueta de identidad de anfitrión de un protocolo de identidad de anfitrión como identificador de auto-certificación.

13. El aparato según cualquier reivindicación anterior, en el que el módulo de procesamiento (502) se configura además para utilizar un intercambio básico de protocolo de identidad de anfitrión como parte del proceso de autenticación.

14. Un método que comprende:

introducir (802) un identificador de auto-certificación del aparato en el aparato, el identificador de auto-certificación hace referencia a un identificador que puede verificarse sin consultar o confiar en un tercero; y

el aparato realiza (804) un proceso de autenticación utilizando el identificador de auto-certificación del aparato con otros aparatos dentro del alcance de comunicación inalámbrica del aparato;

caracterizado porque el método comprende además:

añadir (806) rutas a esos otros aparatos que pasaron el proceso de autenticación a una tabla de encaminamiento;

ir a buscar por lo menos una ruta de la tabla de encaminamiento, y

enviar por unidifusión una solicitud de ruta cifrada que incluye un identificador de auto-certificación de un aparato de destino a través de por la lo menos una ruta.

15. El método de la reivindicación 14, que comprende además:

introducir información en identificadores de auto-certificación de otros aparatos amistosos; y

utilizar la información en los identificadores de auto-certificación de los otros aparatos amistosos en el proceso de autenticación.

16. El método de la reivindicación 14 ó 15, que comprende además:

colocar el identificador de auto-certificación de los aparatos en un mensaje de hola; y

enviar por multidifusión el mensaje de hola a los otros aparatos en el alcance de comunicación inalámbrica del aparato como parte del proceso de autenticación.

17. El método de la reivindicación 16, que comprende además:

colocar una dirección de protocolo de internet del aparato en el mensaje de hola.

18. El método según cualquiera de las reivindicaciones anteriores 14 a 17, que comprende además:

mantener una tabla de asignaciones que incluye pares de identificador de auto-certificación/dirección de protocolo de internet de los otros aparatos;

eliminar esos otros aparatos que no pasen el proceso de autenticación a partir de la tabla de asignaciones.

19. El método según cualquiera de las reivindicaciones anteriores 14 a 18, que comprende además:

recibir una respuesta cifrada de ruta a través de la por lo menos una ruta; y

añadir una ruta al aparato de destino, incluyendo la dirección del otro aparato que ha transmitido la respuesta de ruta, a la tabla de encaminamiento.

20. El método según cualquiera de las reivindicaciones anteriores 14 a 18, que comprende además:

medir el tiempo de unidifusión de la solicitud de ruta; y

añadir una ruta al aparato de destino, incluyendo una dirección de un nodo de pasarela a una red estática, a la tabla de encaminamiento, si no se recibe una respuesta cifrada de ruta en un período de tiempo predeterminado después de la unidifusión de la solicitud de ruta.

21. El método según cualquiera de las reivindicaciones anteriores 14 a 18, que comprende además:

colocar el identificador de auto-certificación del aparato en la solicitud de ruta.

22. El método según cualquiera de las reivindicaciones anteriores 14 a 21, que comprende además:

realizar un proceso de autenticación utilizando el identificador de auto-certificación del aparato con el aparato de destino a través de la ruta al aparato de destino.

23. El método de la reivindicación 22, que comprende además:

intercambiar datos cifrados con el aparato de destino a través de la ruta hacia el aparato de destino.

24. El método según cualquiera de las reivindicaciones anteriores 14 a 23, que comprende además:

funcionar en un entorno de red dinámica.

25. El método según cualquiera de las reivindicaciones anteriores 14 a 24, que comprende además:

utilizar una etiqueta de identidad de anfitrión de un protocolo de identidad de anfitrión como el identificador de auto-certificación.

26. El método según cualquiera de las reivindicaciones anteriores hasta la 25, que comprende además:

utilizar un intercambio básico de protocolo de identidad de anfitrión como parte del proceso de autenticación.

27. Un programa informático que comprende medios de codificación adaptados para realizar las etapas del método de las reivindicaciones 14-26.

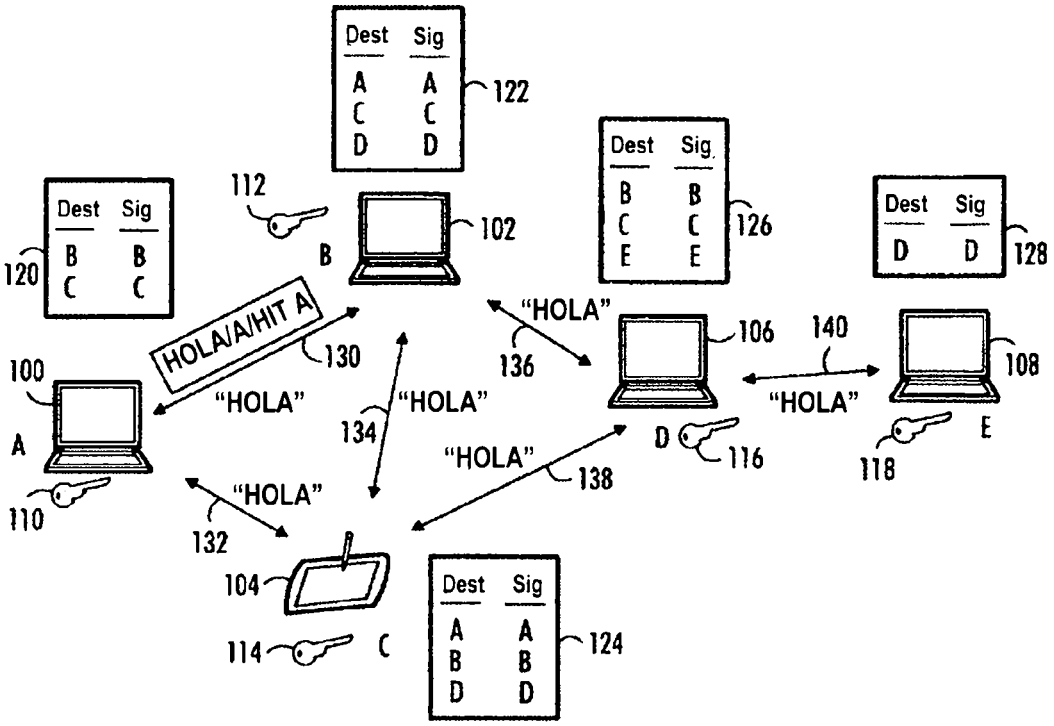

Dest Sig
A A
C C
D D
122
Dest Sig
B B
C C
120
Dest Sig
B B
C C
126
Dest Sig
D D
128
112
B
102
HOLA/A/HIT A
130
"HOLA"
100
A
110
"HOLA"
134
"HOLA"
136
106
140
108
"HOLA"
D
116
E
118
"HOLA"
138
"HOLA"
132
104
114
C
Dest Sig
A A
B B
D D
124

FIG. 1

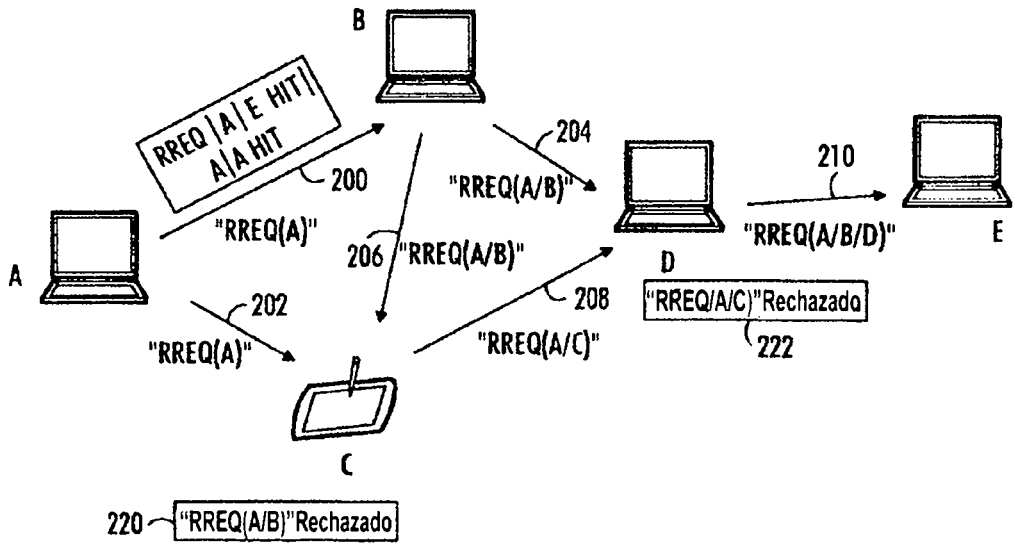

B
RREQ|A|E HIT|
A|A HIT
200
"RREQ(A)"
204
"RREQ(A/B)"
210
"RREQ(A/B/D)"
A
206 "RREQ(A/B)"
D
E
202
"RREQ(A)"
208
"RREQ(A/C)"
"RREQ/A/C)"Rechazado
222
C
220
"RREQ(A/B)"Rechazado

FIG. 2

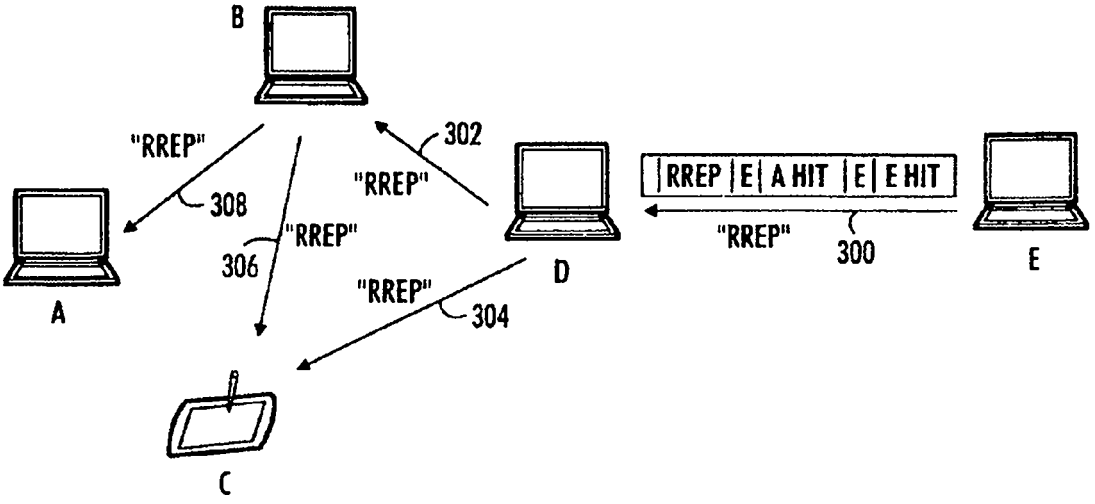

B
"RREP"
308
302
"RREP"
"RREP"
306
"RREP"
304
A
D
C
RREP | E | A HIT | E | E HIT
"RREP"
300
E

FIG. 3

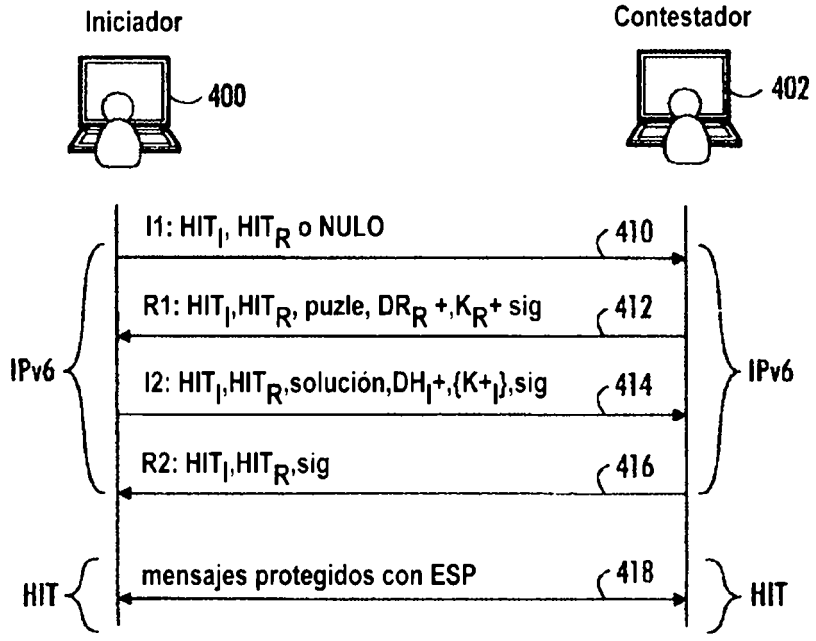

Iniciador
400
Contestador
402
I1: HIT$_I$, HIT$_R$ o NULO
410
R1: HIT$_I$,HIT$_R$, puzle, DR$_R$ +,K$_R$+ sig
412
I2: HIT$_I$,HIT$_R$,solución,DH$_I$+,{K+$_I$},sig
414
R2: HIT$_I$,HIT$_R$,sig
416
mensajes protegidos con ESP
418
IPv6
IPv6
HIT
HIT

FIG. 4

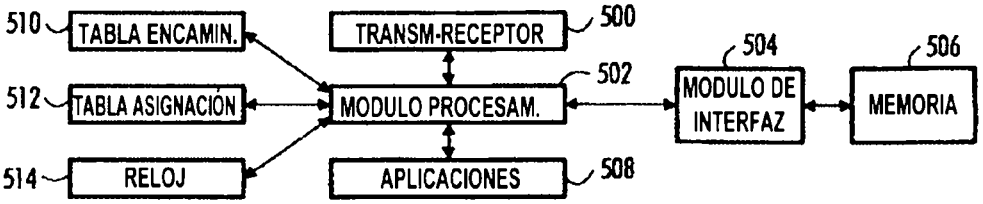


FIG. 5

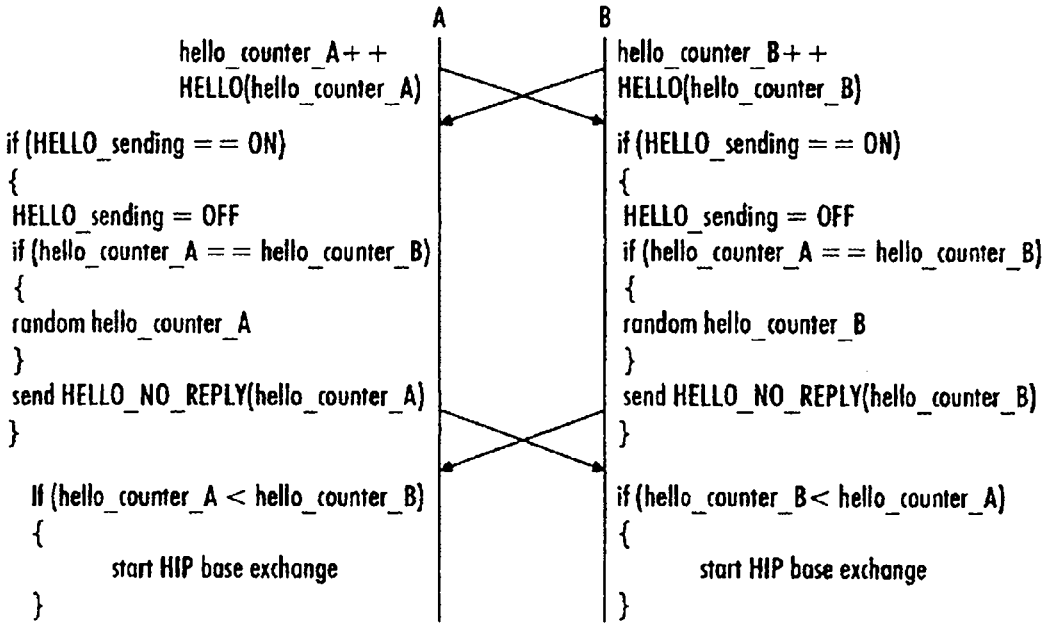


FIG. 7

FIG. 8

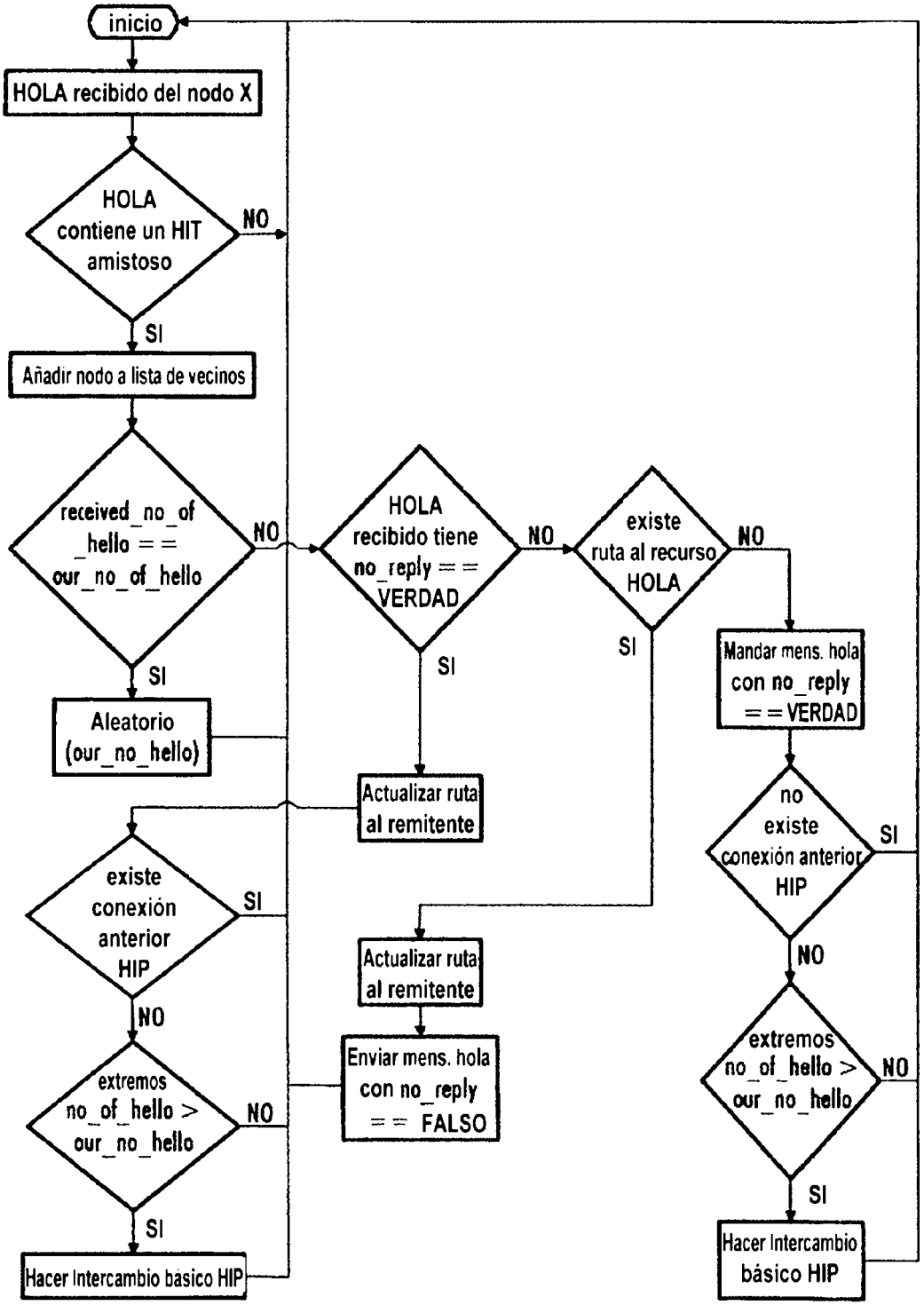
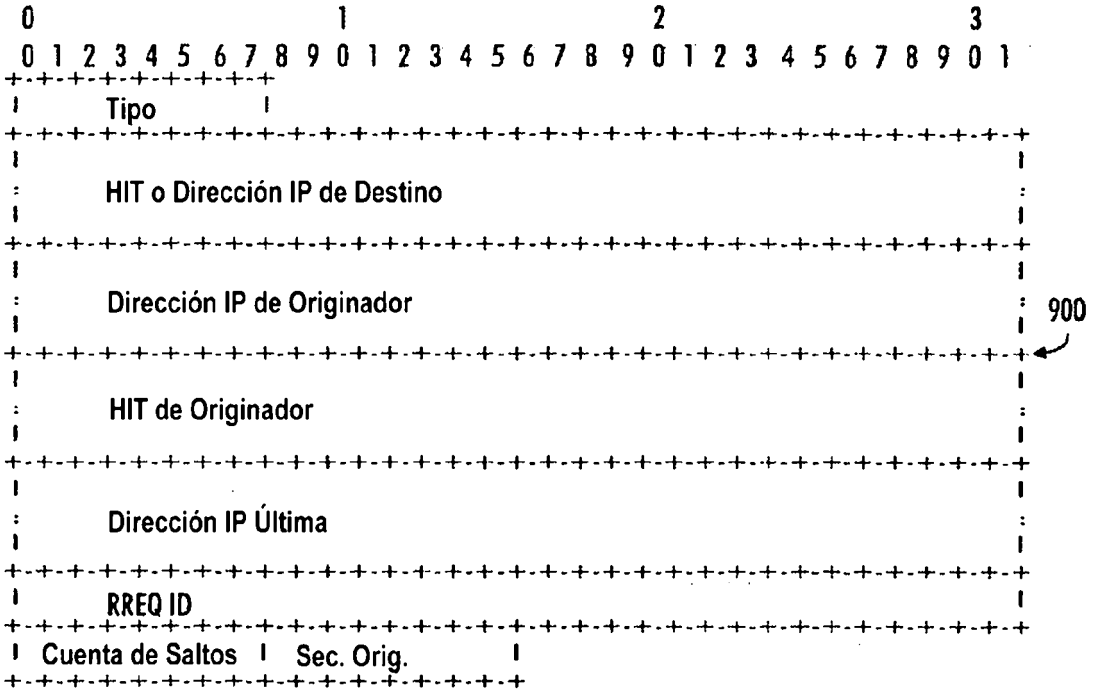

inicio
HOLA recibido del nodo X
HOLA contiene un HIT amistoso
NO
SI
Añadir nodo a lista de vecinos
received_no_of_hello == our_no_of_hello
NO
SI
Aleatorio (our_no_hello)
HOLA recibido tiene no_reply == VERDAD
NO
SI
existe ruta al recurso HOLA
NO
SI
Mandar mens. hola con no_reply == VERDAD
Actualizar ruta al remitente
existe conexión anterior HIP
SI
NO
Actualizar ruta al remitente
Enviar mens. hola con no_reply == FALSO
extremos no_of_hello > our_no_hello
NO
SI
Hacer Intercambio básico HIP
no existe conexión anterior HIP
SI
NO
extremos no_of_hello > our_no_hello
NO
SI
Hacer Intercambio básico HIP

FIG. 6


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Tipo
HIT o Dirección IP de Destino
Dirección IP de Originador
900
HIT de Originador
Dirección IP Última
RREQ ID
Cuenta de Saltos
Sec. Orig.

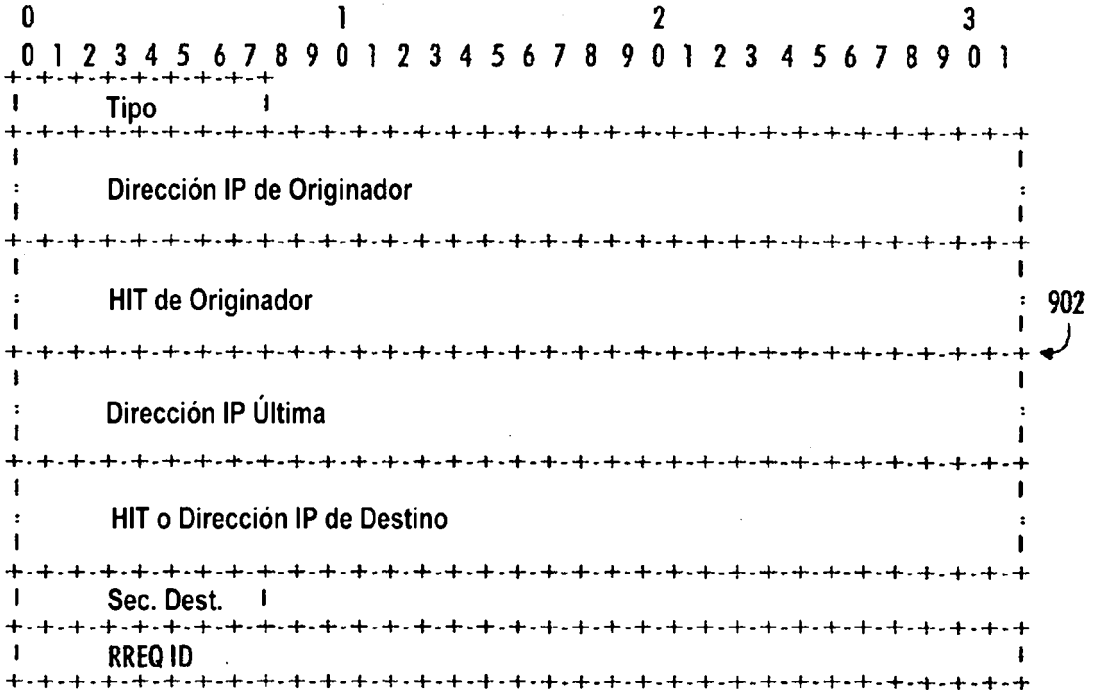

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Tipo
Dirección IP de Originador
HIT de Originador
902
Dirección IP Última
HIT o Dirección IP de Destino
Sec. Dest.
RREQ ID

FIG. 9

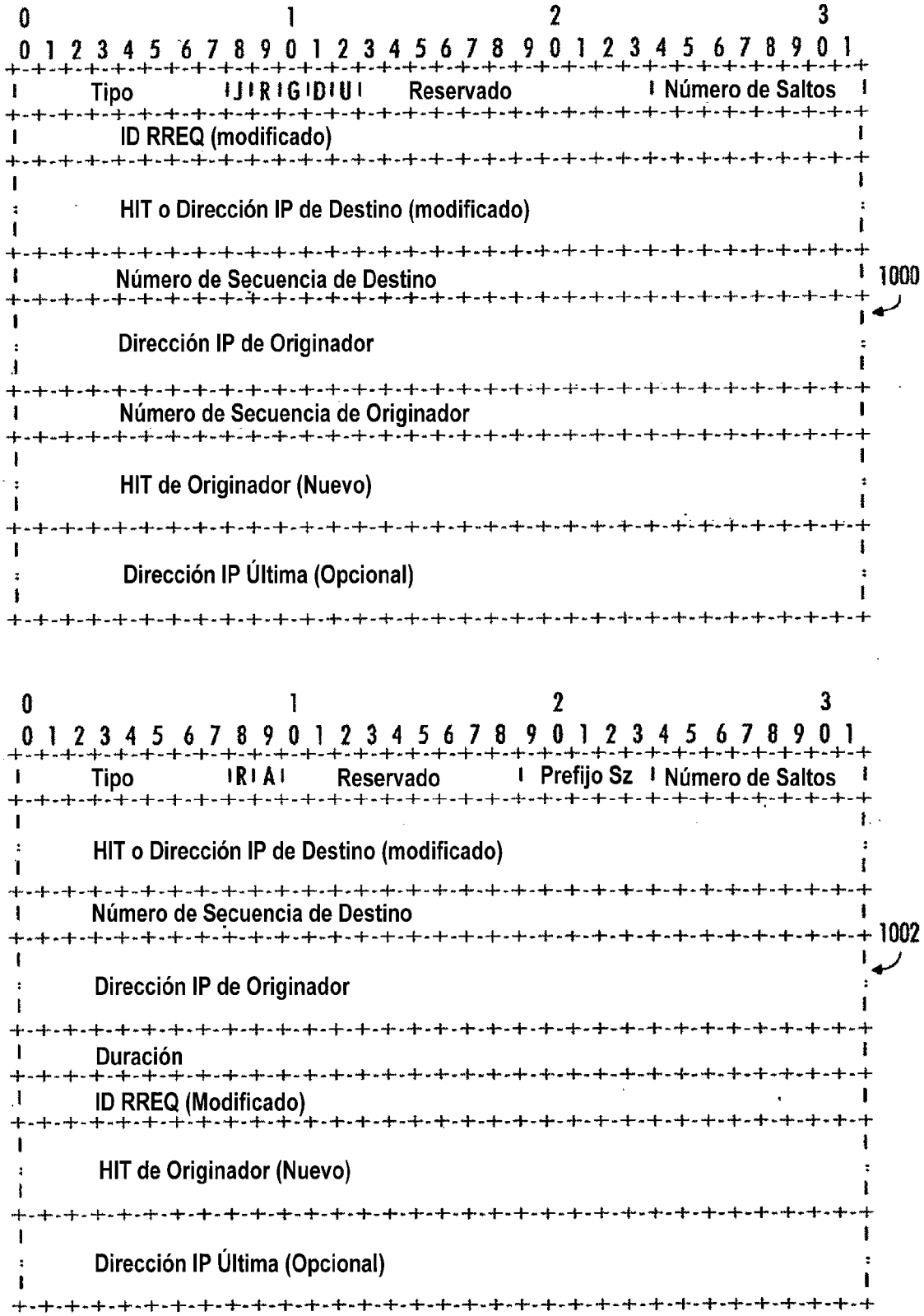

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Tipo
J R G D U
Reservado
Número de Saltos
ID RREQ (modificado)
HIT o Dirección IP de Destino (modificado)
Número de Secuencia de Destino
1000
Dirección IP de Originador
Número de Secuencia de Originador
HIT de Originador (Nuevo)
Dirección IP Última (Opcional)
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Tipo
R A
Reservado
Prefijo Sz
Número de Saltos
HIT o Dirección IP de Destino (modificado)
Número de Secuencia de Destino
1002
Dirección IP de Originador
Duración
ID RREQ (Modificado)
HIT de Originador (Nuevo)
Dirección IP Última (Opcional)

FIG. 10


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Tipo
J R G D U
Reservado
Número de Saltos
ID RREQ (modificada)
LSI o Dirección IP de Destino (modificado)
Número de Secuencia de Destino
Dirección IP del Originador
Número de Secuencia del Originador
LSI del Originador (Nuevo)
Dirección IP Última (Opcional)
1100


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Tipo
R A
Reservado
Prefijo Sz
Número de Saltos
LSI o Dirección IP de Destino (modificado)
Número de Secuencia de Destino
Dirección IP del Originador
Duración
LSI del Originador (Nuevo)
Dirección IP Última (Opcional)
1102

FIG. 11