(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 368 566**

(51) Int. CI.:
H04L 12/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04766569 .0**
(96) Fecha de presentación: **20.08.2004**
(97) Número de publicación de la solicitud: **1782574**
(97) Fecha de publicación de la solicitud: **09.05.2007**

(54) Título: **CONEXIÓN RÁPIDA A RED.**

(45) Fecha de publicación de la mención BOPI:
18.11.2011

(45) Fecha de la publicación del folleto de la patente:
18.11.2011

(73) Titular/es:
TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)
164 83 STOCKHOLM, SE

(72) Inventor/es:
ARKKO, Jari y
NIKANDER, Pekka

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

DESCRIPCIÓN

Conexión rápida a red.

Campo de la invención

La presente invención se refiere a un mecanismo de conexión rápida a red para una red inalámbrica móvil.

Antecedentes de la invención

En el contexto de una red inalámbrica de comunicaciones móviles, el término "conexión" se refiere al procedimiento mediante el cual un dispositivo de usuario se conecta a una red inalámbrica doméstica (tal como un punto de acceso LAN inalámbrico) y es capaz de usar al menos algunos de los servicios ofrecidos por esa red. En la práctica, este procedimiento implica múltiples capas de protocolos relacionadas, por ejemplo, con la identificación de las frecuencias de radio correctas, negociación de capa de radio para permitir las comunicaciones con el punto de acceso, procedimientos de autorización y autenticación de acceso a red, iniciación de protección de seguridad de la capa de enlace, búsqueda de enrutadores y direcciones en la capa IP, y restablecimiento de los mecanismos de movilidad a una nueva dirección IP. Desafortunadamente, estas tareas requieren tiempo para completarse, y la interacción y los efectos generales de las tareas individuales no se comprenden bien, porque la mayoría del trabajo sobre temas de acceso inalámbrico se ha centrado sólo en un aspecto particular.

Un área con probabilidades de sufrir particularmente un fallo debido a temas de interrelación de múltiples protocolos es el de la movilidad entre diferentes tipos de redes. Por ejemplo, los investigadores en esta área han tendido a ignorar los efectos de tener que tener un control de acceso en el enlace (necesario debido a requerimientos legales y/o de negocios). Los usuarios reales están sólo empezando a aprovechar la movilidad entre diferentes tipos de redes y, por lo tanto, los problemas asociados no han sido vistos o apreciados completamente.

IP móvil es un conjunto de protocolos que permiten la itinerancia de los abonados entre redes de acceso, mientras que al mismo tiempo aseguran que los abonados son accesibles por nodos correspondientes que no conocen las ubicaciones actuales de los abonados. La Figura 1 ilustra esquemáticamente una arquitectura de red para la implementación de IP móvil. Un abonado 1 está conectado a un enrutador 2 de acceso de una red 3 de acceso. Es fundamental para IP móvil la provisión de un agente 4 doméstico en una red 5 doméstica del abonado, el cual conoce la ubicación actual del abonado 1 (la ubicación actual se define por una dirección IP conocida como "dirección dinámica") y es capaz de enrutar los mensajes dirigidos a la dirección IP fija del abonado a la ubicación actual. Se usan mensajes de actualización de unión para permitir que el abonado 1 actualice su dirección dinámica en el agente 4 doméstico, por ejemplo, en el caso en el que el abonado realiza una itinerancia a una nueva red de acceso. Cuando un abonado cambia su dirección dinámica, un procedimiento de optimización de ruta puede ser invocado para garantizar que los paquetes enviados posteriormente desde los servidores 6 correspondientes conectados a las redes 7 de acceso respectivas son enrutados al abonado a través de la ruta óptima. Un servidor 8 de autenticación, autorización y contabilidad (AAA), situado en la red 5 doméstica, se comunica con el agente 4 doméstico.

En el caso del protocolo de Internet, versión 6 (IPv6), el procedimiento de conexión a red en un enlace inalámbrico típico es el siguiente:

- Conexión de capa de enlace, tal como la detección y la conexión a un punto de acceso de una red de área local inalámbrica (LAN) específica.

- Procedimientos de control de acceso. Para ello, se usan mecanismos tales como 802.1 X y EAP. Típicamente, esto implica tres mensajes de control EAP (solicitud de identidad, respuesta y éxito, encapsulados en el mensaje EAPOL-éxito), y un procedimiento de autenticación específico. Los procedimientos de autenticación sencillos se completan en dos mensajes, pero muchos procedimientos requieren más.

- Búsqueda de enrutador. Este es el procedimiento de búsqueda del enrutador por defecto para el nodo y la determinación de los prefijos de enrutamiento para este enlace. En el caso más simple, esto requiere dos mensajes, con un período de espera entre los mismos.

- Detección de direcciones duplicadas (Duplicate Address Detection, DAD). Esto se usa para garantizar que la dirección que el nodo móvil selecciona para su uso en este enlace es única. Típicamente, esto implica un mensaje y un período de espera.

- Procedimientos de gestión de movilidad. Estos incluyen una mensajería con un agente doméstico y, posiblemente, con los nodos correspondientes y un enrutador previo. La mensajería consiste, típicamente, en dos mensajes intercambiados entre el terminal de usuario y el agente doméstico, cinco mensajes (parcialmente simultáneos) con cada nodo correspondiente y un mensaje con el enrutador previo.

El protocolo de Internet, versión 4 (Ipv4), se comporta, en gran medida, de la misma manera que el IPv6. Sin embargo, la búsqueda de enrutador, la búsqueda de vecindad y la autoconfiguración de direcciones son

reemplazadas por el protocolo de control de servidor dinámico (Dynamic Host Control Protocol, DHCP), y no hay soporte para DAD. DHCP requiere, típicamente, cuatro mensajes. IPv4 móvil no tiene optimización de ruta y, por lo tanto, implica sólo dos mensajes adicionales relacionados con la movilidad. En IPv4 no hay soporte para un traspaso suave desde un enrutador de acceso antiguo a uno nuevo.

En resumen, con Ipv6, hay al menos 16 mensajes en el caso completo, suponiendo que hay sólo un nodo correspondiente, y dos períodos de espera distintos (aunque cuatro de los mensajes pueden ser enviados en paralelo). En el caso de IPv4, el número de mensajes es algo menor debido a la menor funcionalidad de IPv4 y al papel central de DHCP. Sin embargo, todavía se necesitan al menos 11 mensajes.

Se está trabajando para tratar de optimizar algunos de los procedimientos de señalización expuestos anteriormente. En particular:

- La denominada DAD “optimizada" intenta evitar los retrasos asociados con DAD, y puede permitir también el uso de la dirección provisional antes de que DAD se haya completado. El beneficio potencial de este enfoque es la eliminación de un período de espera, y un posible paralelismo adicional en la secuencia de mensajes. Otro enfoque propuesto usa el enrutador de acceso para ayudar en el procedimiento DAD.

- Detección optimizada de movimiento intenta hacer que se detecte más rápidamente cuándo se ha producido un movimiento (de un terminal de usuario), y para identificar los parámetros de red en la nueva red. Esto implica nuevos algoritmos para la reducción de los periodos de espera asociados con la publicidad del enrutador IPv6, pero no reduce la cantidad total de mensajes.

- IP móvil jerárquica (HMIP) intenta localizar movimientos, de manera que el número de actualizaciones de ubicación enviadas al agente doméstico y a los nodos correspondientes pueda ser minimizado.

Estos enfoques de optimización se refieren principalmente a la eliminación de tiempos de espera innecesarios. No parecen tener un impacto significativo en la cantidad de señalización necesaria, con la excepción de HMIP. Sin embargo, HMIP no reduce la cantidad de señalización básica de acceso a la red, sólo acorta el camino que debe tomar esta señalización.

El documento WO01/76134 describe un procedimiento de autenticación y acuerdo de clave para permitir a un nodo móvil y a una red de datos por paquetes generar un clave de sesión secreta, compartida.

Resumen de la invención

Un objeto de la presente invención es reducir el número de mensajes necesarios para facilitar un acceso a red de un nodo móvil. Esto se consigue delegando, de manera segura, determinadas tareas, realizadas actualmente por el nodo móvil, a un enrutador de acceso de la red de acceso.

Un objeto de la invención es proporcionar un esquema conocido como esquema de seguridad basado en delegación, en lugar de enviar mensajes extremo a extremo entre el nodo móvil y cualquier entidad de red troncal con la que tiene que hablar, envía certificados desde el nodo móvil a un enrutador de acceso, que delega algunas de las tareas al enrutador de acceso, que de otra manera tendrían que ser realizadas por el nodo móvil.

Según un primer aspecto de la presente invención, se proporciona un procedimiento para facilitar un acceso de protocolo de Internet por un nodo móvil a una red de acceso, comprendiendo el procedimiento:

enviar una solicitud de conexión desde el nodo móvil a un enrutador de acceso de la red de acceso, conteniendo la solicitud un identificador de nodo móvil y un identificador de interfaz o medios para derivar un identificador de interfaz, y estando firmada por el nodo móvil usando una calve privada de un par de claves privada-pública, para permitir que el mensaje sea autenticado como procedente de un nodo móvil, y

recibir la solicitud en el enrutador de acceso y autenticar el mensaje en el mismo, usando la firma y la clave pública de dicho par de claves privada-pública, caracterizado porque

en respuesta a la recepción y autenticación del mensaje, realiza un conjunto predefinido de tareas delegadas al enrutador de acceso y que son necesarias para autorizar el nodo móvil y facilitar, de esta manera, dicho acceso, y

devolver un acuse de recibo desde el enrutador de acceso al nodo móvil, confirmando el permiso de acceso, conteniendo el acuse de recibo un prefijo de enrutamiento de red y medios para autenticar el enrutador de acceso al nodo móvil.

La aplicación de la presente invención puede resultar en una reducción considerable en el número de mensajes de señalización necesarios para proporcionar una conexión a red para un nodo móvil, mediante la aplicación de un enfoque holístico en lugar de centrarse en tareas y protocolos particulares. Mejora las posibilidades de una itinerancia casi transparente entre redes de acceso.

Preferentemente, la solicitud de conexión contiene uno o más de los elementos siguientes:

identificador de acceso a red (NAI) del nodo móvil,

clave pública propia del nodo móvil,

una raíz de confianza para cualquier enrutador de acceso que el nodo móvil desea aceptar, una dirección del agente doméstico del nodo móvil,

direcciones de los nodos correspondientes con los que el nodo móvil desea establecer una optimización de ruta,

un identificador de interfaz (IID), construido mediante generación criptográfica de direcciones (Cryptographically Generated Address, CGA),

la identidad del enrutador de acceso (si se conoce),

los parámetros deseados para la conexión de enlace inalámbrico (si es necesario),

una cookie, calculada en una manera conocida sólo por el nodo móvil,

una firma, firmada con la clave privada del nodo móvil.

Preferentemente, la recepción de la solicitud de conexión en el enrutador de acceso desencadena uno o más de los procedimientos siguientes en el enrutador de acceso:

Conexión en capa de enlace;

Un procedimiento de control de acceso;

Búsqueda de enrutador;

Generación de dirección IP:

Detección de direcciones duplicadas

Preferentemente, dicho conjunto predefinido de tareas comprende:

Implementar un procedimiento de acceso, autorización y contabilidad con una infraestructura adecuada (AAA servidor) en la red doméstica del nodo móvil;

Realizar una actualización de unión en nombre del nodo móvil con un agente doméstico del nodo móvil;

Realizar una optimización de ruta con uno o más nodos correspondientes del nodo móvil.

Según un segundo aspecto de la presente invención, se proporciona un procedimiento de funcionamiento de un nodo móvil para facilitar un acceso de protocolo de Internet por parte del nodo móvil a una red de acceso, comprendiendo el procedimiento el envío de una solicitud de conexión desde el nodo móvil a un enrutador de acceso de la red de acceso, conteniendo la solicitud un identificador de nodo móvil y un identificador de interfaz o medios para derivar un identificador de interfaz, y estando firmada por el nodo móvil usando una clave privada de un par de claves privada-pública, para permitir que el mensaje sea autenticado por el enrutador de acceso como procedente de ese nodo móvil, caracterizado porque el mensaje contiene una autorización para el enrutador de acceso para realizar un conjunto predefinido de tareas delegadas al enrutador de acceso y que son necesarias para autorizar al nodo móvil y, de esta manera, facilitar dicho acceso

Según un tercer aspecto de la presente invención, se proporciona un procedimiento de funcionamiento de un enrutador de acceso dispuesto para facilitar el acceso de protocolo de Internet por parte de un nodo móvil a una red de acceso, comprendiendo el procedimiento:

recibir una solicitud de acceso en el enrutador de acceso y autenticar el mensaje en el mismo usando la firma y una clave pública de un par de claves privada-pública, y,

en respuesta a la recepción y autenticación del mensaje, caracterizado por las etapas de

realizar un conjunto predefinido de tareas delegadas al enrutador de acceso, las cuales son necesarias para autorizar al nodo móvil y facilitar, de esta manera, dicho acceso, y

devolver un acuse de recibo desde el enrutador de acceso al nodo móvil, confirmando el permiso de acceso, conteniendo el acuse de recibo un prefijo de red (enrutamiento) y medios para autenticar el enrutador de acceso al nodo móvil.

Otros aspectos de la invención se exponen en las reivindicaciones adjuntas.

Breve descripción de los dibujos

La Figura 1 ilustra esquemáticamente una arquitectura de sistema de comunicación móvil que emplea IP móvil, y

La Figura 2 muestra una señalización asociada a un procedimiento de conexión rápida a red.

Descripción detallada de ciertas realizaciones

Al optimizar el procedimiento de conexión a red para un nodo móvil, deben tenerse en cuenta una serie de requisitos básicos. Desde el punto de vista del nodo móvil, el nodo móvil necesita demostrar a la red de acceso que tiene un derecho de acceso. También necesita demostrar al agente doméstico que tiene un derecho a actualizar su información de unión almacenada en el mismo, y a los nodos correspondientes que está accesible en la dirección doméstica y en la dirección dinámica. Finalmente, el nodo móvil necesita demostrar a otros nodos en la red visitada que es propietario de su dirección dinámica. Otros requisitos son:

- El enrutador doméstico necesita demostrar su autoridad al nodo móvil, tanto en términos de autenticación de acceso como en términos de capacidad de actuar como un enrutador.
- La infraestructura de acceso, autorización y contabilidad (AAA) necesita tener una prueba de que el nodo móvil es quien dice ser (para garantizar la seguridad y confirmar que se realizará el pago).
- El agente doméstico necesita tener una prueba de que el nodo móvil ha solicitado, de hecho, una actualización de ubicación.
- El procedimiento de conexión a red eficiente propuesto en la presente memoria se basa en las construcciones siguientes:
- Una única solicitud (junto con sus credenciales asociadas) para que la red de acceso pueda ser usada para adquirir el permiso necesario desde el enrutador de acceso, el agente doméstico y, opcionalmente, la infraestructura AAA.
- La creación de una dirección para un nodo móvil puede realizarse en dos etapas por nodos separados: el nodo móvil puede crear la parte identificador de interfaz (IID) de la dirección y asegurar su propiedad de la IID por medio de direcciones generadas criptográficamente (véase GB2367986) o los certificados de dirección EUI-64. El enrutador de acceso puede crear la parte prefijo de la dirección.
- Los agentes domésticos (o servidores AAA domésticos) pueden actuar en nombre de los nodos móviles para verificar la confianza hacia el enrutador de acceso, y la exactitud de la construcción de dirección dinámica.
- Los agentes domésticos pueden actuar en nombre de los nodos móviles para adquirir tokens “keygen” domésticos que son los valores criptográficos necesarios para realizar una optimización de rutas con los nodos correspondientes.
- De manera similar, el enrutador de acceso puede actuar en nombre de los nodos móviles para adquirir tokens keygen dinámicos.
- La prevención del ataque denegación de servicio sólo necesita ser empleada cuando los nodos implicados están siendo atacados, de lo contrario, los procedimientos de prevención solo causan un retardo extra.

Hay una serie de maneras diferentes para crear un protocolo de enlace inalámbrico basado en las construcciones anteriores. Una solución consiste en la secuencia de mensajes siguiente:

1. En algunos tipos de capas de enlace, puede ser posible para el nodo móvil recibir un mensaje "baliza" o de publicidad antes de que intente una conexión. Cuando dicho mensaje está disponible, contiene la información siguiente:

la identidad del enrutador de acceso, y,

opcionalmente, las capacidades y las propiedades del enrutador de acceso.

2. Cuando el nodo móvil está preparado para conectarse a un enlace, envía un "mensaje de nueva conexión" al enrutador de acceso apropiado. Este mensaje es una declaración firmada desde el nodo móvil, quizás en forma de un certificado. La declaración indica que el nodo móvil desea acceder, y contiene la información siguiente:

identificador de acceso a red (NAI) del nodo móvil,

la clave pública propia del nodo móvil,

una raíz de confianza para cualquier enrutador de acceso que aceptará el nodo móvil,

la dirección del agente doméstico del nodo móvil,

las direcciones de los nodos correspondientes con los que el nodo móvil desea establecer una optimización de rutas,

un identificador de interfaz (IID), construido e mediante generación criptográfica de direcciones (CGA),

la identidad del enrutador de acceso (si se conoce),

los parámetros deseados para la conexión de enlace inalámbrico (si es necesario),

una cookie, calculada en una manera conocida sólo por el nodo móvil,

una firma, firmada con la clave privada del nodo móvil.

3. Una vez que el enrutador de acceso ha verificado la solicitud de acceso (los detalles de esto se exponen más adelante), envía un acuse de recibo al nodo móvil y le permite acceder a la red. Este acuse de recibo es una declaración firmada desde el enrutador de acceso de que ha realizado las tareas que le han sido delegadas. Además, el acuse de recibo transporta una declaración firmada desde la red AAA doméstica de que ha registrado la solicitud de acceso y ha verificado que la red de acceso es de confianza. El acuse de recibo transporta una declaración firmada similar desde el agente doméstico del nodo móvil de que ha registrado la nueva ubicación del nodo móvil, y ha verificado también que el enrutador de acceso es de confianza. El acuse de recibo contiene la información siguiente:

la cookie desde el nodo móvil,

el prefijo de red asignado para el nodo móvil,

la identidad y la clave pública del enrutador de acceso,

una firma del enrutador de acceso,

una firma de la red AAA doméstica del usuario,

y una firma del agente doméstico del usuario.

4. El nodo móvil verifica que la cookie contenida en el acuse de recibo fue producida por él mismo, y verifica las firmas en el mensaje (para ello, puede usar las claves públicas conocidas). Suponiendo que las firmas son correctas, el nodo móvil empieza a enviar paquetes de datos.

5. Una vez que el enrutador de acceso, el agente doméstico y un nodo correspondiente han concluido la necesaria señalización de movilidad necesaria para establecer la optimización de rutas, el enrutador de acceso envía un mensaje al nodo móvil, que contiene la información siguiente:

la cookie desde el nodo móvil,

la dirección del nodo correspondiente,

una firma del enrutador de acceso.

6. El nodo móvil verifica de nuevo que la cookie contenida en este mensaje fue producida por él mismo, y verifica la firma en el mensaje. Suponiendo que la información es correcta, el nodo móvil procede a usar la optimización de rutas en los paquetes de datos que envía al nodo correspondiente en cuestión.

Una vez completado este procedimiento, el nodo móvil ha sido autenticado a la red doméstica (con los posibles registros contables creados), se ha registrado con su agente doméstico y se ha registrado con todos sus nodos correspondientes.

Los paquetes de datos pueden fluir cuando el nodo móvil (a) ha recibido un acuse de recibo desde el enrutador de acceso de que se han realizado todas las etapas 1. a 6., (b) ha recibido al menos la información de prefijo, en cuyo caso podría empezar (de manera optimista) a enviar datos, o (c) inmediatamente si el enrutador de acceso "rellena" la parte prefijo de la dirección IP de origen en los paquetes del nodo móvil.

El uso de un único mensaje de solicitud - respuesta con la criptografía de clave pública tiene, potencialmente, una vulnerabilidad de tipo denegación de servicio (DoS). Un atacante podría generar un gran número de solicitudes, y el receptor, por ejemplo, el enrutador de acceso, debe realizar una gran cantidad de cálculos antes de que pueda determinar que las solicitudes no son válidas. La defensa normal tomada contra este ataque DoS es el intercambio de algunos paquetes verificados (débilmente) antes de realizar cálculos realmente pesados. Por ejemplo, el procedimiento de intercambio de clave de Internet (IKE) intercambia cookies y comprueba que el homólogo puede, de hecho, recibir paquetes en la dirección IP reivindicada antes de realizar cualquiera de los cálculos Diffie-Hellman o RSA.

Una defensa similar puede ser usada en el procedimiento descrito en la presente memoria (que implica, típicamente, enviar una cookie desde la red de acceso al nodo móvil, y la inclusión de esta cookie en la solicitud de acceso inicial enviada por el nodo móvil), pero con el fin de evitar un retraso para un problema relativamente raro, los nodos implicados no invocan normalmente el intercambio extra. Por el contrario, lo invocan sólo cuando se consideran ellos mismos bajo una carga pesada o un potencial ataque de denegación de servicio. Específicamente, en dicha situación, el enrutador de acceso o la infraestructura subyacente puede negarse a verificar las firmas inmediatamente. En su lugar, puede enviar un mensaje de respuesta preliminar que contiene el mensaje original y la cookie del emisor, y adjuntar su propia cookie. Si la solicitud era real, el emisor recibirá este mensaje y responderá reenviando la solicitud con la cookie adicional del mensaje de respuesta preliminar. Esto garantiza que al menos el nodo en cuestión existe en una dirección IP conocida, y es capaz de enviar y recibir paquetes. En este caso, la secuencia de señalización es la siguiente:

1. El nodo móvil envía un "mensaje de nueva conexión" cuando se conecta a un nuevo enlace.

2. El enrutador de acceso o un nodo de infraestructura subyacente solicita una verificación adicional. El mensaje contiene la información siguiente:

la cookie desde el nodo móvil,

la cookie o las cookies desde el nodo o nodos enrutador de acceso (e infraestructura).

3. El nodo móvil verifica que la cookie contenida en su interior fue producida por él mismo, y reenvía su solicitud original con un parámetro adicional, concretamente, la cookie o las cookies desde el nodo o los nodos enrutador de acceso (e infraestructura).

4. A partir de este punto, el procedimiento continúa tal como se ha descrito anteriormente.

La parte infraestructura del procedimiento de conexión a red puede ser implementada en un número de maneras diferentes, dependiendo de si pueden emplearse nuevos protocolos o pueden reusarse unos existentes. En adelante, en la presente memoria, se proporciona solo una visión general de la provisión de la funcionalidad deseada en el enrutador de acceso, y cómo puede contactar con la infraestructura AAA, el agente doméstico y los nodos correspondientes, usando los protocolos existentes.

1. La infraestructura AAA puede ser contactada usando mecanismos de autenticación existentes. Por ejemplo, el enrutador de acceso podría ejecutar EAP-TLS dentro de un protocolo RADIUS, y usar su propia clave para la autenticación de TLS cliente. Al incluir la solicitud de acceso firmada del nodo móvil en forma de certificado, la infraestructura AAA puede determinar que el nodo móvil ha delegado la tarea de autenticación al enrutador de acceso.

2. El enrutador de acceso puede verificar la IID enviada por el nodo móvil, o bien manteniendo su propia base de datos de IIDs usadas en la actualidad en este enlace, o bien enviando una solicitud DAD IPv6 en el enlace en nombre del nodo móvil.

3. El enrutador de acceso puede autenticarse a sí mismo al agente doméstico del nodo móvil usando su propia clave pública, y al igual que anteriormente, incluye la solicitud firmada del nodo móvil como un certificado. Además, el enrutador de acceso puede proporcionar la información de prefijo de red. A continuación, el agente doméstico puede determinar la nueva ubicación y verificar que, realmente, el nodo móvil ha hecho la solicitud para ser movido. Dependiendo de si el nodo móvil conocía o no la identidad del enrutador de acceso antes de realizar su solicitud, el agente doméstico puede ser capaz también de comprobar que el nodo móvil, el enrutador de acceso y el agente doméstico están de acuerdo, todos ellos, acerca de la identidad del enrutador de acceso.

4. Una vez que el enrutador de acceso ha recibido una respuesta desde la infraestructura AAA y desde el agente doméstico, y ha verificado las firmas y las cookies recibidas, puede proceder al envío de un acuse de recibo al nodo móvil y permitirle acceder a la red.

5. Cuando el agente doméstico ha aprobado la solicitud de acceso, el mismo puede enviar, en paralelo, un número de mensajes “init” de comprobación doméstica IPv6 móvil a los nodos correspondientes de la lista. De manera similar, el enrutador de acceso puede enviar un número de mensajes “init” comprobación dinámica a los mismos nodos correspondientes. Las respuestas a los mensajes de comprobación doméstica serán enviadas al enrutador de acceso desde el agente doméstico. Cuando se ha respondido a ambos mensajes de comprobación doméstica y dinámica, el enrutador de acceso puede combinar los valores de los mismos para enviar una actualización de unión al nodo correspondiente. (A diferencia de otros nodos implicados en este intercambio, el nodo correspondiente no necesita las declaraciones firmadas, ya que opera únicamente en base a comprobaciones de accesibilidad de dirección, que tienen éxito debido al agente doméstico y al enrutador de acceso que los realizan.)

Un resumen del flujo de mensajes se ilustra en la Figura 2.

Se apreciará que el procedimiento ilustrado puede ser optimizado aún más incluyendo la invocación paralela de los

mensajes a los diferentes nodos de infraestructura.

El modelo presentado puede actuar también como un mecanismo de seguridad de una capa de enlace (enlace inalámbrico), por ejemplo, para permitir una encriptación entre el servidor y el enrutador de acceso. El intercambio criptográfico necesario para derivar las claves de sesión necesarias puede estar incluido en el "mensaje de nueva conexión" y su acuse de recibo. Por ejemplo, puede realizarse un intercambio Diffie-Hellman con el fin de llegar a un acuerdo acerca de las claves de sesión.

En su mínima expresión, el procedimiento descrito en la presente memoria permite un mecanismo seguro de conexión a red, con un único mensaje, en el enlace inalámbrico, suponiendo, por supuesto, que pueden enviarse, de manera optimista, paquetes de datos antes de recibir un acuse de recibo. En cualquier caso, el mecanismo descrito requiere como máximo 3 mensajes en el enlace inalámbrico para realizar una conexión a red para un nodo móvil.

REIVINDICACIONES

1. Procedimiento para facilitar un acceso de protocolo de Internet por parte de un nodo móvil a una red de acceso, comprendiendo el procedimiento:

enviar una solicitud de conexión desde el nodo móvil a un enrutador de acceso de la red de acceso, conteniendo la solicitud un identificador de nodo móvil y un identificador de interfaz o medios para derivar un identificador de interfaz, y estando firmada por el nodo móvil usando una clave privada de un par de claves privada-pública, para permitir que el mensaje sea autenticado como procedente de ese nodo móvil, y

recibir la solicitud en el enrutador de acceso y autenticar el mensaje en el mismo, usando la firma y la clave pública de dicho par de claves privada-pública,

en respuesta a la recepción y autenticación del mensaje, realizar un conjunto predefinido de tareas delegadas al enrutador de acceso y que son necesarias para autorizar al nodo móvil y facilitar, de esta manera, dicho acceso, y

devolver un acuse de recibo desde el enrutador de acceso al nodo móvil, confirmando el permiso de acceso, conteniendo el acuse de recibo un prefijo de enrutamiento de red y medios para autenticar el enrutador de acceso al nodo móvil.

2. Procedimiento según la reivindicación 1, en el que la solicitud de conexión contiene uno o más de los siguientes:

el identificador de acceso a red del nodo móvil,

la clave pública propia del nodo móvil,

una raíz de confianza para cualquier enrutador de acceso que el nodo móvil está dispuesto a aceptar,

una dirección del agente doméstico del nodo móvil,

las direcciones de los nodos correspondientes con los que el nodo móvil desea establecer una optimización de rutas,

un identificador de interfaz, construido mediante generación criptográfica de direcciones,

la identidad del enrutador de acceso,

los parámetros deseados para la conexión de enlace inalámbrico,

una cookie, calculada de una manera conocida sólo por el nodo móvil,

una firma, firmada con la clave privada del nodo móvil.

3. Procedimiento según la reivindicación 1 ó 2, en el que la recepción de la solicitud de conexión en el enrutador de acceso desencadena uno o más de los procedimientos siguientes en el enrutador de acceso:

Conexión en capa de enlace;

Un procedimiento de control de acceso;

Búsqueda de enrutador;

Creación de dirección IP:

Detección de direcciones duplicadas

4. Procedimiento según una cualquiera de las reivindicaciones anteriores, en el que dicho conjunto predefinido de tareas comprende:

Implementar un procedimiento de acceso, autorización y contabilidad con una infraestructura apropiada en la red doméstica del nodo móvil;

Realizar una actualización de unión en nombre del nodo móvil con un agente doméstico del nodo móvil;

Realizar una optimización de rutas con uno o más nodos correspondientes del nodo móvil.

5. Procedimiento de funcionamiento de un nodo móvil para facilitar un acceso de protocolo de Internet por parte del nodo móvil a una red de acceso, comprendiendo el procedimiento enviar una solicitud de conexión desde el nodo móvil a un enrutador de acceso de la red de acceso, conteniendo la solicitud un identificador de nodo móvil y un identificador de interfaz o medios para derivar un identificador de interfaz, y estando firmada por el nodo móvil usando una clave privada de un par de claves privada-pública, para permitir que el mensaje sea autenticado como procedente de ese nodo móvil, conteniendo el mensaje una autorización para que el enrutador de acceso realice un

conjunto predefinido de tareas delegadas al enrutador de acceso y que se requieren para autorizar el nodo móvil y facilitar, de esta manera, dicho acceso

6. Procedimiento de funcionamiento de un enrutador de acceso dispuesto para facilitar un acceso de protocolo de Internet por parte de un nodo móvil a una red de acceso, comprendiendo el procedimiento:

recibir una solicitud de acceso en el enrutador de acceso y autenticar el mensaje en el mismo, usando la firma y una clave pública de un par de claves privada-pública, y en respuesta a la recepción y autenticación del mensaje, las etapa de realizar un conjunto predefinido de tareas delegadas al enrutador de acceso y que se requieren para autorizar el nodo móvil y facilitar, de esta manera, dicho acceso, y

devolver un acuse de recibo desde el enrutador de acceso al nodo móvil confirmando el permiso de acceso, conteniendo el acuse de recibo un prefijo de red (enrutamiento) y medios para autenticar el enrutador de acceso al nodo móvil.

7. Procedimiento según la reivindicación 1, en el que una de dichas tareas comprende realizar un procedimiento de acceso, autorización y contabilidad con una infraestructura apropiada en una red doméstica del nodo móvil.

8. Enrutador de acceso dispuesto para facilitar un acceso de protocolo de Internet por parte de un nodo móvil a una red de acceso, comprendiendo el enrutador de acceso:

medios para recibir una solicitud de conexión en el enrutador de acceso y autenticar la solicitud en el mismo, usando la firma y una clave pública de un par de claves privada-pública,

estos medios son dispuestos adicionalmente, en respuesta a la recepción y autenticación de la solicitud, para realizar un conjunto predefinido de tareas delegadas al enrutador de acceso y que se requieren para autorizar el nodo móvil y facilitar, de esta manera, dicho acceso, y

medios para devolver un acuse de recibo desde el enrutador de acceso al nodo móvil confirmando el permiso de acceso, conteniendo el acuse de recibo un prefijo de red (enrutamiento) y medios para autenticar el enrutador de acceso al nodo móvil.

9. Enrutador de acceso según la reivindicación 8, dispuesto para gestionar una solicitud de conexión que contiene uno o más de los siguientes:

identificador de acceso a red del nodo móvil,

clave pública propia del nodo móvil,

una raíz de confianza para cualquier enrutador de acceso que el nodo móvil está dispuesto a aceptar,

una dirección del agente doméstico del nodo móvil,

las direcciones de los nodos correspondientes con los que el nodo móvil desea establecer una optimización de rutas,

un identificador de interfaz, construido mediante generación criptográfica de direcciones,

la identidad del enrutador de acceso,

los parámetros deseados para la conexión de enlace inalámbrico,

una cookie, calculada en una manera conocida solo por el nodo móvil,

una firma, firmada con la clave privada del nodo móvil.

10. Enrutador de acceso según la reivindicación 8 ó 9, que comprende medios para desencadenar uno o más de los procedimientos siguientes en respuesta a una recepción y autenticación de la solicitud:

Conexión en capa de enlace,

Un procedimiento de control de acceso,

Búsqueda de enrutador,

Generación de dirección IP,

Detección de direcciones duplicadas.

11. Enrutador de acceso según una cualquiera de las reivindicaciones 8 a 10, en el que dicho conjunto de tareas predefinidas comprende:

Implementar un procedimiento de acceso, autorización y contabilidad con una infraestructura apropiada en la red doméstica del nodo móvil;

Realizar una actualización de unión en nombre del nodo móvil con un agente doméstico del nodo móvil;

Realizar una optimización de ruta con uno o más nodos correspondientes del nodo móvil.

12. Nodo móvil dispuesto para comunicarse con una red de acceso para facilitar el acceso de protocolo de Internet, comprendiendo el nodo:

medios para enviar una solicitud de conexión desde el nodo móvil a un enrutador de acceso de la red de acceso, conteniendo la solicitud un identificador de nodo móvil y un identificador de interfaz o medios para derivar un identificador de interfaz, y estando firmada por el nodo móvil usando una clave privada de un par de claves privada-pública, para permitir que el mensaje sea autenticado por el enrutador de acceso como procedente de ese nodo móvil, conteniendo el mensaje una autorización para que el enrutador de acceso realice un conjunto predefinido de tareas delegadas al enrutador de acceso y que se requieren para autorizar el nodo móvil y facilitar, de esta manera, dicho acceso.

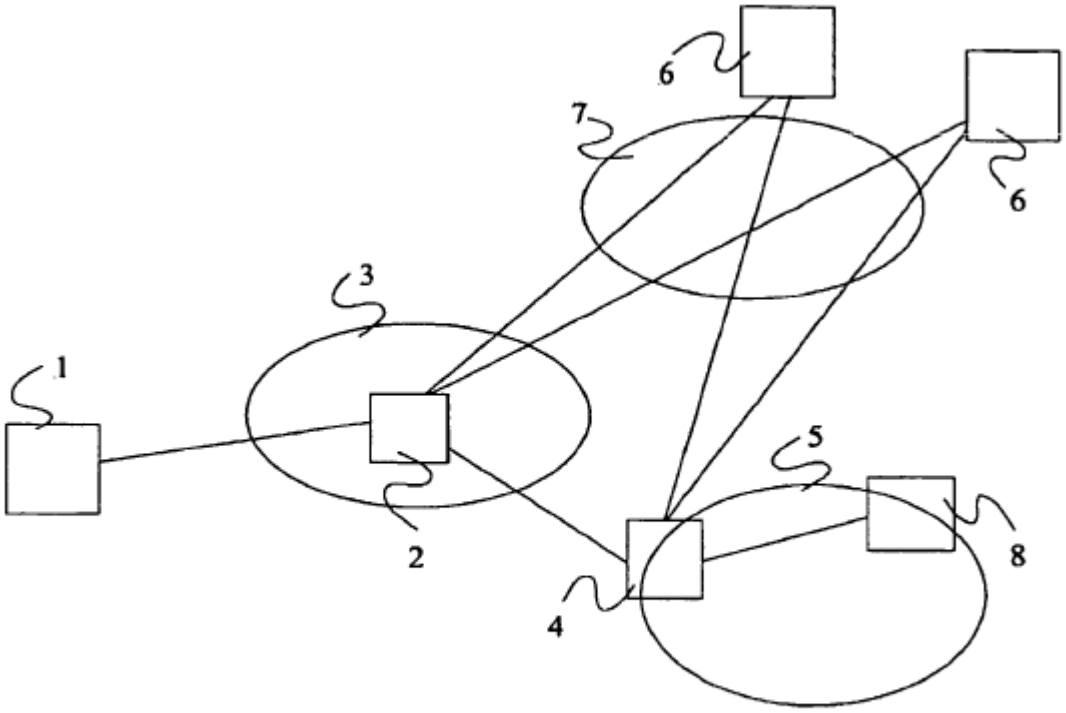

Figura 1

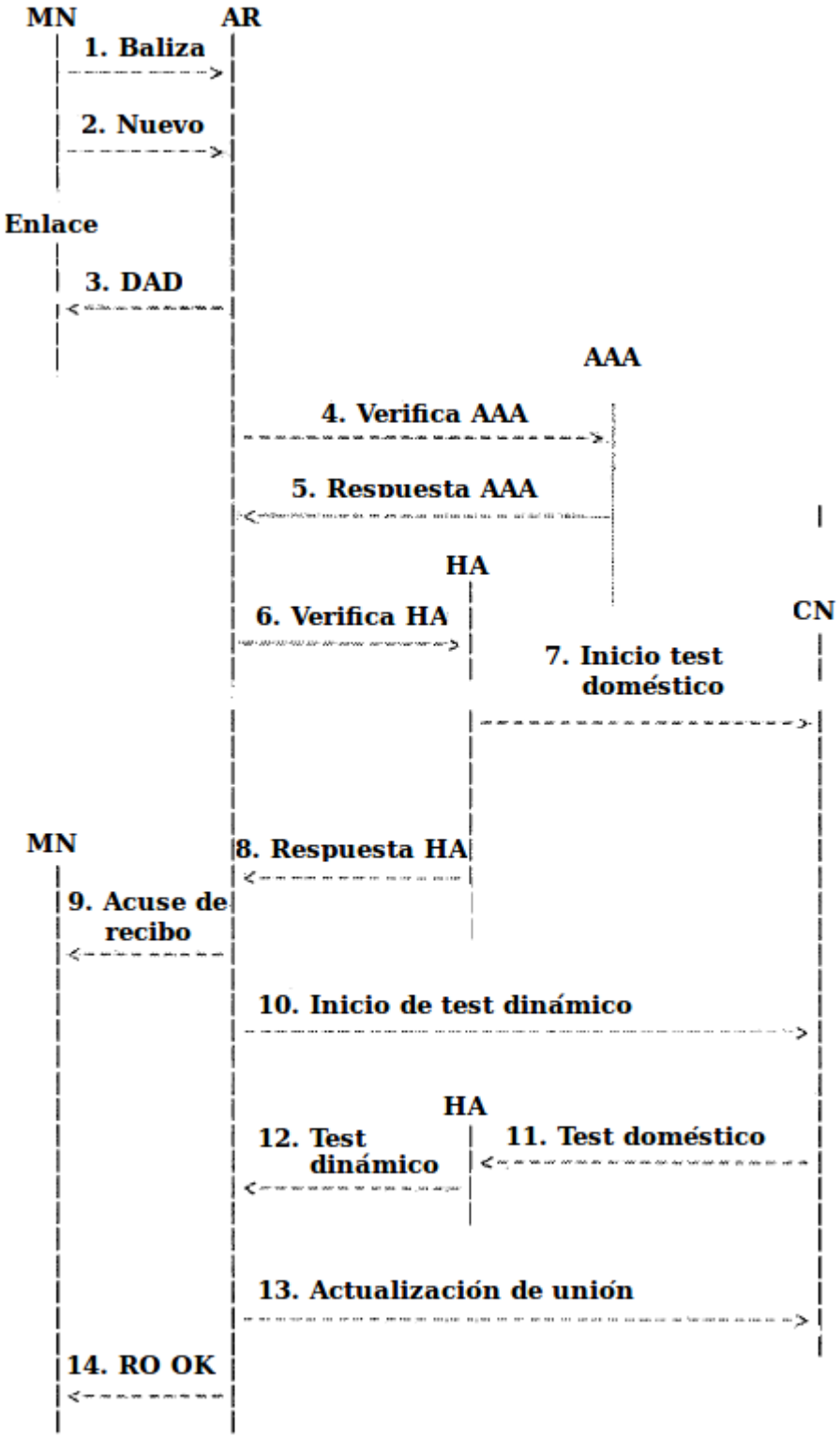
MN
AR
1. Baliza
2. Nuevo
Enlace
3. DAD
AAA
4. Verifica AAA
5. Respuesta AAA
HA
CN
6. Verifica HA
7. Inicio test doméstico
MN
8. Respuesta HA
9. Acuse de recibo
10. Inicio de test dinámico
HA
12. Test dinámico
11. Test doméstico
13. Actualización de unión
14. RO OK

Figura 2