(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 378 783**

(51) Int. CI.:
H04L 29/06 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07712208 .3**
(96) Fecha de presentación: **12.02.2007**
(97) Número de publicación de la solicitud: **2119181**
(97) Fecha de publicación de la solicitud: **18.11.2009**

(54) Título: **Delegación de señalización en una red en movimiento**

(45) Fecha de publicación de la mención BOPI:
17.04.2012

(45) Fecha de la publicación del folleto de la patente:
17.04.2012

(73) Titular/es:
Telefonaktiebolaget LM Ericsson (publ)
164 83 Stockholm, SE

(72) Inventor/es:
MELÉN, Jan;
YLITALO, Jukka;
NIKANDER, Pekka y
JOKELA, Petri

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Delegación de señalización en una red en movimiento

Campo técnico

La presente invención se refiere a delegación de señalización en una red en movimiento y en particular, aunque no necesariamente, a delegación de derechos de actualización de posición desde un nodo móvil a un encaminador móvil.

Antecedentes

Trenes, autobuses, aviones y redes de áreas personales (PANs: Personal Area Networks) son ejemplos de casos de uso donde pueden ser aplicadas tecnologías de redes en movimiento. Una red inalámbrica en movimiento es un grupo consistente en nodos móviles (MNs: Mobile Nodes) y encaminadores móviles (MRs: Mobile Routers). Un encaminador móvil encamina el tráfico IP (Internet Protocol) entre un nodo móvil e Internet (u otra red IP). El encaminador móvil actúa como un punto de acceso para el nodo móvil. Un encaminador móvil puede ser conectado a otra red en movimiento o directamente a Internet por vía de un punto de acceso (AP: access point). En el primer caso, se produce un conjunto de redes móviles encajadas (anidadas). La Figura 1A ilustra un escenario donde un nodo móvil está unido inicialmente a un encaminador móvil. En la Figura 1B, el nodo móvil es transferido a un segundo encaminador móvil, mientras en la Figura 1C el nodo móvil es transferido desde el segundo encaminador móvil a un encaminador fijo de acceso.

Un encaminador móvil difunde radiobalizas para anunciar su existencia y que proporciona un servicio de encaminamiento móvil. Las radiobalizas pueden contener un identificador de operador, por ejemplo, para ayudar a la selección de una red apropiada por un usuario. Cuando un nodo móvil encuentra un encaminador móvil adecuado, el nodo móvil activa un intercambio de unión con el encaminador móvil.

Se apreciará que cuando un encaminador móvil cambia su punto de unión a Internet, o es transferido a otro encaminador móvil, cambiarán las posiciones (o sea, direcciones IP) de todos los nodos móviles corriente abajo. Para mantener la continuidad de servicio durante y después de la transferencia de un encaminador móvil, algún mecanismo es necesario para asegurar que los datos enviados desde nodos iguales (o correspondientes) implicados en una sesión de comunicación con el nodo móvil son enviados al nodo móvil en la nueva posición de nodo. Un número de procedimientos son posibles.

Primero, el propio nodo móvil puede ser responsable de notificar al (a los) nodo(s) igual(es) su nueva posición. Sin embargo, este procedimiento produce un gran volumen de señalización relacionada con actualización de posición incluso para redes en movimiento relativamente pequeñas y produce tiempos de reacción de transferencia relativamente prolongados. Un segundo procedimiento implica la creación de un túnel entre el encaminador móvil y algún encaminador de origen (o “agente de origen”) dentro de la red fija. Todo el tráfico enviado desde un nodo igual a un nodo móvil (y posiblemente el tráfico enviado en la dirección inversa) es encaminado a través del túnel. Cuando el encaminador móvil cambia su posición, envía una actualización al encaminador de origen. Dos problemas de este procedimiento son el uso de encaminamiento subóptimo (triangular) y el tamaño incrementado de paquete debido a las operaciones auxiliares de tunelización. Un ejemplo de este segundo procedimiento es el mecanismo de movilidad de red de IETF (Internet Engineering Task Force). Un tercer procedimiento implica la delegación de derechos de señalización desde los nodos móviles al encaminador móvil para permitir que el encaminador móvil envíe señalización de actualización de posición a nodos iguales en nombre de los nodos móviles.

Un ejemplo del tercer procedimiento es descrito en el documento WO03036916, donde un nodo móvil genera un certificado de autorización firmando una clave pública del encaminador móvil con su propia clave privada. Entonces, el certificado es provisto al encaminador móvil, que incluye el certificado en cualquier mensaje de actualización de posición que envía en nombre del nodo móvil. El mensaje también es firmado con la clave privada del encaminador móvil. Usando las claves públicas del encaminador móvil y del nodo móvil, un nodo igual puede verificar tanto que la actualización se refiere al nodo móvil reclamado y que el encaminador móvil está autorizado a realizar la actualización en nombre del nodo móvil. Un encaminador móvil puede delegar además responsabilidad en otro encaminador móvil (corriente arriba) firmando la clave pública del encaminador corriente arriba con su propia clave privada, añadiendo esta al certificado y pasando el certificado al encaminador corriente arriba. Sin embargo, este procedimiento necesita que el nodo igual procese una cadena de certificados relativamente larga para cada actualización de posición recibida.

Sumario

Un objeto de la presente invención es permitir la delegación de derechos de señalización en y entre redes en movimiento de tal modo que los derechos delegados puedan ser pasados entre entidades sin introducir una carga excesiva de procesamiento en nodos iguales. Este y otros objetos son conseguidos proveyendo a un encaminador móvil de una segunda clave simétrica generada por un nodo móvil usando una primera clave simétrica compartida entre el nodo móvil y un nodo igual. El encaminador móvil es provisto adicionalmente de un “certificado” que autentica la segunda clave simétrica usando la primera clave simétrica. De este modo, el encaminador móvil puede

firmar mensajes relacionados con actualización de posición enviados al nodo igual con la segunda clave simétrica, y puede proveer al nodo igual del certificado para permitir que el nodo igual autentique el derecho del encaminador móvil a actuar en nombre del nodo móvil.

Según un primer aspecto de la presente invención, se proporciona un nodo móvil dispuesto en uso para comunicar con un encaminador móvil que aprovisiona una red inalámbrica en movimiento, comprendiendo el nodo móvil:

medios para establecer una asociación de seguridad con un nodo igual, comprendiendo dicha asociación de seguridad una primera clave simétrica;

medios para establecer una asociación de seguridad con dicho encaminador móvil;

medios para delegar derechos de señalización de actualización de posición para el nodo móvil al encaminador móvil, estando los medios para delegar dispuestos para proveer al encaminador móvil de un tique de autorización que contiene una segunda clave simétrica derivada de dicha primera clave simétrica, e información de autorización que identifica dicha segunda clave simétrica y confirma la autenticidad de dicha segunda clave simétrica usando dicha primera clave simétrica.

Los diversos medios referidos anteriormente son implementados típicamente por medio de una combinación de software y datos almacenados en una memoria de nodo, y medios de procesamiento en hardware, por ejemplo un microprocesador y circuitos de radiofrecuencia (RF).

La información de autorización provista al encaminador móvil no está limitada al encaminador móvil. Por tanto, la información, o información adicional derivada de ella, puede ser pasada por el encaminador a otro encaminador corriente arriba u otra entidad corriente arriba y puede ser usada libremente por el otro encaminador o entidad.

Preferiblemente, el nodo móvil es un nodo habilitado por protocolo de identidad de anfitrión (ordenador nodal), y dichos medios para establecer asociaciones de seguridad con el nodo igual y con el encaminador móvil sin medios para establecer asociaciones de seguridad de protocolo de identidad de anfitrión. En este caso, dicha primera clave simétrica es una clave de código de autenticación de mensaje basado en dirección calculada (HMAC: Hash-based Message Autentication Code). Dicha segunda clave simétrica es una clave de HMAC adicional derivada de la primera clave de HMAC, o sea la primera clave simétrica. Dicha información de autorización puede comprender una duración de dicha segunda clave simétrica, dicha segunda clave simétrica y un HMAC que protege la información de autorización y generado usando dicha primera clave simétrica. El HMAC es protegido con el material de codificación de extremo a extremo.

Preferiblemente, dicha información de autorización contiene dicha integridad de segunda clave simétrica protegida usando dicha primera clave simétrica. La información puede ser cifrada usando, por ejemplo, dicha primera clave simétrica. Más bien que contener dicha segunda clave simétrica, la información puede contener un puntero a esa clave, por ejemplo en el caso donde el nodo móvil y el nodo igual comparten un libro de códigos común, y dicho puntero en un índice al libro de códigos.

Según un segundo aspecto de la presente invención, se proporciona un encaminador móvil para aprovisionar una red inalámbrica en movimiento a nodos móviles, comprendiendo el encaminador móvil:

medios para establecer una asociación de seguridad con un nodo móvil;

medios para recibir desde el nodo móvil un tique de autorización que contiene una segunda clave simétrica derivada de una primera clave simétrica conocida por el nodo móvil y por un nodo igual con el que el nodo móvil ha establecido una asociación de seguridad, e información de autorización que identifica dicha segunda clave simétrica y confirma la autenticidad de dicha segunda clave simétrica usando dicha primera clave simétrica;

medios para enviar un mensaje de actualización de posición a dicho nodo igual en nombre del nodo móvil, conteniendo el mensaje una posición nueva del nodo móvil y dicha información de autorización, y una firma generada usando dicha segunda clave simétrica.

Los diversos medios referidos anteriormente son implementados típicamente por medio de una combinación de software y datos almacenados en una memoria del nodo, y medios de procesamiento en hardware, por ejemplo un microprocesador y circuitos de radiofrecuencia (RF).

La invención es aplicable en particular a un encaminador habilitado por protocolo de identidad de anfitrión que está dispuesto en uso para comunicar con nodos móviles o iguales habilitados por protocolo de identidad de anfitrión. En este caso, dicha primera clave simétrica es una clave de HMAC y dicha segunda clave simétrica es una clave adicional de HMAC.

Preferiblemente, el encaminador móvil comprende medios para establecer una asociación de seguridad con un encaminador móvil adicional o nodo de lado de red fija y para proporcionar dicho tique al encaminador o nodo, mediante lo que el otro encaminador o nodo puede realizar señalización de actualización de posición en nombre del nodo móvil. Alternativamente, el encaminador móvil puede derivar una tercera clave simétrica de dicha segunda

clave simétrica, y sustituir la segunda clave simétrica en el tique por la tercera clave simétrica antes de enviar el tique al encaminador o nodo adicional. Cuando se envía una actualización de posición, el encaminador móvil o entidad adicional incluye en el mensaje la información de autorización modificada y firma el mensaje con la tercera clave simétrica.

Según un tercer aspecto de la presente invención, se proporciona un método para delegar derechos de señalización de actualización de posición desde un nodo móvil a un encaminador móvil que aprovisiona una red inalámbrica en movimiento, comprendiendo el método:

establecer una asociación de seguridad entre dicho nodo móvil y un nodo igual, comprendiendo dicha asociación de seguridad una primera clave simétrica;

establecer una asociación de seguridad entre dicho nodo móvil y dicho encaminador móvil;

enviar un tique de autorización desde dicho nodo móvil a dicho encaminador móvil, conteniendo el tique una segunda clave simétrica derivada de dicha primera clave simétrica, e información de autorización que identifica dicha segunda clave simétrica y confirma la autenticidad de dicha segunda clave simétrica usando dicha primera clave simétrica.

Cuando es necesario que el encaminador móvil envíe una actualización de posición al nodo igual en nombre del nodo móvil, el encaminador móvil incluye con el mensaje de actualización de posición dicha información de autenticación y una firma generada usando dicha segunda clave simétrica. Al recibir el mensaje, el nodo igual identifica u obtiene la segunda clave simétrica, confirma la autenticidad de la segunda clave simétrica usando la primera clave simétrica que es conocida por él y autentica la firma usando la segunda clave simétrica.

Una implementación preferida del método emplea el protocolo de identidad de anfitrión (HIP: Host Identity Protocol). En particular, dichas asociaciones de seguridad son negociadas usando el protocolo de identidad de anfitrión, y dichas claves simétricas primera y segunda son una primera clave de HMAC y una segunda clave de HMAC derivada de la primera clave de HMAC. El mensaje de actualización de posición enviado desde el encaminador móvil al nodo igual es una actualización de posición de protocolo de identidad de anfitrión.

Descripción breve de los dibujos

La Figura 1A ilustra esquemáticamente una red inalámbrica en movimiento que comprende un nodo móvil unido a un encaminador móvil;

la Figura 1B ilustra la red de la Figura 1A con el nodo móvil habiendo sido transferido a un segundo encaminador móvil;

la Figura 1C ilustra la red de la Figura 1A con el nodo móvil habiendo sido transferido a un encaminador fijo de acceso,

la Figura 2 ilustra el procedimiento de intercambio de base de protocolo de identidad de anfitrión (HIP);

la Figura 3 ilustra el procedimiento de intercambio de base de HIP con extensión de registro;

la Figura 4 ilustra un tique de autenticación para inclusión en un mensaje I2 del intercambio de base de HIP con extensión de registro;

la Figura 5 ilustra información de autenticación para inclusión en una actualización de posición;

la Figura 6 ilustra el proceso de delegación de señalización con subdelegación desde un primer encaminador móvil a un segundo encaminador móvil; y

la Figura 7 ilustra el uso de un proxy (representante) de señalización estática en una red fija con delegación de señalización al proxy.

Descripción detallada

El documento de IETF (Internet Engineering Task Force) draft-ietf-hip-base-06 titulado “Protocolo de identidad de anfitrión” introduce un mecanismo de direccionamiento que separa una identidad direccionable de anfitrión (la “identidad de anfitrión”) de su posición física (o sea, una dirección IP encaminable). De hecho, una identidad de anfitrión es una clave pública de un par de claves asimétricas poseídas por el anfitrión, lo que permite que un anfitrión demuestre la propiedad de identidad de anfitrión mientras proporciona al mismo tiempo unos medios para establecer un canal de comunicación protegida entre anfitriones. El protocolo de identidad de anfitrión (HIP) requiere la introducción en la pila de protocolos de una capa de HIP que realiza esencialmente una transformación entre identidades de anfitriones (o etiquetas de identidades de anfitriones (HITs: Host Identity Tags) derivadas de identidades de anfitriones) y direcciones IP. Un anfitrión dado puede actualizar su entrada en la tabla de transformación de un anfitrión de igual enviando una actualización de posición al igual. El anfitrión emisor debe

firmar una actualización de posición con una denominada clave de HMAC. Esta clave (una “primera” clave simétrica) representa un secreto compartido entre los anfitriones y es determinada durante el intercambio de base de HIP. El intercambio de base usa el método Diffie-Hellman como la base para generar la clave de HMAC y las claves para la asociación de seguridad de carga útil de seguridad encapsuladora (ESP: Encapsulating Security Payload).

La Figura 2 ilustra el intercambio de base de HIP efectuado entre un par de anfitriones de HIP, identificados como un nodo móvil y un nodo igual. A modo de ejemplo, el nodo móvil puede ser un teléfono móvil o similar, mientras que el nodo igual también puede ser un teléfono móvil o un terminal de usuario de línea fija o un servidor de red. El borrador de IETF “Extensión de registro de protocolo de identidad de anfitrión (HIP)” (draft-ietf-hip-registration-02) describe una extensión (introduciendo tipos – longitudes – valores (TLVs) nuevos) al protocolo de base de HIP destinado a permitir el registro de un nodo móvil con un encaminador móvil. El intercambio extendido es mostrado en la Figura 3. Información relacionada con registro es incluida en los mensajes intercambiados. Una vez registrado, el nodo móvil solicita un servicio de encaminamiento del encaminador móvil. Aquí se propone enviar un “tique de delegación” desde el nodo móvil al encaminador móvil como parte de la extensión de registro, protegido usando la asociación de seguridad de carga útil de seguridad encapsuladora (ESP) negociada. Este tique incluye una nueva clave de HMAC (una “segunda” clave simétrica) generada por el nodo móvil usando el material de codificación compartido entre el nodo móvil y el nodo igual. El tique también incluye la nueva clave de HMAC de integridad protegida y cifrada usando la clave original de HMAC. Como tal, el encaminador móvil no puede descifrar o modificar esta información de autenticación sin que esto sea evidente para cualquier nodo igual (véase a continuación). Así como la clave de HMAC de integridad protegida, la información de autenticación contenida dentro del tique puede incluir una duración de autorización y/o un tipo de autenticación (también de integridad protegida). La Figura 4 ilustra una posible implementación del tique, donde la clave $K_{MN\text{-}PEER}$ es la clave original de HMAC conocida solo por el nodo móvil y el nodo igual. En el primer caso, $K_{issuer\text{-}subjet}$ es una clave compartida entre el nodo móvil (la clave “issuer”) y el encaminador móvil (la clave “subject”). Como el tique es protegido usando la asociación de seguridad establecida entre el nodo móvil y el encaminador móvil, la nueva clave de HMAC no es filtrada a ningún nodo de tercer corresponsal.

Para un nodo móvil registrado recientemente con un encaminador móvil, el encaminador móvil debe enviar un mensaje de actualización de posición a todos los nodos iguales del nodo móvil (donde asociaciones de protocolo de identidad de anfitrión (HIP) ya han sido establecidas entre el nodo móvil y estos nodos iguales) que identifica la nueva dirección IP del encaminador móvil. El nodo móvil habrá notificado al encaminador móvil las transformaciones de etiqueta de identidad de anfitrión/dirección IP durante el intercambio de base, o estas pueden ser aprendidas por el encaminador móvil cuando paquetes pasan a través de él en tránsito entre el nodo móvil y los nodos iguales. En el caso de que el nodo móvil ya esté unido al encaminador móvil cuando intenta conectar con un nodo igual nuevo, el intercambio de base con el nodo igual es traspasado a, y visible para, el encaminador móvil y el encaminador móvil puede establecer la información de estado necesaria. El nodo móvil también ejecuta un intercambio de registro con el encaminador móvil para enviar el nuevo tique al encaminador móvil. En la práctica, el nodo móvil y el encaminador móvil ejecutan el intercambio de registro completo solo una vez, y después de establecer una asociación de seguridad entre ellos, el nodo móvil puede ejecutar un intercambio extendido de actualización de HIP con el encaminador móvil. Este intercambio aumentado de actualización de tres vías incluye el nuevo tique de autorización para el nodo igual.

De modo similar, cuando el encaminador móvil cambia su punto de unión (a Internet), el encaminador móvil debe enviar actualizaciones de posición a todos los nodos iguales asociados con nodos móviles corriente abajo del encaminador móvil. El encaminador móvil firma cada actualización de posición con la clave apropiada de HMAC para el nodo móvil y el nodo igual (un nodo móvil genera una clave diferente de HMAC para cada nodo igual). Además, el encaminador móvil incluye en el mensaje la información de autenticación no modificada recibida desde el nodo móvil para ese nodo igual, o sea la clave HMAC de integridad protegida (y cifrada). Esta información es ilustrada en la Figura 5.

Más bien que incluir la propia clave nueva de HMAC en el tique, el nodo móvil puede incluir solo un puntero a tal clave nueva. Esto puede aplicarse donde los nodos extremos, o sea el nodo móvil y el nodo igual, generan inicialmente material de codificación compartido (intercambio de base de HIP). Los nodos tienen mucho material de codificación en masa (bytes aleatorios en la práctica) que es almacenado como una matriz. El nodo móvil puede enviar un índice a la matriz que señala una parte específica del material de codificación. Como un resultado, los nodos extremos son mantenidos en sincronía y conocen que parte usar del material de codificación. Además, el índice, o sea el puntero, no revela nada sobre las claves secretas a intrusos.

El encaminador móvil puede construir el mensaje de actualización de posición tal que parece un mensaje de actualización que habría sido enviado por el nodo móvil, excepto por la inclusión de la información de autenticación y la firma por la nueva clave de HMAC. En particular, el mensaje puede incluir la etiqueta de identidad de anfitrión (HIT) del nodo móvil como la HIT de fuente. Sin embargo, el mensaje también puede incluir una etiqueta de identidad de anfitrión (HIT) del encaminador móvil como un parámetro adicional. Esto permitiría, por ejemplo, que el nodo igual identifique una asociación de seguridad diferente para uso con esta sesión de comunicación. El mensaje también debe contener el valor de índice para la asociación de HIT y que es usado por el nodo igual para identificar el material de codificación correcto, o sea la clave original de HMAC. El valor de índice está incluido en el tique de autorización provisto por el nodo móvil al encaminador móvil.

Al recibir una actualización de posición, un nodo igual debe autenticar el derecho del encaminador móvil para actuar en nombre de nodo móvil. Hace esto verificando primero que la información de autenticación incluida con la actualización es protegida usando la clave original de HMAC, y obtiene esa clave usando un puntero contenido en la actualización o directamente (descifrando la clave si está contenido en el mensaje). Entonces, el nodo igual conoce si la nueva clave de HMAC ha sido emitida válidamente o no por el nodo móvil reclamado (si los datos protegidos incluyen solo un puntero a una clave nueva de HMAC, el nodo igual debe obtener o derivar la clave nueva). Después, el nodo igual comprueba si el mensaje está firmado correctamente o no con la nueva clave de HMAC, autenticando así el encaminador móvil. Suponiendo que la nueva clave de HMAC y el encaminador móvil son autenticados, el nodo igual actualiza sus transformaciones de HIP con la posición nueva para el nodo móvil.

Para evitar ataques relacionados con el intercambio de actualización de posición, los nodos iguales deben enviar retos a la posición reclamada de nodo móvil (o sea, ensayo de asequibilidad). En la práctica, estos mensajes de reto son destinados al encaminador móvil. El encaminamiento móvil en trayecto de envío usa la nueva clave de HMAC para proteger el mensaje de respuesta y devuelve el mensaje a los nodos iguales en nombre de los nodos móviles.

Es importante observar que no es realizado ningún intercambio de base de HIP entre el encaminador móvil y el nodo igual. Por tanto, no existe asociación de seguridad entre estos nodos y no es realizado proceso de autenticación. El nodo igual confía en el nodo móvil para que envíe la nueva clave de HMAC solo a encaminadores móviles autorizados.

En el caso de que el encaminador móvil se mueva detrás de otro encaminador móvil, los encaminadores deben realizar el intercambio de base de HIP con extensión de registro. Como resultado, el encaminador corriente arriba recibe desde el encaminador corriente abajo tiques de autenticación para todos los nodos móviles que han delegado responsabilidad de actualización de posición al encaminador corriente abajo. Cada tique contiene la información de autenticación original provista al encaminador móvil corriente abajo por el nodo móvil, y es firmado por una clave ($K_{issuer\text{-}subjet}$) compartida entre los encaminadores móviles. Entonces, el encaminador corriente arriba puede realizar a su vez actualizaciones de posición en nodos iguales basadas en la información recibida en estos tiques. Como no hay asociación entre el nodo igual y el encaminador móvil, no hay necesidad de proporcionar ninguna información adicional sobre el encaminador móvil anterior y la misma información de autenticación puede ser usada por el nuevo encaminador móvil para actualizaciones de posición. La Figura 6 ilustra el flujo de señalización asociado con un nodo móvil que delega primero la responsabilidad de señalización a un primer encaminador móvil (MR1), con el primer encaminador móvil delegando subsiguientemente además esa responsabilidad a un segundo encaminador móvil (MR2).

Si un nodo móvil sale de una red móvil, debe revocar la(s) clave(s) antigua(s) de HMAC. Envía un mensaje de actualización a su(s) nodo(s) igual(es) que identifica las claves que ya no son válidas. Específicamente, esto puede ser efectuado usando un mensaje aumentando de actualización de posición que contiene una dirección calculada de la clave revocada de HMAC. Después de recibir esta información, un nodo igual no acepta ningunas actualizaciones nuevas de posición con la clave revocada. Actualizaciones de posición enviadas subsiguientemente son firmadas usando la clave antigua de HMAC (o una clave adicional si ocurre la delegación a otro encaminador móvil).

Considerando ahora el caso de red en movimiento encajada, una extensión al proceso de generación de claves de HMAC hace posible revocar claves en el caso de encaminador móvil encajado. Cuando un encaminador móvil (nº 1) delega derechos de señalización en otro encaminador móvil corriente arriba (nº 2), el primero no revela la clave de HMAC de actualización de posición inicial (provista por el nodo móvil). En cambio, el encaminador móvil nº 1 calcula una dirección calculada unidireccional (por ejemplo, SHA256) sobre la clave recibida desde el nodo móvil. El encaminador móvil nº 1 sustituye la clave (nueva) de HMAC, dentro del tique recibido desde el nodo móvil, por la clave de dirección calculada. Sin embargo, el tique contiene todavía la misma información de autorización, es decir la nueva clave de HMAC protegida y cifrada con la clave original de HMAC. El tique también incluye una indicación de que la clave de dirección calculada es la n-sima clave en la cadena de direcciones calculadas. El tique modificado es enviado seguramente al segundo encaminador móvil durante el intercambio de base. El segundo encaminador móvil corriente arriba usa la clave de dirección calculada para proteger sus mensajes de actualización de posición enviados al nodo igual, incluyendo también estos mensajes la información de autenticación (original). El nodo igual es capaz de autenticar la firma por sí mismo descifrando la nueva clave de HMAC y calculando la dirección de esa clave (n veces) para derivar la clave de firma.

Este procedimiento hace posible que el primer encaminador móvil se separe del segundo encaminador móvil y revoque el tique de segundo encaminador móvil. En otras palabras, cada encaminador móvil en una red en movimiento encajada usa un valor de dirección calculada de una clave usada por el encaminador móvil anterior. Los encaminadores móviles más bajos en la jerarquía pueden revocar claves más altas en la jerarquía.

Por ejemplo, considérese una clave creada como sigue “MR#3-key =sha256 (MR#2-key-sha256 (MR#1-key)). Ahora si el encaminador móvil nº 2 (MR#2) sale de la red en movimiento del encaminador móvil nº 3 (MR#3), el primero envía un mensaje de revocacion al nodo igual. El nodo igual conoce que la clave del encaminador móvil nº 2 (MR#2) estaba más alta en la cadena de claves. Po tanto, se permite que el encaminador móvil nº 2 revoque la clave del encaminador móvil nº 3. Como los nodos iguales siempre conocerán la clave original, son capaces de calcular todos los valores necesarios de claves de dirección calculada en la cadena de direcciones calculadas.

Los procedimientos descritos anteriormente reducen significativamente la señalización relacionada con actualización de posición puesto que un encaminador móvil actúa como un proxy de señalización entre nodos móviles y nodos iguales, realizando actualizaciones de posición en bloque para todos los nodos móviles corriente abajo. Además, los procedimientos son más sencillos de implementar y hacer funcionar que el procedimiento de certificado basado en par de claves pública-privada de técnica anterior, puesto que la autenticación por un nodo igual solo requiere la autenticación de un par de firmas de claves simétricas (realizada usando las claves antigua y nueva de HMAC).

Para optimizar la señalización por el aire entre los encaminadores móviles e Internet, un proxy de señalización estática puede ser introducido como se ilustra en la Figura 7. El encaminador móvil registra sus clientes y delega los derechos de señalización al proxy de señalización estática situado en la red fija. Cuando el encaminador móvil efectúa una transferencia, ejecuta un solo intercambio de actualización de posición con el proxy de señalización estática. La dirección multiplexada de encaminador móvil (o sea, la combinación de la dirección IP de encaminador y alguna identidad tal como número de puerto o etiqueta de identidad de anfitrión (HIT)) puede representar la posición actual de todos los clientes pertenecientes a la red en movimiento detrás de ella. El proxy de señalización estática en la red fija puede usar la anchura de banda alta disponible para enviar una “ráfaga” de actualizaciones de posición a los nodos iguales en nombre de los nodos móviles. Los nodos iguales envían los mensajes de reto al localizador multiplexado del encaminador móvil si el proxy de señalización estática no está en el trayecto de envío para verificar que los nodos móviles están en la posición donde el proxy de señalización estática les reclama que estén. Si el proxy de señalización estática está en el trayecto de envío, el proxy responde directamente a los mensajes de reto enviados por los nodos iguales.

Los procedimientos descritos aquí tienen algunas semejanzas con el modelo Kerberos de técnica anterior para establecer asociaciones de seguridad autenticadas. Kerberos es descrito en IETF RFC (Internet Engineering Task Force Request for Comments) 4120. En particular, el nodo móvil actúa como un centro de distribución de claves (KDC: Key Distribution Center). Sin embargo, según Kerberos, el tique provisto a un cliente es limitado a ese cliente. Por tanto, el procedimiento Kerberos imposibilita, de un modo escalable, la delegación adicional a un encaminador corriente arriba. En contraste, el procedimiento descrito aquí no une el tique a ninguna entidad particular y como tal puede ser transferido corriente arriba sin aprobación desde el nodo móvil de origen.

La persona experta en la técnica apreciará que diversas modificaciones pueden ser efectuadas en las realizaciones descritas anteriormente sin apartarse del alcance de la presente invención.

REIVINDICACIONES

1. Un nodo móvil dispuesto en uso para comunicar con un encaminador móvil que aprovisiona una red inalámbrica en movimiento, comprendiendo el nodo móvil:

medios para establecer una asociación de seguridad con un nodo igual, comprendiendo dicha asociación de seguridad un primera clave simétrica;

medios para establecer una asociación de seguridad con dicho encaminador móvil;

medios para delegar derechos de señalización de actualización de posición para el nodo móvil al encaminador móvil, estando los medios para delegar dispuestos para proveer al encaminador móvil de un tique de autorización que contiene una segunda clave simétrica derivada de dicha primera clave simétrica, e información de autorización que identifica dicha segunda clave simétrica y confirma la autenticidad de dicha segunda clave simétrica usando dicha primera clave simétrica.

2. Un nodo móvil según la reivindicación 1, en el que el nodo móvil es un código habilitado por protocolo de identidad de anfitrión (HIP), y dichos medios para establecer asociaciones de seguridad con el nodo igual y con el encaminador móvil están dispuestos para establecer asociaciones de seguridad de protocolo de identidad de anfitrión (HIP).

3. Un nodo móvil según la reivindicación 2, siendo dicha primera clave simétrica una clave de código de autenticación de mensaje basado en dirección calculada (HMAC).

4. Un nodo móvil según la reivindicación 3, siendo dicha segunda clave simétrica una clave adicional de HMAC derivada de dicha primera clave mencionada de HMAC.

5. Un nodo móvil según una cualquiera de las reivindicaciones precedentes, comprendiendo dicha información de autorización una duración de dicha segunda clave simétrica, dicha segunda clave simétrica y una firma que protege la información de autorización y generada usando dicha primera clave simétrica.

6. Un nodo móvil según una cualquiera de las reivindicaciones precedentes, conteniendo dicha información de autorización dicha segunda clave simétrica de integridad protegida usando dicha primera clave simétrica.

7. Un nodo móvil según una cualquiera de las reivindicaciones 1 a 4, conteniendo dicha información de autorización un puntero a dicha segunda clave simétrica.

8. Un nodo móvil según una cualquiera de las reivindicaciones precedentes, siendo dicha información de autorización cifrada usando dicha primera clave simétrica.

9. Un encaminador móvil para aprovisionar una red inalámbrica en movimiento a nodos móviles, comprendiendo el encaminador móvil:

medios para establecer una asociación de seguridad con un nodo móvil;

medios para recibir desde el nodo móvil un tique de autorización que contiene una segunda clave simétrica derivada de una primera clave simétrica conocida por el nodo móvil y por un nodo igual con el que el nodo móvil ha establecido una asociación de seguridad, e información de autorización que identifica dicha segunda clave simétrica y confirma la autenticidad de dicha segunda clave simétrica usando dicha primera clave simétrica;

medios para enviar un mensaje de actualización de posición a dicho nodo igual en nombre del nodo móvil, conteniendo el mensaje una posición nueva del nodo móvil y dicha información de autorización, y una firma generada usando dicha segunda clave simétrica.

10. Un encaminador móvil según la reivindicación 9, siendo el encaminador un encaminador habilitado por protocolo de identidad de anfitrión (HIP) que está dispuesto en uso para comunicar con nodo móvil habilitado por protocolo de identidad de anfitrión y con nodos iguales.

11. Un encaminador móvil según la reivindicación 10, en el que dicha primera clave simétrica es una clave de HMAC y dicha segunda clave simétrica es una clave adicional de HMAC.

12. Un encaminador móvil según una cualquiera de las reivindicaciones 9 a 11 y comprendiendo medios para establecer una asociación de seguridad con un encaminador móvil adicional o nodo de lado de red fija y para proporcionar dicho tique a ese encaminador o nodo, mediante lo que el otro encaminador o nodo puede realizar señalización de actualización de posición en nombre del nodo móvil.

13. Un encaminador móvil según la reivindicación 12 y comprendiendo medios para derivar una tercera clave simétrica de dicha segunda clave simétrica, y sustituir la segunda clave simétrica en el tique por la tercera clave simétrica antes de enviar el tique al encaminador o nodo adicional.

14. Un método para delegar derechos de señalización de actualización de posición desde un nodo móvil a un encaminador móvil que aprovisiona una red inalámbrica en movimiento, comprendiendo el método:

establecer una asociación de seguridad entre dicho nodo móvil y un nodo igual, comprendiendo dicha asociación de seguridad una primera clave simétrica;

establecer una asociación de seguridad entre dicho nodo móvil y dicho encaminador móvil;

enviar un tique de autorización desde dicho nodo móvil a dicho encaminador móvil, conteniendo el tique una segunda clave simétrica derivada de dicha primera clave simétrica, e información de autorización que identifica dicha segunda clave simétrica y confirma la autenticidad de dicha segunda clave simétrica usando dicha primera clave simétrica.

15. Un método según la reivindicación 14, en el que dichas asociaciones de seguridad son establecidas usando el protocolo de identidad de anfitrión (HIP).

16. Un método para realizar una actualización de posición con respecto a un nodo móvil que sigue la delegación de derechos de señalización de actualización de posición desde el nodo móvil a un encaminador móvil según el método de la reivindicación 14 o 15, comprendiendo el método incluir en un mensaje de actualización de posición, enviado desde el encaminador móvil a un nodo igual, dicha información de autenticación y una firma generada usando dicha segunda clave simétrica y, al recibir el mensaje en el nodo igual, identificar u obtener la segunda clave simétrica, confirmar la autenticación de la segunda clave simétrica usando la primera clave simétrica, y autenticar la firma usando la segunda clave simétrica.

17. Un método según la reivindicación 16 cuando adjuntada a la reivindicación 15, siendo dicho mensaje de actualización de posición una actualización de posición de protocolo de identidad de anfitrión.

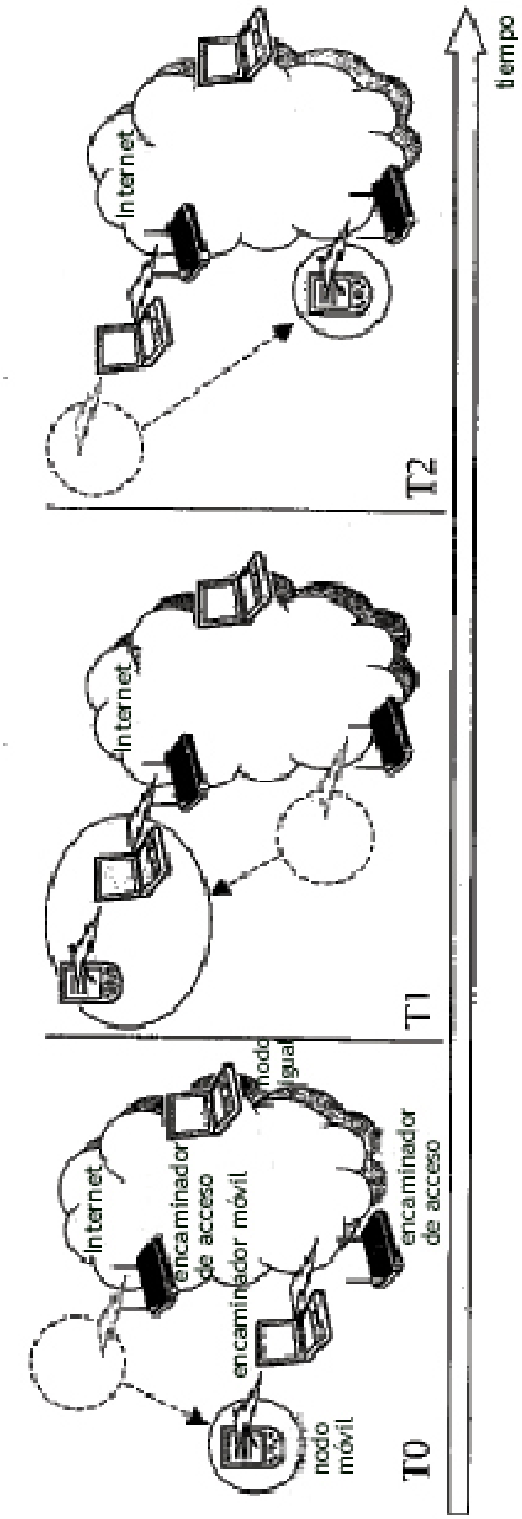
Internet
encaminador de acceso
encaminador móvil
nodo móvil
encaminador de acceso
T0
T1
T2
tiempo

Figura 1

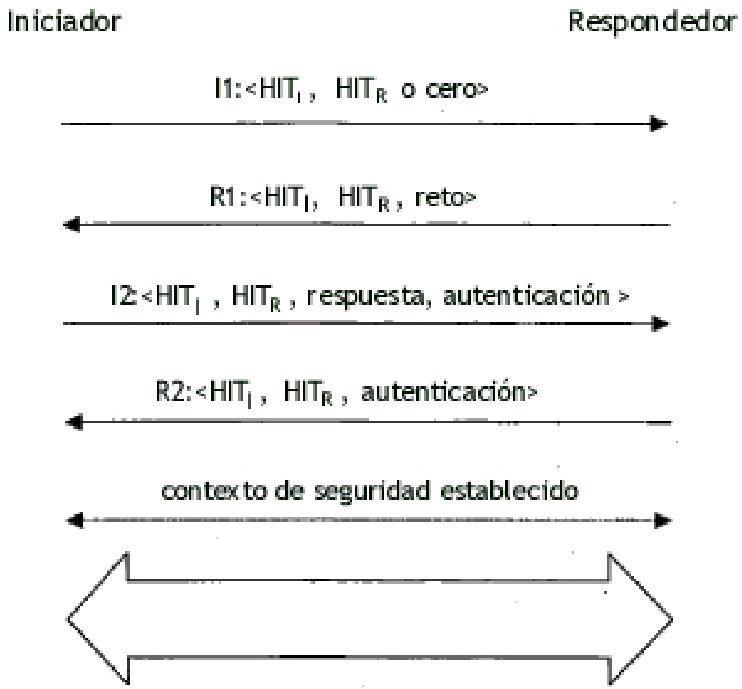
Iniciador
Respondedor
I1:<HIT_I , HIT_R o cero>
R1:<HIT_I, HIT_R , reto>
I2:<HIT_I , HIT_R , respuesta, autenticación >
R2:<HIT_I , HIT_R , autenticación>
contexto de seguridad establecido

Figura 2

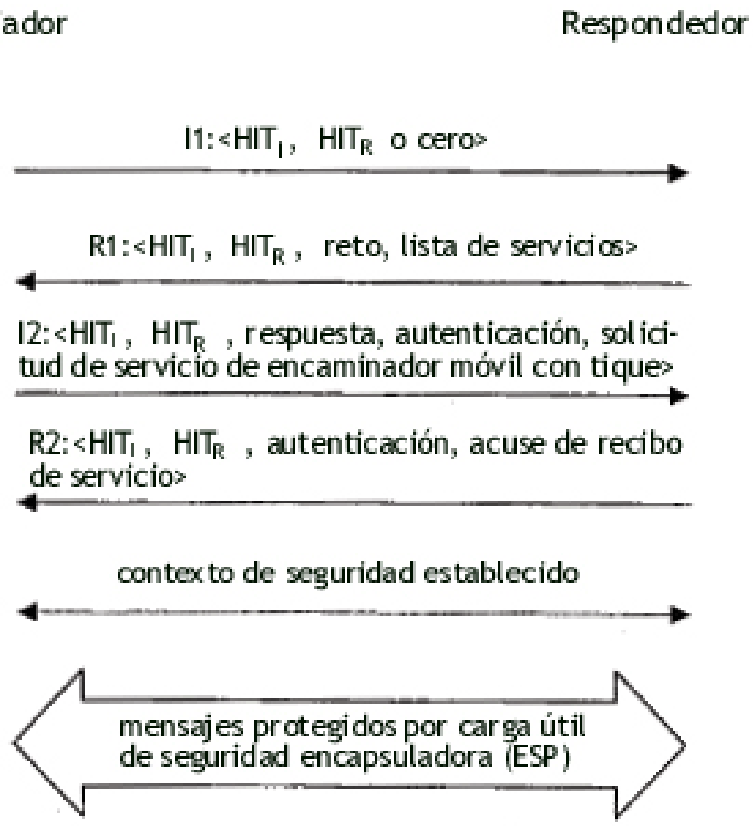
Iniciador
Respondedor
I1:<HIT_I , HIT_R o cero>
R1:<HIT_I , HIT_R , reto, lista de servicios>
I2:<HIT_I , HIT_R , respuesta, autenticación, solicitud de servicio de encaminador móvil con tique>
R2:<HIT_I , HIT_R , autenticación, acuse de recibo de servicio>
contexto de seguridad establecido
mensajes protegidos por carga útil de seguridad encapsuladora (ESP)

Figura 3

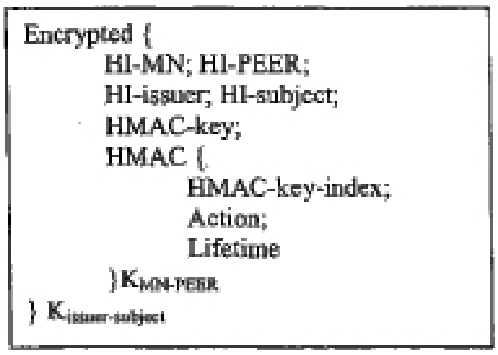

Figura 4

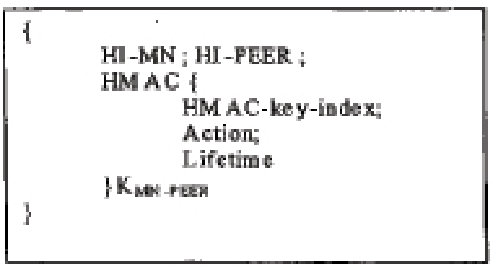

Figura 5

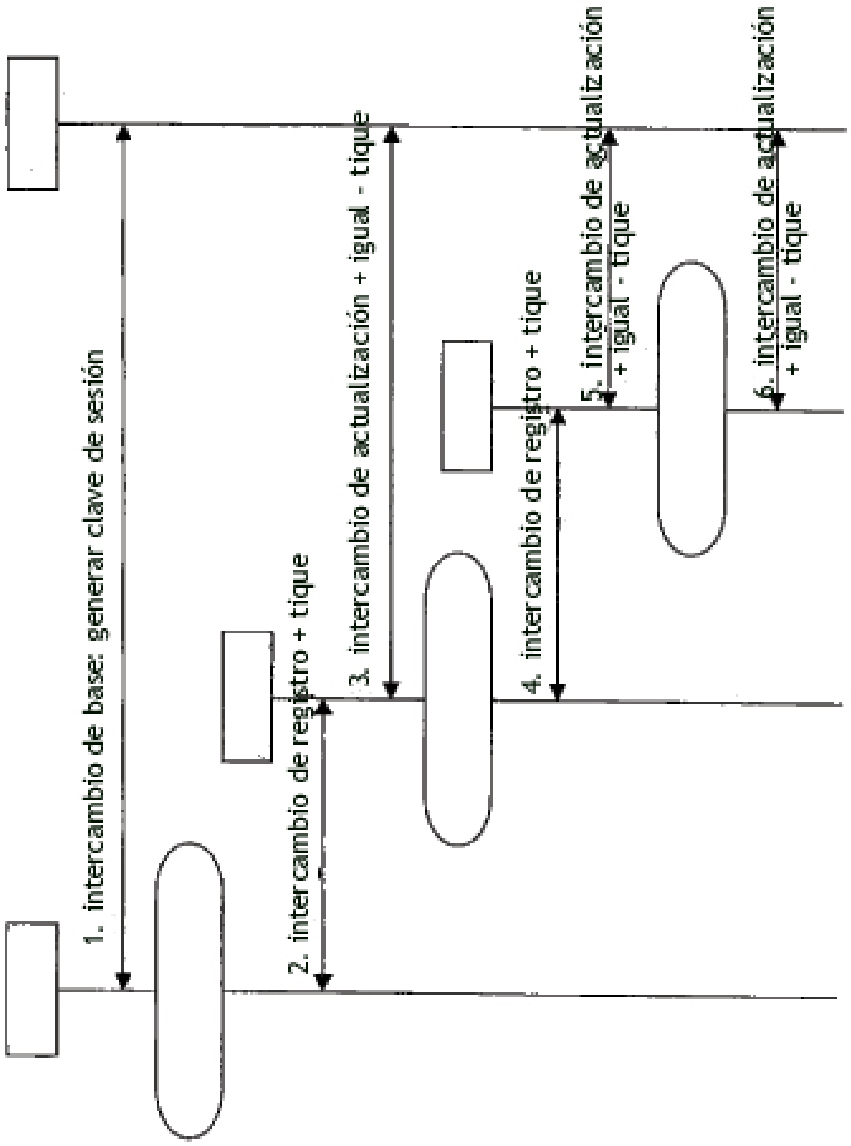
1. intercambio de base: generar clave de sesión
2. intercambio de registro + tique
3. intercambio de actualización + igual - tique
4. intercambio de registro + tique
5. intercambio de actualización + igual - tique
6. intercambio de actualización + igual - tique

Figura 6

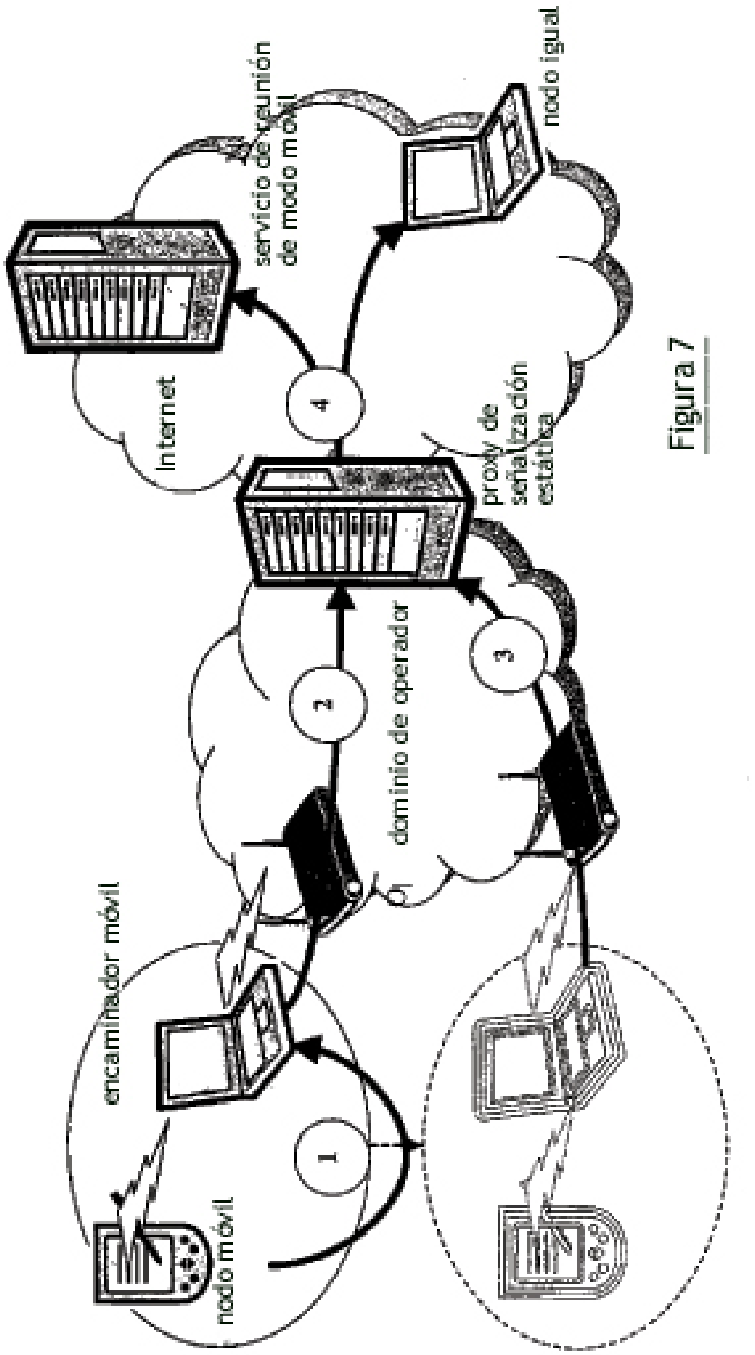
nodo igual
servicio de reunión de modo móvil
Internet
proxy de señalización estática
dominio de operador
encaminador móvil
nodo móvil
1
2
3
4

Figura 7