(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 374 317**

(51) Int. CI.:
H04L 9/08 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07764283 .3**
(96) Fecha de presentación: **26.07.2007**
(97) Número de publicación de la solicitud: **2056520**
(97) Fecha de publicación de la solicitud: **06.05.2009**

(54) Título: **MÉTODO PARA UNA ACTUALIZACIÓN DE ENLACE EN EL SISTEMA MÓVIL IPv6 Y SISTEMA DE COMUNICACIÓN MÓVIL IPv6.**

(30) Prioridad:
31.08.2006 CN 200610111876

(45) Fecha de publicación de la mención BOPI:
15.02.2012

(45) Fecha de la publicación del folleto de la patente:
15.02.2012

(73) Titular/es:
Huawei Technologies Co., Ltd.
Huawei Administration Building Bantian
Longgang District, Shenzhen
Guangdong 518129 , CN

(72) Inventor/es:
LI, Chunqiang

(74) Agente: **Lehmann Novo, Isabel**

DESCRIPCIÓN

Método para una actualización de enlace en el sistema móvil IPv6 y sistema de comunicación móvil IPv6

Antecedentes de la invención

CAMPO DE LA INVENCIÓN

La presente invención se refiere al campo técnico de la comunicación de redes y más en particular, a un método para la actualización de enlace en la versión 6 del Protocolo Internet móvil (IPv6) y un sistema de comunicación IPv6 móvil.

DESCRIPCIÓN DE LA TÉCNICA ANTERIOR

La versión 6 del Protocolo de Internet móvil (IPv6) es una solución de movilidad en la capa de red. El sistema IPv6 móvil tiene tres entidades de red básicas, esto es, un nodo móvil (MN), un nodo correspondiente (CN) y un agente de origen (HA).

Un MN se puede identificar, de forma unívoca, con una dirección de origen (HoA). Cuando el nodo MN realiza una itinerancia para una red ajena, se generará una dirección temporal (CoA) en un modo determinado. Según el IPv6 móvil, en el proceso en el que un nodo MN se desplaza desde un enlace a otro, la comunicación permanente del MN utilizando la HoA no se puede interrumpir. La movilidad del nodo es transparente para la capa de transferencia y otros protocolos de capa superior. El sistema IPv6 móvil define dos modos distintos para resolver el problema de la movilidad, esto es, un modo de túnel bidireccional y un modo de optimización de ruta.

En el modo de túnel bidireccional, el nodo MN informa al HA de la CoA a través de un mensaje de actualización de enlace (BU). El HA intercepta paquetes enviados a la red de origen del MN para comunicación con el MN y reenvía los paquetes al MN en el modo de túnel. Cuando el MN envía paquetes a un CN, los paquetes deben enviarse al HA en el modo de túnel y el HA desencapsula y reenvía los paquetes de túnel al CN.

En el modo de optimización de ruta, el MN necesita el registro con el CN. En primer lugar, se realiza un procedimiento de enrutabilidad de retorno (RRP). El procedimiento RRP incluye el intercambio de dos pares de mensajes entre los nodos MN y el CN: el mensaje de inicialización de prueba de origen (HoTI) y el mensaje de prueba de origen (HoT) y el mensaje de inicialización de prueba temporal (CoTI) y el mensaje de prueba temporal (CoT). Los mensajes HoTI y HoT se reenvían por el HA y los mensajes CoTI y CoT se intercambian directamente entre el MN y el CN. Una vez realizado satisfactoriamente el procedimiento RRP, el MN es capaz de la actualización de enlace de la CoA y de la HoA en una lista de memoria de enlace del CN mediante un mensaje de BU y transmite directamente paquetes al CN en la comunicación subsiguiente. De este modo, los paquetes no necesitan reenviarse por el agente HA.

La privacidad de localización es muy importante en la comunicación de IPv6 móvil. Sin ocultamiento, los datos sensibles de un abonado se pueden recoger y analizar y las actividades del abonado se pueden detectar y seguir, lo que constituye una amenaza grave para la seguridad del abonado móvil. Cuando el MN está en un enlace ajeno, la cabecera interior del paquete transmitido entre el MN y el HA, a través de un túnel, transmite la HoA del MN. Cuando el MN se comunica con el CN en el modo de optimización de ruta, la opción de HoA contenida en el paquete enviado desde el MN al CN incluye la HoA del MN y la cabecera de enrutamiento de tipo 2 contenida en el paquete enviado desde el CN al MN incluye también la HoA del MN.

Con el fin de no exponer la HoA del MN en un enlace ajeno a un *eavesdropper* ('fisgón informático') de escucha secreta, actualmente, se utiliza un sustituto de HoA (SHoA) para sustituir la HoA real. Sin embargo, para poner en práctica este método, además de la HoA y de la CoA del MN, la SHoA y la HoA necesitan también estar actualizadas en su enlace en el proceso BU.

A continuación se describe un método de puesta en práctica. 16 bits del espacio de dirección de 128 bits de IPv6 se asignan como un prefijo de identificadores móviles temporales (TMIs) y todas las direcciones, que utilizan el prefijo, se consideran como los identificadores TMIs que se especifican para ser enrutables. Un TMI de 128 bits se asigna a cada MN y el identificador TMI cambia periódicamente en función de un algoritmo determinado. En el proceso de BU para el CN, el identificador TMI se coloca en la opción de HoA y la HoA real se coloca en una subopción de BU redefinida. El CN enlaza el TMI, la HoA y la CoA. En la comunicación subsiguiente, el MN y el CN adoptan el TMI para sustituir la HoA actual en la opción de HoA y la cabecera de enrutamiento de tipo 2.

En la puesta en práctica de la presente invención, el inventor encuentra que el método anterior al menos presenta los defectos siguientes: 1. La HoA en el procedimiento RRP no está protegida y el paquete de BU todavía no ha de transmitir directamente la HoA; 2. El espacio de direcciones del IPv6 está permanentemente ocupado; 3. Si el cambio periódico del TMI y el cambio de la CoA no son síncronos, necesitan realizarse procedimientos RRPs extras y se consumirán más recursos de red y 4. Si múltiples HoAs de un MN están enlazadas con la misma CoA, puede producirse una confusión operativa.

Además, cuando el MN realiza la actualización del enlace, los números de secuencia contenidos en los paquetes de BU pueden exponer también las actividades del abonado móvil. Si se fija el incremento de los números de secuencia de los paquetes de BU o las reglas del cambio de los números de secuencia se pueden identificar con facilidad, el *eavesdropper* de escucha secreta todavía puede adivinar el movimiento del MN detectando una serie de mensajes de BU.

El documento XP015045182 (draft-irtf-mobopts-location-privacy-solutions-02 – Soluciones de privacidad de localización de IPv6 móvil) describe que el IPv6 móvil habilita que los nodos móviles permanezcan alcanzables mientras están en régimen de itinerancia en Internet. Con su especificación actual, la localización de un nodo móvil puede revelarse y su movimiento puede ser objeto de seguimiento controlando simplemente sus paquetes de IP. En este documento se trata el problema de la privacidad de localización de MIP6 y se proponen técnicas eficientes y seguras para proteger la privacidad de localización de un nodo móvil.

El documento US 2004/236937 A1 da a conocer una privacidad de localización contra terceros al mismo tiempo que se permite una comunicación con un enrutamiento optimizado entre el nodo correspondiente y el nodo móvil. La dirección de origen del nodo móvil se oculta de un observador externo con lo que se produce un antagonismo de los ataques basados en el análisis del tráfico, en donde la dirección de origen está en correlación con una dirección temporal de un nodo móvil, MN. Una “etiqueta de privacidad” se utiliza en lugar de una dirección de origen asociada con el nodo móvil. La etiqueta de privacidad se suministra por el nodo móvil al nodo correspondiente, de tal modo que permita que la etiqueta de privacidad esté enlazada con la dirección de origen, pero presenta la carencia de permitir que la dirección de origen sea visible durante el intercambio. La etiqueta de privacidad puede utilizarse también para ayudar a impedir los ataques de reproducción.

SUMARIO DE LA INVENCIÓN

En consecuencia, la presente invención se refiere a un método para la actualización de enlace en el sistema IPv6 móvil y un sistema de comunicación IPv6 móvil correspondiente, de modo que se mejore la seguridad de las direcciones de origen (HoAs) en un proceso de actualización de enlace (BU).

Para conseguir el objetivo de la presente invención, se dan a conocer soluciones técnicas según se describe a continuación. Un método para la actualización de enlace, en el sistema IPv6 móvil, comprende las etapas siguientes: la realización, por un nodo correspondiente (CN), de un procedimiento de enrutabilidad de retorno (RRP), en donde una dirección de origen (HoA) de un nodo móvil (MN) se sustituye con un sustituto de dirección de origen (SHoA); la recepción, por el CN, de un mensaje de actualización de enlace (BU) procedente del nodo MN, en donde el mensaje de BU transmite la SHoA, con la que se sustituye la HoA del MN y la HoA cifrada con una clave de gestión de enlace (Kbm); en donde la Kbm se genera en función de las fichas generadoras de claves obtenidas por el MN a partir del CN en el procedimiento RRP y el enlace, por el CN, de la SHoA, la HoA y una dirección temporal (CoA) en función del mensaje de BU; en donde la HoA cifrada se transmite en una opción de HoA cifrada en el mensaje de BU; el mensaje de BU comprende, además, un índice HoA, cuyo valor es un valor de puntero y está en correspondencia con cada HoA del MN y el enlace por el CN, en función del mensaje de BU, comprende, además, que el CN se enlaza con la SHoA, la HoA, el índice HoA y la CoA en función del mensaje de BU.

Un sistema de comunicación IPv6 móvil que incluye un MN, un CN y un agente de origen (HA) se da a conocer en esta invención. El nodo MN (100) está adaptado para enviar un mensaje de inicialización de prueba temporal (CoTI) al CN (200), para enviar un mensaje de inicialización de prueba de origen (HoTI) al agente HA (300), para recibir un mensaje de prueba temporal (CoT) que contiene una ficha generadora de claves temporal reenviada por el CN (200), para recibir un mensaje de prueba de origen (HoT) que contiene una ficha generadora de claves de origen reenviada por el HA (300), para generar una clave de gestión de enlace (Kbm) en función de la ficha generadora de claves de origen y la ficha generadora de claves temporal y para enviar al CN un mensaje de BU que incluye un sustituto de la dirección de origen (SHoA), con la que se sustituye una dirección de origen (HoA) del nodo MN. El agente HA (300) está adaptado para reenviar el mensaje de HoTI al CN (200), que transmite la SHoA en una cabecera de extensión de opción de destino que contiene una opción de SHoA del mensaje HoTI, para recibir el mensaje HoT enviado por el CN (200), para buscar la HoA correspondiente del nodo MN (100), en función de la SHoA en una cabecera de enrutamiento de tipo 2 del mensaje de HoT y para reenviar el mensaje HoT al nodo MN (100) en un modo operativo de túnel. El nodo CN (200) está adaptado para recibir el mensaje de HoTI reenviado por el HA (300), para sustituir la HoA con la SHoA para generar la ficha generadora de claves de origen, para reenviar el mensaje de HoT que contiene la ficha generadora de claves de origen al agente HA (300) y que transmite la SHoA en la cabecera de enrutamiento de tipo 2 del mensaje HoT y para enlazar la SHoA, la HoA y una dirección temporal (CoA) en función del mensaje de BU enviado desde el MN; en donde la HoA, que está cifrada con la Kbm, se transmite en una opción de HoA cifrada en el mensaje de BU y el mensaje de BU comprende, además, un índice de HoA, cuyo valor es un valor de puntero y está en correspondencia con cada HoA del MN.

En una forma de realización de la presente invención, se da a conocer un nodo MN en un sistema de comunicación IPv6. El MN comprende una primera unidad de enrutabilidad de retorno (110), adaptada para realizar un procedimiento de enrutabilidad de retorno (RRP) en el que una dirección de origen (HoA) del nodo MN se sustituye con un sustituto de dirección de origen (SHoA) y durante el cual se obtienen fichas generadoras de claves a partir de un nodo

correspondiente (CN); una unidad de claves de gestión de enlace (Kbm) (140), adaptada para calcular y generar la Kbm en función de las fichas generadoras de claves y una primera unidad de actualización de enlace (BU) (120), adaptada para enviar un mensaje de BU al CN sustituyendo la HoA del MN con la SHoA y para transmitir la HoA cifrada con la Kbm en el mensaje de BU; en donde la HoA cifrada se transmite en una opción de HoA cifrada en el mensaje de BU y el mensaje de BU comprende, además, un índice de HoA, cuyo valor es un valor de puntero y está en correspondencia con cada HoA del nodo MN.

En una forma de realización de la presente invención, se da a conocer un nodo CN, en un sistema de comunicación IPv6. El CN comprende una segunda unidad de enrutabilidad de retorno (210), adaptada para realizar un procedimiento de enrutabilidad de retorno (RRP), en el que una dirección de origen (HoA) del nodo MN se sustituye con un sustituto de dirección de origen (SHoA) y durante el cual fichas generadoras de claves son reenviadas a un nodo móvil (MN) en el procedimiento RRP; una unidad de clave de gestión de enlace (Kbm) (240), adaptada para calcular y generar la Kbm en función de las fichas generadoras de claves y una segunda unidad de actualización de enlace (BU) (220), adaptada para obtener una dirección de origen (HoA) del nodo MN a partir de un mensaje de BU enviado por el MN y para enlazar un sustituto de dirección de origen (SHoA) del MN, la HoA del MN y una dirección temporal (CoA) del nodo MN; en donde la HoA está cifrada con la Kbm y en donde la HoA cifrada se transmite en una opción de HoA cifrada en el mensaje de BU; el mensaje de BU comprende, además, un índice de HoA, cuyo valor es un valor de puntero y está en correspondencia con cada HoA del nodo MN; la HoA se obtiene mediante recuperación desde la opción de HoA cifrada con la Kbm y la segunda unidad de BU (220) comprende un módulo de índice de direcciones adaptado para enlazar un valor del índice HoA, la SHoA, la HoA y la CoA.

En el método según la presente invención, la SHoA sustituye a la HoA para realizar el procedimiento RRP y la HoA en el paquete de BU se envía en una forma de una opción cifrada después de que se obtenga la Kbm. Como tal, la HoA aparece solamente una vez en una forma cifrada en el paquete enviado al CN en el proceso de BU, con lo que se mejora la seguridad de la HoA en el proceso de BU.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La presente invención se hará más evidente a partir de la descripción dada a continuación con fines ilustrativos solamente y por lo tanto, no limitativa del alcance de la presente invención y en donde:

La Figura 1 es un diagrama de flujo esquemático de un método para la actualización de enlace en el sistema IPv6 móvil, según una primera forma de realización de la presente invención;

La Figura 2 es un diagrama de flujo esquemático de un método para la actualización de enlace en el sistema IPv6 móvil, según una segunda forma de realización de la presente invención;

La Figura 3 es un diagrama de flujo esquemático de un método para la actualización de enlace en el sistema IPv6 móvil, según una tercera forma de realización de la presente invención;

La Figura 4 es una vista estructura esquemática de un sistema de transmisión de IPv6 móvil, según una cuarta forma de realización de la presente invención y

La Figura 5 es una vista esquemática que ilustra estructuras internas de un nodo MN, un nodo CN y un agente HA en el sistema de transmisión de IPv6 móvil, según la cuarta forma de realización de la presente invención.

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN

En un método para actualización de enlace en el sistema IPv6 móvil, dado a conocer en la presente invención, un sustituto de dirección de origen (SHoA) sustituye a una dirección de origen (HoA) para realizar un procedimiento de enrutabilidad de retorno (RRP) y después de que se obtenga una clave de gestión de enlace (Kbm), la HoA en un paquete de actualización de enlace (BU) se envía en una forma de una opción cifrada. En el proceso de BU, se puede enlazar también un índice de HoA. La presente invención da a conocer, además, un método preferido para calcular una SHoA y un número de secuencia de un paquete de BU. Además, la presente invención da a conocer, además, un sistema de transmisión de IPv6 móvil relacionado. Los métodos y el sistema de la presente invención se ilustran en detalle a continuación.

Forma de realización 1: un método para actualización de enlace en el sistema IPv6 móvil. La Figura 1 ilustra el proceso del método que incluye las etapas siguientes.

A1. Un nodo móvil (MN) realiza un procedimiento RRP con un agente de origen (HA) y un nodo correspondiente (CN) utilizando una SHoA para sustituir una HoA del nodo MN.

El RRP es un procedimiento principalmente para garantizar la seguridad de la comunicación entre un nodo MN y un nodo CN. El principio del procedimiento RRP es autenticar el registro entre el nodo MN y el nodo CN cifrando la señalización intercambiada entre ambos nodos. El nodo CN puede determinar si puede acceder al MN en el modo de enrutamiento

optimizado y en el modo de enrutamiento triangular a través del procedimiento RRP. Si falla la prueba del RRP, el CN no puede recibir el mensaje de BU procedente del MN, ni tampoco enviar directamente paquetes a una dirección temporal (CoA) del nodo MN. La prueba incluye, por lo general, la transmisión de dos pares de mensajes: el mensaje de inicialización de prueba de origen (HoTI) y el mensaje de prueba de origen (HoT) así como el mensaje de inicialización de prueba temporal (CoTI) y el mensaje de prueba temporal (CoT). Los mensajes CoTI y CoT se intercambian directamente entre los nodos MN y CN y los mensajes HoTI y HoT se reenvían por el agente HA entre los nodos MN y CN. Para el nodo MN, los mensajes HoTI y CoTI se pueden transmitir al mismo tiempo y para el CN, los mensajes HoT y CoT se pueden transmitir también al mismo tiempo.

Puesto que los paquetes en la interacción de los mensajes CoTI y CoT no implican la HoA del MN, esta parte de interacción se puede realizar por los procedimientos existentes en la presente invención. La interacción entre los mensajes HoTI y HoT incluye una parte entre el nodo MN y el agente HA y una parte entre el HA y el CN. Los paquetes se envían en un modo de túnel, entre el MN y el HA, por lo que el paquete interior está protegido mediante una cabecera de carga útil de seguridad de encapsulado (ESP) del modo de túnel y el nivel de seguridad es alto. Por lo tanto, la presente invención se refiere, principalmente, a la parte de la interacción entre el agente HA y el modo CN en el procedimiento RRP.

En esta forma de realización, el procedimiento RRP se realiza como sigue:

A11. El mensaje CoTI interacciona con el mensaje CoT. Esta etapa comprende, además, la dos sub-etapas siguientes:

A111. El nodo MN envía el mensaje CoTI al nodo CN. En una cabecera de IPv6 del paquete, una dirección de origen es la CoA, una dirección de destino es el CN y una cabecera de movilidad es el mensaje CoTI.

A112. Después de recibir el mensaje CoTI, el CN calcula y genera una ficha generadora de claves temporal en función de la CoA y a continuación, envía el mensaje CoT que contiene la ficha generadora de claves temporal al MN. En una cabecera de IPv6 del paquete, una dirección de origen es el CN, una dirección de destino es la CoA y una cabecera de movilidad es el mensaje CoT.

A12. El mensaje HoTI interacciona con el mensaje HoT. Esta etapa comprende, además, las cuatro sub-etapas siguientes:

A121. El MN envía el mensaje HoTI al HA en el modo de túnel. En una cabecera de IPv6 exterior del paquete, una dirección de origen es la CoA y una dirección de destino es el HA. En una cabecera de IPv6 interior, protegida por la cabecera ESP en el modo de túnel, una dirección de origen es la HoA, una dirección de destino es el CN y una cabecera de movilidad es el mensaje HoTI.

A122. Después de recibir el mensaje HoTI enviado por el MN en el modo de túnel, el HA realiza un procesamiento de seguridad de protocolos IP (IPSec) para obtener el paquete de IPv6 interior. La dirección de origen, en el paquete interior, se sustituye por el HA y se añade una cabecera de extensión de opción de destino entre el paquete de IPv6 y la cabecera de movilidad para reenviar el mensaje HoTI y CN. Por lo general, una opción de HoA se coloca en la cabecera de extensión de la opción de destino para transmitir la HoA. En esta forma de realización, el agente HA sustituye la HoA con una SHoA correspondiente con el fin de ocultar la HoA del MN. De este modo, una nueva opción, es decir, una opción de SHoA se utiliza para transmitir la SHoA en la cabecera de extensión de destino.

Para garantizar la privacidad de la SHoA y para asegurar que la SHoA pueda obtenerse por el agente HA y el nodo MN mediante cálculo, el método para calcular la SHoA, en esta forma de realización, es como sigue:

SHoA = Primera (128, PRF (Kmh, Mensaje1))

en donde Kmh es una clave compartida entre el MN y el HA y Mensaje1 está constituido por la información que se puede compartir por el MN y el HA, tal como la dirección CoA, HoA y CN y la dirección HA. En esta forma de realización, Mensaje1 = CoA / HoA / CN), es decir, el Mensaje1 se forma conectando la CoA, la HoA y el CN. La SHoA puede cambiar con la CoA añadiendo la CoA en la expresión para generar la SHoA, diferentes HoAs enlazadas a la misma CoA pueden generar diferentes SHoAs añadiendo la HoA en la expresión y diferentes comunicaciones del CN pueden utilizar diferentes SHoAs añadiendo el CN en la expresión. PRF es una función pseudo-aleatoria, que indica que la Kmh se utiliza para procesar el mensaje Mensaje1 para generar una salida pseudo-aleatoria. En este caso, PRF puede ser una función de algoritmo de código de autenticación de mensaje Hash, por ejemplo, HMAC_SHA1. 'Primera' es una función de corte para realizar el corte de los primeros bits del encadenamiento separado (hash) de salida de PRF. Cuando la SHoA se utiliza para sustituir la HoA, la longitud de la SHoA debe ser coherente con la de la HoA y de este modo, se cortan 128 bits en la expresión anterior. Después de que el HA calcule la SHoA, se memoriza la asociación entre la SHoA y la HoA.

A123. Después de recibir el mensaje HoTI, el CN conoce que la SHoA se utiliza en función del tipo de opción en la cabecera de extensión de la opción de destino. Por lo tanto, cuando se calcula una ficha generadora de claves de origen, se utiliza la SHoA. A continuación, se envía el mensaje HoT que contiene la ficha generadora de claves de origen. En

general, una cabecera de enrutamiento de tipo 2 necesita configurarse en un paquete enviado para transmitir la HoA del MN. En la presente invención, el CN utiliza la SHoA correspondiente para sustituir la HoA. En una cabecera de IPv6 del paquete enviado, una dirección de origen es el CN, una dirección de destino es el HA, la cabecera de enrutamiento de tipo 2 transmite la SHoA y una cabecera de movilidad es el mensaje HoT.

A124. Después de recibir el mensaje HoT enviado por el CN, el agente HA necesita reenviar el mensaje HoT al MN en el modo de túnel. En primer lugar, el HoA correspondiente se encuentra en función de la SHoA en la cabecera de enrutamiento de tipo 2 y a continuación, la dirección de destino en la cabecera de IPv6 del mensaje HoT se sustituye por la HoA. A continuación, se realiza el encapsulado del túnel y el envío del paquete. En la cabecera de IPv6 exterior del paquete enviado, una dirección de origen es el HA, una dirección de destino es la CoA, una dirección de origen en la cabecera de IPv6 interior protegida por la cabecera ESP en el modo de túnel, es el CN, una dirección de destino es la HoA y una cabecera de movilidad es el mensaje HoT.

En este caso, las etapas A11 y A12 se pueden realizar simultáneamente.

A2. Después de que el MN reciba el mensaje CoT directamente enviado por el CN y el mensaje HoT reenviado por el HA, el procedimiento RRP finaliza y el MN genera una Kbm en función de la ficha generadora de claves de origen y de la ficha generadora de claves temporal reenviada por el CN. En general, la Kbm se calcula aplicando la expresión siguiente:

Kbm = HMAC_SHA1 (Home Keygen Token / Care-of Keygen Token)

Es decir, la Kbm se obtiene realizando un algoritmo de Hash HMAC_SHA1 en la secuencia constituida por la ficha generadora de claves de origen y la ficha generadora de claves temporal.

A3. El MN envía el mensaje de BU al CN para realizar la actualización de enlace. En condiciones normales, el paquete en el mensaje de BU transmite la cabecera de extensión de opción de destino, que incluye la opción de HoA para transmitir la HoA. En la presente invención, para ocultar la HoA, el MN coloca la SHoA correspondiente en la opción de HoA para sustituir la HoA. Mientras tanto, para enviar la asociación entre la HoA y la SHoA al CN, el MN utiliza la opción de HoA cifrada en el mensaje de BU y coloca la HoA cifrada con la Kbm en la opción de HoA cifrada. En una cabecera de IPv6 del paquete de BU, una dirección de origen es la CoA y la dirección de destino es el CN. La cabecera de extensión de opción de destino transmite la opción de HoA para colocar la SHoA, y una cabecera de movilidad es el mensaje de BU que incluye las opciones del número de secuencia, la opción de HoA cifrada, el índice de números aleatorios temporal de origen, el índice de número aleatorio temporal y el código de autorización de mensajes. Entre lo que antecede, la opción de HoA cifrada se añade recientemente en la presente invención.

A4. Después de recibir el mensaje de BU desde el MN, el CN recupera la HoA a partir de la opción de HoA cifrada por intermedio de la Kbm y a continuación actualiza el enlace de la SHoA, la HoA y la CoA para la lista de memorización de enlace. En condiciones normales, el CN reenvía un mensaje de confirmación de enlace (BA) al MN, indicando que está completado el proceso de BU. A continuación, el MN y el CN pueden realizar la transmisión de paquetes directamente en el modo de optimización de rutas.

Para evitar que la HoA del MN quede expuesta a un *eavesdropper* en la transmisión de paquetes subsiguiente, la opción de HoA de la cabecera de extensión de la opción de destino transmite la SHoA en el paquete enviado al CN desde el MN y la cabecera de enrutamiento de tipo 2 transmite la SHoA en el paquete enviado al MN desde el CN. De este modo, el *eavesdropper* no puede obtener la HoA de un abonado móvil mediante la intercepción del paquete.

Forma de realización 2: un método para la actualización de enlace en el sistema IPv6 móvil. La Figura 2 ilustra el proceso del método, que incluye etapas similares a las descritas en la forma de realización 1. La diferencia entre la forma de realización 2 y la forma de realización 1 radica en que esta forma de realización adopta un método para generar un número de secuencia aleatorio de un paquete de BU en las etapas siguientes.

B1. Una SHoA sustituye una HoA para realizar un procedimiento RRP entre un agente HA y un nodo CN. Para más detalles, referirse a la etapa A1 de la forma de realización 1.

B2. Después de que un MN reciba un mensaje CoT directamente enviado por el CN y un mensaje HoT reenviado por el HA, finaliza el procedimiento RRP. El nodo MN genera una Kbm en función de una ficha generadora de claves de origen y una ficha generadora de claves temporal reenviada por el nodo CN.

B3. El MN envía un mensaje de BU al CN para realizar la actualización de enlace. Esta etapa comprende, además, las cuatro sub-etapas siguientes:

B31. El MN coloca la SHoA correspondiente en una opción de HoA de una cabecera de extensión de opción de destino de un paquete para enviar el mensaje de BU para sustituir la HoA.

B32. El mensaje de BU utiliza una opción de HoA cifrada y coloca la HoA cifrada con una Kbm en la opción de HoA cifrada.

B33. Se calcula un incremento del número de secuencia aleatorio (seq_increment). El seq_increment obtenido se añade a un número de secuencia anterior para obtener un número de secuencia del mensaje de BU y el número de secuencia se coloca en una opción del mensaje de BU. En esta forma de realización, la expresión para calcular el incremento seq_increment es como sigue:

Seq_increment = Primera (8, PRF (Kbm, Mesaje2))

en donde el Mensaje2 es un mensaje que contiene un número de secuencia anterior (Seq#) o un incremento seq_increment anterior y se expresa como sigue:

Mensaje2 (Seq#Expresión) o

Mensaje2 = (seq_increment# / Expresión);

en donde la Expresión se obtiene combinando la información asociada con, y compartida por, lo nodos MN y CN, por ejemplo, la CoA y HoA del MN y la dirección de CN. Po supuesto, la Expresión puede ser nula. En esta forma de realización, la función pseudo-aleatoria PRF es HMAC_SHA1 y la función Primera corta los primeros ocho bits.

En particular, para mejorar la intractabilidad de los números de secuencia, si el incremento seq_increment calculado, según el método anterior, es cero, se calcula un número seq_increment con la expresión siguiente:

Seq_increment = Primera (8, Kbm XOR HoA)

en donde XOR es una función lógica de OR exclusiva para realizar una operación de OR exclusiva en la Kbm y la HoA.

En este caso, las etapas B31 a B33 se pueden realizar simultáneamente.

B34. El paquete de BU se envía. En una cabecera de IPv6 del paquete de BU, una dirección de origen es la CoA y una dirección de destino es el CN. Una cabecera de extensión de opción de destino transmite una opción de HoA para colocar la SHoA y una cabecera de movilidad es el mensaje de BU que incluye opciones tales como el número de secuencia y la opción HoA cifrada.

B4. Después de recibir el mensaje de BU desde el MN, el CN recupera la HoA desde la opción de HoA cifrada a través de la Kbm y a continuación, realiza la actualización de enlace de la SHoA, la HoA y la CoA para la lista de memorización de enlaces.

Forma de realización 3: un método para la actualización de enlace en el sistema IPv6 móvil. La Figura 3 ilustra el proceso del método, que incluye etapas similares a las de la forma de realización 1. La diferencia entre las formas de realización 3 y 1 radica en que, en esta forma de realización, cuando un MN envía un paquete de BU para realizar la actualización de enlace, un índice de HoA correspondiente a cada HoA se transmite también para el enlace de la HoA, CoA, SHoA y el índice HoA. La forma de realización 3 incluye las etapas siguientes.

C1: Una SHoA sustituye una HoA para realizar un procedimiento RRP entre un HA y un CN. Para más detalles, referirse a la etapa A1 de la forma de realización 1.

C2: Después de que un MN reciba un mensaje CoT directamente enviado por el CN y un mensaje HoT reenviado por el HA, finaliza el procedimiento RRP. El MN genera una Kbm en función de una ficha generadora de claves de origen y una ficha generadora de claves temporal reenviada por el CN.

C3: El MN envía un mensaje de BU al CN para realizar la actualización de enlace. Esta etapa comprende, además, las cuatro sub-etapas siguientes.

C31: El MN coloca la SHoA correspondiente en una opción de HoA de un paquete para enviar el mensaje de BU para sustituir la HoA.

C32: El mensaje de BU utiliza una opción de HoA cifrada y coloca la HoA cifrada con una Kbm en la opción de HoA cifrada.

C33: El mensaje de BU transmite un índice de HoA.

El índice de HoA es un valor correspondiente a cada HoA del MN proporcionado por el MN. Cuando un MN tiene una o más HoAs, una lista de HoA se almacena en una memoria caché del MN. La lista se memoriza en una matriz, una lista encadenada o en otros formatos. Cada una de las n (n> =1) HoAs del MN es objeto de mapeado único para un conjunto de números desde 0 a n-1 (o desde 1 a n). Por ejemplo, 0 a n-1 (o 1 a n) son subíndices de matriz de la lista de HoA almacenada como la matriz o marcas de las posiciones de memoria de las HoAs. Por lo tanto, los subíndices de la matriz

de la lista de HoA del MN y se pueden utilizar como el índice de HoA, mediante el cual se pueden obtener directamente las HoAs correspondientes.

En este caso, las etapas C31 a C33 se pueden realizar simultáneamente.

C34: El paquete de BU es enviado. En una cabecera de IPv6 del paquete de BU, una dirección de origen es la CoA y una dirección de destino es el CN. Una cabecera de extensión de opción de destino transmite una opción de HoA para colocar la SHoA y una cabecera de movilidad es el mensaje de BU que incluye opciones tales como el número de secuencia, la opción de HoA cifrada y el índice de HoA.

C4: Después de recibir el mensaje de BU desde el MN, el CN recupera la HoA desde la opción de HoA cifrada a través de la Kbm y a continuación, actualiza el enlace de la SHoA, la HoA, la CoA y el índice de HoA en la lista de memoria caché de enlaces.

Por supuesto, puesto que el índice de HoA necesita memorizarse, las entradas de la memoria de enlace de la HA y del CN deben añadirse, además, con un campo de índice de HoA.

Después de que se complete la actualización de enlace de esta forma de realización, en el envío de paquetes subsiguiente, una nueva “cabecera de extensión de índice de enlace”, que transporta el índice HoA, se puede utilizar para sustituir la opción de HoA o la cabecera de enrutamiento de tipo 2. El índice de HoA es, no obstante, un valor de puntero corto y la opción de HoA y la cabecera de enrutamiento de tipo 2 tienen ambas 128 bits sin importar la transmisión de la HoA o la SHoA. Por lo tanto, la longitud de la cabecera se reduce en gran medida. Además, puesto que el parámetro correspondiente a la HoA que aparece en el paquete es solamente el índice de HoA, se mejora la seguridad. Por supuesto, la “cabecera de extensión del índice de enlace” no es obligatoria y se puede añadir una “opción de índice de enlace” a la cabecera de movilidad para transmitir el índice de HoA.

Forma de realización 4: un sistema de comunicación IPv6 móvil. Según se ilustra en la Figura 4, el sistema incluye un MN 100, un CN 200 y un HA 300.

El MN 100 está adaptado para enviar un mensaje de CoTI al CN 200, para enviar un mensaje HoTI al HA 300, para recibir un mensaje CoT que contiene una ficha generadora de claves temporal reenviada por el CN 200, para recibir un mensaje HoT que contiene una ficha generadora de claves de origen reenviada por el HA 300, para generar una Kbm basada en la ficha generadora de claves de origen y la ficha generadora de claves temporal, para añadir una opción de HoA cifrada en un mensaje de BU que transmite una HoA cifrada con la Kbm y para utilizar una SHoA para sustituir la HoA para enviar el mensaje de BU al CN 200.

El HA 300 está adaptado para reenviar el mensaje de HoTI al CN 200, para transmitir una cabecera de extensión de opción de destino que contiene una opción SHoA y para transmitir la SHoA en un paquete enviado, para recibir el mensaje HoT enviado por el CN 200, para buscar la HoA correspondiente en función de la SHoA en una cabecera de enrutamiento de tipo 2 en el paquete y para reenviar el mensaje de HoT al MN 100 en un modo de túnel.

El CN 200 está adaptado para recibir el mensaje HoTI reenviado por el HA 300, para sustituir la HoA con la SHoA, para generar la ficha generadora de claves de origen, para reenviar el mensaje HoT que contiene la ficha generadora de claves de origen al HA 300, para transmitir la cabecera de enrutamiento de tipo 2 que transmite la SHoA en el paquete enviado y para enlazar la SHoA, la HoA y una CoA en función del mensaje de BU.

El sistema de esta forma de realización se puede aplicar en los métodos de BU de las formas de realización 1 a 3.

La Figura 5 ilustra las estructuras internas del nodo MN 100, el nodo CN 200 y el agente HA 300 del sistema de comunicación IPv6 móvil en la forma de realización 4.

El MN 100 incluye una primera unidad de enrutabilidad de retorno 110, una primera unidad de BU 120 y una unidad de Kbm 140 y puede incluir, además, una unidad de SHoA 130 y una primera unidad de número de secuencia 150.

La unidad SHoA 130 está adaptada para calcular y generar la SHoA en función de una clave compartida con el HA 300 y un mensaje que contiene la CoA, la HoA, una dirección del CN 200 y/o una dirección del HA 300 y para proporcionar la SHoA a la primera unidad de enrutabilidad de retorno 110 y la primera unidad de BU 120 para su uso.

La primera unidad de enrutabilidad de retorno 110 está adaptada para realizar un procedimiento de enrutabilidad de retorno (RRP) que incluye la obtención de fichas generadoras de claves a partir de una segunda unidad de enrutabilidad de retorno (220) del CN 200, en donde las fichas generadoras de claves incluyen la ficha generadora de claves temporal y la ficha generadora de claves de origen obtenida partir del mensaje CoT y del mensaje HoT, respectivamente y proporcionar a la salida las fichas generadoras de claves a la unidad de Kbm 140.

La unidad de Kbm 140 está adaptada para generar la Kbm basada en las fichas generadoras de claves y proporcionar la Kbm a la primera unidad de enrutabilidad de retorno 110 y la primera unidad de BU 120 para su uso.

La primera unidad de BU 120 está adaptada para utilizar la SHoA para sustituir la HoA para enviar el mensaje de BU a una segunda unidad de BU 220 del CN 200 y para transmitir la HoA cifrada con la Kbm en el mensaje de BU. De este modo, el CN 200 puede actualizar el enlace de la SHoA, la HoA y la CoA, en consecuencia. La primera unidad de BU 120 puede transmitir un índice de HoA correspondiente a cada HoA en el mensaje de BU, de modo que el CN 200 pueda enlazar el índice de HoA, SHoA, HoA y CoA.

El mensaje de BU suele transmitir un número de secuencia, que se puede proporcionar por la primera unidad de BU 150. La primera unidad de BU 150 añade un número de secuencia anterior y un incremento del número de secuencia actual para generar un número de secuencia actual. En este caso, el incremento del número de secuencia actual se calcula en función de la Kbm y del número de secuencia anterior o un incremento del número de secuencia anterior. Los detalles del algoritmo para calcular el incremento del número de secuencia se describen en las formas de realización anteriores del método y no se describirá aquí de nuevo.

El CN 200 incluye una segunda unidad de enrutabilidad de retorno 210, una segunda unidad de BU 220 y una unidad de Kbm 240 y puede incluir, además, una segunda unidad de número de secuencia 250.

La segunda unidad de enrutabilidad de retorno 210 está adaptada para realizar un procedimiento RRP que incluye la sustitución de la HoA con la SHoA para realizar un procedimiento RRP con una tercera unidad de enrutabilidad de retorno 310 del HA 300 y reenviar las fichas generadoras de claves a la primera unidad de enrutabilidad de retorno 110 del MN 100. Las fichas generadoras de claves incluyen la ficha generadora de claves de origen y la ficha generadora de claves temporal. La ficha generadora de claves temporal se genera por la segunda unidad de enrutabilidad de retorno 210 en función de la CoA del MN 100 y se envía al MN 100 en el mensaje CoT en el procedimiento RRP. La ficha generadora de claves de origen se genera por la segunda unidad de enrutabilidad de retorno 210 en función de la SHoA y se envía al nodo MN 100 en el mensaje de HoT en el procedimiento RRP.

La segunda unidad de enrutabilidad de retorno 210 proporciona a la salida las fichas generadoras de claves obtenidas para la unidad de Kbm 240. La unidad de Kbm 240 calcula y genera la Kbm en función de las fichas generadoras de claves y proporciona la Kbm a la segunda unidad de BU 220.

La segunda unidad de BU 220 está adaptada para recibir el mensaje de BU enviado por la primera unidad de BU 120 del nodo MN 100, para descifrar la HoA en el mensaje de BU en función de la Kbm proporcionada por la unidad de Kbm 240 y para enlazar la SHoA, la HoA y la CoA del nodo MN 100. Si el mensaje de BU incluye el índice de HoA, la segunda unidad de BU 220 puede incluir, además, un módulo de índice de direcciones para enlazar el valor de índice de HoA, la SHoA, la HoA y la CoA.

Si el nodo MN 100 incluye la primera unidad de número de secuencia 150, el CN 200 incluirá una segunda unidad de número de secuencia 250 correspondiente. La segunda unidad de número de secuencia 250 utiliza el mismo método para calcular el número de secuencia actual como para el primer número de secuencia 150, con el fin de recibir correctamente el mensaje de BU procedente del nodo MN 100.

El agente HA 300 incluye una tercera unidad de enrutabilidad de retorno 310, una segunda unidad de BU 220 y una unidad de SHoA 130. La unidad de SHoA 130 está adaptada para calcular y generar la SHoA en función de una clave compartida con el nodo MN 100 y un mensaje que contiene la CoA, la HoA, una dirección del CN 200 y/o una dirección del HA 300 y para proporcionar la SHoA a la tercera unidad de enrutabilidad de retorno 310 para su uso. La tercera unidad de enrutabilidad de retorno 310 está adaptada para realizar un procedimiento de RRP que incluye la sustitución de la HoA con la SHoA para realizar el procedimiento RRP con la segunda unidad de enrutabilidad de retorno 210 del CN 200.

Según las formas de realización de la presente invención, la HoA es sustituida con la SHoA en el procedimiento RRP. Después de que se obtenga la Kbm, la HoA en el paquete de BU se envía como una opción cifrada, de modo que la HoA aparezca solamente una vez en una forma cifrada en el paquete enviado al CN en el proceso de BU, con lo que se mejora la seguridad de la HoA en el proceso de BU. Además, según las formas de realización de la presente invención, la HoA puede añadirse a la expresión para generar la SHoA y de este modo múltiples HoAs enlazadas a la misma CoA son diferentes entre sí para impedir la confusión operativa. Además, en función de las formas de realización de la presente invención, el índice de HoA está enlazado con la HoA y la CoA, de modo que una nueva cabecera de extensión que contiene el índice de HoA se pueda utilizar para sustituir la opción de HoA o la cabecera de enrutamiento de tipo 2 que transmite la HoA en la transmisión de paquetes subsiguiente, lo que ahorra, en gran medida, el espacio de la cabecera, proporciona una más alta seguridad a los abonados móviles y no causa confusión cuando múltiples HoAs de MN están enlazadas con la misma CoA. Además, según las formas de realización de la presente invención, un método para calcular los números de secuencia de los paquetes de BU se da a conocer también para hacer que los números de secuencia tengan un incremento aleatorio que pueda conocerse por el MN y el CN y de este modo, se hace no susceptible de seguimiento los números de secuencia.

Considerando lo anterior, el método para la actualización de enlace en el sistema IPv6 móvil y el sistema de comunicación IPv6 han sido descritos con detalle. El principio y la puesta en práctica de la presente invención se ilustran con formas de realización especificadas.

Sin embargo, las anteriores formas de realización solamente están previstas para explicar el método y los puntos clave en la presente invención y no para limitar su alcance.

REIVINDICACIONES

1. Un nodo móvil, MN, en un sistema de comunicación IPv6, que comprende:

una primera unidad de enrutabilidad de retorno (110), adaptada para realizar un procedimiento de enrutabilidad de retorno, RRP, en donde una dirección de origen, HoA, del MN se sustituye por un sustituto de dirección de origen, SHoA, y en el curso del cual se obtienen fichas de generación de claves de un nodo correspondiente, CN;

una unidad de clave de gestión de enlace Kbm (140), adaptada para calcular y generar la Kbm en función de las fichas generadoras de claves y

una primera unidad de actualización de enlace, BU, (120), adaptada para enviar un mensaje de BU al CN sustituyendo la HoA del MN por la SHoA y para transmitir la HoA cifrada con la Kbm en el mensaje de BU;

en donde la HoA cifrada se transmite en una opción HoA cifrada en el mensaje de BU y

en donde el mensaje de BU comprende, además, un índice de HoA, cuyo valor es un valor de puntero y que corresponde a cada HoA del nodo MN.

2. El nodo móvil MN de un sistema de comunicación IPv6, según la reivindicación 1, que comprende, además, una unidad SHoA (130) adaptada para generar la SHoA según una clave compartida con un agente de origen, HA, y un mensaje que contiene una dirección temporal, CoA, del nodo MN, la HoA, una dirección de CN y/o una dirección del HA.

3. El nodo móvil MN en un sistema de comunicación IPv6 según la reivindicación 1, en donde el índice HoA es una marca de una posición de memoria o de un subíndice de matriz de una lista HoA del MN.

4. El nodo móvil MN en un sistema de comunicación IPv6 según la reivindicación 1 o 2, en donde el mensaje de BU comprende, además, un número de secuencia y el MN comprende, además, una primera unidad de número de secuencia (150) adaptada para obtener un número de secuencia actual añadiendo un número de secuencia anterior y un incremento de número de secuencia actual y el incremento de número de secuencia actual se calcula según la Kbm y el número de secuencia anterior o un incremento del número de secuencia anterior.

5. Un método de actualización de enlace del sistema IPv6 móvil, que comprende:

la realización, por un nodo correspondiente, CN, de un procedimiento de enrutabilidad de retorno, RRP, en donde una dirección de origen, HoA, de un nodo móvil, MN, se sustituye por un sustituto de dirección de origen, SHoA;

la recepción, por el nodo CN, de un mensaje de actualización de enlace BU, procedente del nodo MN, en donde el mensaje de BU transmite la SHoA, con la que se sustituye la HoA del MN y la HoA cifrada con una clave de gestión de enlace, Kbm, en donde la Kbm se genera en función de fichas de generación de claves obtenidas por el nodo MN desde el CN en el procedimiento RRP y

el enlace, por el CN, de la SHoA, la HoA y una dirección temporal, CoA, en función del mensaje de BU;

en donde la HoA cifrada se transmite en una opción HoA cifrada en el mensaje de BU;

en donde el mensaje de BU comprende, además, un índice HoA, cuyo valor es un valor de puntero y que corresponde a cada HoA de MN y

en donde el enlace por el CN según el mensaje de BU, comprende, además, el hecho de que el CN enlace la SHoA, la HoA, el índice de HoA y la CoA en función del mensaje de BU.

6. El método de actualización de enlace del sistema IPv6 móvil según la reivindicación 5, en donde el RRP es un procedimiento destinado a garantizar la seguridad de la comunicación entre el MN y el CN, que comprende el envío, por el CN, del mensaje CoT y del mensaje HoT al MN.

7. El método de actualización de enlace del sistema IPv6 móvil según la reivindicación 6, en donde las fichas generadoras de claves comprenden una ficha generadora de claves de origen y

el procedimiento de enrutabilidad de retorno, RRP, comprende:

la recepción, por el CN, de un mensaje de inicialización de prueba de origen, HoTI, reenviado por un agente de origen HA, procedente del MN y la SHoA se transmite en una cabecera de extensión de opción de destino del mensaje HoTI;

el cálculo, por el CN, de la ficha generadora de claves de origen según la SHoA y la SHoA se transmite en una cabecera de enrutamiento de tipo 2 de un mensaje de prueba de origen HoT y la ficha generadora de claves de origen está contenida en el mensaje HoT y

el reenvío, por el CN, del mensaje HoT al MN transmitido por el HA en un modo de túnel buscando la HoA correspondiente del MN según la SHoA en la cabecera de enrutamiento de tipo 2.

8. El método de actualización de enlace del sistema IPv6 móvil según la reivindicación 6, en donde las fichas generadoras de claves comprenden una ficha generadora de claves temporal y

el procedimiento RRP comprende:

la recepción, por el CN, de un mensaje de inicialización de prueba temporal, CoTI, procedente del MN y

el reenvío, por el CN, de un mensaje de prueba temporal, CoT, que contiene la ficha generadora de claves temporal al MN.

9. El método de actualización de enlace del sistema IPv6 móvil según la reivindicación 5, en donde cada valor del índice HoA es una marca de posición de memoria o un subíndice de matriz de cada HoA de una lista HoA conservada en memoria en el MN.

10. El método de actualización de enlace del sistema IPv6 móvil según la reivindicación 5, en donde la SHoA se calcula en función de una clave compartida entre el MN y el HA y un mensaje que contiene la CoA, la HoA, una dirección de CN y/o una dirección del HA.

11. El método de actualización de enlace del sistema IPv6 móvil según la reivindicación 9, en donde la SHoA se obtiene según una expresión como sigue:

SHoA = Primera (M, PRF (Kmh, Mensaje1))

en donde la SHoA es la dirección sustituto de la dirección de origen del MN, la Kmh es la clave compartida entre el MN y el HA, el Mensaje1 es el mensaje que contiene la CoA y la HoA del MN, la dirección del CN y/o la dirección del HA, la PRF es una función pseudo-aleatoria, la Primera es una función de corte y M es un número natural más pequeño que, o igual a, 128.

12. El método para actualización de enlace del sistema IPv6 móvil según cualquiera de las reivindicaciones 5 a 11, en donde el mensaje de BU comprende, además, un número de secuencia, el número de secuencia es una suma de un número de secuencia anterior y un incremento del número de secuencia, siendo el incremento del número de secuencia calculado en función de la Kbm y del número de secuencia anterior o de un incremento del número de secuencia anterior.

13. El método para actualización de enlace del sistema IPv6 móvil según la reivindicación 12, en donde el incremento del número de secuencia se obtiene según una expresión como sigue:

seq_increment = Primera (N, PRF (Kbm, Mensaje2))

en donde seq_increment es el incremento del número de secuencia, Kbm es la clave de gestión de enlace, el Mensaje2 es un mensaje que contiene el número de secuencia anterior o el incremento del número de secuencia anterior, la HoA y la CoA del MN y/o la dirección del CN, la PRF es una función pseudo-aleatoria, Primera es una función de corte y N es un número natural.

14. El método para actualización de enlace del sistema IPv6 móvil según la reivindicación 13, en donde si el incremento del número de secuencia es 0, se calcula otro incremento del número de secuencia según una expresión como sigue:

seq_increment = Primera (N, Kbm XOR HoA)

en donde la HoA es la dirección de origen del MN y XOR es una función de OR exclusiva.

15. Un sistema de comunicación de IPv6 móvil, que comprende un nodo móvil, MN, (100), un nodo correspondiente, CN, (200) y un agente de origen HA (300), en donde

el MN (100) está adaptado para enviar un mensaje de inicialización de prueba temporal, CoTI, al CN (200), para enviar un mensaje de inicialización de prueba de origen, HoTI, al HA (300), para recibir un mensaje de prueba temporal, CoT, que contiene una ficha generadora de claves temporal reenviada por el CN (200), para recibir un mensaje de prueba de origen, HoT, que contiene una ficha generadora de claves de origen transmitida por el HA (300), para generar una unidad de clave de gestión de enlace, Kbm, basada en la ficha generadora de claves de origen y la ficha generadora de claves

temporal y para enviar al CN un mensaje de BU que contiene un sustituto de dirección de origen, SHoA, con la que se sustituye una dirección de origen, HoA, del MN;

el HA (300) está adaptado para enviar el mensaje HoTI al CN (200), con la transmisión de la SHoA en una cabecera de extensión de opción de destino que contiene una opción SHoA del mensaje HoTI, para recibir el mensaje HoT enviado por el CN (200) para buscar la HoA correspondiente del MN (100) en función de la SHoA en una cabecera de enrutamiento de tipo 2 del mensaje HoT y para transmitir el mensaje HoT al MN (100) en un modo de túnel y

el CN (200) está adaptado para recibir el mensaje HoTI transmitido por el HA (300), para sustituir la HoA por la SHoA con el fin de generar la ficha generadora de claves de origen, para reenviar el mensaje HoT que contiene la ficha generadora de claves de origen al HA (300) y para transmitir la SHoA en la cabecera de enrutamiento de tipo 2 del mensaje HoT y para enlazar la SHoA, la HoA y una dirección temporal, CoA, en función del mensaje de BU enviado a partir del MN;

en donde la HoA, que está cifrada con la Kbm, se transmite en una opción HoA cifrada en el mensaje de BU y

en donde el mensaje de BU comprende, además, un índice HoA, cuyo valor es un valor de puntero y que corresponde a cada HoA del MN.

16. Un nodo correspondiente, CN, de un sistema de comunicación IPv6, que comprende:

una segunda unidad de enrutabilidad de retorno (210), adaptada para realizar un procedimiento de enrutabilidad de retorno, RRP, en donde una dirección de origen, HoA, del MN es sustituida por un sustituto de dirección de origen, SHoA, y durante el cual, se reenvían fichas de generación de claves a un nodo móvil, MN, en el RRP;

una unidad de claves de gestión de enlace, Kbm, (240), adaptada para calcular y generar la Kbm en función de las fichas de generación de claves y

una segunda unidad de actualización de enlace, BU, (220), adaptada para obtener una dirección de origen, HoA, del MN a partir de un mensaje de BU enviado por el MN y para enlazar un sustituto de dirección de origen, SHoA de MN, la HoA desde MN y una dirección temporal CoA, del MN, en donde la HoA está cifrada con la Kbm;

en donde la HoA cifrada se transmite en una opción HoA cifrada en el mensaje de BU;

en donde el mensaje de BU comprende, además, un índice HoA, cuyo valor es un valor de puntero y que corresponde a cada HoA del MN;

en donde la HoA se obtiene recuperándose a partir de la opción HoA cifrada con la Kbm y

en donde la segunda unidad BU (220) comprende un módulo de índice de dirección adaptado para enlazar un valor del índice HoA, la SHoA, la HoA y la CoA.

17. El nodo correspondiente CN de un sistema de comunicación IPv6 según la reivindicación 16, en donde las fichas generadores de claves comprenden una ficha generadora de claves de origen y una ficha generadora de claves temporal, siendo la ficha generadora de claves temporal generada por la segunda unidad de enrutabilidad de retorno (210), según la CoA, del MN y se envía al MN en un mensaje de prueba temporal, CoT, en el procedimiento RRP y la ficha generadora de claves de origen se genera por la segunda unidad de enrutabilidad de retorno (210) en función de la SHoA del MN y se envía al MN en un mensaje de prueba de origen, HoT, en el RRP.

18. El nodo correspondiente CN de un sistema de comunicación IPv6 según la reivindicación 16, en donde:

el RRP es un procedimiento destinado a garantizar la seguridad de la comunicación entre el MN y el CN, que comprende: el envío, por el CN, del mensaje CoT y del mensaje HoT al MN.

19. El nodo correspondiente CN de un sistema de comunicación IPv6 según una cualquiera de las reivindicaciones 16 a 18, en donde el mensaje de BU comprende, además, un número de secuencia y

el CN comprende, además, una segunda unidad de número de secuencia (250) adaptada para obtener un número de secuencia actual añadiendo un número de secuencia anterior y un incremento del número de secuencia actual, siendo el incremento del número de secuencia actual calculado según la Kbm y el número de secuencia anterior o un incremento del número de secuencia anterior.

20. El nodo móvil MN de un sistema de comunicación IPv6 según la reivindicación 1, en donde el RRP es un procedimiento destinado a garantizar la seguridad de la comunicación entre el MN y el CN que comprende: el envío, por el CN, del mensaje CoT y del mensaje HoT al nodo MN.

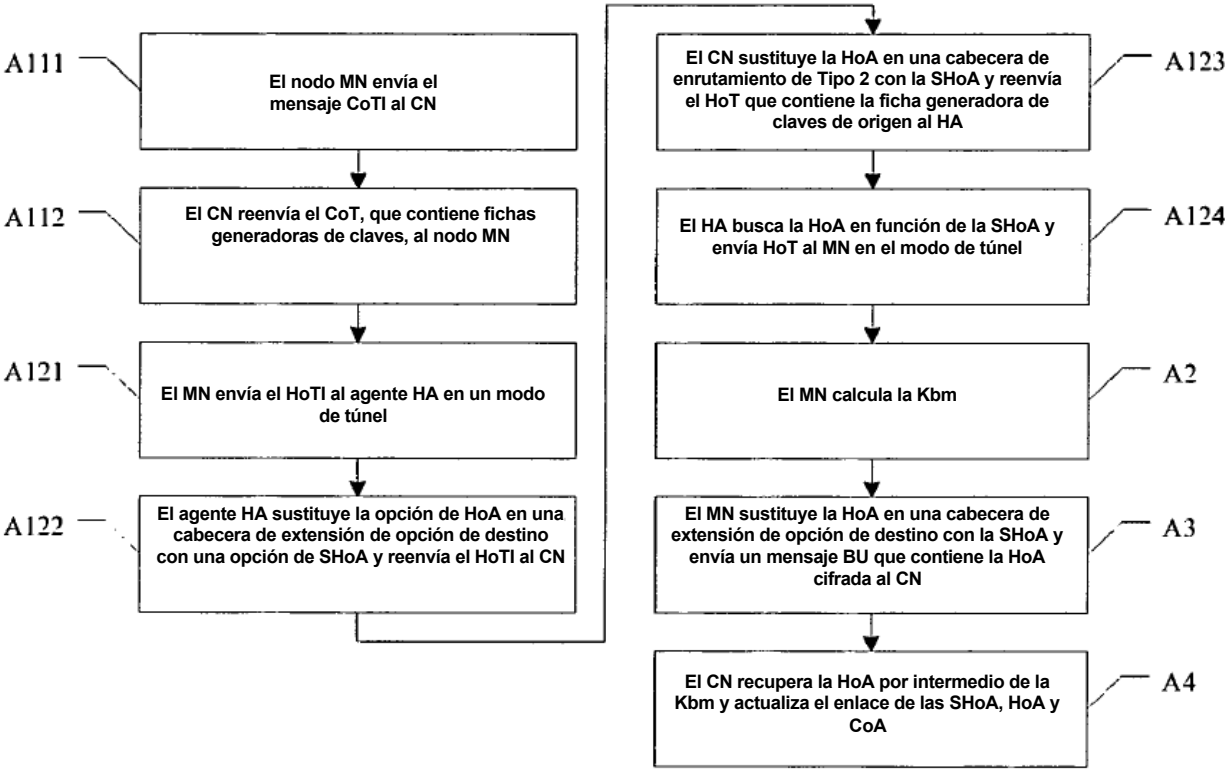
A111
El nodo MN envía el mensaje CoTI al CN
A112
El CN reenvía el CoT, que contiene fichas generadoras de claves, al nodo MN
A121
El MN envía el HoTI al agente HA en un modo de túnel
A122
El agente HA sustituye la opción de HoA en una cabecera de extensión de opción de destino con una opción de SHoA y reenvía el HoTI al CN
A123
El CN sustituye la HoA en una cabecera de enrutamiento de Tipo 2 con la SHoA y reenvía el HoT que contiene la ficha generadora de claves de origen al HA
A124
El HA busca la HoA en función de la SHoA y envía HoT al MN en el modo de túnel
A2
El MN calcula la Kbm
A3
El MN sustituye la HoA en una cabecera de extensión de opción de destino con la SHoA y envía un mensaje BU que contiene la HoA cifrada al CN
A4
El CN recupera la HoA por intermedio de la Kbm y actualiza el enlace de las SHoA, HoA y CoA

Figura 1

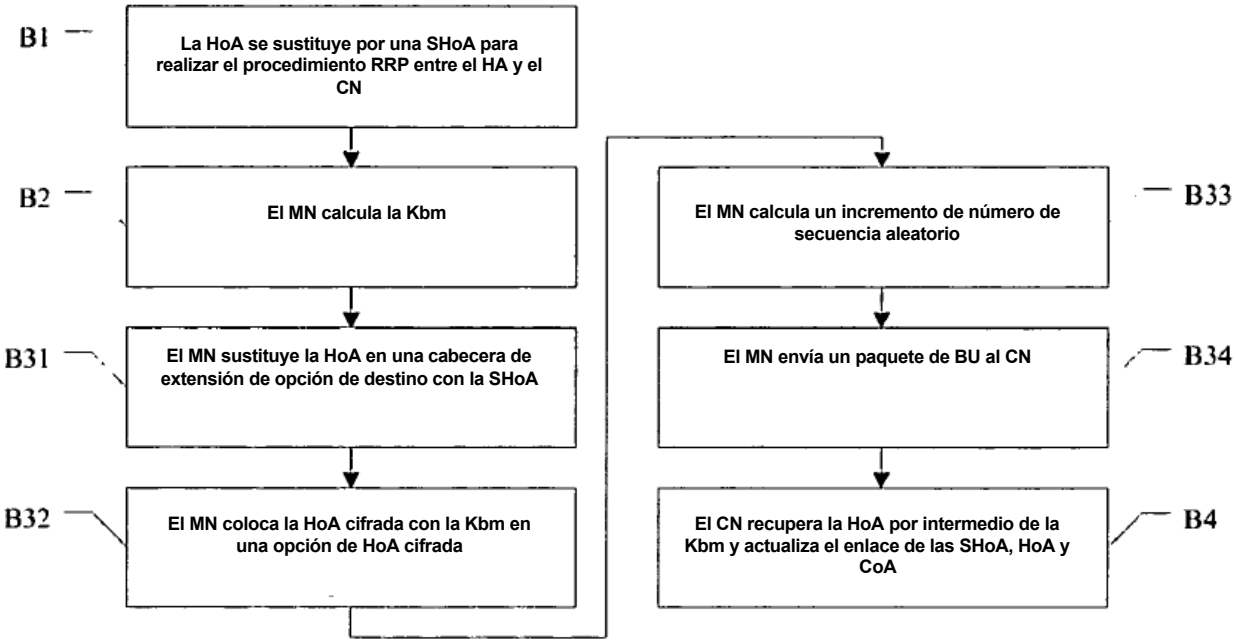

Figura 2

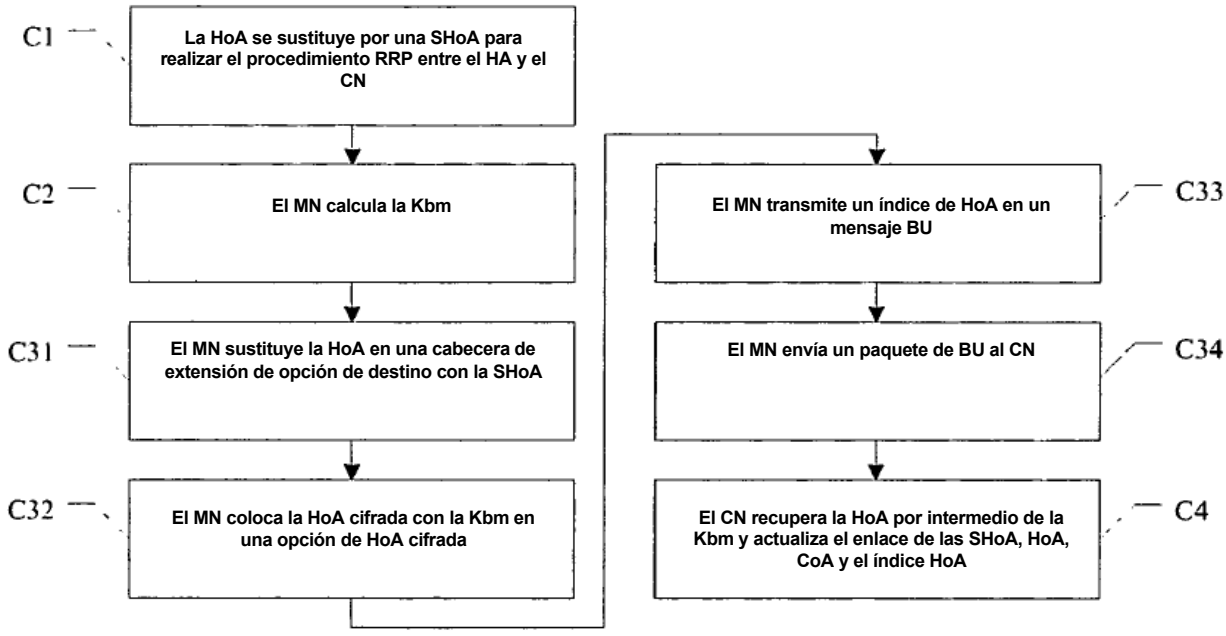

Figura 3

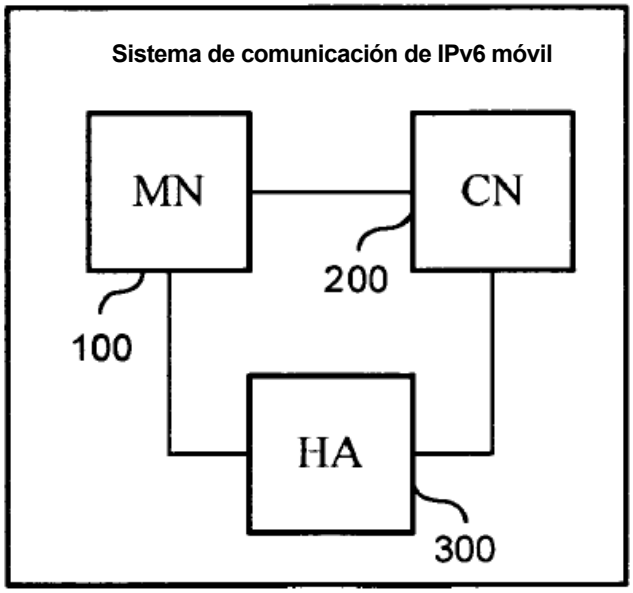

Figura 4

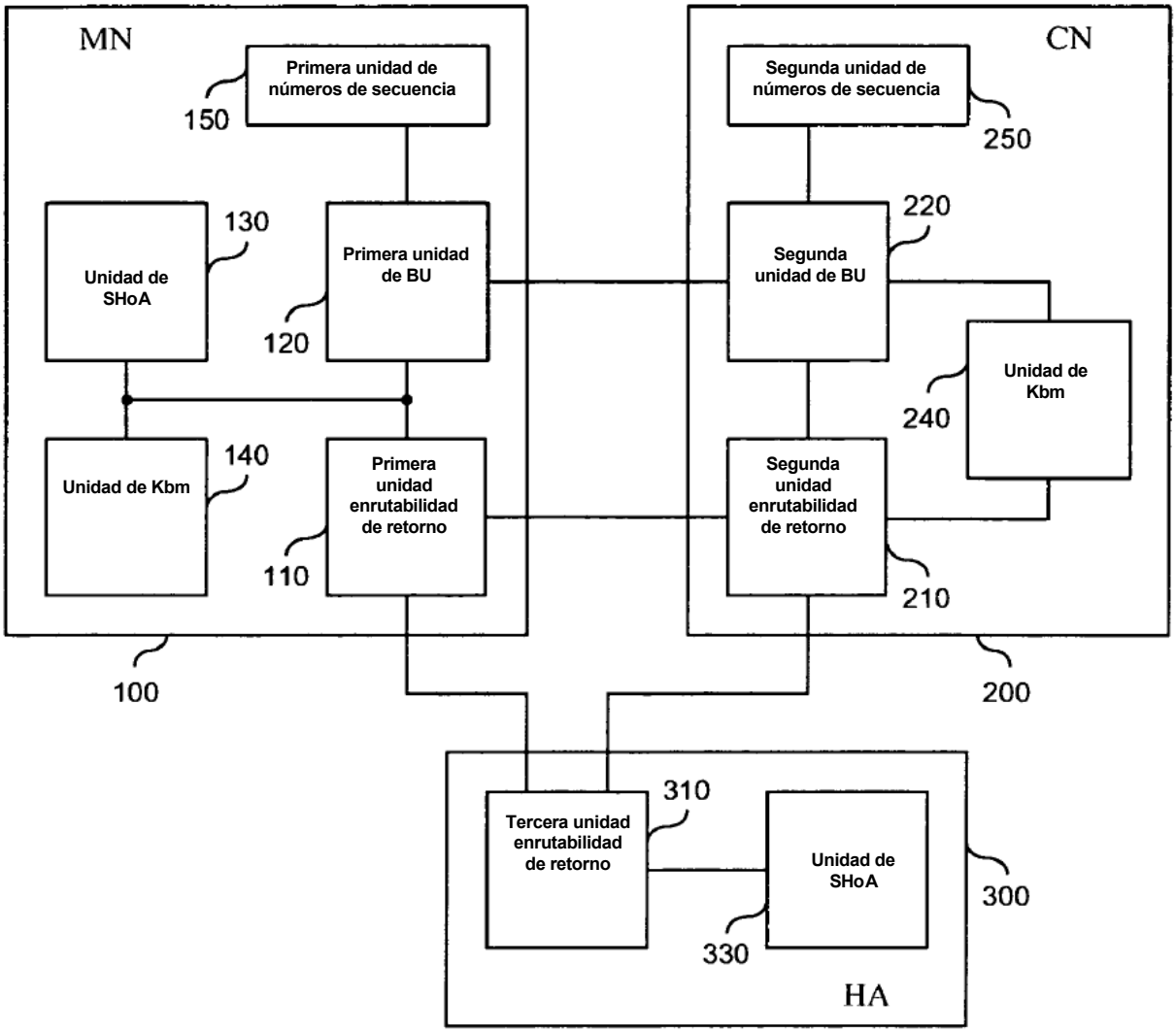
MN
Primera unidad de números de secuencia
150
Unidad de SHoA
130
Primera unidad de BU
120
Unidad de Kbm
140
Primera unidad enrutabilidad de retorno
110
100
CN
Segunda unidad de números de secuencia
250
Segunda unidad de BU
220
Unidad de Kbm
240
Segunda unidad enrutabilidad de retorno
210
200
Tercera unidad enrutabilidad de retorno
310
Unidad de SHoA
330
300
HA

Figura 5