(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 377 317**

(51) Int. CI.:
H04L 9/08 (2006.01)
H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07764233 .8**
(96) Fecha de presentación: **17.07.2007**
(97) Número de publicación de la solicitud: **2086159**
(97) Fecha de publicación de la solicitud: **05.08.2009**

(54) Título: **Procedimiento de gestión de clave de red y de actualización de clave de sesión**

(30) Prioridad:
23.09.2006 CN 200610104679

(45) Fecha de publicación de la mención BOPI:
26.03.2012

(45) Fecha de la publicación del folleto de la patente:
26.03.2012

(73) Titular/es:
China Iwncomm Co., Ltd
A201, Qinfeng Ge Xi'an Software Park No. 68 Keji 2nd Road Xi'an High-Tech Industry Dev. Zone
Xi'an
Shaanxi 710075, CN

(72) Inventor/es:
PANG, Liaojun;
CAO, Jun;
TIAN, Haibo;
HUANG, Zhenhai y
ZHANG, Bianling

(74) Agente/Representante:
Pons Ariño, Ángel

DESCRIPCIÓN

Procedimiento de gestión de clave de red y de actualización de clave de sesión

La presente solicitud reivindica la prioridad respecto a la solicitud de patente china n.º 200610104b79.4, titulada "METHOD FOR MANAGING NETWORK KEY AND UPDATING TRAFFIC ENCRYPTION KEY", presentada en la Oficina de Patentes china el 23 de septiembre de 2006.

Campo de la invención

La presente invención se refiere a un procedimiento para gestionar una clave de red y actualizar una clave de cifrado de tráfico. En particular, el procedimiento se puede aplicar en una red de cable y una red inalámbrica tal como una red inalámbrica de área local (WLAN), una red inalámbrica de área metropolitana (WMAN) y una red inalámbrica multimedia de banda ancha (BWM).

Antecedentes de la invención

El problema de seguridad de la red inalámbrica es mucho más importante que el de la Ethernet por cable. El Instituto de Ingenieros Eléctricos y Electrónicos de EE.UU. (IEEE) ha establecido los estándares con número de serie 802.11 y 802.16 para mejorar la seguridad de las redes inalámbricas de área local y las redes inalámbricas de área metropolitana y para proporcionar un acceso seguro a una estación base desde una estación móvil. China ha promulgado el estándar nacional de red inalámbrica de área local GB15629.11, que generalmente recibe el nombre de protocolo de infraestructura de confidencialidad y autenticación en WLAN (WLAN Authentication and Privacy Infrastructure, WAPI). La red BWM, al ser una nueva arquitectura de redes inalámbricas, integra la comunicación de datos y la comunicación de difusión *(broadcast).* Los problemas de acceso seguro y comunicación segura se deben tratar en la red BWM. Uno de los problemas fundamentales para tratar la comunicación segura es el de cómo gestionar diversas claves en el sistema.

El estándar IEEE802.11 propone el protocolo de confidencialidad equivalente al cableado (Wired Equivalent Privacy, WEP) para aplicar la seguridad de WLAN, en la que la gestión de las claves es muy sencilla; es decir, se configura manualmente una clave compartida para su uso entre una estación móvil y un punto de acceso. Las dificultades radican en que no existe una solución perfecta para la gestión de claves, lo que dificulta la ampliación del sistema y perjudica a la flexibilidad del sistema.

El protocolo criptográfico WEP posee un grave fallo de seguridad. El estándar IEEE802.11i emplea cuatro protocolos de establecimiento de comunicación *(handshake)* para gestionar y deducir las claves, con lo cual se encarga del problema de seguridad de la WEP, pero posee los siguientes inconvenientes: la gestión de claves no puede estar basada en niveles de servicio, es decir, la deducción de la clave se lleva a cabo entre terminales y nodos de acceso específicos y no se pueden deducir claves diferentes para distintos servicios con el fin de lograr niveles de servicio diferenciados. La eficiencia de la negociación de claves de multidifusión es escasa, es decir, para actualizar una clave de multidifusión es necesario que el nodo de acceso y cada estación móvil lleven a cabo la actualización, lo cual reduce la eficiencia. No se pueden proporcionar diferentes claves de cifrado de multidifusión para diferentes servicios.

Algunos de los inconvenientes del protocolo WEP se solventan en el estándar nacional chino GB 15629.11. No obstante, el protocolo de gestión de claves de GB 15629.11 posee los mismos inconvenientes que el de IEEE802.11i.

Los criterios para WMAN del estándar IEEE802.16 propuestos por la IEEE de EE.UU. no pueden evitar que un atacante imite una estación base para engañar a una estación móvil, con lo que la gestión de claves no es segura. El estándar IEEE802.16e utiliza el procedimiento del estándar IEEE802.11i como referencia para proponer una solución mejorada. Dicha solución posee los siguientes inconvenientes:

La gestión de claves se lleva a cabo empleando una sincronización temporal, y esto complica la gestión de estados. El uso y el desuso de una nueva clave se determinan en función del tiempo. Resulta complicado mantener relojes de sincronización en un sistema distribuido. Existen muchos estados del sistema, lo que complica la gestión.

Resumen de la invención

La presente invención proporciona un procedimiento para la gestión de claves de red y la actualización de claves de cifrado de tráfico, que puede resolver los problemas técnicos de la escasa eficiencia en la negociación y actualización de claves de multidifusión y de la complicada gestión de los estados del sistema de la técnica anterior.

Las soluciones técnicas de la presente invención se definen en las reivindicaciones adjuntas.

Breve descripción de los dibujos

La figura 1 es un diagrama de un procedimiento de gestión de claves de unidifusión en una red de acuerdo con la presente invención; y

La figura 2 es un diagrama de un procedimiento de gestión de claves de cifrado de tráfico de multidifusión en una red de acuerdo con la presente invención

Descripción detallada de la invención

Las soluciones técnicas según formas de realización de la presente invención se describen de forma clara y completa a continuación, haciendo referencia a los dibujos de las formas de realización de la presente invención. Aparentemente, las formas de realización descritas constituyen tan solo una parte de las formas de realización de la presente invención, pero no todas las formas de realización de la presente invención. Todas las demás formas de realización que puedan realizar los expertos en la materia, sin actividad creadora, basadas en las anteriores formas de realización quedarán dentro del alcance de la presente invención.

En referencia a la figura 1, un procedimiento de gestión de claves de multidifusión en una red de acuerdo con la presente invención incluye las siguientes etapas.

110. Construcción de un paquete de solicitud de negociación de clave.

En el caso de una negociación de clave inicial, o si una estación móvil solicita una actualización de clave o recibe un paquete de notificación de actualización de clave procedente de una estación base, la estación móvil envía el paquete de solicitud de negociación de clave a la estación base, con el fin de activar un proceso de negociación de clave.

El paquete de notificación de actualización de clave incluye: una identidad de la estación base (BS)ID_{BS}, un identificador de asociación de seguridad SAID, un identificador de clave de autoridad AKID, un identificador de clave de cifrado de tráfico TEKID, y un código de integridad de mensaje MIC. El identificador de clave de cifrado de tráfico TEKID está adaptado para identificar una clave de cifrado de tráfico que se vaya a actualizar, y se calcula un valor del código de integridad de mensaje MIC a partir de una clave de comprobación de integridad deducida a partir de una clave de autoridad AK correspondiente al AKID. El identificador de asociación de seguridad SAID corresponde a un servicio particular. El ID del SAID puede diferenciar una asociación de seguridad (SA) de unidifusión de una SA de multidifusión.

El paquete de solicitud de negociación de clave incluye una identidad de la estación móvil (MS)ID_{MS}, un identificador de asociación de seguridad SAID, un identificador de clave de autoridad AKID, un identificador de clave de cifrado de tráfico TEKID, un número aleatorio seleccionado por la estación móvil N_{MS}, y un código de integridad de mensaje MIC. El identificador de clave de cifrado de tráfico TEKID está adaptado para identificar una clave de cifrado de tráfico que se vaya a actualizar, y se calcula un valor del código de integridad de mensaje MIC a partir de una clave de comprobación de integridad deducida a partir de una clave de autoridad AK correspondiente al AKID.

120. Construcción de un paquete de respuesta de negociación de clave.

(2.1) La estación base construye el paquete de respuesta de negociación de clave al recibir el paquete de solicitud de negociación de clave procedente de la estación móvil.

El paquete de respuesta de negociación de clave incluye: la identidad de la estación móvil ID_{MS}, la identidad de la estación base ID_{BS}, un identificador de asociación de seguridad SAID, el identificador de clave de autoridad AKID, un identificador de clave de cifrado de tráfico TEKID, un número aleatorio seleccionado por la estación móvil N_{MS}, un número aleatorio seleccionado por la estación base N_{BS}, un texto cifrado E_{KEK} (TEKM) de un material de clave de cifrado de tráfico TEKM seleccionado por la estación base y cifrado con una clave de cifrado de clave deducida a

partir de una clave de autoridad correspondiente al identificador de clave de autoridad AKID, un periodo de validez del material de clave de cifrado de tráfico TEKM $Life_{TEK}$, y un código de integridad de mensaje MIC. Un valor del número aleatorio seleccionado por la estación móvil N_{MS} debe ser el mismo que el de un campo correspondiente en el paquete de solicitud de negociación de clave, y se calcula un valor del código de integridad de mensaje MIC a partir de una clave de comprobación de integridad deducida a partir del TEKM, el N_{MS} y el N_{BS}.

(2.2) Si la estación base envía el paquete de notificación de actualización de clave antes de recibir el paquete de solicitud de negociación de clave, la estación base comprueba si los valores de los campos correspondientes del paquete de notificación de actualización de clave y el paquete de solicitud de negociación de clave son iguales entre sí; en caso afirmativo, la estación base construye el paquete de respuesta de negociación de clave; en caso contrario, la estación base desestima el paquete de solicitud de negociación de clave sin procesarlo.

(2.3) La estación base envía el paquete de respuesta de negociación de clave a la estación móvil, y deduce una clave de cifrado de sesión de unidifusión y una clave de comprobación de integridad.

130. Construcción de un paquete de reconocimiento de negociación de clave.

Al recibir el paquete de respuesta de negociación de clave procedente de la estación base, la estación móvil descifra el paquete de respuesta de negociación de clave con una clave de cifrado de clave deducida a partir de una clave de autoridad correspondiente al identificador de clave de autoridad AICID para obtener el material de clave de cifrado de tráfico TEKM, y construye el paquete de reconocimiento de negociación de clave.

El paquete de reconocimiento de negociación de clave incluye: la identidad de la estación base ID_{BS}, la identidad de la estación móvil ID_{MS}, un identificador de asociación de seguridad SAID, el identificador de clave de autoridad AKID, un identificador de clave de cifrado de tráfico TEKID, un número aleatorio seleccionado por la estación base N_{BS}, y un código de integridad de mensaje MIC. Un valor del número aleatorio seleccionado por la estación base N_{BS} debe ser el mismo que el de un campo correspondiente en el paquete de respuesta de negociación de clave, y se calcula un valor del código de integridad de mensaje MIC a partir de una clave de comprobación de integridad deducida a partir del TEKM, el N_{MS} y el N_{BS}.

En referencia a la figura 2, un procedimiento de gestión de claves de multidifusión de acuerdo con la presente invención incluye las siguientes etapas.

210. Un protocolo de de negociación de clave maestra de multidifusión.

(1.1) Construcción de un paquete de notificación de actualización de clave.

En el caso de que una estación base necesite actualizar una clave de cifrado de tráfico pero una estación móvil no inicie una solicitud de actualización de clave de cifrado de tráfico, la estación base envía el paquete de notificación de actualización de clave a la estación móvil, para comunicar a la estación móvil que actualice la clave de cifrado de tráfico. El paquete de notificación de actualización de clave se usa únicamente para actualizar la clave de cifrado de tráfico, no para una negociación de clave inicial.

El paquete de notificación de actualización de clave de cifrado de tráfico incluye: una identidad de la estación base ID_{BS}, un identificador de asociación de seguridad SAID, el identificador de clave de autoridad AKID, un identificador de clave de cifrado de tráfico TEKID, y un código de integridad de mensaje MIC. El identificador de clave de cifrado de tráfico está adaptado para identificar una clave de cifrado de tráfico que se vaya a actualizar, y se calcula un valor del código de integridad de mensaje MIC a partir de una clave de comprobación de integridad deducida a partir de una clave de autoridad correspondiente al AKID.

(1.2) Construcción de un paquete de solicitud de negociación de clave.

En el caso de una negociación de clave inicial, o si la estación móvil recibe el paquete de notificación de actualización de clave procedente de la estación base, la estación móvil envía el paquete de solicitud de negociación de clave a la estación base, con el fin de activar un proceso de negociación de clave.

El paquete de solicitud de negociación de clave incluye: una identidad de la estación móvil ID_{MS}, un identificador de asociación de seguridad SAID, un identificador de clave de autoridad AKID, un identificador de clave de cifrado de tráfico TEKID, un número aleatorio seleccionado por la estación móvil N_{MS}, y un código de integridad de mensaje

MIC. El identificador de clave de cifrado de tráfico TEKID está adaptado para identificar la clave de cifrado de tráfico que se vaya a actualizar, y se calcula un valor del código de integridad de mensaje MIC a partir de una clave de comprobación de integridad deducida a partir de una clave de autoridad AK correspondiente al AKID.

(1.3) Construcción de un paquete de respuesta de negociación de clave.

(1.3.1) La estación base construye el paquete de respuesta de negociación de clave al recibir el paquete de solicitud de negociación de clave procedente de la estación móvil.

El paquete de respuesta de negociación de clave incluye: la identidad de la estación móvil ID_{MS}, la identidad de la estación base DD_{BS}, un identificador de asociación de seguridad SAID, el identificador de clave de autoridad AKID, un identificador de clave de cifrado de tráfico TEKID, un número aleatorio seleccionado por la estación móvil N_{MS}, un número aleatorio seleccionado por la estación base N_{BS}, un texto cifrado E_{KEK} (TEKM) de un material de clave de cifrado de tráfico TEKM seleccionado por la estación base y cifrado con una clave de cifrado de clave deducida a partir de una clave de autoridad correspondiente al identificador de clave de autoridad AKID, un periodo de validez de la clave de cifrado de tráfico $Life_{TEK}$, y un código de integridad de mensaje MIC. Un valor del número aleatorio seleccionado por la estación móvil N_{MS} debe ser el mismo que el de un campo correspondiente en el paquete de solicitud de negociación de clave, y se calcula un valor del código de integridad de mensaje MIC a partir de una clave de comprobación de integridad deducida a partir del TEKM, el N_{MS} y el N_{BS}.

(1.3.2) Si la estación base envía el paquete de notificación de actualización de clave antes de recibir el paquete de solicitud de negociación de clave, la estación base comprueba si los valores de los campos correspondientes del paquete de notificación de actualización de clave y el paquete de solicitud de negociación de clave son iguales entre sí; en caso afirmativo, la estación base construye el paquete de respuesta de negociación de clave; en caso contrario, la estación base desestima el paquete de solicitud de negociación de clave sin procesarlo.

(1.3.3) La estación base envía el paquete de respuesta de negociación de clave a la estación móvil, y deduce una clave de cifrado de clave de grupo GKEK y una clave de integridad de mensaje de grupo GMIK.

(1.4) Construcción de un paquete de reconocimiento de negociación de clave.

Al recibir el paquete de respuesta de negociación de clave procedente de la estación base, la estación móvil descifra el paquete de respuesta de negociación de clave con una clave de cifrado de clave deducida a partir de una clave de autoridad correspondiente al identificador de clave de autoridad AKID para obtener un texto plano como material de clave de cifrado de tráfico TEKM, y construye el paquete de reconocimiento de negociación de clave. La estación móvil envía el paquete de reconocimiento de negociación de clave a la estación base, para deducir la clave de cifrado de clave de grupo GKEK y la clave de integridad de mensaje de multidifusión GMIK.

El paquete de reconocimiento de negociación de clave incluye: la identidad de la estación base ID_{BS}, la identidad de la estación móvil ID_{MS}, un identificador de asociación de seguridad SAID, el identificador de clave de autoridad AKID, un identificador de clave de cifrado de tráfico TEKID, un número aleatorio seleccionado por la estación base N_{BS}, y un código de integridad de mensaje MIC. Un valor del número aleatorio seleccionado por la estación base N_{BS} debe ser el mismo que el de un campo correspondiente en el paquete de respuesta de negociación de clave, y se calcula un valor del código de integridad de mensaje MIC a partir de una clave de comprobación de integridad deducida a partir del TEKM, el N_{MS} y el N_{BS}.

220. Un protocolo de distribución de clave de cifrado de tráfico de multidifusión.

(2.1) Solicitud de clave de cifrado de tráfico de multidifusión.

La estación móvil envía un paquete de solicitud de clave de cifrado de tráfico de multidifusión a la estación base si la estación móvil necesita negociar o actualizar una clave de cifrado de tráfico de multidifusión.

El paquete de solicitud de clave de cifrado de tráfico de multidifusión incluye: un identificador de asociación de seguridad SAID, un identificador de clave de cifrado de tráfico TEKID, un identificador de clave de cifrado de tráfico de grupo GTEKID, un número aleatorio seleccionado por la estación móvil N_{MS}, y un código de integridad de mensaje MIC. El identificador de clave de cifrado de tráfico de grupo GTEKID está adaptado para identificar la clave de cifrado de tráfico multidifusión que se vaya a negociar o solicitar, y se calcula un valor del código de integridad de mensaje MIC a partir de la clave de integridad de mensaje de grupo GMIK deducida a partir del TEKM

correspondiente al TEKID.

(2.2) Distribución de claves de cifrado de tráfico de multidifusión.

Al recibir el paquete de solicitud de clave de cifrado de tráfico de multidifusión procedente de la estación móvil, la estación base envía un paquete de distribución de claves de cifrado de tráfico de multidifusión a la estación móvil; o, si la estación base necesita actualizar una clave de multidifusión, la estación base emite por difusión un paquete de distribución de claves de cifrado de tráfico de multidifusión a todas las estaciones móviles.

El paquete de distribución de claves de cifrado de tráfico de multidifusión incluye: un identificador de asociación de seguridad SAID, un identificador de clave de cifrado de tráfico TEKID, un identificador de clave de cifrado de tráfico de grupo GTEKID, un número aleatorio seleccionado por la estación móvil N_{MS}, un texto cifrado E_{KEK} (GTEKM) de un material de clave de cifrado de tráfico de grupo GTEKM seleccionado por la estación base y cifrado con una clave de cifrado de clave de grupo GKEK deducida a partir del TEKM correspondiente al GTEKID, un periodo de validez de la clave de cifrado de tráfico de grupo $Life_{GTEK}$, y un código de integridad de mensaje MIC. El número aleatorio seleccionado por la estación móvil N_{MS} debe ser el mismo que el de la solicitud de clave de cifrado de tráfico de multidifusión. No obstante, si el proceso de actualización de clave lo inicia la estación base, el número aleatorio lo puede determinar la estación base, y se calcula un valor del código de integridad de mensaje MIC a partir de la clave de integridad de mensaje de grupo GMIK deducida a partir del TEKM correspondiente al TEKID.

La presente invención posee las siguientes ventajas:

La presente invención puede proporcionar diferentes niveles de claves de cifrado de tráfico para diferentes servicios. Dicho de otro modo, diferentes servicios corresponden a diferentes claves de cifrado.

La negociación de clave de cifrado de tráfico de multidifusión utiliza el canal de difusión de manera racional, mejorando el rendimiento. La estación base no necesita negociar la clave de cifrado de tráfico de multidifusión con cada estación móvil respectivamente.

El protocolo de negociación de claves y el protocolo de distribución de claves de cifrado de tráfico de multidifusión se utilizan para lograr la actualización eficiente de la clave de cifrado de tráfico de multidifusión, lo cual hace que la clave de cifrado de tráfico de multidifusión sea más flexible.

El mecanismo de activación de clave se vale del reconocimiento de mensajes, mediante el cual evita los inconvenientes del mantenimiento de múltiples sincronizaciones temporales y estados, lo que simplifica la gestión de los estados.

Las anteriores formas de realización se describen para ilustrar el principio de la presente invención. Se entiende que las formas de realización detalladas de la presente invención no se limitan a estas. Las diversas variaciones y modificaciones realizadas por los expertos en la materia dentro del alcance de la presente invención entrarán en el alcance de la presente invención tal como se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Procedimiento de gestión de claves de multidifusión, que comprende:

la construcción de un paquete de solicitud de negociación de clave y el envío del paquete de solicitud de negociación de clave a una estación base desde una estación móvil;

la construcción de un paquete de respuesta de negociación de clave al recibir el paquete de solicitud de negociación de clave, y el envío del paquete de respuesta de negociación de clave a la estación móvil desde la estación base;

tras la recepción del paquete de respuesta de negociación de clave, el descifrado del paquete de respuesta de negociación de clave con una clave de cifrado de claves deducida a partir de una clave de autoridad correspondiente a un identificador de clave de autoridad AKID para obtener un material de clave de cifrado de tráfico TEKM, construcción de un paquete de reconocimiento de negociación de clave y envío del paquete de reconocimiento de negociación de clave a la estación base desde la estación móvil; y la deducción de una clave de cifrado de claves de grupo GKEK y una clave de integridad de mensajes de grupo GMIK, por parte de la estación móvil;

el envío desde la estación móvil de un paquete de solicitud de clave de cifrado de tráfico de multidifusión a la estación base si la estación móvil necesita negociar o actualizar una clave de cifrado de tráfico de multidifusión;

tras la recepción del paquete de solicitud de clave de cifrado de tráfico de multidifusión procedente de la estación móvil, el envío desde la estación base de un paquete de distribución de claves de cifrado de tráfico de multidifusión a la estación móvil; o, si la estación base necesita actualizar una clave de multidifusión, la difusión desde la estación base de un paquete de distribución de claves de cifrado de tráfico de multidifusión a todas las estaciones móviles,

en el que el paquete de notificación de actualización de clave comprende: una identidad de la estación base ID_{BS}, un identificador de asociación de seguridad SAID, el identificador de clave de autoridad AKID, un identificador de clave de cifrado de tráfico TEKID, y un código de integridad de mensaje MIC; en el que el identificador de clave de cifrado de tráfico TEKID está adaptado para identificar una clave de cifrado de tráfico que se vaya a actualizar, y se calcula un valor del código de integridad de mensaje MIC a partir de una clave de comprobación de integridad deducida a partir de una clave de autoridad correspondiente al AKID;

el paquete de solicitud de negociación de clave comprende: una identidad de la estación móvil ID_{MS}, un identificador de asociación de seguridad SAID, un identificador de clave de autoridad AKID, un identificador de clave de cifrado de tráfico TEKID, un número aleatorio seleccionado por la estación móvil N_{MS}, y un código de integridad de mensaje MIC; en el que el identificador de clave de cifrado de tráfico TEKID está adaptado para identificar una clave de cifrado de tráfico que se vaya a actualizar, y se calcula un valor del código de integridad de mensaje MIC a partir de una clave de comprobación de integridad deducida a partir de una clave de autoridad AK correspondiente al AKID;

el paquete de respuesta de negociación de clave comprende: la identidad de la estación móvil ID_{MS}, la identidad de la estación base ID_{BS}, un identificador de asociación de seguridad SAID, el identificador de clave de autoridad AKID, un identificador de clave de cifrado de tráfico TEKID, un número aleatorio seleccionado por la estación móvil N_{MS}, un número aleatorio seleccionado por la estación base N_{BS}, un texto cifrado E_{KEK} (TEKM) de un material de clave de cifrado de tráfico TEKM seleccionado por la estación base y cifrado con una clave de cifrado de clave deducida a partir de una clave de autoridad correspondiente al identificador de clave de autoridad AKID, un periodo de validez de la clave de cifrado de tráfico $Life_{TEK}$, y un código de integridad de mensaje MIC; en el que un valor del número aleatorio seleccionado por la estación móvil N_{MS} debe ser el mismo que el de un campo correspondiente en el paquete de solicitud de negociación de clave, y se calcula un valor del código de integridad de mensaje MIC a partir de una clave de comprobación de integridad deducida a partir del TEKM, el N_{MS} y el N_{BS};

el paquete de reconocimiento de negociación de clave comprende: la identidad de la estación base ID_{BS}, la identidad de la estación móvil ID_{MS}, un identificador de asociación de seguridad SAID, el identificador de clave de autoridad AKID, un identificador de clave de cifrado de tráfico TEKID, un número aleatorio seleccionado por la estación base N_{BS}, y un código de integridad de mensaje MIC; en el que un valor del número aleatorio seleccionado por la estación base N_{BS} debe ser el mismo que el de un campo correspondiente en el paquete de respuesta de negociación de clave, y se calcula un valor del código de integridad de mensaje MIC a partir de una clave de comprobación de integridad deducida a partir del TEKM, el N_{MS} y el N_{BS};

el paquete de solicitud de clave de cifrado de tráfico de multidifusión comprende: un identificador de asociación de

seguridad SAID, un identificador de clave de cifrado de tráfico TEKID, un identificador de clave de cifrado de tráfico de grupo GTEKID un número aleatorio seleccionado por la estación móvil N_{MS}, y un código de integridad de mensaje MIC; en el que el identificador de clave de cifrado de tráfico de grupo GTEKID está adaptado para identificar una clave de cifrado de tráfico multidifusión que se vaya a negociar o solicitar, y se calcula un valor del código de integridad de mensaje MIC a partir de la clave de integridad de mensaje de grupo GMIK deducida a partir del TEKM correspondiente al TEKID;

el paquete de distribución de claves de cifrado de tráfico de multidifusión incluye: un identificador de asociación de seguridad SAID, un identificador de clave de cifrado de tráfico TEKID, un identificador de clave de cifrado de tráfico de grupo GTEKID, un número aleatorio seleccionado por la estación móvil N_{MS}, un texto cifrado E_{KEK} (GTEKM) de un material de clave de cifrado de tráfico de grupo GTEKM seleccionado por la estación base y cifrado con una clave de cifrado de clave de grupo GKEK deducida a partir del TEKM correspondiente al TEKID, un periodo de validez de la clave de cifrado de tráfico de grupo $Life_{GTEK}$, y un código de integridad de mensaje MIC; en el que el número aleatorio seleccionado por la estación móvil N_{MS} debe ser el mismo que el del paquete de solicitud de clave de cifrado de tráfico de multidifusión; no obstante, si el proceso de actualización de clave lo inicia la estación base, el número aleatorio lo determina la estación base, y se calcula un valor del código de integridad de mensaje MIC a partir de la clave de integridad de mensaje de grupo GMIK deducida a partir del TEKM correspondiente al TEKID.

2. El procedimiento de gestión de claves de multidifusión según la reivindicación 1, que también comprende:

el envío desde la estación base del paquete de notificación de actualización de clave a la estación móvil, para comunicar a la estación móvil que actualice la clave de cifrado de tráfico, en el caso de que una estación base necesite actualizar una clave de cifrado de tráfico pero la estación móvil no inicie una solicitud de actualización de clave de cifrado de tráfico.

3. El procedimiento de gestión de claves de multidifusión según la reivindicación 2, donde en caso de una negociación de clave inicial, o si la estación móvil recibe un paquete de notificación de actualización de clave procedente de la estación base, la estación móvil envía el paquete de solicitud de negociación de clave a la estación base, con el fin de activar un proceso de negociación de clave.

4. El procedimiento de gestión de claves de multidifusión según la reivindicación 1,que adicionalmente comprende: si la estación base envía el paquete de notificación de actualización de clave antes de recibir el paquete de solicitud de negociación de clave, la comprobación por parte de la estación base de si los valores de los campos correspondientes del paquete de notificación de actualización de clave y el paquete de solicitud de negociación de clave son iguales entre sí; en caso afirmativo, la estación base construye el paquete de respuesta de negociación de clave; en caso contrario, la estación base desestima el paquete de solicitud de negociación de clave sin procesarlo.

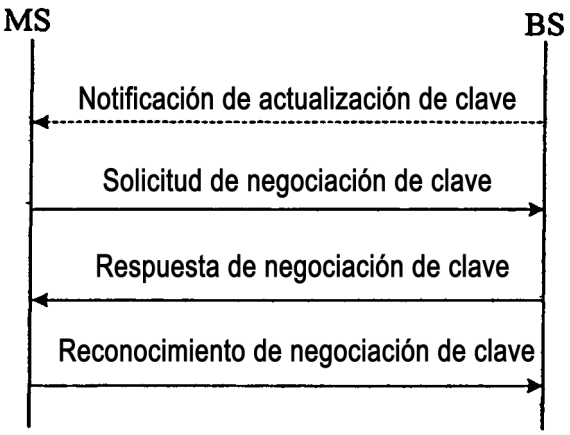
MS
BS
Notificación de actualización de clave
Solicitud de negociación de clave
Respuesta de negociación de clave
Reconocimiento de negociación de clave

Figura 1

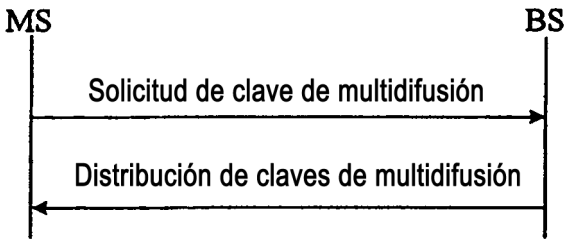
MS
BS
Solicitud de clave de multidifusión
Distribución de claves de multidifusión

Figura 2