(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 401 039**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.08.2008 E 08784154 (0)**

(97) Fecha y número de publicación de la concesión europea: **26.12.2012 EP 2139175**

(54) Título: **Método, sistema y dispositivo para negociar la capacidad de la seguridad cuando se desplaza un terminal**

(30) Prioridad:

31.08.2007 CN 200710145703
26.09.2007 CN 200710151700

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.04.2013

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building Bantian Longgang District, Shenzhen Guangdong 518129, CN

(72) Inventor/es:

HE, CHENGDONG

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método, sistema y dispositivo para negociar la capacidad de la seguridad cuando se desplaza un terminal

Campo de la tecnología

La presente invención está relacionada con el campo de la tecnología de comunicaciones inalámbricas y, más en particular, con un método y un sistema para negociar la capacidad de la seguridad cuando se desplaza un terminal, una entidad de gestión de la movilidad (MME) y un equipo de usuario (UE).

Antecedentes de la invención

Una red inalámbrica incluye una red de acceso por radio y una red básica. La red básica de una red inalámbrica de evolución a largo plazo (LTE) incluye una MME. La MME tiene funciones similares a las de un nodo de soporte (SGSN) del servicio general de radio por paquetes de servicio (GPRS) de una red de segunda/tercera generación (2G/3G), y es principalmente responsable de la gestión de la movilidad y de la autenticación del usuario. Cuando un UE está en estado de reposo en una red inalámbrica 2G/3G o LTE, el UE necesita negociar respectivamente la capacidad de la seguridad de la señalización sin acceso (NAS) con el SGSN o la MME. La capacidad de la seguridad incluye un algoritmo de cifrado de la señalización NAS, una clave correspondiente de protección de la integridad de NAS, Knas-int, un algoritmo de protección de la integridad NAS y una correspondiente clave de protección de la confidencialidad de NAS, Knas-enc, que se utilizan para la transmisión de señalización entre el UE y un sistema, asegurando con ello la recepción normal de la señalización del UE y la seguridad del sistema de comunicaciones.

Cuando un UE que accede a una red de acceso radio edge (GERAN) de un sistema global 2G para las comunicaciones móviles (GSM), o a una red terrestre de acceso por radio (UTRAN) de un sistema universal de telecomunicaciones móviles 3G (UMTS), se desplaza en el estado de reposo, el UE puede desplazarse a una zona de seguimiento de una red de acceso radio LTE, y por tanto el UE puede acceder a la red nuevamente a través de una LTE. En ese momento tiene lugar un procedimiento de actualización de la zona de seguimiento (TAU), es decir, tiene lugar un procedimiento TAU entre redes heterogéneas. Durante el procedimiento, como la entidad que realiza la negociación de la capacidad de la seguridad del UE cambia, por ejemplo desde un SGSN a la MME, y las entidades pueden tener diferentes capacidades de seguridad, necesita realizarse de nuevo el procedimiento de negociación de la capacidad de la seguridad, para asegurar la seguridad de la interacción subsiguiente entre el UE y la red. Debe indicarse que, para la red LTE, la negociación de la capacidad de la seguridad incluye la negociación de un algoritmo de protección de la confidencialidad de NAS y un algoritmo de protección de la integridad de NAS, un algoritmo de protección de la confidencialidad del control de recursos radio (RRC) y un algoritmo de protección de la integridad del RRC, y un algoritmo de protección de la confidencialidad del plano de usuario (UP).

Para el procedimiento TAU iniciado por el UE en estado de reposo, necesita resolverse la negociación del algoritmo de protección de la confidencialidad de NAS, el algoritmo de protección de la integridad de NAS y las correspondientes claves de protección de NAS.

Durante la implementación de la presente invención, el inventor averiguó que no se puede encontrar en la técnica anterior ningún método para negociar la capacidad de la seguridad durante el procedimiento TAU entre las redes heterogéneas, de manera que cuando el UE se desplaza desde la red 2G/3G a la red LTE, la negociación de la capacidad de la seguridad no puede ser realizada, dando como resultado que no puede asegurarse la seguridad de la interacción subsiguiente entre el UE y la red.

El documento “Proyecto de asociación de 3ª generación; Servicios del Grupo de Especificaciones Técnicas y Aspectos del sistema; mejoras del GPRS para el acceso E-UTRAN (Edición 8)” del ESTÁNDAR 3GPP; 3GPP TS 23.401, PROYECTO DE ASOCIACIÓN DE LA 3ª GENERACIÓN (3GPP), CENTRO DE COMPETENCIA DE MÓVILES; 650, ROUTE DES LUCIOLES; F-06921 SOPHIA ANTIPOLIS CEDEX, FRANCIA, NÚM. V1.1.0, de 1 de Julio de 2007 (2007-07-01), páginas 1 - 78, XP050363612, define mejoras del GPRS para el acceso E-UTRAN.

El documento de NOKIA SIEMENS NETWORKS ET AL: “PseudoCR a TR 33.821: Gestión de claves de la movilidad en modo de reposo”, BORRADOR del 3GPP; S3-070529, PROYECTO DE ASOCIACIÓN DE 3ª GENERACIÓN (3GPP), CENTRO DE COMPETENCIA DE MÓVILES; 650, ROUTE DES LUCIOLES; F-06921 SOPHIA ANTIPOLIS CEDEX, FRANCIA, volumen SA WG3, núm. Montreal; 20070703, 3 de Julio de 2007 (2007-07-03), XP050279999, estudia la gestión de claves en la movilidad del modo de reposo cuando el UE se desplaza desde una LTE anterior a una nueva LTE.

El documento de 3GPP: “Proyecto asociación de 3ª generación; Servicios del Grupo de Especificaciones Técnicas y Aspectos del sistema; Racionalidad y seguimiento de las decisiones de seguridad en la Evolución de la Arquitectura del Sistema (SAE) del RAN/3GPP EVOLUCIONADO A LARGO PLAZO (LTE) (Edición 8”) BORRADOR del 3GPP; S3-070625- TR33821- V040-CL, PROYECTO DE ASOCIACIÓN DE 3ª GENERACIÓN (3GPP), CENTRO DE COMPETENCIA DE MÓVILES; 650, ROUTE DES LUCIOLES; F-06921 SOPHIA ANTIPOLIS CEDEX, FRANCIA,

volumen SA WG3, núm. Montreal; 20070714, 14 de Julio de 2007 (2007-07-14), XP050280077, estudia la Racionalidad y seguimiento de las decisiones de seguridad en la SAE de LTE RAN/3GPP.

El documento “Proyecto de Asociación de tercera generación; Servicios del Grupo de Especificaciones Técnicas y Aspectos del sistema; Evolución de la Arquitectura del sistema 3GPP: Informe sobre Opciones Técnicas y Conclusiones (Edición 7)” del ESTÁNDAR 3GPP; 3GPP TR 23.882, PROYECTO DE ASOCIACIÓN DE LA TERCERA GENERACIÓN (3GPP), CENTRO DE COMPETENCIA DE MÓVILES; 650, ROUTE DES LUCIOLES; F-06921 SOPHIA ANTIPOLIS CEDEX, FRANCIA, NÚM. V1.11.0, de 1 de Julio de 2007 (2007-07-01), páginas 147 - 176, XP050364123, resume la evolución de la arquitectura del sistema 3GPP: Informe sobre opciones técnicas y conclusiones.

Consecuentemente, la presente invención está dirigida a métodos que tienen las características de las reivindicaciones 1 y 12, un sistema que tiene las características de la reivindicación 6, una entidad de gestión de la movilidad que tiene las características de la reivindicación 8, y un equipo de usuario que tiene las características de la reivindicación 10. En las respectivas reivindicaciones dependientes se definen modos de realización ventajosos de la misma.

Breve descripción de los dibujos

La figura 1 es un diagrama de flujo de un método, de acuerdo con un primer modo de realización de la presente invención, para negociar la capacidad de la seguridad cuando se desplaza un terminal;

La figura 2 es un diagrama de flujo de un método, de acuerdo con un segundo modo de realización de la presente invención, para negociar la capacidad de la seguridad cuando se desplaza un terminal;

La figura 3 es un diagrama de flujo de un método de acuerdo con un tercer modo de realización de la presente invención, para negociar la capacidad de la seguridad cuando se desplaza un terminal; y

La figura 4 es una vista estructural de un sistema, de acuerdo con un modo de realización de la presente invención, para negociar la capacidad de la seguridad cuando se desplaza un terminal.

Descripción detallada de los modos de realización

En un método para negociar la capacidad de la seguridad cuando se desplaza un terminal, proporcionado en los modos de realización de la presente invención, cuando se desplaza un UE desde una red 2G/3G a una red LTE, una MME recibe un mensaje de petición de TAU enviado desde el UE, y adquiere un algoritmo de seguridad de NAS soportado por el UE, y una clave de autenticación relacionada con vectores o una clave raíz obtenida de acuerdo con la clave de autenticación relacionada con vectores. Después, la MME selecciona un algoritmo de seguridad de NAS de acuerdo con el algoritmo de seguridad de NAS soportado por el UE, obtiene una clave de protección de NAS de acuerdo con la clave de autenticación relacionada con vectores o la clave raíz, obtenida de acuerdo con la clave de autenticación relacionada con vectores, y envía al UE un mensaje que transporta el algoritmo de seguridad de NAS seleccionado. El UE obtiene una clave de protección de NAS de acuerdo con una clave de autenticación relacionada con vectores.

Los modos de realización de la presente invención se ilustran en detalle a continuación con referencia a modos de realización específicos y a los dibujos que se acompañan.

Se supone que un UE ha accedido a una UTRAN/GERAN cuando está en estado de reposo. En este caso, cuando se desplaza a una zona de seguimiento de una red LTE, el UE inicia un procedimiento TAU.

La figura 1 es un diagrama de flujo de un método, de acuerdo con un primer modo de realización de la presente invención, para negociar la capacidad de la seguridad cuando se desplaza un terminal. Haciendo referencia a la figura 1, el método incluye los pasos siguientes:

En el paso 100, un UE envía una petición TAU a una MME.

En este paso, el UE envía la petición TAU a una nueva MME a través de un nodo B evolucionado (eNB) de una red de acceso radio LTE. Por conveniencia de la descripción, la comunicación entre el UE y la MME a través del eNB se simplifica a la comunicación entre el UE y la MME en la descripción siguiente.

La petición TAU enviada desde el UE a la MME en este paso, no solamente transporta algunos parámetros tales como la identidad temporal del abonado de móviles (TMSI), conocida por las personas expertas en la técnica, sino que también puede transportar información de la capacidad de la seguridad soportada por el UE. La información de la capacidad de la seguridad incluye un algoritmo de seguridad de NAS (un algoritmo de protección de integridad de NAS y/o un algoritmo de protección de la confidencialidad de NAS), y puede incluir también un algoritmo de seguridad de RRC (un algoritmo de protección de la integridad de RRC y/o un algoritmo de protección de la confidencialidad de RRC) o un algoritmo de seguridad de UP (un algoritmo de protección de la confidencialidad de

UP).

En los pasos 101 - 102, la MME adquiere un algoritmo de seguridad de NAS soportado por el UE, y envía un mensaje de petición del contexto de gestión de la movilidad a un SGSN. Tras recibir el mensaje, el SGSN envía un mensaje de respuesta en el contexto de la gestión de la movilidad, que transporta una clave de autenticación relacionada con vectores a la MME.

Si en el paso 100, el UE no transporta el algoritmo de seguridad de NAS soportado por el UE en la petición TAU enviada a la MME, tras recibir el mensaje de petición de contexto de gestión de la movilidad, el SGSN interroga al algoritmo de seguridad de NAS soportado por el UE, y transporta el algoritmo de seguridad de NAS interrogado soportado por el UE en el mensaje de respuesta del contexto de gestión de la movilidad enviado a la MME. El algoritmo de seguridad de NAS es el algoritmo de protección de la integridad de NAS y/o el algoritmo de protección de la confidencialidad de NAS.

Cuando el UE se desplaza desde la red 2G a la zona de seguimiento de la red LTE, el SGSN del proceso anterior es un SGSN de la red 2G, y la clave de autenticación relacionada con vectores incluye al menos una clave de cifrado Kc, o un valor Kc' obtenido tras realizar en la Kc una conversión unidireccional. Cuando el UE se desplaza desde la red 3G a la zona de seguimiento de la red LTE, el SGSN del proceso anterior es un SGSN de la red 3G, y la clave de autenticación relacionada con vectores incluye al menos una clave de integridad IK y una clave de cifrado CK, o unos valores IK' y CK' tras realizar en la IK y la CK una conversión unidireccional.

La conversión unidireccional se refiere a un procedimiento de conversión en el cual un parámetro original se convierte utilizando un cierto algoritmo para obtener un parámetro objetivo, pero el parámetro original no puede ser obtenido de acuerdo con el parámetro objetivo. Por ejemplo, para la Kc, si se obtiene la Kc' utilizando un algoritmo f(Kc), pero no puede obtenerse la Kc de acuerdo con la Kc' utilizando un algoritmo inverso, la conversión es una conversión unidireccional.

En al paso 103, la MME selecciona un nuevo algoritmo de seguridad de NAS, de acuerdo con al algoritmo de seguridad de NAS soportado por el UE y el algoritmo de seguridad de NAS soportado por el MME, así como un algoritmo de seguridad de NAS permitido por el sistema, obtiene una clave raíz Kasme de acuerdo con la clave de autenticación relacionada con vectores, y después obtiene una clave de protección de NAS de acuerdo con la Kasme. La clave de protección de NAS incluye una clave de protección de la integridad de NAS, Knas-int, y/o una clave de protección de la confidencialidad de NAS, Knas-enc.

En el paso 104, la MME genera un mensaje de aceptación de TAU que transporta el algoritmo seleccionado de seguridad de NAS.

En este paso, la MME puede realizar además una protección de la integridad de NAS en el mensaje de aceptación de TAU. Por ejemplo, la MME obtiene un valor del código de autenticación del mensaje de protección de la integridad del NAS (NAS-MAC) de acuerdo con la clave de protección de integridad del NAS, Knas-int, obtenida en el paso 103, la información en la aceptación del TAU, y el algoritmo de protección de la integridad del NAS en el algoritmo seleccionado de seguridad del NAS, y después transporta el valor en el mensaje de aceptación de TAU y envía el mensaje de aceptación de TAU al UE.

El mensaje de aceptación de TAU de este paso puede transportar además información de la capacidad de seguridad soportada por el UE.

En el paso 105, el UE recibe el mensaje de aceptación del TAU que transporta el algoritmo de seguridad de NAS seleccionado por la MME, y adquiere el algoritmo de la seguridad de NAS negociada; y después obtiene una clave raíz Kasme de acuerdo con una clave de autenticación actual relacionada con vectores de la misma (por ejemplo, la IK y la CK, o la IK' y la CK' obtenidos de acuerdo con la IK y la CK cuando la red que las origina es la 3G, o la Kc o la Kc' obtenidas de acuerdo con la Kc, cuando la red que las origina es la 2G), y obtiene la clave de protección de NAS de acuerdo con la clave raíz. La clave de protección de NAS incluye la clave de protección de integridad de NAS, Knas-int, y/o la clave de protección de confidencialidad de NAS, Knas-enc.

En este paso, el UE puede detectar además si la protección de integridad realizada en el mensaje de aceptación de TAU es correcta. Si no lo es, se determina que falla la negociación de la capacidad de la seguridad actual, y se puede iniciar de nuevo el proceso de negociación de la capacidad de la seguridad. Por ejemplo, el UE obtiene la NAS-MAC de acuerdo con la clave de protección de confidencialidad de NAS, Knas-enc, obtenida, la información en la aceptación de TAU, y el algoritmo de protección de integridad de NAS transportado en el mensaje de aceptación de TAU, y después compara si la NAS-MAC obtenida es la misma que la NAS-MAC transportada en el mensaje de aceptación de TAU. Si es así, indica que el mensaje no se modifica durante la transmisión; en otro caso, se estima que el mensaje se modifica durante la transmisión, y se determina por tanto que falla la negociación de la capacidad de la seguridad actual.

En el paso 104, el mensaje de aceptación de TAU transporta además la información de la capacidad de la seguridad

soportada por el UE. En este paso, el UE puede comparar además la información de la capacidad de la seguridad soportada por el UE y transportada en el mensaje de aceptación de TAU con la información de la capacidad de la seguridad almacenada en él. Si las dos son consistentes entre sí, se determina que no hay ataque a la degradación; en otro caso, se determina que tiene lugar un ataque a la degradación, y que falla la negociación actual de la capacidad de la seguridad, y se puede iniciar nuevamente el proceso de negociación de la capacidad de la seguridad, impidiendo con ello el ataque a la degradación.

Para el ataque a la degradación, se supone que el UE admite dos algoritmos de seguridad al mismo tiempo, es decir, un algoritmo A1 de alta fortaleza y un algoritmo A2 de baja fortaleza, y la MME admite también los dos algoritmos. De esta manera, el algoritmo A1 de alta fortaleza debe ser negociado entre el UE y la MME. Sin embargo, si en un camino a lo largo del cual el UE envía la información de capacidad de la seguridad soportado por el UE a la MME, el atacante modifica la información de la capacidad de la seguridad del UE, por ejemplo, solamente se mantiene el algoritmo A2 de baja fortaleza, o cuando la MME selecciona el algoritmo de seguridad de NAS, la información de la capacidad de la seguridad soportada por el UE es modificada por el atacante, y solamente se mantiene el algoritmo A2 de baja fortaleza, la MME puede seleccionar solamente y enviar al algoritmo A2 de baja fortaleza al UE. Es decir, el algoritmo A2 de baja fortaleza, en lugar del algoritmo A1 de alta fortaleza, se obtiene a través de la negociación entre el UE y la MME, de manera que el atacante puede realizar un ataque más fácilmente, que es denominado ataque a la degradación. En un modo de realización de la presente invención, la MME envía la información de la capacidad de la seguridad soportada por el UE al UE, y el UE detecta si la información de la capacidad de la seguridad soportada por el UE es consistente con la información de capacidad de la seguridad soportada por el UE, detectando con ello e impidiendo además el ataque a la degradación.

El procedimiento en el que la MME obtiene finalmente la clave de protección de NAS de acuerdo con la clave de autenticación relacionada con vectores del paso 103, no está limitado a ninguna secuencia de tiempo con respecto al paso 104 y el paso 105, y el procedimiento puede ser realizado antes del paso 104, o entre el paso 104 y el paso 105, o después del paso 105.

En el proceso anterior, la MME y el UE puede obtener también directamente la clave de protección de NAS de acuerdo con la clave de autenticación relacionada con vectores, sin obtener la clave raíz, y después obtener la clave de protección de NAS de acuerdo con la clave raíz.

Debe entenderse por las personas expertas en la técnica que, en el proceso anterior, el método de obtención utilizado por el UE para obtener la clave de protección de NAS de acuerdo con la clave de autenticación relacionada con vectores, debe ser el mismo que el utilizado por el lado de la red para obtener la clave de protección de NAS de acuerdo con la clave de autenticación relacionada con vectores. El método de obtención puede adoptar cualquier conversión unidireccional, por ejemplo, Kasme = f (IK, CK, otros parámetros), Knas-enc = f (Kasme, algoritmo de protección de la confidencialidad de NAS, otros parámetros), y Knas-int = f (Kasme, algoritmo de protección de la integridad de NAS, otros parámetros).

Además, con el fin de resaltar este modo de realización de la presente invención, los procedimientos que no están relacionados con la seguridad se han omitido entre los pasos 102 y 104 en el proceso anterior.

A través del proceso anterior, el UE y la MME pueden compartir el algoritmo de seguridad de NAS y la clave de protección de NAS, implementando con ello la negociación de la capacidad de la seguridad de NAS.

La figura 2 es un diagrama de flujo de un método, de acuerdo con un segundo modo de realización de la presente invención, para negociar la capacidad de la seguridad cuando se desplaza un terminal. Haciendo referencia a la figura 2, el método incluye los pasos siguientes.

Paso 200, es el mismo paso 100, de manera que se omite aquí la descripción del mismo.

En los pasos 201 - 203, la MME adquiere un algoritmo de seguridad de NAS soportado por el UE, y envía un mensaje de petición del contexto a un SGSN. Tras recibir el mensaje de petición del contexto, el SGSN obtiene una clave raíz de acuerdo con una clave de autenticación relacionada con vectores del mismo, y después envía un mensaje de respuesta del contexto que transporta la clave raíz a la MME.

En otros modos de realización de la presente invención, si en el paso 200 el UE no transporta el algoritmo de seguridad de NAS soportado por el UE en la petición TAU enviada a la MME, tras recibir el mensaje de petición del contexto de la gestión de movilidad, el SGSN solicita el algoritmo de seguridad de NAS soportado por el UE, y transporta el algoritmo de seguridad de NAS transportado por el UE en el mensaje de respuesta del contexto de la gestión de movilidad enviado a la MME. El algoritmo de seguridad de NAS en el algoritmo de protección de la integridad de NAS y/o al algoritmo de protección de confidencialidad de NAS.

Cuando el UE se desplaza desde una red 2G a la zona de seguimiento de la red LTE; el SGSN del proceso anterior es un SGSN de la red 2G, y la clave raíz es la clave raíz Kasme obtenida por el SGSN de acuerdo con la Kc o la Kc', obtenida tras realizar la conversión unidireccional en la Kc. Cuando el UE se desplaza desde la red 3G a la zona de

seguimiento de la red LTE, el SGSN del proceso anterior es un SGSN de la red 3G, y la clave raíz es la Kasme obtenida por el SGSN de acuerdo con la IK y la CK, o la IK' y la CK' tras realizar la conversión unidireccional en la IK y la CK.

En el paso 204, la MME selecciona un nuevo algoritmo de seguridad de NAS, de acuerdo con el algoritmo de seguridad de NAS soportado por el UE y un algoritmo de seguridad de NAS soportado por la MME, así como un algoritmo de seguridad de NAS permitido por el sistema; y después obtiene una clave de protección de NAS de acuerdo con la clave raíz. La clave de protección de NAS incluye una clave de protección de la integridad de NAS, Knas-int, y/o una clave protección de la confidencialidad de NAS Knas-enc.

En el paso 205, la MME genera un mensaje de aceptación de TAU que transporta el algoritmo de seguridad de NAS seleccionado.

En este paso, la MME puede realizar además una protección de integridad de NAS en el mensaje de aceptación de TAU. El mensaje de aceptación de TAU de este paso puede transportar además la información de capacidad de la seguridad soportada por el UE.

En el paso 206, el UE recibe el mensaje de aceptación de TAU que transporta el algoritmo de seguridad de NAS seleccionado por la MME, y adquiere el algoritmo de seguridad de NAS negociado; y después obtiene una clave raíz Kasme de acuerdo con una clave de autenticación relacionada con vectores actual (por ejemplo, la IK y la CK, o la IK' y la CK', obtenidos de acuerdo con la IK y la CK cuando la red originaria es la 3G, o la Kc o la Kc' obtenidas de acuerdo con la Kc, cuando la red originaria es la 2G), y obtiene la clave de protección de NAS de acuerdo con la clave raíz. La clave de protección de NAS incluye la clave de protección de la integridad de NAS, Knas-int, y/o la clave de protección de la confidencialidad de NAS, Knas-enc.

En este paso, el UE puede detectar además si la protección de integridad realizada en el mensaje de aceptación de TAU es correcta. Si no lo es, se determina que falla la negociación de la capacidad de la seguridad actual, y el procedimiento de negociación de la capacidad de la seguridad puede iniciarse de nuevo.

En otros modos de realización de la presente invención, si en el paso 205, el mensaje de aceptación de TAU transporta además la información de la capacidad de la seguridad soportada por el UE, en este paso, el UE puede comparar además la información de capacidad de la seguridad soportada por el UE y transportada en el mensaje de aceptación de TAU, con la información de capacidad de la seguridad soportada por el UE. Si las dos son consistentes entre sí, se determina que no ocurre un ataque a la degradación; en otro caso, se determina que ocurre un ataque a la degradación, y que falla la negociación de la capacidad de la seguridad actual, y se puede iniciar de nuevo el procedimiento de negociación de la capacidad de la seguridad, impidiendo con ello el ataque a la degradación.

En otros modos de realización de la presente invención, el procedimiento en el que la MME obtiene la clave de protección de NAS de acuerdo con la clave raíz del paso 204, no está limitado a ninguna secuencia de tiempos con respecto al paso 205 y al paso 206, y el proceso puede ser realizado antes del paso 205, o entre el paso 205 y el paso 206, o después del paso 206.

Debe entenderse por las personas expertas en la técnica, que en el proceso anterior, un método de obtención utilizado por el UE para obtener la clave de protección de NAS de acuerdo con la clave de autenticación relacionada con vectores, debe ser el mismo que el utilizado por el lado de la red para obtener la clave de protección de NAS, de acuerdo con la clave de autenticación relacionada con vectores.

A través del proceso anterior, el UE y la MME pueden compartir el algoritmo de seguridad de NAS y la clave de protección de NAS, implementando con ello la negociación de la capacidad de la seguridad de NAS.

La figura 3 es un diagrama de flujo de un método, de acuerdo con un tercer modo de realización de la presente invención, para negociar una capacidad de la seguridad cuando se desplaza un terminal. Haciendo referencia a la figura 3, el método incluye los pasos siguientes.

El paso 300 es el mismo que el paso 100, de manera que en este caso se omite la descripción del mismo.

En los pasos 301 - 302, la MME adquiere un algoritmo de seguridad de NAS soportado por el UE desde un SGSN, a partir de la petición de contexto de la gestión de movilidad y de los mensajes de respuesta.

En otros modos de realización de la presente invención, si en el paso 300, el UE no transporta el algoritmo de seguridad de NAS soportado por el UE en la petición de TAU enviada a la MME, tras recibir el mensaje de petición del contexto de la gestión de movilidad, el SGSN solicita el algoritmo de seguridad de NAS soportado por el UE, y transporta el algoritmo de seguridad de NAS solicitado soportado por el UE en el mensaje de respuesta del contexto de la gestión de la movilidad, enviado a la MME. El algoritmo de seguridad de NAS es el algoritmo de protección de la integridad de NAS y/o el algoritmo de protección de confidencialidad de NAS.

En el paso 303, la MME adquiere una clave raíz Kasme obtenida de acuerdo con una clave de autenticación relacionada con vectores desde un servidor de abonados locales (HSS) a través de una autenticación y un procedimiento de acuerdo de claves (AKA).

En el paso 304, la MME selecciona un nuevo algoritmo de seguridad de NAS, de acuerdo con el algoritmo de seguridad de NAS soportado por el UE y un algoritmo de seguridad de NAS soportado por la MME, así como un algoritmo de seguridad de NAS permitido por el sistema; y después obtiene las claves de protección de NAS de acuerdo con la Kasme. Las claves de protección de NAS incluyen una clave de protección de la integridad de NAS, Knas-int, y una clave de protección de la confidencialidad de NAS, Knas-enc.

En el paso 305, la MME genera y envía al UE un mensaje de petición de una orden del modo de seguridad (SMC) de NAS que transporta el algoritmo de seguridad de NAS seleccionado. El mensaje de petición de SMC puede ser transportado en un mensaje de aceptación de TAU.

En este paso, la MME puede realizar además una protección de la integridad de NAS en el mensaje de aceptación de la SMC. Por ejemplo, la MME obtiene un valor de un código de autenticación del mensaje de la protección de la integridad de NAS (NAS-MAC) , de acuerdo con la clave de protección de la integridad de NAS, Knas-int, obtenida en el paso 304, la información del mensaje de petición de SMC y el algoritmo de protección de la integridad de NAS del algoritmo de seguridad de NAS seleccionado, y después transporta el valor en el mensaje de petición de SMC y envía el mensaje de petición de SMC al UE.

El mensaje de petición de SMC de este paso puede transportar también la información de la capacidad de la seguridad soportada por el UE.

En el paso 306, el UE recibe el mensaje de petición de SMC que transporta el algoritmo de seguridad de NAS seleccionado por la MME, y adquiere el algoritmo de seguridad de NAS soportado por el UE y seleccionado por la MME; y después obtiene una clave raíz de acuerdo con una clave actual de autenticación relacionada con vectores obtenida en el proceso AKA de la misma, y obtiene una clave de protección de NAS de acuerdo con la clave raíz. La clave de protección de NAS incluye la clave de protección de la integridad de NAS, Knas-int, y la clave de protección de confidencialidad de NAS, Knas-enc.

En este modo de realización, en este paso, el UE puede detectar también si la protección de integridad realizada en el mensaje de aceptación de TAU es correcta. SI no lo es, se determina que falla la actual negociación de capacidad de la seguridad, y se puede iniciar de nuevo el proceso de negociación de la capacidad de la seguridad. Por ejemplo, el UE obtiene un NAS-MAC de acuerdo con la clave de protección de confidencialidad de NAS obtenida, Knas-enc, la información del mensaje de aceptación de TAU y el algoritmo de protección de la integridad de NAS transportado en el mensaje de aceptación de TAU, y después compara si el NAS-MAC obtenido es el mismo NAS-MAC transportado en el mensaje de aceptación de TAU. Si es así, indica que el mensaje no se modifica durante la transmisión; en otro caso, se estima que el mensaje se modifica durante la transmisión, y se determina por tanto que falla la actual negociación de la capacidad de la seguridad.

En otros modos de realización de la presente invención, si en el paso 305 el mensaje de petición de SMC transporta la información de la capacidad de la seguridad soportada por el UE, en este paso el UE puede comparar también la información de capacidad de la seguridad soportada por el UE y transportada en el mensaje de petición de SMC con la información de capacidad de la seguridad soportada por el UE. Si las dos son consistentes entre sí, se determina que no tiene lugar un ataque a la degradación; en otro caso, se determina que ocurre un ataque a la degradación, y que falla la negociación actual de la capacidad de la seguridad, y se puede iniciar de nuevo el proceso de negociación de la capacidad de la seguridad, impidiendo con ello el ataque a la degradación.

En el paso 307, el UE envía un mensaje completo de respuesta de SMC a la MME. El mensaje completo de respuesta de SMC puede ser transportado en un mensaje completo de TAU.

En el paso 308, la MME devuelve un mensaje de aceptación de TAU.

En otros modos de realización de la presente invención, cuando el mensaje de petición de SMC es enviado al UE transportando el mensaje de petición de SMC en el mensaje de aceptación de TAU del paso 305, el paso 308 se combina con el paso 305.

En el paso 309, el UE devuelve un mensaje completo de TAU.

En otros modos de realización de la presente invención, cuando el mensaje completo de respuesta de SMC es transportado en el mensaje completo de TAU del paso 307, el paso 309 se combina con el paso 307.

Por medio del proceso anterior, se implementa la negociación de la capacidad de la seguridad de NAS.

Las personas con experiencia normal en la técnica, deben comprender que todos o parte de los pasos del método de acuerdo con los modos de realización de la presente invención pueden ser implementados por un programa que

instruye el hardware relevante, y el programa puede ser almacenado en un medio de almacenamiento legible por ordenador, tal como una memoria de sólo lectura (ROM)/memoria de acceso aleatorio (RAM), un disco magnético o un disco óptico.

La figura 4 es una vista estructural de un sistema, de acuerdo con un modo de realización de la presente invención, para negociar la capacidad de la seguridad cuando se desplaza un terminal. Haciendo referencia a la figura 4, el sistema incluye un UE y una MME.

El UE está adaptado para enviar un mensaje de petición de TAU a la MME, recibir un mensaje que transporta un algoritmo de seguridad de NAS seleccionado y enviado desde la MME, y obtener una clave de protección de NAS de acuerdo con una clave de autenticación relacionada con vectores.

La MME está adaptada para: recibir el mensaje de petición de TAU enviado desde el UE; adquirir la clave de autenticación relacionada con vectores o una clave raíz obtenida de acuerdo con la clave de autenticación relacionada con vectores, y un algoritmo de seguridad de NAS soportado por el UE; seleccionar un algoritmo de seguridad de NAS de acuerdo con el algoritmo de seguridad de NAS soportado por el UE, y generar y enviar un mensaje que transporte el algoritmo de seguridad de NAS al UE; y obtener una clave de protección de NAS de acuerdo con la clave de autenticación adquirida relacionada con vectores o con la clave raíz obtenida de acuerdo con la clave de autenticación relacionada con vectores.

En el sistema, la MME adquiere también información de la capacidad de la seguridad soportada por el UE, y transporta también la información de capacidad de la seguridad soportada por el UE en el mensaje que transporta el algoritmo seleccionado de seguridad de NAS al UE, y el UE determina además si tiene lugar un ataque a la degradación, determinando si la información de capacidad de la seguridad soportada por el UE y enviada desde la MME es consistente con la información de capacidad de la seguridad soportada por el UE.

Específicamente, la MME incluye un módulo de adquisición, un módulo de selección y un módulo de obtención de claves.

El módulo de adquisición está adaptado para recibir el mensaje de petición de TAU enviado desde el UE, adquirir la clave de autenticación relacionada con vectores o la clave raíz obtenida de acuerdo con la clave de autenticación relacionada con vectores, y el algoritmo de seguridad de NAS soportado por el UE. El módulo de selección está adaptado para seleccionar el algoritmo de seguridad de NAS de acuerdo con el algoritmo de seguridad de NAS soportado por el UE y adquirido por el módulo de adquisición, generar y enviar el mensaje que transporta el algoritmo de seguridad de NAS seleccionado al UE. El módulo de obtención de claves está adaptado para obtener la clave de protección de NAS, de acuerdo con la clave de autenticación relacionada con vectores o la clave raíz obtenida de acuerdo con la clave de autenticación relacionada con vectores, adquirida por el módulo de adquisición y el algoritmo de seguridad de NAS seleccionado.

El módulo de adquisición adquiere además la información de capacidad de la seguridad soportada por el UE, y el módulo de selección transporta además la información de capacidad de la seguridad soportada por el UE y adquirida por el módulo de adquisición en el mensaje que transporta el algoritmo de seguridad de NAS seleccionado.

El UE incluye un módulo de actualización, un módulo de obtención de claves, un módulo de almacenamiento y un módulo de detección.

El módulo de actualización está adaptado para enviar a la MME el mensaje de petición de TAU que transporta la información de capacidad de la seguridad soportada por el UE y almacenada en el módulo de almacenamiento, y recibir el mensaje que transmite el algoritmo de seguridad de NAS enviado desde la MME. El módulo de obtención de claves está adaptado para obtener la clave de protección de NAS de acuerdo con la clave de autenticación relacionada con vectores y con el algoritmo de seguridad de NAS seleccionado y recibido por el módulo de actualización. El módulo de almacenamiento está adaptado para almacenar la información de capacidad de la seguridad soportada por el UE. El módulo de detección está adaptado para determinar que tiene lugar un ataque a la degradación cuando se detecta que la información de capacidad de la seguridad soportada por el UE y recibida desde la MME es inconsistente con la información de capacidad de la seguridad soportada por el UE y almacenada en el módulo de almacenamiento. El mensaje que transporta el algoritmo de seguridad de NAS seleccionado enviado desde la MME transporta además información de capacidad de la seguridad soportada por el UE.

Por la descripción precedente, puede observarse que, en las soluciones técnicas proporcionadas en los modos de realización de la presente invención, la MME recibe el mensaje de petición de TAU enviado desde el UE, y adquiere el algoritmo de seguridad de NAS soportado por el UE y la clave de autenticación relacionada con vectores, o la clave raíz obtenida de acuerdo con la clave de autenticación relacionada con vectores, y después selecciona el algoritmo de seguridad de NAS de acuerdo con el algoritmo de seguridad de NAS soportado por el UE, y genera y envía al UE el mensaje que transporta el algoritmo de seguridad de NAS seleccionado, permitiendo con ello que el UE y la MME compartan el algoritmo de seguridad de NAS. Además, el UE y la MME obtienen la clave de protección de NAS de acuerdo con la clave de autenticación relacionada con vectores o con la clave raíz obtenida de acuerdo

con la clave de autenticación relacionada con vectores, permitiendo con ello que la MME y el UE compartan la clave de protección de NAS. De esta manera, cuando se desplaza desde una red 2G/3G a la red LTE, el UE puede negociar el algoritmo de seguridad de NAS y la clave de protección de NAS con la MME, de manera que se consigue el proceso de negociación de la capacidad de la seguridad en el procedimiento TAU entre redes heterogéneas, asegurando con ello la seguridad de la interacción subsiguiente entre el UE y la red.

Por medio de la presente invención se puede impedir el ataque a la degradación. La MME devuelve también la información de capacidad de la seguridad soportada por el UE a través del mensaje de aceptación de TAU, y el UE detecta si la información de capacidad de la seguridad soportada por el UE es consistente con la información actual de capacidad de la seguridad soportada por el UE. Si es así, la actual negociación de la capacidad de la seguridad tiene éxito, y se puede utilizar el algoritmo de seguridad de NAS y la clave de protección de NAS obtenidos en la negociación. SI no es así, se determina que ocurre un ataque a la degradación, la negociación actual de la capacidad de la seguridad falla, y se necesita realizar de nuevo la negociación de la capacidad de la seguridad. Por medio de las soluciones anteriores, se puede detectar si la información de capacidad de la seguridad soportada por el UE es atacada antes de que la MME adquiera la información de capacidad de la seguridad soportada por el UE, impidiendo con ello el ataque a la degradación y asegurando la seguridad de la interacción subsiguiente entre el UE y la red.

REIVINDICACIONES

1. Un método para negociar la capacidad de la seguridad cuando se desplaza un equipo de usuario, UE, en el que, cuando el UE está en reposo, se desplaza desde una red de segunda generación/tercera generación, 2G/3G, a una red de evolución a largo plazo, LTE, comprendiendo el método:

recibir, por una entidad de gestión de la movilidad, MME, un mensaje de petición de actualización del área de seguimiento, TAU, enviado (100) desde el UE;

adquirir (101), por la MME, un algoritmo de seguridad de un nivel sin acceso, NAS, soportado por el UE;

adquirir (102), por la MME, una clave de autenticación relacionada con vectores desde un mensaje de respuesta del contexto de gestión de movilidad, enviado desde un nodo de soporte de servicios generales (SGSN) de paquetes por radio,

seleccionar (103) por la MME, un algoritmo de seguridad de NAS de acuerdo con el algoritmo de seguridad de NAS soportado por el UE, obteniendo una clave raíz de acuerdo con la clave de autenticación relacionada con vectores, y después obtener una clave de protección de NAS de acuerdo con la clave raíz obtenida, y enviar (104) un mensaje que transporte el algoritmo de seguridad de NAS seleccionado al UE; y

recibir (104) por el UE, el mensaje que transporta el algoritmo de seguridad de NAS seleccionado enviado por la MME;

obtener (105), por el UE, una clave raíz de acuerdo con la clave actual de autenticación relacionada con vectores, y después obtener la clave de protección de NAS, de acuerdo con la clave raíz obtenida, en el que

cuando el SGSN es un SGSN de la red 2G, la clave de autenticación relacionada con vectores comprende al menos una clave de cifrado Kc, o un valor obtenido tras realizar una conversión unidireccional en la clave de cifrado Kc; o

cuando el SGSN es un SGSN de la red 3G, la clave de autenticación relacionada con vectores comprende al menos una clave de integridad IK y un clave de cifrado CK, o valores obtenidos tras realizar una conversión unidireccional en la IK y en la clave de cifrado CK.

2. El método según la reivindicación 1, en el que la adquisición, por la MME, del algoritmo de seguridad de NAS soportado por el UE comprende:

adquirir, por la MME, la información de capacidad de la seguridad soportada por el UE, desde el mensaje de petición de TAU enviado desde el UE, donde el mensaje de petición de TAU contiene el algoritmo de seguridad de NAS soportado por el UE.

3. El método según la reivindicación 1, en el que la adquisición, por la MME, del algoritmo de seguridad de NAS soportado por el UE comprende:

adquirir, por la MME, la información de capacidad de la seguridad soportada por el UE desde el mensaje de respuesta del contexto enviado desde el SGSN, donde el mensaje de respuesta del contexto contiene el algoritmo de seguridad de NAS soportado por el UE.

4. El método según la reivindicación 1, en el que antes del envío, por la MME, del mensaje que transporta el algoritmo de seguridad de NAS seleccionado al UE, el método comprende además:

realizar, por la MME, una protección de la integridad del mensaje que transporta el algoritmo de seguridad de NAS seleccionado; y

detectar, por el UE, si la protección de integridad realizada en el mensaje que transporta el algoritmo de seguridad de NAS seleccionado es correcto, de acuerdo con la clave de protección de NAS obtenida, tras recibir el mensaje que transporta el algoritmo de seguridad de NAS seleccionado.

5. El método según la reivindicación 2 o 3, en el que el mensaje que transporta el algoritmo de seguridad de NAS seleccionado, transporta además la información de capacidad de la seguridad soportada por el UE; y

el método comprende además: la determinación, por el UE, de si tiene lugar un ataque a la degradación, determinando si la información de capacidad de la seguridad recibida soportada por el UE es consistente con la información de capacidad de la seguridad soportada por el UE.

6. Un sistema para negociar una capacidad de la seguridad cuando se desplaza un equipo de usuario, UE, en el que cuando el UE está en reposo, se desplaza desde una red de segunda/tercera generación, 2G/3G a una red de evolución a largo plazo, LTE, el sistema comprende el UE y la entidad de gestión de la movilidad, MME, donde

el UE está adaptado para enviar un mensaje de petición de actualización del área de seguimiento, TAU, a la MME, recibir un mensaje que transporte el nivel sin acceso seleccionado, NAS, el algoritmo de seguridad enviado desde la MME, y obtener una clave de protección de NAS de acuerdo con una clave raíz que se obtiene de acuerdo con una clave actual de autenticación relacionada con vectores; y

la MME está adaptada para: recibir el mensaje de petición de TAU enviado desde el UE; adquirir una clave de autenticación relacionada con vectores desde el mensaje de respuesta del contexto de la gestión de movilidad enviado desde un nodo de soporte de servicios generales, SGSN, de paquetes por radio, y un algoritmo de seguridad de NAS soportado por el UE; seleccionar un algoritmo de seguridad de NAS de acuerdo con el algoritmo de seguridad de NAS soportado por el UE, y generar y enviar un mensaje que transporte el algoritmo de seguridad de NAS seleccionado al UE; y obtener una clave de protección de NAS de acuerdo con una clave raíz que se obtiene de acuerdo con la clave de autenticación adquirida relacionada con vectores, en la que

cuando el SGSN es un SGSN de la red 2G, la clave de autenticación relacionada con vectores comprende al menos una clave de cifrado Kc, o un valor obtenido tras realizar una conversión unidireccional en la clave de cifrado Kc; o

cuando el SGSN es un SGSN de la red 3G, la clave de autenticación relacionada con vectores comprende al menos una clave de integridad IK y un clave de cifrado CK, o valores obtenidos tras realizar una conversión unidireccional en la IK y en la clave de cifrado CK.

7. El sistema según la reivindicación 6, en el que la MME está adaptada además para adquirir información de capacidad de la seguridad soportada por el UE, y está adaptada también para transportar la información de capacidad de la seguridad soportada por el UE en el mensaje que transporta el algoritmo de seguridad de NAS seleccionado y enviado al UE; y

el UE está adaptado también para determinar si ocurre un ataque a la degradación, determinando si la información de capacidad de la seguridad soportada por el UE y enviada desde la MME es consistente con la información de capacidad de la seguridad soportada por el UE.

8. Una entidad de gestión de la movilidad, MME, que comprende un módulo de adquisición, un módulo de selección y un módulo de obtención de claves, en la que

el módulo de adquisición está adaptado para recibir un mensaje de petición de la actualización del área de seguimiento, TAU, enviado desde un equipo de usuario, UE, adquirir una clave de autenticación relacionada con vectores desde el mensaje de respuesta del contexto de gestión de la movilidad, enviado desde un nodo de soporte de servicios generales, SGSN, de paquetes por radio y un algoritmo de seguridad del nivel sin acceso, NAS, soportado por el UE;

el módulo de selección está adaptado para seleccionar el algoritmo de seguridad de NAS de acuerdo con el algoritmo de seguridad de NAS soportado por el UE y adquirido por el módulo de adquisición, generar y enviar el mensaje que transporta el algoritmo de seguridad de NAS seleccionado al UE; y.

el módulo de obtención de claves está adaptado para obtener la clave de protección de NAS, de acuerdo con una clave raíz obtenida de acuerdo con la clave de autenticación relacionada con vectores, adquirida por el módulo de adquisición y el algoritmo de seguridad de NAS seleccionado por el módulo de selección, en la que

cuando el SGSN es un SGSN de la red 2G, la clave de autenticación relacionada con vectores comprende al menos una clave de cifrado Kc, o un valor obtenido tras realizar una conversión unidireccional en la clave de cifrado Kc; o

cuando el SGSN es un SGSN de la red 3G, la clave de autenticación relacionada con vectores comprende al menos una clave de integridad IK y un clave de cifrado CK, o valores obtenidos tras realizar una conversión unidireccional en la IK y en la clave de cifrado CK.

9. La MME según la reivindicación 8, en la que el módulo de adquisición está adaptado también para adquirir la información de capacidad de la seguridad soportada por el UE, y el módulo de selección está adaptado también para transportar la información de capacidad de la seguridad soportada por el UE y adquirida por el módulo de adquisición en el mensaje que transporta el algoritmo de seguridad de NAS seleccionado.

10. Un equipo de usuario, UE, en el que, cuando el UE en reposo, se desplaza desde una red de segunda generación/tercera generación, 2G/3G, a una red de evolución a largo plazo, LTE, el UE comprende un módulo de actualización, un módulo de obtención de claves, un módulo de almacenamiento y un módulo de detección, en el que

el módulo de actualización está adaptado para enviar un mensaje de petición de la actualización del área de seguimiento, TAU, que transporta la información de capacidad de la seguridad soportada por el UE y almacenada en el módulo de almacenamiento, a la entidad de gestión de la movilidad, MME, y para recibir un mensaje que transporta un algoritmo de seguridad del nivel sin acceso, NAS, enviado desde la MME;

el módulo de obtención de claves está adaptado para obtener una clave de protección de NAS de acuerdo con una clave raíz que se obtiene de acuerdo con una clave actual de autenticación relacionada con vectores y con el algoritmo de seguridad de NAS recibido por el módulo de actualización;

el módulo de almacenamiento está adaptado para almacenar la información de capacidad de la seguridad soportada por el UE; y

el módulo de detección está adaptado para determinar si ocurre un ataque a la degradación cuando se detecta que la información de capacidad de la seguridad soportada por el UE y recibida desde la MME es inconsistente con la información de capacidad de la seguridad soportada por el UE y almacenada en el módulo de almacenamiento.

11. El UE según la reivindicación 10, en el que el mensaje que transporta el algoritmo de seguridad de NAS seleccionado y enviado desde la MME transporta además la información de capacidad de la seguridad soportada por el UE.

12. Un método para negociar la capacidad de la seguridad cuando se desplaza un equipo de usuario, UE, en el que cuando el UE está en reposo, se desplaza desde una red de segunda/tercera generación 2G/3G a una red de evolución a largo plazo, LTE, comprendiendo el método:

recibir (300), por una entidad de gestión de la movilidad, MME, un mensaje de actualización del área de seguimiento, TAU, enviado desde el UE;

adquirir (301, 302) por la MME, un algoritmo de seguridad del nivel sin acceso, NAS, soportado por el UE;

adquirir (303) por la MME, una clave raíz, Kasme, obtenida de acuerdo con una clave de autenticación relacionada con vectores desde un servidor de abonados locales, HSS, a través de un procedimiento de autenticación y acuerdo de clave, AKA;

seleccionar (304) por la MME, un algoritmo de seguridad de NAS de acuerdo con al algoritmo de seguridad de NAS soportado por el UE y un algoritmo de seguridad de NAS soportado por la MME; y

obtener (304), por la MME, una clave de protección de NAS de acuerdo con la clave raíz;

generar (305) y enviar, por la MME, un mensaje de petición de una orden del modo de seguridad, SMC, de NAS, que transporta el algoritmo de seguridad de NAS seleccionado, al UE;

recibir (306), por el UE, el mensaje de petición de la SMC que transporta el algoritmo de seguridad de NAS seleccionado por la MME, adquirir el algoritmo de seguridad de NAS soportado por el UE y seleccionado por la MME; y después obtener (306) una clave raíz de acuerdo con la clave actual de autenticación relacionada con vectores obtenida en el procedimiento AKA, y obtener (306) una clave de protección de NAS de acuerdo con la clave raíz.

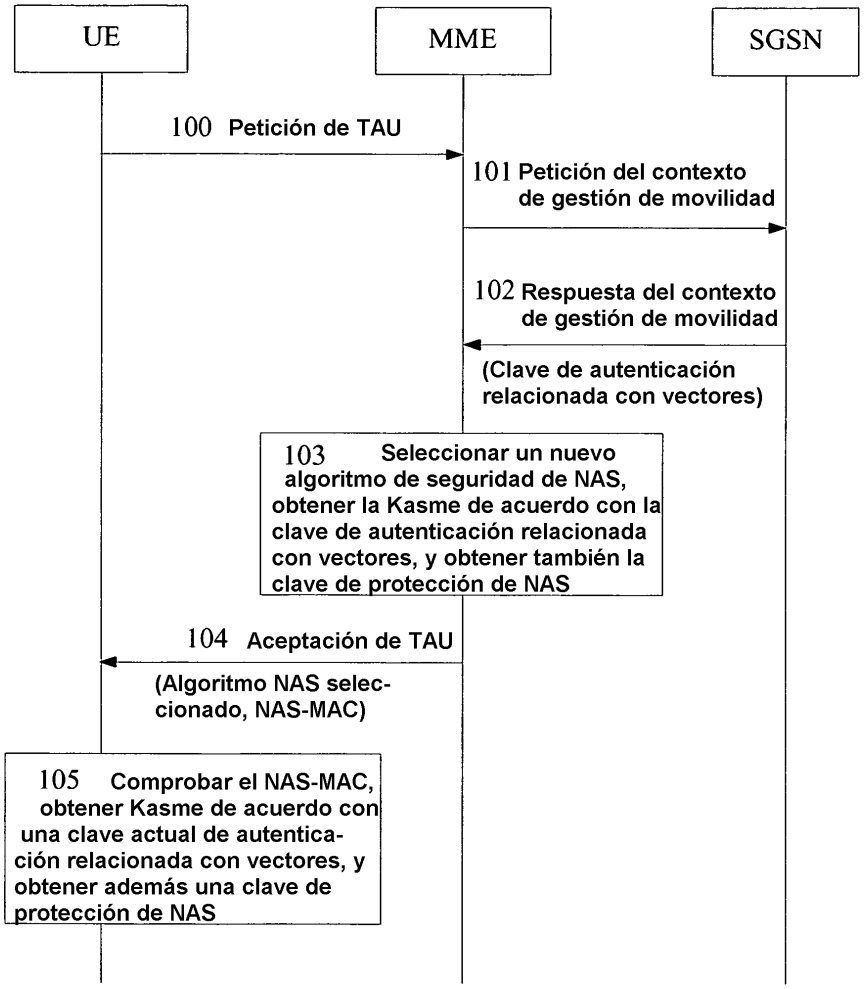
UE
MME
SGSN
100 Petición de TAU
101 Petición del contexto de gestión de movilidad
102 Respuesta del contexto de gestión de movilidad
(Clave de autenticación relacionada con vectores)
103 Seleccionar un nuevo algoritmo de seguridad de NAS, obtener la Kasme de acuerdo con la clave de autenticación relacionada con vectores, y obtener también la clave de protección de NAS
104 Aceptación de TAU
(Algoritmo NAS seleccionado, NAS-MAC)
105 Comprobar el NAS-MAC, obtener Kasme de acuerdo con una clave actual de autenticación relacionada con vectores, y obtener además una clave de protección de NAS

FIG. 1

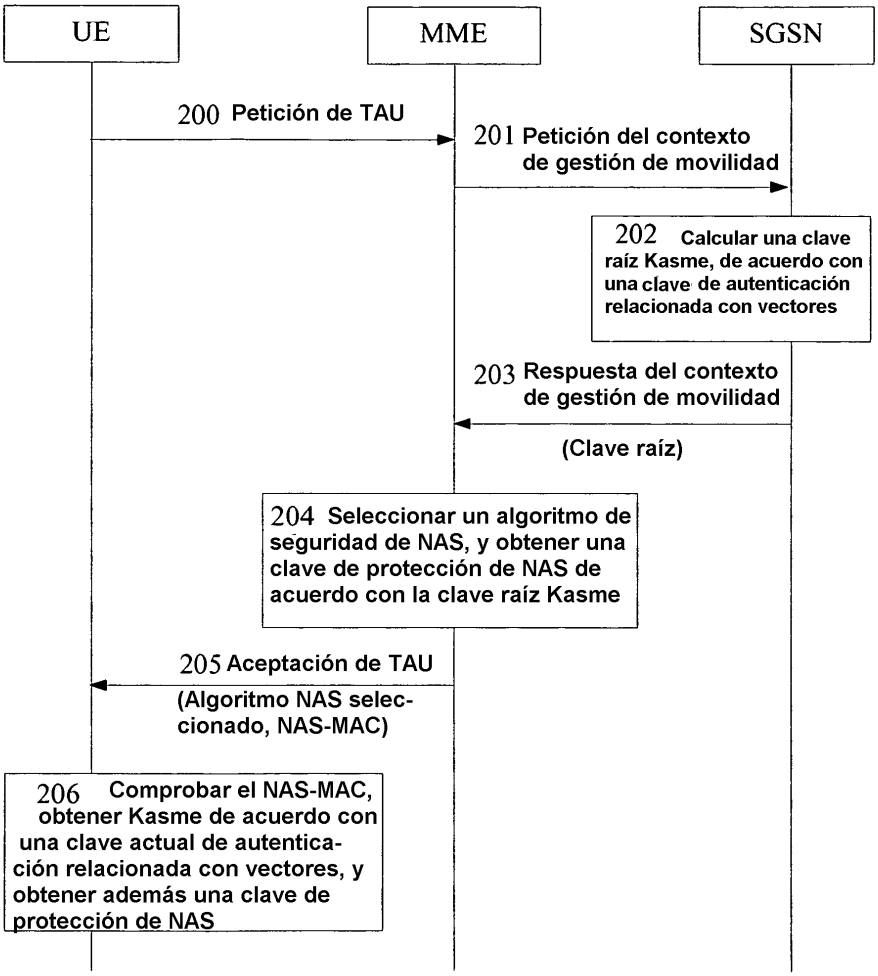
UE
MME
SGSN
200 Petición de TAU
201 Petición del contexto de gestión de movilidad
202 Calcular una clave raíz Kasme, de acuerdo con una clave de autenticación relacionada con vectores
203 Respuesta del contexto de gestión de movilidad
(Clave raíz)
204 Seleccionar un algoritmo de seguridad de NAS, y obtener una clave de protección de NAS de acuerdo con la clave raíz Kasme
205 Aceptación de TAU
(Algoritmo NAS seleccionado, NAS-MAC)
206 Comprobar el NAS-MAC, obtener Kasme de acuerdo con una clave actual de autenticación relacionada con vectores, y obtener además una clave de protección de NAS

FIG. 2

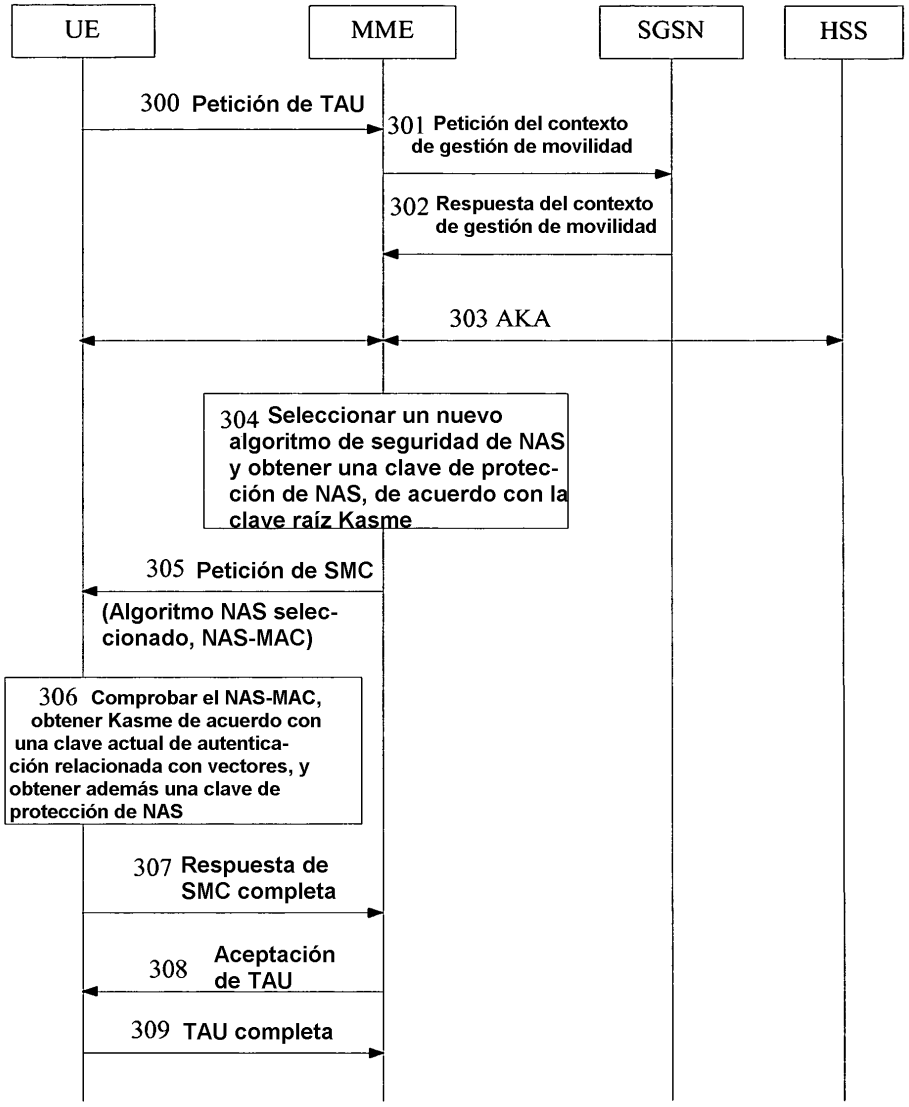
UE
MME
SGSN
HSS
300 Petición de TAU
301 Petición del contexto de gestión de movilidad
302 Respuesta del contexto de gestión de movilidad
303 AKA
304 Seleccionar un nuevo algoritmo de seguridad de NAS y obtener una clave de protección de NAS, de acuerdo con la clave raíz Kasme
305 Petición de SMC
(Algoritmo NAS seleccionado, NAS-MAC)
306 Comprobar el NAS-MAC, obtener Kasme de acuerdo con una clave actual de autenticación relacionada con vectores, y obtener además una clave de protección de NAS
307 Respuesta de SMC completa
308 Aceptación de TAU
309 TAU completa

FIG. 3

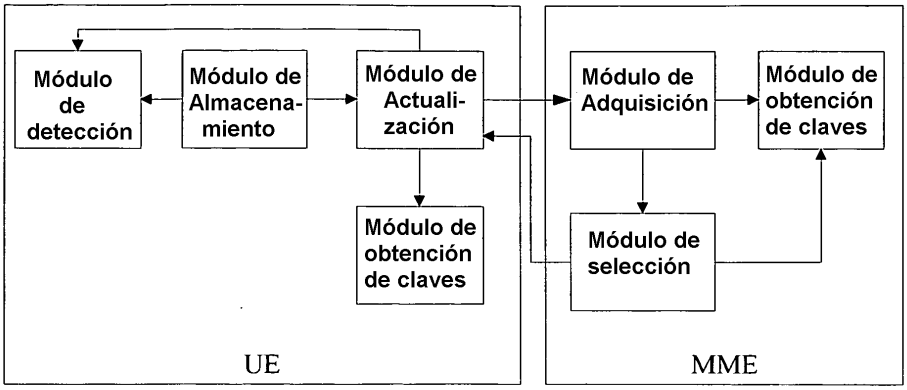
Módulo de detección
Módulo de Almacena-miento
Módulo de Actuali-zación
Módulo de obtención de claves
UE
Módulo de Adquisición
Módulo de obtención de claves
Módulo de selección
MME

FIG. 4