(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 554 808**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/02 (2009.01)
H04W 36/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.05.2008 E 08734236 (6)**

(97) Fecha y número de publicación de la concesión europea: **16.09.2015 EP 2117248**

(54) Título: **Método, sistema y equipamiento de negociación de capacidad de seguridad**

(30) Prioridad:

08.05.2007 CN 200710074333

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.12.2015

(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 equipamiento de negociación de capacidad de seguridad

CAMPO

El presente invento se refiere al campo de las comunicaciones, y más particularmente al método, sistema y equipamiento de negociación de capacidad de seguridad.

ANTECEDENTES

Con referencia a la fig. 1, una red de radio de Proyecto de Asociación de 3ª Generación (3GPP) existente es dividida en una red de acceso de radio (RAN) de 3GPP y una red central o de núcleo (CN).

La RAN de 3GPP es clasificada además en tres tipos como sigue.

Red de acceso de radio de borde (GERAN) de GSM: red de acceso 2G/2.5G, colectivamente denominada como una red de acceso 2G en lo que sigue, y que incluye una estación transceptora base (BTS) y un controlador de estación base (BSC).

Red de acceso de radio terrestre universal (UTRAN): red de acceso 3G, que incluye un nodo B (NodeB) y un controlador de red de radio (RNC).

Red de acceso de radio terrestre UMTS evolucionada (EUTRAN): conocida también como red de acceso de evolución a largo plazo (LTE) futura, que incluye un nodo B evolucionado (eNodoB, y eNB para abreviar de aquí en adelante).

Las tres RAN anteriores son configuradas todas para implementar funciones relacionadas con servicios de radio, y mientras tanto realizar negociación de capacidad de seguridad con terminales.

Una red central 2G/3G es dividida además en un dominio de circuito conmutado (CS) y un dominio de paquete conmutado (PS). Por facilidad de ilustración, las entidades relacionadas con CS son omitidas, y solamente es mantenido el dominio PS. El dominio PS realiza intercambio de servicio de datos y encaminamiento con redes basadas en paquetes externos de antemano, e incluye un nodo de soporte GPRS de servicio (SGSN) y un nodo de soporte GPRS de pasarela (GGSN). El SGSN es configurado principalmente para realizar reenvío de ruta, gestión de movilidad, gestión de sesión, y autentificación de usuario, y el GGSN es configurado principalmente para realizar la conexión con las redes basadas en paquetes externos, y también para implementar la trasmisión de datos sobre el plano del usuario.

Una red central evolucionada futura se refiere también a una evolución de arquitectura de sistema (SAE), que incluye entidades tales como una entidad de gestión de movilidad (MME) y una pasarela SAE (SAE GW)/pasarela de red de datos de paquetes (PDN GW)/servidor local de abonado (HSS). De manera similar al SGSN, la MME es configurada principalmente para realizar gestión de movilidad y autentificación de usuario. La SAE GW/PDN GW sirve como puntos de anclaje en el plano del usuario entre diferentes sistemas de acceso. El HSS es configurado principalmente para almacenar datos de suscripción del usuario.

En la red 2G, el SGSN realiza la negociación de algoritmo de capacidad de seguridad entre el plano de señalización y el plano del usuario. En la red 3G, el RNC realiza la negociación de algoritmo de capacidad de seguridad entre el plano de señalización y el plano del usuario. En la red evolucionada LTE/SAE, como RNC/SGSN no existe, la MME realiza la negociación de algoritmo de señalización de no acceso (NAS), y el eNB realiza la negociación de algoritmo de control de recurso de radio (RRC)/plano del usuario (UP).

Cuando un usuario es transferido desde una red 2G/3G (2G/3G) a una red LTE, o desde una red LTE a una red 2G/3G, como las entidades responsables para la negociación de capacidad de seguridad cambian y las capacidades de seguridad de las mismas pueden ser diferentes, la negociación de capacidad de seguridad necesita ser realizada otra vez. Aquí, la negociación de capacidad de seguridad significa algoritmo de encriptación para la red 2G, significa algoritmo de protección de integridad y algoritmo de encriptación para la red 3G y significa algoritmo NAS (algoritmo de encriptación y algoritmo de protección de integridad), el algoritmo RRC (algoritmo de encriptación y algoritmo de protección de integridad), y el algoritmo UP (algoritmo de encriptación) para la red LTE.

Particularmente, durante la transferencia desde la red LTE a la red 2G/3G, un equipo de usuario (UE) envía su propio GERAN (algoritmo de encriptación)/capacidad de seguridad UTRAN (algoritmo de encriptación y algoritmo de protección de integridad) llevados en un mensaje inicial de Capa 3 a la MME. La MME envía a continuación las capacidades del UE al SGSN. El SGSN selecciona y envía el algoritmo de capacidad de seguridad GERAN/UTRAN correspondiente al UE a través de la MME. Durante la transferencia desde la LTE a la 2G el SGSN selecciona el algoritmo de capacidad de seguridad. Sin embargo, durante la transferencia desde la LTE a la 3G, de acuerdo con la descripción anterior acerca de la red 3G, el RNC, en vez del SGSN, selecciona el algoritmo de capacidad de seguridad; de lo contrario, el SGSN tiene que introducir un nuevo requisito para seleccionar el algoritmo de capacidad de seguridad. Mientras tanto, el SGSN debe conocer la capacidad de seguridad del RNC de una cierta manera, y envía a continuación el algoritmo seleccionado al RNC, de manera que la interacción adicional entre el SGSN y el RNC necesita ser construida.

Durante la transferencia desde la 2G/3G a la LTE, el SGSN consulta al UE para la capacidad de seguridad de NAS (algoritmo de encriptación y algoritmo de protección de integridad)/UP (algoritmo de encriptación)/RRC (algoritmo de encriptación y algoritmo de protección de integridad). Durante la transferencia desde la 2G/3G a la LTE, el SGSN envía las capacidades del UE a la MME. A continuación, la MEE selecciona y envía todos los algoritmos de capacidad de seguridad de NAS/RRC/UP al UE a través del SGSN.

En la implementación del presente invento, se ha encontrado en la técnica anterior que, cuando la MME selecciona todos los algoritmos de capacidad de seguridad de NAS/RRC/UP, la MME debe conocer las capacidad de seguridad del eNB correspondiente de una cierta manera (por ejemplo, configurando o extendiendo mensajes interactivos con el eNB), dando como resultado así en una configuración inflexible y un flujo de proceso complicado.

El documento D1 (WO 2007/025487 A1) proporciona un método para transferencia entre sistemas. Después de que un terminal de usuario transfiera desde un primer sistema de comunicaciones a un segundo sistema de comunicaciones, un dispositivo de control de comunicaciones del segundo sistema de comunicaciones obtiene y guarda información de encriptación del terminal de usuario. Cuando el terminal de usuario ha de ser transferido desde el segundo sistema de comunicaciones de nuevo al primer sistema de comunicaciones, el dispositivo de control de comunicaciones del segundo sistema de comunicaciones envía la información de encriptación del terminal de usuario a un primer dispositivo de red de acceso del primer sistema de comunicaciones.

El documento D2 (US 2006/0026671 A1) describe un método para determinar las capacidades de autenticación de un solicitante antes de iniciar una conversación de autenticación con un cliente, por ejemplo, utilizando el Protocolo de Autenticación Extensible (EAP).

3GPP TR 33.821 sugiere que, durante la transferencia desde la 2G/3G a la LTE, el SGSN de la primera red incluye las capacidades de seguridad del UE en la solicitud de transferencia a la MME, que selecciona a continuación el algoritmo a utilizar.

RESUMEN

Las realizaciones del presente invento están dirigidas a un método, sistema, y equipamiento de negociación de capacidad de seguridad, de modo que faciliten la negociación de capacidad de seguridad durante la transferencia de red.

En una realización del presente invento, se ha proporcionado un método de negociación de capacidad de seguridad, que es aplicable para realizar la negociación de capacidad de seguridad durante una transferencia de red móvil. El método incluye el siguiente proceso:

Una segunda red recibe una solicitud de transferencia enviada por una primera red.

Una entidad de red de acceso de la segunda red selecciona una capacidad de seguridad correspondiente, o una entidad de red de acceso y una entidad de red central (CN) de la segunda red seleccionan respectivamente una capacidad de seguridad correspondiente.

La segunda red envía la capacidad de seguridad seleccionada al UE mediante la primera red. La primera red es una red 2G o 3G, la segunda red es una red de evolución a largo plazo (LTE), la entidad de red de acceso de la segunda red es un nodo B evolucionado (eNodoB), y la entidad de red central de la segunda red es una entidad de gestión de movilidad (MME). La MME envía un mensaje de solicitud de preparación de transferencia que lleva un algoritmo RRC y un algoritmo UP que son soportados por el UE al eNodoB, en que el algoritmo RRC comprende un algoritmo de encriptación y un algoritmo de protección de integridad. El eNodoB selecciona un algoritmo RRC y un algoritmo UP que son soportados por el UE y el eNodoB de acuerdo con el algoritmo RRC y el algoritmo UP que son soportados por el UE y un algoritmo RRC y un algoritmo UP que son soportados por el eNodoB. La MME selecciona una señalización de No Acceso, NAS, el algoritmo soportado por el UE, un sistema y la MME de acuerdo con un algoritmo NAS soportado por el UE, un algoritmo NAS permitido por el sistema y un algoritmo NAS soportado por la MME.

En una realización del presente invento, se ha proporcionado un sistema de negociación de capacidad de seguridad, que es aplicable para realizar negociación de capacidad de seguridad durante una transferencia de red móvil. El sistema incluye una entidad de red de acceso y una entidad de red central de una primera red, y una entidad de red de acceso y una entidad de red núcleo de una segunda red. La primera red es una red 2G o 3G, y la segunda red es una red de evolución a largo plazo (LTE). La segunda entidad de red de acceso es un nodo B evolucionado (eNodoB). La segunda entidad de red núcleo es una entidad de gestión de movilidad (MME).

La entidad de red de acceso de la segunda red está configurada para seleccionar un algoritmo de control de recurso de radio (RRC) y un algoritmo de plano de usuario (UP) cuando la primera red solicita la transferencia a la segunda red.

La entidad de red central de la segunda red está configurada para seleccionar un algoritmo de señalización de No Acceso (NAS) cuando la primera red solicita la transferencia a la segunda red.

La entidad de red central y la entidad de red de acceso de la primera red están configuradas para enviar el algoritmo

NAS seleccionado y el algoritmo RRC seleccionado y el algoritmo UP al UE.

Un método para la negociación de capacidad de seguridad, que es aplicable para realizar una negociación de capacidad de seguridad durante una transferencia de red móvil desde 2G/3G a LTE, comprende:

recibir, por un nodo B evolucionado, eNodoB, un mensaje de solicitud de preparación de transferencia enviado por una entidad de gestión de movilidad, MME, llevando el mensaje de solicitud de preparación de transferencia un algoritmo de control de recurso de radio, RRC, y un algoritmo de plano de usuario, UP, que son soportados por un UE, en el que el algoritmo RRC comprende un algoritmo de encriptación y un algoritmo de protección de integridad;

seleccionar, por el eNodoB, un algoritmo RRC y un algoritmo UP que son soportados por el UE y el eNodoB de acuerdo con el algoritmo RRC y el algoritmo UP que son soportados por el UE y un algoritmo RRC y un algoritmo UP que son soportados por el eNodoB;

enviar, por el eNodoB, el algoritmo RRC seleccionado y el algoritmo UP a un UE mediante la primera red.

Un nodo B evolucionado, eNodoB cuando es programado para llevar a cabo el método de la reivindicación 6, que tiene

medios para recibir, un mensaje de solicitud de preparación de transferencia enviado por una entidad de gestión de movilidad, MME, llevando el mensaje de solicitud de preparación de transferencia un algoritmo de control de recurso de radio, RRC, y un algoritmo de plano de usuario, UP, que son soportados por el UE, en que el algoritmo RRC comprende un algoritmo de encriptación y un algoritmo de protección de integridad

medios para seleccionar, un algoritmo RRC y un algoritmo UP que son soportados por el UE y el eNodoB de acuerdo con el algoritmo RRC y el algoritmo UP que son soportados por el UE y un algoritmo RRC y un algoritmo UP que son soportados por el eNodoB; y

medios para enviar, por el eNodoB, las capacidades de seguridad seleccionadas a un UE mediante la primera red.

Las realizaciones del presente invento pueden conseguir las siguientes eficacias. Durante la transferencia de la red 2G/3G a la red LTE, la MME y el eNB implementan respectivamente la negociación del algoritmo de seguridad NAS y del algoritmo de seguridad RRC/UP, de manera que es innecesario que la MME conozca la capacidad de seguridad del eNB correspondiente de una cierta manera (por ejemplo, configurando o extendiendo mensajes interactivos con el eNB). Mientras tanto, durante la transferencia desde la red LTE a la red 3G, se evita un nuevo requisito para el SGSN, y la interacción entre el SGSN y el RNC es también innecesaria.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La fig. 1 es una vista estructural de una red de radio 3GPP convencional.

La fig. 2 es un diagrama de flujo que ilustra un método de negociación de capacidad de seguridad durante la transferencia de una red 2G/3G a una red LTE de acuerdo a una primera realización del presente invento.

La fig. 3 es un diagrama de flujo que ilustra un método de negociación de capacidad de seguridad durante la transferencia de una red LTE a una red 3G de acuerdo a una segunda realización del presente invento.

La fig. 4 es una vista estructural esquemática que ilustra un sistema de negociación de capacidad de seguridad de acuerdo a una tercera realización del presente invento.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES

Las realizaciones del presente invento están ilustradas en detalle más adelante con referencia a los dibujos adjuntos.

Con referencia a la fig. 2, el método de negociación de capacidad de seguridad de acuerdo con la primera realización incluye los siguientes procesos.

En esta realización, el UE es transferido desde la red 2G/3G a la red LTE. En primer lugar, se asume que un UE accede a servicios a través de una red de acceso 2G/3G (Acceso 2G/3G).

En el proceso 201, la red de acceso 2G/3G determina iniciar una transferencia.

En el proceso 202, la red de acceso 2G/3G inicia un mensaje de solicitud de transferencia al SGSN.

En el proceso 203, el SGSN inicia un mensaje de solicitud de preparación de transferencia a la MME. El mensaje de solicitud de preparación de transferencia lleva distintos conjuntos de capacidades de seguridad soportados por el UE, incluyendo el algoritmo NAS (algoritmo de encriptación y algoritmo de protección de integridad), el algoritmo RRC (algoritmo de encriptación y algoritmo de protección de integridad), y el algoritmo UP (algoritmo de encriptación).

Aquí, el SGSN puede obtener los conjuntos de capacidad de seguridad soportados por el UE en los siguientes métodos.

El SGSN solicita directamente al UE enviar los conjuntos de capacidad de seguridad soportados por el mismo.

Una entidad de red de acceso 2G/3G (BSS o RNC) determina en primer lugar iniciar una transferencia, a continuación solicita al UE los conjuntos de capacidad de seguridad soportados por el mismo, y envía los conjuntos de capacidad al SGSN en el proceso 202.

En el proceso 204, la MME selecciona un algoritmo NAS (algoritmo encriptación y algoritmo de protección de integridad) de acuerdo con el algoritmo NAS soportado por el UE (algoritmo de encriptación y algoritmo de protección de integridad), el algoritmo NAS permisible por el sistema (algoritmo de encriptación y algoritmo de protección de integridad), junto con el algoritmo NAS (algoritmo de encriptación y algoritmo de protección de integridad) soportado por la propia MME.

Debería observarse que, cuando el algoritmo NAS soportado por el UE (algoritmo de encriptación y algoritmo de protección de integridad), el algoritmo NAS permisible por el sistema (algoritmo de encriptación y algoritmo de protección de integridad, y el algoritmo NAS (algoritmo de encriptación y algoritmo de protección de integridad) soportados por la propia MME son todos distintos, el algoritmo NAS seleccionado (algoritmo de encriptación y algoritmo de protección de integridad) es un algoritmo NAS (algoritmo de encriptación y algoritmo de protección de integridad) soportado por la totalidad del UE, del sistema y de la MME.

En el proceso 205, la MME envía un mensaje de solicitud de preparación de transferencia al eNB. El mensaje de solicitud de preparación de transferencia lleva el algoritmo RRC soportado por el UE (algoritmo de encriptación y algoritmo de protección de integridad) y el algoritmo UP (algoritmo de encriptación), y puede llevar también el algoritmo RRC permisible por el sistema (algoritmo de encriptación y algoritmo de protección de integridad) y el algoritmo UP (algoritmo de encriptación).

En el proceso 206, es establecido un recurso portador entre el eNB y la MME, incluyendo el establecimiento de un recurso de radio.

En el proceso 207, el eNB selecciona el algoritmo RRC (algoritmo de encriptación y algoritmo de protección de integridad) y el algoritmo UP (algoritmo de encriptación) de acuerdo con el algoritmo RRC soportado por el UE (algoritmo de encriptación y algoritmo de protección de integridad) y el algoritmo UP (algoritmo de encriptación) junto con los conjuntos de capacidad de seguridad del RRC (algoritmo de encriptación y algoritmo de protección de integridad) y los conjuntos de capacidad de seguridad del UP (algoritmo de encriptación) soportados por el propio eNB.

Debería observarse que, cuando el algoritmo RRC soportado por el UE (algoritmo de encriptación y algoritmo de protección de integridad) y el algoritmo UP (algoritmo de encriptación), el algoritmo RRC permisible por el sistema (algoritmo de encriptación y algoritmo de protección de integridad) y el algoritmo UP (algoritmo de encriptación), y el algoritmo RRC (algoritmo de encriptación y algoritmo de protección de integridad) y el algoritmo UP (algoritmo de encriptación) soportado por el propio eNB son distintos, la selección significa aquí seleccionar el algoritmo RRC (algoritmo de encriptación y algoritmo de protección de integridad) y el algoritmo UP (algoritmo encriptación) que son ambos soportados por el UE y la MME.

En el proceso 205, si el mensaje de solicitud de preparación de transferencia enviado por la MME al eNB lleva también el algoritmo RRC permisible por el sistema (algoritmo de encriptación y algoritmo de protección de integridad) y el algoritmo UP (algoritmo de encriptación), el eNB puede combinar además el algoritmo RRC permisible por el sistema (algoritmo de encriptación y algoritmo de protección de integridad) y el algoritmo UP (algoritmo de encriptación), para seleccionar el algoritmo RRC (algoritmo de encriptación y algoritmo de protección de integridad) y el algoritmo UP (algoritmo de encriptación), que son soportados por la totalidad del UE, de la MME y del sistema.

En el proceso 208, el eNB envía un mensaje de reconocimiento de preparación de transferencia a la MME. El mensaje de reconocimiento de preparación de transferencia lleva el algoritmo RRC (algoritmo de encriptación y algoritmo de protección de integridad) y el algoritmo UP (algoritmo de encriptación) seleccionados.

En el proceso 209, la MME envía un mensaje de reconocimiento de preparación de transferencia al SGSN. El mensaje de reconocimiento de preparación de transferencia lleva el algoritmo NAS (algoritmo de encriptación y algoritmo de protección de integridad), el algoritmo RRC (algoritmo de encriptación y algoritmo de protección de integridad) y el algoritmo UP (algoritmo de encriptación) seleccionados.

En los proceso 210 a 211, el SGSN envía un mensaje de orden de transferencia al UE mediante la red de acceso 2G/3G, para indicar al UE que se transfiera a una red de destino. El mensaje de orden de transferencia lleva el algoritmo NAS (algoritmo de encriptación y algoritmo de protección de integridad), el algoritmo RRC (algoritmo de encriptación y algoritmo de protección de integridad) y el algoritmo UP (algoritmo de encriptación) seleccionados.

En el proceso 212, es implementado el proceso de transferencia subsiguiente.

Por ello, se completa la negociación de capacidad de seguridad entre el UE y el equipo de red (eNB/MME).

El proceso 204 puede ser realizado también entre los procesos 205 y 209. El proceso 207 puede ser realizado también antes del proceso 206.

En esta realización, durante la transferencia de la red 2G/3G a la red LTE, la protección del algoritmo NAS es implementada entre el UE y la MME, la protección del algoritmo RRC/UP es implementada entre el UE y el eNB, y la MME y el eNB son configurados respectivamente para realizar la negociación del algoritmo de seguridad NAS y del algoritmo de seguridad RRC/UP, de manera que es innecesario que la MME conozca las capacidades de seguridad del eNB correspondientes de una cierta manera (por ejemplo, configurando o extendiendo mensajes interactivos con el eNB) como en la técnica anterior.

Con referencia a la fig.3, en un segundo ejemplo del presente invento, un método de negociación de capacidad de seguridad incluye los siguientes procesos.

En este ejemplo, un UE se transfiere desde una LTE a una 3G. En primer lugar, se ha asumido que un UE accede a servicios a través una red de acceso LTE (eNB).

En el proceso 301, el eNB determina iniciar una transferencia.

En el proceso 302, el eNB inicia un mensaje de solicitud de transferencia a la MME.

En el proceso 303, la MME inicia un mensaje de solicitud de preparación de transferencia al SGSN. El mensaje de solicitud de preparación de transferencia lleva conjuntos de capacidad de seguridad 3G soportados por el UE, incluyendo algoritmo de encriptación y algoritmo de protección de integridad.

Aquí, la MME puede obtener los conjuntos de capacidad de seguridad 3G soportados por el UE en los siguientes métodos.

Antes de la transferencia, un mensaje inicial de Capa 3 lleva ya los conjuntos de capacidad de seguridad 3G soportados por el UE, y el UE envía los conjuntos de capacidad a la MME.

La MME solicita directamente al UE enviar los conjuntos de capacidad de seguridad 3G soportados por el UE.

El eNB determina en primer lugar iniciar una transferencia, a continuación solicita al UE los conjuntos de capacidad de seguridad 3G soportados por el UE, y envía los conjuntos de capacidad a la MME en el proceso 302.

En el proceso 304, el SGSN envía un mensaje de solicitud de preparación de transferencia a la red de acceso 3G (RNC). El mensaje de solicitud de preparación de transferencia lleva los conjuntos de capacidad de seguridad 3G soportados por el UE. Los conjuntos de capacidad de seguridad 3G soportados por el UE incluyen algoritmo de encriptación y algoritmo de protección de integridad, y la solicitud de preparación de transferencia puede llevar también los conjuntos de capacidades de seguridad 3G permisibles por el sistema.

En el proceso 305, es establecido un recurso portador entre la red de acceso 3G (RNC) y el SGSN, incluyendo el establecimiento de un recurso de radio.

En el proceso 306, la red de acceso 3G (RNC) selecciona los conjuntos de capacidad de seguridad 3G de acuerdo con los conjuntos de capacidad de seguridad 3G soportados por el UE junto con los conjuntos de capacidad de seguridad 3G soportados por la propia red de acceso 3G.

Debería observarse que, cuando los conjuntos de capacidad de seguridad 3G soportados por el UE y los conjuntos de capacidad de seguridad 3G soportados por la propia red de acceso 3G (RNC), son distintos, la selección significa aquí seleccionar los conjuntos de capacidad de seguridad 3G soportados por el UE y la red de acceso 3G (algoritmo de encriptación y algoritmo de protección de integridad) a partir de las dos categorías anteriores de los conjuntos de capacidad de seguridad 3G.

En el proceso 304, si el mensaje de solicitud de preparación de transferencia enviado por el SGSN a la red de acceso 3G (RNC) lleva también los conjuntos de capacidad de seguridad 3G permisibles por el sistema, la red de acceso 3G (RNC) puede combinar además los conjuntos de capacidad de seguridad 3G permisibles por el sistema para seleccionar los conjuntos de capacidad de seguridad 3G.

En el proceso 307, la red de acceso 3G (RNC) envía un mensaje de reconocimiento de preparación de transferencia al SGSN. El mensaje de reconocimiento de preparación de transferencia lleva los conjuntos de capacidad de seguridad 3G seleccionados.

En el proceso 308, el SGSN envía un mensaje de reconocimiento de preparación de transferencia a la MME. El mensaje de reconocimiento de preparación de transferencia lleva los conjuntos de capacidad de seguridad 3G seleccionados.

En los procesos 309 a 310, la MME envía un mensaje de orden de transferencia al UE mediante el eNB, indicando que el UE se transfiera a una red de destino. El mensaje lleva los conjuntos de capacidad de seguridad 3G seleccionados.

En el proceso 311, es implementado el proceso de transferencia subsiguiente.

Por tanto, se completa la negociación de capacidad de seguridad entre el UE y el equipo de red (RNC).

El proceso 306 puede ser realizado también antes que el proceso 305.

En esta realización, el SGSN no necesita introducir nuevos requisitos durante la transferencia de la red LTE a la 3G.

Con referencia a la fig. 4, en una tercera realización del presente invento, se ha proporcionado un sistema de negociación de capacidad de seguridad, que es aplicable para realizar la negociación de capacidad de seguridad durante una transferencia de red móvil. El sistema incluye una entidad de red de acceso 401 y una entidad de red central 402 de una primera red, y una entidad de red de acceso 403 y una entidad de red central 404 de una segunda red. La entidad de red de acceso 403 de la segunda red está configurada para seleccionar una capacidad de seguridad correspondiente cuando la primera red solicita que sea transferida a la segunda red. La entidad de red central 404 de la segunda red está configurada para seleccionar una capacidad de seguridad correspondiente junto con la entidad de red de acceso 403 de la segunda red cuando la primera red solicita que sea transferida a la segunda red. La entidad de red central 402 y la entidad de red de acceso 401 de la primera red están configuradas para enviar las capacidades de seguridad seleccionadas por la segunda red a un UE 405.

En esta realización, es proporcionada además una red que incluye una entidad de red de acceso y una entidad CN. La entidad de red de acceso está configurada para recibir una solicitud de transferencia enviada por una red de par extremo. La entidad CN está configurada para seleccionar y enviar una capacidad de seguridad correspondiente al UE mediante la red de par extremo junto con la entidad de red de acceso de la red cuando la red de par extremo solicita ser transferida a la red actual.

Cuando el UE se traslada desde la red 2G/3G a la red LTE, la primera red es una red 2G o una red 3G, la entidad de red de acceso de la red 2G incluye un BTS y un BSC. La entidad de red de acceso de la red 3G incluye un nodo (NodeB) y un RNC. La entidad de red central de la red 2G/3G incluye un SGSN. La segunda red es una LTE RAN, la entidad de red de acceso de la misma es un nodo evolucionado (eNodoB), y la entidad de red de acceso de la misma es una MME. La capacidad de seguridad incluye el algoritmo de protección de integridad y de encriptación NAS, el algoritmo de protección de integridad y de encriptación RRC, y el algoritmo de encriptación UP. La MME es seleccionada para configurar el algoritmo de encriptación y la protección de integridad NAS, y el eNodoB es configurado para seleccionar el algoritmo de encriptación, la protección integridad RRC y el algoritmo de encriptación UP. El principio y el proceso de trabajo están mostrados en la fig. 2, y los detalles no serán repetidos aquí. La MME y el eNB son adoptados para realizar la negociación del algoritmo de seguridad NAS y del algoritmo de seguridad RRC/UP respectivamente, de manera que es innecesario que la MME conozca la capacidad de seguridad del eNB de cierta manera (por ejemplo, configurando o extendiendo mensajes interactivos con el eNB) como en la técnica anterior.

En un ejemplo, cuando el UE se transfiere desde la red LTE a la red 3G, la entidad de red de acceso de la primera red es eNodoB, la entidad de red de acceso central de la primera red es MME, la entidad de red de acceso de la segunda red es RNC, y la entidad de red central de la segunda red es SGSN. La capacidad de seguridad incluye conjuntos de capacidad de seguridad 3G, y los conjuntos de capacidad de seguridad 3G incluyen además el algoritmo de encriptación y el algoritmo de protección de integridad. El principio y el proceso de trabajo están mostrados en la fig. 2, y los detalles no serán repetidos aquí. El RNC está configurado para seleccionar los conjuntos de capacidad de seguridad 3G, de manera que el SGSN no necesita introducir nuevos requisitos durante la transferencia desde la red LTE a la 3G, y la interacción entre el SGSN y el RNC es también innecesaria.

A través de la descripción anterior de las realizaciones, es evidente para los expertos en la técnica que las realizaciones pueden ser conseguidas mediante software sobre una plataforma hardware universal necesaria, y pueden ser conseguidos definitivamente también mediante hardware. Por lo tanto, las soluciones técnicas del presente invento pueden ser sustancialmente realizadas en forma de un producto de software. El producto de software puede ser almacenado en un medio de almacenamiento no volátil, tal como un CD-ROM, un disco USB, un disco duro desmontable, y contiene varias instrucciones para indicar a un equipamiento de comunicación (por ejemplo, un ordenador personal, un servidor, o un equipo de red) que realice el método como se ha descrito en las realizaciones del presente invento.

Será evidente para los expertos en la técnica que pueden hacerse distintas modificaciones y variaciones al presente invento sin desviarse del marco o espíritu del invento. En vista de lo anterior, se pretende que el presente invento cubra las modificaciones y variaciones de este invento proporcionadas que caen dentro del marco de las siguientes reivindicaciones y de sus equivalencias.

REIVINDICACIONES

1. Un método para la negociación de capacidad de seguridad, que es aplicable para realizar la negociación de capacidad de seguridad durante una transferencia de red móvil, que comprende:

A. recibir (202, 203), por una segunda red, una solicitud de transferencia enviada por una primera red;

B. seleccionar (207), por una entidad de red de acceso de la segunda red, una capacidad de seguridad correspondiente; y

C. enviar (210, 211), por la segunda red, las capacidades de seguridad seleccionadas a un UE mediante la primera red;

en el que la primera red es una red 2G o 3G; la segunda red es una red de evolución a largo plazo, LTE, la entidad de red de acceso de la segunda red es un nodo B evolucionado, eNodoB.

en el que la operación B comprende:

B1. enviar (205), por una entidad de gestión de movilidad, MME, un mensaje de solicitud de preparación de transferencia al eNodoB, llevando el mensaje de solicitud de preparación de transferencia un algoritmo de control de recurso de radio, RRC, y un algoritmo de plano de usuario, UP que son soportados por el UE, en que el algoritmo RRC comprende un algoritmo de encriptación y un algoritmo de protección de integridad; y

B2. seleccionar (207), por el eNodoB, un algoritmo RRC y un algoritmo UP que son soportados por el UE y el eNodoB de acuerdo con el algoritmo RRC y el algoritmo UP que son soportados por el UE y un algoritmo RRC y un algoritmo UP que son soportados por el eNodoB.

2. El método según la reivindicación 1, en el que el proceso de recepción comprende además:

enviar (202), por una entidad de red de acceso de la primera red, un mensaje de solicitud de transferencia a una entidad de red central de la primera red; y

enviar (203) por la entidad de red central de la primera red, un mensaje de solicitud de preparación de transferencia a la MME, en el que el mensaje de solicitud de preparación de transferencia lleva los conjuntos de capacidad de seguridad soportados por el UE.

3. El método según la reivindicación 1, en el que la operación B1 comprende:

enviar, por la MME, un algoritmo RRC y un algoritmo UP permitidos por un sistema para el eNodoB;

la operación B2 comprende:

seleccionar, por el eNodoB, el algoritmo RRC seleccionado, y el algoritmo UP combinando un algoritmo RRC y un algoritmo UP permitidos por el sistema.

4. El método según la reivindicación 1, en el que la operación C comprende:

C1. enviar (208), por el eNodoB, un mensaje de reconocimiento de preparación de transferencia que lleva el algoritmo RRC seleccionado y el algoritmo UP a la MME.

C2. enviar (209) por la MME, un mensaje de reconocimiento de preparación de transferencia que lleva el algoritmo NAS seleccionado, el algoritmo RRC seleccionado y el algoritmo UP a un Nodo de Soporte GPRS de Servicio, SGSN; y

C3. enviar (210), por el SGSN, una orden de transferencia al UE mediante una red de acceso de la primera red para indicar que el UE se transfiera a la segunda red, en el que la orden de transferencia lleva el algoritmo NAS seleccionado, el algoritmo RRC seleccionado y el algoritmo UP.

5. Un sistema para negociación de capacidad de seguridad, que comprende: una primera entidad (401) de red de acceso y una primera entidad (402) de red central de una primera red, y una segunda entidad (403) de red de acceso y una segunda entidad (404) de red central de una segunda red, en el que la primera red es una red 2G o 3G, la segunda red es una red de evolución a largo plazo, LTE, la segunda entidad de red de acceso es un nodo B evolucionado, eNodoB, y la segunda entidad de red central es una entidad de gestión de movilidad, MME,

en el que el sistema está caracterizado por que,

la segunda entidad de red de acceso está configurada para seleccionar un algoritmo de control de recurso de radio, RRC, y un algoritmo de plano de usuario, UP, cuando la primera red solicita transferir a la segunda red;

la segunda entidad de red central está configurada para seleccionar un algoritmo de señalización de No

Acceso, NAS, cuando la primera red solicita transferirse a la segunda red; y

la primera entidad de red de acceso y la primera entidad de red central están configuradas para enviar el algoritmo NAS seleccionado, el algoritmo RRC seleccionado y el algoritmo UP a un equipo de usuario, UE (405).

6. Un método para la negociación de capacidad de seguridad, que es aplicable para realizar la negociación de capacidad de seguridad durante una transferencia de red móvil desde 2G/3G a LTE, que comprende:

recibir (205), por un nodo B evolucionado, eNodoB, un mensaje de solicitud de preparación de transferencia enviado por una entidad de gestión de movilidad, MME, el mensaje de solicitud de preparación de transferencia que lleva un algoritmo de control de recurso de radio, RRC, y un algoritmo de plano del usuario, UP, que son soportados por un UE, en el que el algoritmo RRC comprende un algoritmo de encriptación y un algoritmo de protección de integridad;

seleccionar (207), por el eNodoB, un algoritmo RRC y un algoritmo UP que son soportados por el UE y el eNodoB de acuerdo con el algoritmo RRC y el algoritmo UP que son soportados por el UE y un algoritmo RRC y un algoritmo UP que son soportados por el eNodoB;

enviar (209, 210, 211), por el eNodoB, el algoritmo RRC seleccionado y el algoritmo UP a un UE a través de la primera red.

7. Un nodo B evolucionado, eNodoB, cuando es programado para llevar a cabo el método de la reivindicación 6, que tiene:

medios para recibir, un mensaje de solicitud de preparación de transferencia enviado por una entidad de gestión de movilidad, MME, el mensaje de solicitud de preparación de transferencia que lleva un algoritmo de control de recurso de radio, RRC, y un algoritmo de plano de usuario, UP, que son soportados por el UE, en el que el algoritmo RRC comprende un algoritmo de encriptación y un algoritmo de protección de integridad,

medios para seleccionar, un algoritmo RRC y un algoritmo UP que son soportados por el UE y el eNodoB de acuerdo con el algoritmo RRC y el algoritmo UP que son soportados por el UE y un algoritmo RRC y un algoritmo UP que son soportados por el eNodoB; y

medios para enviar, por el eNodoB, las capacidades de seguridad seleccionadas para un UE mediante la primera red.

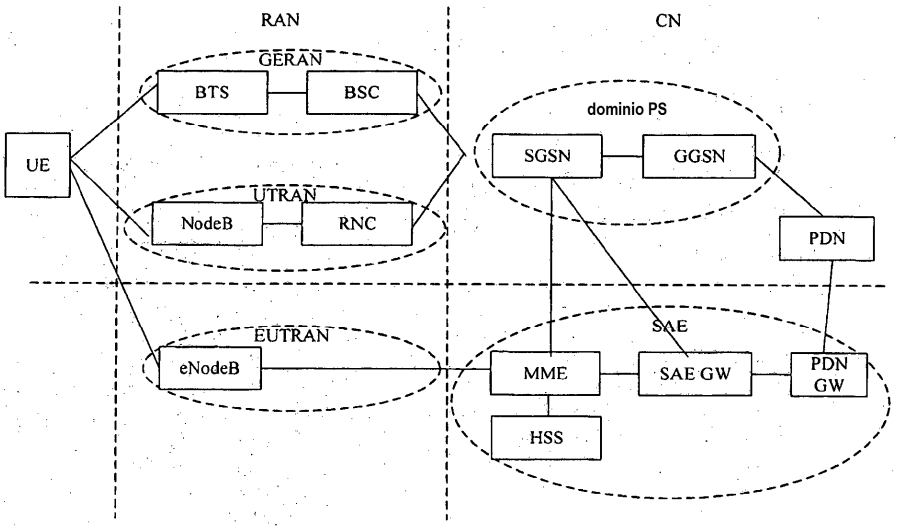
RAN
CN
GERAN
BTS
BSC
dominio PS
UE
SGSN
GGSN
UTRAN
NodeB
RNC
PDN
SAE
EUTRAN
eNodeB
MME
SAE GW
PDN GW
HSS

FIG. 1

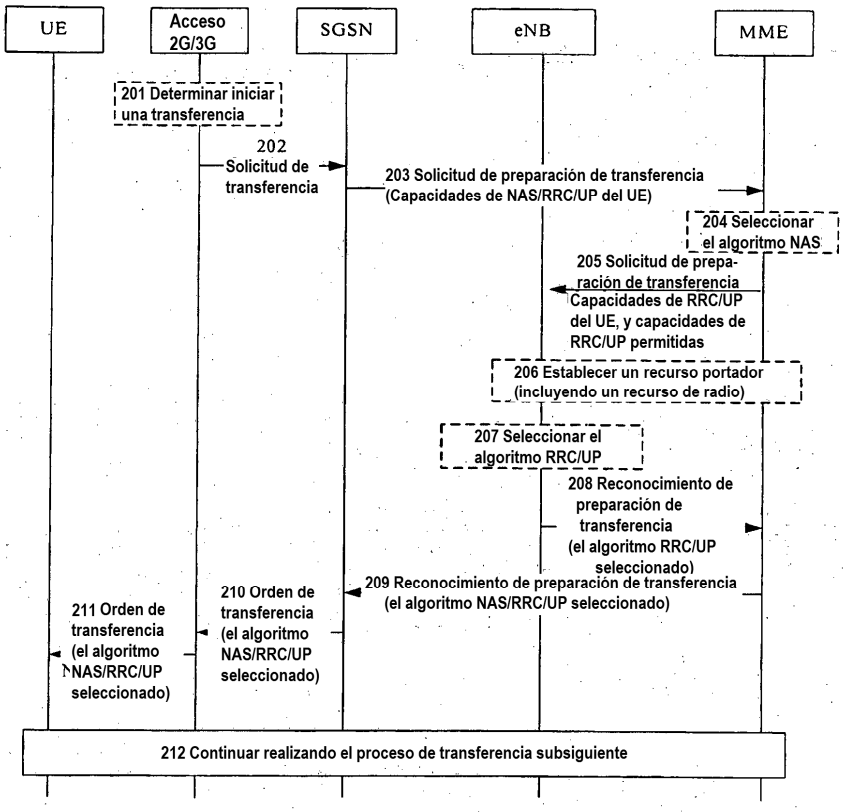
UE
Acceso 2G/3G
SGSN
eNB
MME
201 Determinar iniciar una transferencia
202 Solicitud de transferencia
203 Solicitud de preparación de transferencia (Capacidades de NAS/RRC/UP del UE)
204 Seleccionar el algoritmo NAS
205 Solicitud de preparación de transferencia Capacidades de RRC/UP del UE, y capacidades de RRC/UP permitidas
206 Establecer un recurso portador (incluyendo un recurso de radio)
207 Seleccionar el algoritmo RRC/UP
208 Reconocimiento de preparación de transferencia (el algoritmo RRC/UP seleccionado)
209 Reconocimiento de preparación de transferencia (el algoritmo NAS/RRC/UP seleccionado)
210 Orden de transferencia (el algoritmo NAS/RRC/UP seleccionado)
211 Orden de transferencia (el algoritmo NAS/RRC/UP seleccionado)
212 Continuar realizando el proceso de transferencia subsiguiente

FIG. 2

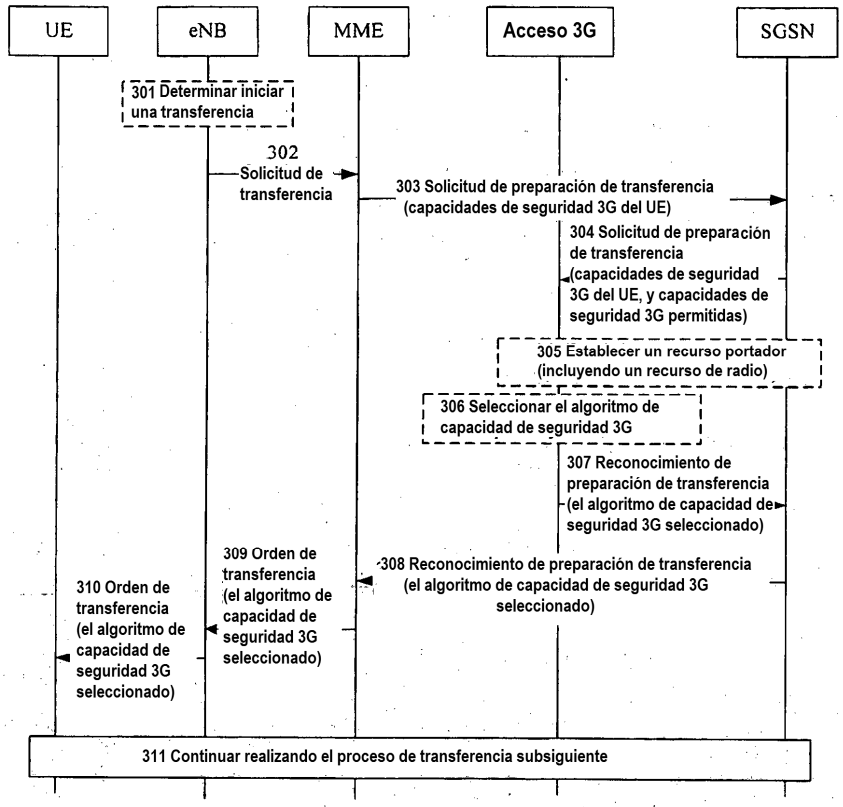
UE
eNB
MME
Acceso 3G
SGSN
301 Determinar iniciar una transferencia
302 Solicitud de transferencia
303 Solicitud de preparación de transferencia (capacidades de seguridad 3G del UE)
304 Solicitud de preparación de transferencia (capacidades de seguridad 3G del UE, y capacidades de seguridad 3G permitidas)
305 Establecer un recurso portador (incluyendo un recurso de radio)
306 Seleccionar el algoritmo de capacidad de seguridad 3G
307 Reconocimiento de preparación de transferencia (el algoritmo de capacidad de seguridad 3G seleccionado)
308 Reconocimiento de preparación de transferencia (el algoritmo de capacidad de seguridad 3G seleccionado)
309 Orden de transferencia (el algoritmo de capacidad de seguridad 3G seleccionado)
310 Orden de transferencia (el algoritmo de capacidad de seguridad 3G seleccionado)
311 Continuar realizando el proceso de transferencia subsiguiente

FIG. 3

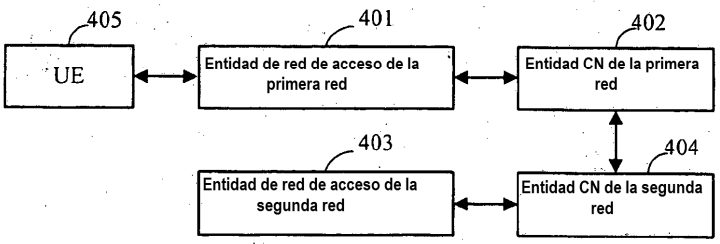
405
UE
401
Entidad de red de acceso de la primera red
402
Entidad CN de la primera red
403
Entidad de red de acceso de la segunda red
404
Entidad CN de la segunda red

FIG. 4