(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 768 275**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 12/06 (2009.01)
H04W 36/04 (2009.01)
H04W 84/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.05.2011 PCT/CN2011/074617**

(87) Fecha y número de publicación internacional: **10.11.2011 WO11137823**

(96) Fecha de presentación y número de la solicitud europea: **25.05.2011 E 11777242 (6)**

(97) Fecha y número de publicación de la concesión europea: **13.11.2019 EP 2603024**

(54) Título: **Método y dispositivo de separación de claves**

(30) Prioridad:

02.08.2010 CN 201010246928

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.06.2020

(73) Titular/es:

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

(72) Inventor/es:

LIU, XIAOHAN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y dispositivo de separación de claves

Campo de la invención

La invención presente guarda relación con el campo de comunicación, y particularmente con un método y dispositivo de separación de claves.

Antecedentes de la invención

La norma UMTS R9 (Sistema Universal de Telecomunicaciones Móviles) define el esquema de entrega entre una macrocélula y un HNB (Nodo B Residencial), así como el esquema de entrega entre HNB. En R9, la entrega entre macrocélula y HNB y la entrega entre HNB puede emplear un procedimiento de entrega duro común, y el SGSN (Nodo de Soporte GPRS servidor) de la Red Central (CN, por sus siglas en inglés) puede participar en todo el procedimiento de entrega.

Dado que el HNB cubre un rango relativamente menor (normalmente cubre el rango de varias decenas de metros), se pueden desplegar varios HNB en el mismo escenario de aplicación, y la entrega entre células HNB puede ocurrir debido al movimiento del usuario móvil. Cuando esta entrega se produce con frecuencia, supone una carga para la red. A fin de reducir el impacto en la CN (Red Central) y en los HNB en el marco de la misma pasarela (GW, por sus siglas en inglés) HNB, puede existir un esquema de optimización de la entrega en el que la señalización de la entrega entre HNB se interrumpe en la GW de HNB en caso de que no exista una interfaz lur entre los HNB, tal como se ilustra en la Fig. 1A; puede haber otro esquema de optimización de la entrega que indique que la señalización de la entrega entre HNB se reenvía a través de la GW de HNB y termina en la GW de HNB en caso de que exista una interfaz lur entre HNB, como se ilustra en la Fig. 1C; o puede haber otro esquema de optimización de la entrega que indique que la señalización de la entrega entre los HNB se transfiere directamente a través de la interfaz lur en caso de que exista una interfaz lur entre los HNB, como se ilustra en la Fig. 1B.

Además, el «3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Release 9)», 3GPP STANDARD 3GPP TS 33.401, n.º V9.4.0 (2010-06-16) ha establecido especificaciones técnicas o informes utilizando sus identidades 3GPP, identidades UMTS o identidades GSM.

Actualmente, en el sistema UMTS, durante el procedimiento de entrega en firme en el que la señalización de entrega finaliza en el SGSN, si el nodo de origen es HNB, la CK (Clave de Cifrado) y la IK (Clave de Integridad) no cambiarán después de que el UE pase del HNB de origen al nodo de destino (incluyendo RNC o HNB) esto es, el HNB de origen conoce la clave utilizada por el nodo destino. Debido a la vulnerabilidad de la ubicación de HNB (a diferencia de la RNC que se encuentra en la sala de ordenadores del operador), un atacante adquirirá la clave del nodo destino si adquiere la clave del HNB de origen. Del mismo modo, con respecto a la entrega entre HNB con la misma GW de HNB en el sistema UMTS, en el caso de que exista una interfaz lur entre HNB, el problema de seguridad de la separación de claves también se planteará una vez que el UE haya pasado del HNB de origen al HNB de destino. Además, en el sistema UMTS, al igual que en el escenario de la entrega anterior, el problema de seguridad de la separación de claves también se producirá cuando el UE pase de un HNB al RNC o a otro HNB en modo inactivo.

Compendio de la invención

La invención se define en las reivindicaciones independientes. En las reivindicaciones dependientes se incluyen características adicionales de la invención.

Las realizaciones y/o los ejemplos divulgados en la descripción siguiente que no estén cubiertos en las reivindicaciones adjuntas no se consideran parte de la invención presente.

Breve descripción de los dibujos

Los dibujos descritos en el presente permiten comprender en mayor profundidad la presente invención y construir una parte de la aplicación presente más bien que limitaciones a la invención presente, en qué:

Las figuras 1A-1C son diagramas esquemáticos de arquitecturas de entrega optimizadas actualmente;

La Fig. 2 es un diagrama de flujo de un método en el lado de SGSN según la primera realización de la invención presente;

La Fig. 3 es un diagrama de bloques constitucionales de un SGSN según la primera realización de la invención presente;

La Fig. 4 es un diagrama de flujo de un método en el lado de la GW de HNB, o lado de HNB, o lado de UE según la primera realización de la invención presente;

La Fig. 5 es un diagrama de bloques constitucionales de una GW de HNB según la primera realización de la invención presente;

La Fig. 6 es un diagrama de bloques constitucionales de un HNB de destino según la primera realización de la invención presente;

La Fig. 7 es un diagrama de bloques constitucionales de un UE según la primera realización de la invención presente;

La Fig. 8 es diagrama de flujo 1 de una interacción de sistema según la primera realización de la invención presente;

La Fig. 9 es diagrama de flujo 2 de una interacción de sistema según la primera realización de la invención presente;

La Fig. 10 es diagrama de flujo 3 de una interacción de sistema según la primera realización de la invención presente;

La Fig. 11 es diagrama de flujo 4 de una interacción de sistema según la primera realización de la invención presente;

La Fig. 12 es un diagrama de flujo de un método en el lado de SGSN según la segunda realización de la invención presente;

La Fig. 13 es un diagrama de bloques constitucionales de un SGSN según realización 2 de la invención presente;

La Fig. 14 es un diagrama de flujo de un método en el lado del UE según la segunda realización de la invención presente;

La Fig. 15 es un diagrama de bloques constitucionales de un UE según la segunda realización de la invención presente;

La Fig. 16 es un diagrama de flujo de una entrega según la segunda realización de la invención presente;

La Fig. 17 es un diagrama de flujo de un método para proporcionar información según la segunda realización de la invención presente;

La Fig. 18 es el diagrama de flujo 1 de una interacción del sistema de acuerdo con la realización mostrada en la Fig. 17;

La Fig. 19 es el diagrama de flujo 2 de una interacción del sistema de acuerdo con la realización mostrada en la Fig. 17;

La Fig. 20 es el diagrama de flujo 3 de una interacción del sistema de acuerdo con la realización mostrada en la Fig. 17;

La Fig. 21 es un diagrama de bloques constitucionales de una pasarela de Nodo B Residencial de acuerdo con la tercera realización de la invención presente.

Descripción detallada de las realizaciones

Para que el objeto, soluciones técnicas y ventajas de las realizaciones de la invención presente sean más aparentes, las realizaciones de la invención presente se describen y detallan a continuación en referencia a las realizaciones y dibujos. Las realizaciones de ejemplo de la invención presente y las descripciones de esta son simplemente explicaciones de la invención presente, en lugar de las limitaciones de esta.

Realización 1:

La Fig. 2 es un diagrama de flujo de un método de separación de claves proporcionado por la realización. En esta realización, el propio SGSN activa un Procedimiento de Autenticación y Acuerdo de Claves (AKA, por sus siglas en inglés) para actualizar la Clave de Cifrado y la Clave de Integridad, CK e IK respectivamente, con el fin de separar las claves del nodo de origen y del nodo de destino. Consulte la Fig. 2, el método se aplica a SGSN, incluyendo lo siguiente:

Paso 201: cuando un Equipo de Usuario entrega desde un nodo de origen a un nodo de destino, o cuando el Equipo de Usuario se mueve del nodo de origen al nodo de destino en estado inactivo, un SGSN determina si el nodo de origen es o no un Nodo B Residencial;

en donde, el método de esta realización se utiliza para una separación de claves, y así el método puede llevarse a cabo cuando se requiere la separación de claves. Por lo tanto, en el paso 201, cuando un Equipo de Usuario entrega desde un nodo de origen a un nodo de destino puede significar que el Equipo de Usuario está haciendo una entrega desde el nodo de origen al nodo de destino o que el Equipo de Usuario ha hecho una entrega desde el nodo de origen al nodo de destino. Además, cuando el Equipo de Usuario se mueve desde un nodo de origen a un nodo de destino en estado inactivo, puede significar que el Equipo de Usuario se está moviendo del nodo de origen al nodo de destino en estado inactivo o que el Equipo de Usuario se ha movido del nodo de origen al nodo de destino. Las expresiones similares tienen significados similares, por lo que se omitirán descripciones redundantes.

En la invención, el método para que SGSN juzgue si el nodo de origen es o no un HNB es el siguiente: si el nodo de origen es un HNB, el mensaje de solicitud de reubicación enviado por el HNB de origen al SGSN lleva un ID RNC de una GW de HNB; el SGSN puede determinar que el mensaje de solicitud de reubicación fue reenviado por la GW de HNB (la GW de HNB se registrará en el SGSN cuando se acceda a la red), por lo que el SGSN puede reconocer que el nodo de origen es un HNB.

En otro ejemplo, el método para que SGSN juzgue si el nodo de origen es o no un HNB puede ser el siguiente: si el mensaje de solicitud de reubicación recibido por el SGSN fue reenviado por la GW de HNB, el SGSN puede determinar que el nodo de origen es un HNB.

Paso 202: si el nodo de origen es el Nodo B Residencial, activar un Procedimiento de Autenticación y Acuerdo de Claves de acuerdo con la política del operador, para actualizar la Clave de Cifrado y la Clave de Integridad.

Según el método de esta realización, el SGSN puede enviar CK e IK al nodo de destino a través de un procedimiento SMC (Comando de Modo de Seguridad), de modo que el nodo de origen y el nodo de destino utilicen diferentes CK e IK para realizar una separación de claves.

En un ejemplo, el SGSN está configurado para confirmar si el nodo de destino es o no un Controlador de Red Radio (RNC, por sus siglas en inglés). En ese momento, el SGSN está configurado para que, cuando el nodo de origen es un HNB y el nodo de destino es un RNC, active la ejecución de AKA de acuerdo con la política del operador para realizar una separación de claves, es decir, para activar el Procedimiento de Autenticación y Acuerdo de Claves de acuerdo con la política del operador a fin de actualizar CK e IK.

En otro ejemplo, si el UE se mueve del nodo de origen (por ejemplo, HNB) al nodo de destino (por ejemplo, RNC) en estado inactivo, el SGSN también activa AKA para actualizar CK e IK después de descubrir que el UE se mueve del HNB al RNC.

Cuando el UE pasa del HNB al RNC en estado inactivo sin una RAU (Actualización de Enrutamiento), el SGSN no puede activar la ejecución de AKA, ya que el SGSN no puede reconocer que el UE ha pasado del HNB al RNC, pero es el UE el que activa el SGSN para ejecutar AKA. Esto se describirá en la siguiente realización.

En esta realización, la activación de la ejecución de AKA de acuerdo con la política del operador puede incluir lo siguiente: la activación de la ejecución de AKA después de que el UE haya pasado del nodo de origen al nodo de destino, o después de que el UE se haya movido del nodo de origen al nodo de destino en estado inactivo, o que una pasarela Nodo B Residencial del nodo de origen reciba un mensaje de liberación de interfaz IU.

En donde, durante el procedimiento de señalización en el que el SGSN envía una CK y una IK actualizadas al nodo de destino (por ejemplo, el HNB o RNC de destino, denominados en lo sucesivo como HNB/RNC de destino) mediante el procedimiento SMC, a fin de garantizar que el nodo de destino pueda seleccionar un algoritmo adecuado de cifrado y protección de la integridad, el nodo de destino puede añadir la capacidad de seguridad del UE a un mensaje de comando de modo de seguridad reenviado al UE, de modo que el UE realice una verificación de acuerdo con la capacidad de seguridad del UE enviada por el nodo de destino a fin de garantizar la seguridad. El método para verificar la capacidad de seguridad del UE incluye lo siguiente:

el nodo de destino reenvía al UE un comando de modo de seguridad enviado por el SGSN, en el que el comando de modo de seguridad incluye la capacidad de seguridad del UE, de modo que el UE verifica la capacidad de seguridad del UE.

En donde, después de verificar la capacidad de seguridad del UE, el UE devuelve el resultado de la verificación al nodo de destino a través de un mensaje de finalización del modo de seguridad, por lo que el nodo de destino puede recibir el mensaje de finalización del modo de seguridad, incluido el resultado de la verificación de la capacidad de seguridad del UE, devuelto por el UE.

Además, el nodo de destino puede solicitar al UE una capacidad de UE a través de un mensaje de solicitud de capacidad de UE independiente después de que se haya completado la entrega, y verificar la capacidad de UE después de que el UE devuelva su capacidad de UE, logrando así de forma similar el objetivo de garantizar la seguridad. El método para verificar la capacidad de seguridad del UE incluye lo siguiente:

una vez completado la entrega, el nodo de destino envía un mensaje de solicitud de capacidad de UE al UE, a fin de pedirle que devuelva su capacidad de seguridad al nodo de destino;

el nodo de destino verifica la capacidad de seguridad del UE de acuerdo con la capacidad de seguridad del UE devuelta por el UE.

El método de esta realización logra la separación de las claves del nodo de origen y del nodo de destino al activar la ejecución de AKA por el propio SGSN y actualizar la Clave de Cifrado y la Clave de Integridad (CK e IK, por sus siglas en inglés) utilizadas por el nodo de destino a través del SMC.

La Fig. 3 es un diagrama de bloques constitucionales de un SGSN de esta realización. Consulte la Fig. 3; el SGSN

incluye lo siguiente:

una unidad determinante 31, configurada para determinar si un nodo de origen es o no un Nodo B Residencial, cuando un Equipo de Usuario entrega desde el nodo de origen a un nodo de destino, o cuando el Equipo de Usuario se mueve del nodo de origen al nodo de destino en estado inactivo;

una unidad disparadora 32, configurada para activar un procedimiento AKA de acuerdo con la política del operador, cuando la unidad determinante 31 determina que el nodo de origen es un Nodo B Residencial a fin de actualizar CK e IK.

En un ejemplo, la unidad determinante 31 se configura además para determinar si el nodo de destino es un Controlador de Red Radio RNC y la unidad activadora 32 se configura específicamente para activar el procedimiento AKA de acuerdo con la política del operador cuando el nodo de origen es un HNB y el nodo de destino es un RNC a fin de actualizar la CK y la IK.

En un ejemplo, la unidad activadora 32 está configurada para activar el procedimiento AKA después de que el Equipo de Usuario haya pasado del nodo de origen al nodo de destino, o de que el Equipo de Usuario se haya movido del nodo de origen al nodo de destino en estado inactivo, o de que una pasarela de Nodo B Residencial del nodo de origen haya recibido un mensaje de liberación de interfaz IU.

El SGSN de esta realización corresponde al método de la realización como se ilustra en la Fig. 2. Los pasos se han descrito al detalle en la realización que se ilustra en la Fig. 2 y, por lo tanto, en el presente se omiten descripciones redundantes. El SGSN de esta realización activa el procedimiento AKA y actualiza la Clave de Cifrado y la Clave de Integridad (CK e IK) utilizadas por el nodo de destino a través del procedimiento SMC, realizando así la separación de las claves del nodo de origen y del nodo de destino.

La Fig. 4 es un diagrama de flujo de un método de separación de claves proporcionado por la realización. El método es aplicable a una GW de HNB, a un HNB de destino o a un UE que envía un mensaje de notificación a un SGSN para que este active un procedimiento AKA, con el fin de actualizar la CK e IK, realizando así el objetivo de la separación de claves. Consulte la Fig. 4, el método incluye lo siguiente:

Paso 401: cuando un Equipo de Usuario entrega desde un nodo de origen a un nodo de destino, o cuando el Equipo de Usuario se mueve del nodo de origen al nodo de destino en estado inactivo, determinar si el nodo de origen es o no un Nodo B Residencial.

En un ejemplo, cuando el método se aplica a una GW de HNB o a un HNB de destino, la GW de HNB o el HNB de destino pueden determinar si el nodo de origen es o no un Nodo B Residencial cuando un Equipo de Usuario entrega desde el nodo de origen al nodo destino.

Dado que el HNB está registrado a partir de la GW de HNB, el HNB envía un mensaje de solicitud de reubicación a la GW de HNB que lleva un ID RNC de la GW de HNB. Por lo tanto, la GW de HNB puede juzgar si la estación base de origen es o no un HNB y, a continuación, notificar al SGSN para que ponga en marcha el procedimiento AKA en el momento oportuno. Además, dado que el mensaje de solicitud de reubicación se enviará a la GW de HNB sólo cuando el nodo de origen sea un HNB, la GW de HNB podrá determinar que el nodo de origen es un HNB al recibir el mensaje de solicitud de reubicación. Los dos métodos anteriores para que la GW de HNB determine si el nodo de origen es o no un HNB son solo ejemplos, y esta realización no se ve limitada a esto.

Cuando se compruebe que una ID RNC contenida en el mensaje de solicitud de reubicación mejorada es igual a su ID RNC, el HNB de destino podrá juzgar si la estación base de origen es o no un HNB basado en ella y, por lo tanto, notificará al SGSN para que active el procedimiento AKA en el momento oportuno. Además, el HNB de destino también puede determinar si el nodo de origen es o no un HNB en base al rango del nodo de origen adquirido a través de la sincronización SGSN. Por ejemplo, el SGSN puede establecer diferentes rangos de direcciones para el HNB y la RNC y sincronizarlos con la GW de HNB y el HNB. Entonces, el HNB de destino puede determinar si el nodo de origen es o no un HNB en base al rango de direcciones cuando se necesita determinarlo. Los dos métodos anteriores para que el HNB de destino determine si el nodo de origen es o no un HNB son solo ejemplos, y esta realización no se ve limitada a esto.

En otro ejemplo, cuando el método se aplica a un Equipo de Usuario, el Equipo de Usuario puede determinar si el nodo de origen es o no un Nodo B Residencial en el caso de que el Equipo de Usuario entrega desde el nodo de origen al nodo de destino, o en el caso de que el Equipo de Usuario se mueva del nodo de origen al nodo de destino en estado inactivo.

En este caso, el UE reconoce por sí mismo si la estación base en la que reside es o no un HNB. Por lo tanto, el UE puede determinar si el nodo de origen es o no un Nodo B Residencial. Además, el UE puede determinar qué estaciones base son HNB leyendo los mensajes de difusión y, a continuación, reconocer si la estación base de origen en la que está registrada es o no un HNB. Los dos métodos anteriores para que el UE de destino determine si el nodo de origen es o no un HNB son solo ejemplos, y esta realización no se ve limitada a esto.

Paso 402: si el nodo de origen es un Nodo B Residencial, enviar un mensaje de notificación al SGSN para notificar al SGSN de que borre el contexto de seguridad al respecto y para hacer que el SGSN active un procedimiento de Autenticación y Acuerdo de Claves con el fin de actualizar CK e IK.

En un ejemplo, cuando el método se aplica a la GW de HNB o al UE, la GW de HNB o el UE pueden determinar además si el nodo de destino es un Controlador de Red Radio (RNC), y cuando el nodo de origen es un HNB y el nodo de destino es un RNC, se activa el SGSN para que realice un procedimiento de AKA para la separación de claves, es decir, se envía un mensaje de notificación al SGSN para informarle de que debe eliminar el contexto de seguridad al respecto y se activa el procedimiento de Autenticación y Acuerdo de Claves para actualizar CK e IK.

En donde, cuando se aplica el método a la GW de HNB, la GW de HNB envía el mensaje de notificación anterior al SGSN para que este ejecute AKA si la GW de HNB recibe un mensaje de liberación de (Release, en inglés) IU, o si el Equipo de Usuario pasa de estado activo a inactivo, o si se completa la entrega del Equipo de Usuario desde el nodo de origen al nodo de destino.

En donde, cuando se aplica el método al HNB de destino, el HNB de destino envía el mensaje de notificación anterior al SGSN para que este realice la función AKA, si se completa la entrega del Equipo de Usuario desde el nodo de origen al nodo de destino, o si el Equipo de Usuario pasa a un estado inactivo desde el estado activo.

En donde, cuando el método se aplica al UE, el Equipo de Usuario envía el mensaje de notificación al SGSN para que este realice la función AKA, si se completa la entrega del Equipo de Usuario desde el nodo de origen al nodo de destino, si se completa el movimiento del Equipo de Usuario desde el nodo de origen al nodo de destino en estado inactivo, si el Equipo de Usuario pasa del estado activo al estado inactivo, o si el Equipo de Usuario establece cada bit de la KSI almacenada localmente en 1, o si el UE establece el valor de estado almacenado localmente como un valor umbral.

Con el método de este ejemplo, la GW de HNB, el HNB de destino o el UE pueden hacer que el SGSN realice AKA a través de un mensaje de notificación en el momento adecuado a fin de actualizar la CK y la IK y permitir que el SGSN envíe la CK y la IK al nodo de destino a través del procedimiento SMC, de modo que el UE utilice la nueva CK y la IK en el nodo de destino, con lo que se separaría la clave del nodo de origen de la del nodo de destino.

En donde, durante el procedimiento de señalización en el que el SGSN envía una CK y una IK actualizadas al nodo de destino (por ejemplo, el HNB o RNC de destino, denominados en lo sucesivo como HNB/RNC de destino) mediante el procedimiento SMC, a fin de garantizar que el nodo de destino pueda seleccionar un algoritmo adecuado de cifrado y protección de la integridad, el nodo de destino puede añadir la capacidad de seguridad del UE a un mensaje de comando de modo de seguridad reenviado al UE, de modo que el UE realice una verificación de acuerdo con la capacidad de seguridad del UE enviada por el nodo de destino a fin de garantizar la seguridad. Además, el nodo de destino puede solicitar al UE una capacidad de UE a través de un mensaje de solicitud de capacidad de UE independiente después de que se haya completado la entrega, y verificar la capacidad de UE después de que el UE devuelva su capacidad de UE, logrando así garantizar la seguridad. Los pasos detallados del método anterior se han descrito en la realización que se ilustra en la Fig. 2 y no se repiten aquí.

La Fig. 5 es un diagrama de bloques constitucionales de una pasarela de Nodo B Residencial de esta realización. Consulte la Fig. 5, la pasarela de Nodo B Residencial incluye lo siguiente:

una unidad determinante 51, configurada para determinar si un nodo de origen es o no un Nodo B Residencial, cuando un Equipo de Usuario entrega desde el nodo de origen a un nodo de destino, y

una unidad emisora 52, configurada para enviar un mensaje de notificación a un SGSN cuando la unidad determinante 51 determine que el nodo de origen es el Nodo B Residencial para activar el SGSN a fin de que realice un Procedimiento de Autenticación y Acuerdo de Claves.

En un ejemplo, la unidad determinante 51 está configurada para determinar además si el nodo de destino es o no un Controlador de Red Radio (RNC), y la unidad emisora 52 está configurada específicamente para enviar un mensaje de notificación al SGSN cuando el nodo de origen sea un HNB y el nodo de destino sea un RNC para activar el SGSN a fin de que lleve a cabo el Procedimiento de Autenticación y Acuerdo de Claves.

La GW de HNB de este ejemplo puede hacer que el SGSN realice un procedimiento de AKA en el momento adecuado, por ejemplo, después de recibir un mensaje de liberación de IU, o de completar la entrega del Equipo de Usuario desde el nodo de origen al nodo de destino, o de que el Equipo de Usuario pase a un estado inactivo desde un estado activo, a fin de actualizar CK e IK, de modo que el SGSN envíe la CK y la IK al nodo de destino mediante el procedimiento SMC y el Equipo de Usuario utilice la nueva CK e IK en el nodo de destino, logrando de este modo la separación de la clave del nodo de origen de la del nodo de destino.

Los componentes de la GW de HNB de este ejemplo se utilizan para implementar los pasos de la realización antes mencionada, en la que se aplica el método ilustrado en la Fig. 4 a la GW de HNB. Los pasos se han descrito al detalle en la realización en la que el método ilustrado en la Fig. 4 se aplica a la GW de HNB y, por lo tanto, se omiten descripciones redundantes.

La Fig. 6 es un diagrama de bloques constitucionales de un Equipo de Usuario de esta realización. Consulte la Fig. 6, el Equipo de Usuario incluye lo siguiente:

una unidad determinante 61, configurada para determinar si un nodo de origen es o no un Nodo B Residencial, cuando un Equipo de Usuario entrega desde el nodo de origen a un nodo de destino, o cuando el Equipo de Usuario se mueve del nodo de origen al nodo de destino en estado inactivo; y

una unidad emisora 62, configurada para enviar un mensaje de notificación a un SGSN cuando la unidad determinante 61 determine que el nodo de origen es el Nodo B Residencial para notificar al SGSN de que debe realizar un Procedimiento de Autenticación y Acuerdo de Claves.

En un ejemplo, la unidad determinante 61 está configurada además para determinar además si el nodo de destino es o no un Controlador de Red Radio (RNC), y la unidad emisora 62 está configurada específicamente para enviar el mensaje de notificación al SGSN cuando el nodo de origen sea un HNB y el nodo de destino sea un RNC para notificar Al SGSN de que debe llevar a cabo el Procedimiento de Autenticación y Acuerdo de Claves.

El UE de este ejemplo puede hacer que el SGSN realice el procedimiento de AKA en el momento adecuado, por ejemplo, después de que se haya completado la entrega del Equipo de Usuario desde el nodo de origen al nodo de destino, o de que se haya completado el movimiento del Equipo de Usuario desde el nodo de origen al nodo de destino en estado inactivo, o de que el Equipo de Usuario pase a un estado inactivo desde el estado activo, o de que el Equipo de Usuario establezca cada bit del KSI almacenado localmente en 1, de que el UE establezca el valor de estado almacenado localmente como valor umbral, a fin de actualizar CK e IK, de modo que el SGSN envía la CK y la IK al nodo de destino mediante el procedimiento SMC y el UE utiliza la nueva CK e IK en el nodo de destino, logrando así la separación de la clave del nodo de origen de la del nodo de destino.

Los componentes del UE de esta realización se utilizan para implementar los pasos de la realización antes mencionada, en la que se aplica el método ilustrado en la Fig. 4 a la GW de HNB. Los pasos se han descrito al detalle en la realización en la que el método ilustrado en la Fig. 4 se aplica a la GW de HNB y, por lo tanto, se omiten descripciones redundantes.

La Fig. 7 es un diagrama de bloques constitucionales de un Nodo B Residencial de destino de este ejemplo. Consulte la Fig. 7; el HNB de destino incluye lo siguiente:

una unidad determinante 71, configurada para determinar si un nodo de origen es o no un Nodo B Residencial cuando el Equipo de Usuario entrega desde el nodo de origen a un nodo de destino; y

una unidad emisora 72, configurada para enviar un mensaje de notificación a un SGSN cuando la unidad determinante 71 determina que el nodo de origen es un Nodo B Residencial para notificar al SGSN que inicie un Procedimiento de Autenticación y Acuerdo de Claves.

El HNB de destino de esta realización puede hacer que el SGSN lleve a cabo un procedimiento de AKA en el momento adecuado, por ejemplo, después de que se haya completado la entrega del Equipo de Usuario desde el nodo de origen al nodo de destino, o que el Equipo de Usuario pase a un estado inactivo desde el estado activo, a fin de actualizar CK e IK, de modo que el SGSN envíe la CK y la IK al nodo de destino y el Equipo de Usuario utilice la CK y la IK nuevas en el nodo de destino, consiguiendo de este modo que se separe la clave del nodo de origen con respecto a la del nodo de destino.

Los componentes del HNB de destino de esta realización se utilizan para implementar los pasos de la realización antes mencionada, en la que se aplica el método ilustrado en la Fig. 4 a la GW de HNB. Los pasos se han descrito al detalle en la realización en la que el método ilustrado en la Fig. 4 se aplica a la GW de HNB y, por lo tanto, se omiten descripciones redundantes.

Para poder ver y entender mejor el método de separación de claves de esta realización, a continuación se incluyen las descripciones de este con referencia al flujo que se ilustra en las Fig. 8-11.

La Fig. 8 es un diagrama de flujo de un método de separación de claves de esta realización en el que una señalización de entrega termina en una NC. Consulte la Fig. 8, el flujo incluye lo siguiente:

Pasos 801-809: igual que el flujo de la entrega existente;

Paso 810.a: el propio SGSN juzga si debe activarse un AKA: cuando el nodo de origen es un HNB, o el nodo de origen es un HNB y el nodo de destino es un RNC, el SGSN realiza UMTS AKA una vez tan pronto como sea posible de acuerdo con la política del operador, a fin de garantizar la eliminación del contexto de seguridad UMTS en el SGSN.

En donde, el método para que el SGSN juzgue si el nodo de origen es o no un HNB se ha descrito en el paso 201 y, por lo tanto, no se repiten descripciones redundantes en el presente.

En donde, la realización utiliza un ejemplo en el que el UE hace una entrega desde el nodo de origen al nodo de objetivo, pero la realización no se ve limitada a esto. Por ejemplo, cuando el UE se mueve del nodo de origen al nodo

destino en estado inactivo, el SGSN puede activar la ejecución del AKA a través del paso 801.a, separando así la clave del nodo de origen de la del nodo destino.

En donde, la política del operador incluye lo siguiente: el Equipo de Usuario pasa a un estado inactivo desde el estado activo, o se completa la entrega del Equipo de Usuario desde el nodo de origen al nodo de destino, o se completa el movimiento del Equipo de Usuario desde el nodo de origen al nodo de destino en estado inactivo, o la GW de HNB recibe un mensaje de liberación de la interfaz de IU, etc., y la realización no se ve limitada a esto, siempre y cuando sea posible garantizar que se pueda eliminar el contexto de seguridad del UMTS en el SGSN.

Paso 810.b1: la GW de HNB notifica al SGSN que active el procedimiento de AKA: realización del paso 810.b2 cuando el nodo de origen es un HNB, o el nodo de origen es un HNB y el nodo de destino es un RNC;

En donde, el método para que la GW de HNB juzgue si el nodo de origen es o no un HNB se ha descrito al detalle en el paso 401 y, por lo tanto, se omiten descripciones redundantes en el presente.

Paso 810.b2: la GW de HNB activa el SGSN para que realice el procedimiento de AKA lo antes posible y en el momento oportuno, por ejemplo, después de que se haya completado la entrega del Equipo de Usuario desde el nodo de origen al nodo de destino, o cuando el Equipo de Usuario pase a estado inactivo desde el estado activo, o cuando la GW de HNB reciba un mensaje de liberación IU (liberación de interfaz IU), etc.; la GW de HNB notifica al SGSN que debe eliminar el contexto de seguridad del SGSN, de modo que el SGSN pueda realizar el procedimiento AKA una sola vez tan pronto como sea posible.

En donde, la GW de HNB puede hacer que el SGSN ejecute el procedimiento AKA lo antes posible mediante un mensaje de notificación, pero la realización no se limita a ello.

Paso 811: el UE y el SGSN realizan el procedimiento AKA.

Con el método anterior, el SGSN puede notificar al RNC de destino de la CK y la IK a través del procedimiento SMC, de forma que el UE utiliza la nueva CK y la IK en la RNC de destino, logrando así la separación de las claves del HNB de origen y la clave de la RNC de destino.

En donde, durante el procedimiento de señalización en el que el SGSN envía una CK y una IK actualizadas al nodo de destino (por ejemplo, el HNB o RNC de destino, denominados en lo sucesivo como HNB/RNC de destino) mediante el procedimiento SMC, a fin de garantizar que el nodo de destino pueda seleccionar un algoritmo adecuado de cifrado y protección de la integridad, el nodo de destino puede añadir la capacidad de seguridad del UE a un mensaje de comando de modo de seguridad reenviado al UE, de modo que el UE realice una verificación de acuerdo con la capacidad de seguridad del UE enviada por el nodo de destino a fin de garantizar la seguridad. Además, el nodo de destino puede solicitar al UE una capacidad de UE a través de un mensaje de solicitud de capacidad de UE independiente después de que se haya completado la entrega, y verificar la capacidad de UE después de que el UE devuelva su capacidad de UE, logrando así garantizar la seguridad. Los pasos detallados del método anterior se han descrito en la realización que se ilustra en la Fig. 2 y no se repiten descripciones redundantes.

La Fig. 9 es un diagrama de flujo de un método de separación de claves de esta realización cuando se termina una señalización de entrega en una GW de HNB, y no existe una interfaz Iur entre el nodo de origen y el nodo destino. Consulte la Fig. 9, el flujo incluye lo siguiente:

Pasos 901-907: el mismo que el procedimiento de entrega existente;

Paso 908.1: la GW de HNB notifica al SGSN para que active el procedimiento AKA con el mismo método que se muestra en la Fig. 8. Cuando el nodo de origen es un HNB, o el nodo de origen es un HNB y el nodo de destino es un RNC, la GW de HNB notifica al SGSN para que active el procedimiento AKA tan pronto como sea posible y en el momento adecuado, por ejemplo, después de que se haya completado la entrega del Equipo de Usuario desde el nodo de origen al nodo de destino, o cuando el Equipo de Usuario pase a estado inactivo desde el estado activo, o cuando la GW de HNB reciba un mensaje de liberación de IU; la GW de HNB notificará al SGSN para que borre el contexto de seguridad del SGSN y que este realice el procedimiento AKA a tiempo lo antes posible.

En el paso 401 se ha descrito detalladamente el método para que la GW de HNB determine si el nodo de origen es o no un HNB, y en el presente documento no se repite la descripción redundante.

Paso 908.2: el UE notifica al SGSN para que active el procedimiento AKA: cuando el nodo de origen es un HNB, o el nodo de origen es un HNB y el nodo de destino es un RNC, el UE notifica al SGSN para que active el procedimiento AKA en el momento adecuado, por ejemplo,

1) después de que se haya completado la entrega del Equipo de Usuario desde el nodo de origen al nodo de destino; o

2) después de que se haya completado el movimiento del Equipo de Usuario desde el nodo de origen al nodo de destino en estado inactivo; o

En donde, el ejemplo utiliza el caso en el que el Equipo de Usuario entrega desde el nodo de origen al nodo de destino como ejemplo, y cuando el Equipo de Usuario se mueve del nodo de origen al nodo de destino en estado inactivo, también es aplicable el método de realización. En ese caso, el UE puede hacer que el SGSN realice el procedimiento AKA una vez finalizado el movimiento.

3) después de que el UE pase a un estado inactivo desde el estado activo; o

4) el UE configura cada bit del KSI (Identificador del Conjunto de Claves) almacenado en 1; o

5) el UE fija el valor memorizado de «START» como valor umbral «STARTTHRESHOLD».

La UE puede hacer que el SGSN realice el procedimiento AKA en los casos anteriores.

En donde, en el paso 401 se ha descrito al detalle el método para que el UE determine si el nodo de origen es o no un HNB y, por lo tanto, se omiten descripciones redundantes.

909.1/909.2: la GW de HNB o el UE activan el SGSN para que realice el procedimiento AKA;

En donde, el SGSN podrá ser activado para realizar la función AKA a través de un mensaje de notificación, pero la realización no se limita a ello.

910: procedimiento AKA.

Con el método anterior, el SGSN puede notificar al HNB de destino de la CK y la IK a través del procedimiento SMC, de forma que el UE utiliza nuevas CK e IK en el HNB de destino, logrando así la separación de la clave del HNB de origen y la clave del HNB de destino.

En donde, durante el procedimiento de señalización en el que el SGSN envía las

CK y una IK actualizadas al nodo de destino (por ejemplo, el HNB o RNC de destino, denominados en lo sucesivo como HNB/RNC de destino) mediante el procedimiento SMC, a fin de garantizar que el nodo de destino pueda seleccionar un algoritmo adecuado de cifrado y protección de la integridad, el nodo de destino puede añadir la capacidad de seguridad del UE a un mensaje de comando de modo de seguridad reenviado al UE, de modo que el UE realice una verificación de acuerdo con la capacidad de seguridad del UE enviada por el nodo de destino a fin de garantizar la seguridad. Además, el nodo de destino puede solicitar al UE una capacidad de UE a través de un mensaje de solicitud de capacidad de UE independiente después de que se haya completado la entrega, y verificar la capacidad de UE después de que el UE devuelva su capacidad de UE, logrando así garantizar la seguridad. Los pasos detallados del método anterior se han descrito en la realización que se ilustra en la Fig. 2 y no se repiten descripciones redundantes.

La Fig. 10 es un diagrama de flujo de un método de separación de claves de esta realización cuando se termina una señalización de entrega en una GW de HNB y existe una interfaz lur entre el nodo de origen y el nodo destino. Consulte la Fig. 10, el flujo incluye lo siguiente:

Pasos 1001-1006: el mismo que el procedimiento de entrega existente;

Paso 1007.1: el HNB de destino notifica al SGSN para que active el procedimiento AKA; cuando el nodo de origen es un HNB, el HNB de destino notifica al SGSN que active el procedimiento AKA tan pronto como sea posible y en el momento adecuado, p. ej., después de que el Equipo de Usuario pase del estado activo al estado inactivo, o de que se haya completado la entrega del Equipo de Usuario desde el nodo de origen al nodo de destino; el HNB de destino notifica al SGSN para que este elimine el contexto de seguridad en el SGSN y este pueda realizar AKA una sola vez.

En el cual, en el paso 401 se ha descrito al detalle el método para que el HNB de destino determine si el nodo de origen es o no un HNB y, por lo tanto, se omiten descripciones redundantes.

Paso 1007.2: el UE notifica al SGSN para que active el procedimiento AKA: si el nodo de origen es un HNB, o el nodo de origen es un HNB y el nodo de destino es un RNC, el UE activa el SGSN para que realice el procedimiento AKA en el momento adecuado, por ejemplo,

1) después de que se haya completado la entrega del Equipo de Usuario desde el nodo de origen al nodo de destino; o

2) después de que se haya completado el movimiento del Equipo de Usuario desde el nodo de origen al nodo de destino en estado inactivo; o

En el cual, el ejemplo utiliza el caso en el que el Equipo de Usuario entrega desde el nodo de origen al nodo de destino como ejemplo, y cuando el Equipo de Usuario se mueve del nodo de origen al nodo de destino en estado inactivo, también es aplicable el método de realización. En ese caso, el UE puede hacer que el SGSN realice el procedimiento AKA una vez finalizado el movimiento.

3) después de que el UE pase a un estado inactivo desde el estado activo; o

4) el UE configura cada bit del KSI almacenado en 1; o

5) el UE fija el valor memorizado de «START» como valor umbral «STARTTHRESHOLD».

La UE puede hacer que el SGSN realice el procedimiento AKA en los casos anteriores.

En el cual, en el paso 401 se ha descrito al detalle el método para que el UE determine si el nodo de destino es o no un RNC y, por lo tanto, se omiten descripciones redundantes.

1008.1/1008.2: el HNB de destino o el UE activan el SGSN para que realice el procedimiento AKA;

En donde, el SGSN podrá ser activado para realizar la función AKA a través de un mensaje de notificación, pero la realización no se limita a ello.

1009: procedimiento AKA.

Con el método anterior, el SGSN puede notificar al HNB de destino de la CK y la IK de nuevo a través del procedimiento SMC, de forma que el UE utiliza nuevas CK e IK en el HNB de destino, logrando así la separación de las claves del HNB de origen y la clave del HNB de destino.

En el cual, durante el procedimiento de señalización en el que el SGSN envía una CK y una IK actualizadas al nodo de destino (por ejemplo, el HNB o RNC de destino, denominados en lo sucesivo como HNB/RNC de destino) mediante el procedimiento SMC, a fin de garantizar que el nodo de destino pueda seleccionar un algoritmo adecuado de cifrado y protección de la integridad, el nodo de destino puede añadir la capacidad de seguridad del UE a un mensaje de comando de modo de seguridad reenviado al UE, de modo que el UE realice una verificación de acuerdo con la capacidad de seguridad del UE enviada por el nodo de destino a fin de garantizar la seguridad. Además, el nodo de destino puede solicitar al UE la capacidad de UE a través de un mensaje de solicitud de capacidad de UE independiente después de que se haya completado la entrega, y verificar la capacidad de UE después de que el UE devuelva su capacidad de UE, logrando así garantizar la seguridad. Los pasos detallados del método anterior se han descrito en la realización que se ilustra en la Fig. 2 y no se repiten descripciones redundantes.

La Fig. 11 es un diagrama de flujo de un método de separación de claves de esta realización cuando una señalización de entrega se reenvía por una pasarela Nodo B Residencial del nodo de origen, y existe una interfaz lógica lur entre el nodo de origen y el nodo de destino, es decir, la señalización de entrega se reenvía a través de la GW de HNB. Consulte la Fig. 11, el flujo incluye lo siguiente:

Pasos 1101-1109: el mismo que el procedimiento de entrega existente;

Paso 1110.1: la GW de HNB notifica al SGSN para que active el procedimiento AKA con el mismo método que se muestra en la Fig. 8. Cuando el nodo de origen es HNB, o el nodo de origen es HNB y el nodo de destino es RNC, la GW de HNB notifica al SGSN para que active el procedimiento AKA lo antes posible y en el momento adecuado, por ejemplo, después de que el Equipo de Usuario pase a un estado inactivo desde el estado activo, o de que la GW de HNB reciba el mensaje de liberación de IU, o de que se haya completado la entrega del Equipo de Usuario desde el nodo de origen al nodo de destino; la GW de HNB notifica al SGSN para que este elimine el contexto de seguridad del SGSN y realice el procedimiento AKA una sola vez tan pronto como sea posible.

En el paso 401 se ha descrito detalladamente el método para que la GW de HNB determine si el nodo de origen es o no un HNB, y en el presente documento no se repite la descripción redundante.

Paso 1110.2: el HNB de destino notifica al SGSN para que active el procedimiento AKA; cuando el nodo de origen es un HNB, el HNB de destino notifica al SGSN que active el procedimiento AKA tan pronto como sea posible y en el momento adecuado, p. ej., después de que el Equipo de Usuario pase del estado activo al estado inactivo, o de que se haya completado la entrega del Equipo de Usuario desde el nodo de origen al nodo de destino; el HNB de destino notifica al SGSN para que este elimine el contexto de seguridad en el SGSN y este pueda realizar AKA una sola vez tan pronto como sea posible.

En el cual, en el paso 401 se ha descrito al detalle el método para que el HNB de destino determine si el nodo de origen es o no un HNB y, por lo tanto, se omiten descripciones redundantes.

Paso 1110.3: el UE notifica al SGSN para que active el procedimiento AKA: si el nodo de origen es un HNB, o el nodo de origen es un HNB y el nodo de destino es un RNC, el UE activa el SGSN para que realice el procedimiento AKA en el momento adecuado, por ejemplo,

1) después de que se haya completado la entrega del Equipo de Usuario desde el nodo de origen al nodo de destino; o

2) después de que se haya completado el movimiento del Equipo de Usuario desde el nodo de origen al nodo de

destino en estado inactivo; o

En el cual, la realización utiliza el caso en el que el UE entrega desde el nodo de origen al nodo de destino como ejemplo y, cuando el UE se mueve del nodo de origen al nodo de destino en estado inactivo, también es aplicable el método de realización. En ese caso, el UE puede hacer que el SGSN realice el procedimiento AKA una vez finalizado el movimiento.

3) después de que el UE pase a un estado inactivo desde el estado activo; o

4) el UE configura cada bit del KSI almacenado en 1;

5) el UE fija el valor memorizado de «START» como valor umbral de «STARTTHRESHOLD».

La UE puede hacer que el SGSN realice el procedimiento AKA en los casos anteriores.

En el cual, en el paso 401 se ha descrito al detalle el método para que el UE determine si el nodo de destino es o no un RNC y, por lo tanto, se omiten descripciones redundantes.

La descripción anterior describe el procedimiento para que el HNB de destino o el UE activen el SGSN para que este realice el procedimiento AKA. En esta realización, cuando se desea que la GW de HNB active el procedimiento AKA, la GW de HNB debe analizar los mensajes relacionados con la entrega, y en este caso se omite la descripción redundante.

Pasos 1111.1/1111.2/1111.3: la GW de HNB, el HNB de destino o el UE activan el SGSN para que realice el procedimiento AKA;

En donde, el SGSN podrá ser activado para realizar la función AKA a través de un mensaje de notificación, pero la realización no se limita a ello.

Paso 1112: procedimiento AKA.

Con el método anterior, el SGSN puede notificar al HNB de destino de la CK y la IK a través del procedimiento SMC, de forma que el UE utiliza nuevas CK e IK en el HNB de destino, logrando así la separación de las claves del HNB de origen y la clave del HNB de destino.

En el cual, durante el procedimiento de señalización en el que el SGSN envía una CK y una IK actualizadas al nodo de destino (por ejemplo, el HNB o RNC de destino, denominados en lo sucesivo como HNB/RNC de destino) mediante el procedimiento SMC, a fin de garantizar que el nodo de destino pueda seleccionar un algoritmo adecuado de cifrado y protección de la integridad, el nodo de destino puede añadir la capacidad de seguridad del UE a un mensaje de comando de modo de seguridad reenviado al UE, de modo que el UE realice una verificación de acuerdo con la capacidad de seguridad del UE enviada por el nodo de destino a fin de garantizar la seguridad. Además, el nodo de destino puede solicitar al UE la capacidad de UE a través de un mensaje de solicitud de capacidad de UE independiente después de que se haya completado la entrega, y verificar la capacidad de UE después de que el UE devuelva su capacidad de UE, logrando así garantizar la seguridad. Los pasos detallados del método anterior se han descrito en la realización que se ilustra en la Fig. 2 y no se repiten descripciones redundantes.

El método de esta realización activa el SGSN de varias maneras para que realice el procedimiento AKA a fin de actualizar la CK y la IK utilizadas por el nodo de destino, logrando así la separación de la clave del nodo de origen de la del nodo de destino.

Realización 2:

La Fig. 12 es un diagrama de flujo de un método de separación de claves proporcionado por esta realización. El método se aplica al SGSN en el escenario de entrega en el que una señalización de entrega pasa por la Red Central para separar la clave de un nodo de origen (por ejemplo, el HNB de origen) y la clave de un nodo de destino (por ejemplo, el HNB de destino o la RNC de destino [en lo sucesivo denominados «HNB⁄RNC de destino»]). Consulte la Fig. 12, el método incluye lo siguiente:

Paso 1201: durante la entrega de un Equipo de Usuario desde un nodo de origen a un nodo de destino, un SGSN determina si el nodo de origen es o no Nodo B Residencial;

en donde, el método para que el SGSN determine si el nodo de origen es o no un Nodo B Residencial es el mismo que el descrito en el paso 201, y en este caso se omite la descripción redundante.

Paso 1202: si el nodo de origen es Nodo B Residencial, seleccione uno de entre una pluralidad de Vectores de Autenticación almacenados localmente y utilice una Clave de Cifrado y una Clave de Integridad (CK e IK) correspondientes al Vector de Autenticación seleccionado como clave utilizada por el Equipo de Usuario en el nodo de destino;

en donde, cuando solo hay un Vector de Autenticación almacenado localmente, es posible solicitar un Sistema de Abonado Residencial (HSS, por sus siglas en inglés) para un grupo de Vectores de Autenticación y, a continuación, seleccionar uno del grupo de Vectores de Autenticación.

En un ejemplo, el SGSN puede determinar además si el nodo de destino es o no un Controlador de Red Radio (RNC). El SGSN está configurado, cuando el nodo de origen es HNB y el nodo de destino es RNC, para activar un procedimiento de separación de claves utilizando Vectores de Autenticación, es decir, seleccionando uno de una pluralidad de Vectores de Autenticación almacenados localmente y utilizando la Clave de Cifrado y la Clave de Integridad correspondientes al Vector de Autenticación seleccionado como clave utilizada por el Equipo de Usuario en el nodo de destino.

Paso 1203: enviar al Equipo de Usuario un número aleatorio RAND correspondiente al Vector de Autenticación seleccionado, a fin de que el Equipo de Usuario genere la CK e IK de acuerdo con el RAND.

En este ejemplo, un indicador de verificación AUTN correspondiente al Vector de Autenticación seleccionado también puede enviarse al Equipo de Usuario para la verificación realizada por el Equipo de Usuario.

En este ejemplo, si el Equipo de Usuario verifica el AUTN o calcula el RES después de generar la CK e IK según el RAND y devuelve un mensaje de respuesta de verificación, el método de este ejemplo además incluye lo siguiente:

Paso 1204: recibir el mensaje de respuesta de verificación devuelto por el Equipo de Usuario, en donde, el mensaje de respuesta de verificación incluye el resultado de la verificación con respecto al AUTN por parte del Equipo de Usuario y/o el RES calculado por el Equipo de Usuario;

Paso 1205: si el resultado de la verificación indica que la verificación falla, o que el RES calculado por el UE es inconsistente con el XRES correspondiente al Vector de Autenticación seleccionado, las CK e IK correspondientes al Vector de Autenticación seleccionado no se utilizarían como claves utilizadas por el Equipo de Usuario en el nodo de destino.

En donde, la realización no se limita a devolver la información anterior utilizando el mensaje de respuesta de verificación, y puede utilizarse otro mensaje, por ejemplo, una parte de otro mensaje de entrega como el mensaje de finalización de la reubicación.

Con el método de esta realización, cuando el UE hace la entrega del HNB de origen al HNB/RNC de destino, el SGSN vuelve a seleccionar un nuevo AV a partir de una pluralidad de Vectores de Autenticación (AV, por sus siglas en inglés) almacenados localmente, y utiliza la CK e IK correspondientes a este AV como claves utilizadas por el UE en el HNB/RNC de destino. El SGSN envía un RAND correspondiente a este AV al UE, y el UE deriva nuevas CK e IK según el RAND, asegurando así la separación de la clave del HNB de origen de la clave del HNB/RNC de destino.

La Fig. 13 es un diagrama de bloques constitucionales de un SGSN de esta realización. Consulte la Fig. 13; el SGSN incluye lo siguiente:

una primera unidad determinante 131, configurada para determinar si un nodo de origen es o no un Nodo B Residencial, cuando un Equipo de Usuario entrega desde el nodo de origen a un nodo de destino;

una unidad de selección 132, configurada para seleccionar uno de una pluralidad de Vectores de Autenticación almacenados localmente cuando la primera unidad determinante 131 determina que el nodo de origen es Nodo B Residencial, y utiliza las CK e IK correspondientes al Vector de Autenticación seleccionado como claves utilizadas por el Equipo de Usuario en el nodo de destino; y

una unidad emisora 133, configurada para enviar el RAND correspondiente al Vector de Autenticación seleccionado por la unidad de selección 132 al Equipo de Usuario, de forma que el Equipo de Usuario genere las CK e IK de acuerdo con el RAND.

En un ejemplo, la primera unidad determinante 131 está configurada además para determinar si el nodo de destino es o no un Controlador de Red Radio RNC, y la unidad de selección 132 está configurada específicamente para seleccionar uno de una pluralidad de Vectores de Autenticación almacenados localmente cuando el nodo de origen es HNB y el nodo de destino es RNC, y utilizar las CK e IK correspondientes al Vector de Autenticación seleccionado como claves utilizadas por el Equipo de Usuario en el nodo de destino.

En un ejemplo, la unidad de selección 132 puede incluir lo siguiente:

un módulo de solicitud 1321, configurado para solicitar el HSS para un grupo de Vectores de Autenticación cuando solo hay un Vector de Autenticación almacenado localmente;

un módulo de selección 1322, configurado para seleccionar uno del grupo de Vectores de Autenticación obtenidos a petición del módulo de petición 1321.

En otro ejemplo, la unidad emisora 133 también puede enviar el AUTN correspondiente al Vector de Autenticación

seleccionado al Equipo de Usuario para su verificación, y el Equipo de Usuario puede calcular el RES de acuerdo con esto. En tal caso, el SGSN podrá incluir además lo siguiente:

una unidad receptora 134, configurada para recibir el mensaje de respuesta de verificación devuelto por el Equipo de Usuario, en donde, el mensaje de respuesta de verificación incluye el resultado de la verificación con respecto al AUTN por parte del Equipo de Usuario y/o el RES calculado por el Equipo de Usuario;

una segunda unidad determinante 135, configurada para determinar que las claves CK e IK correspondientes al Vector de Autenticación seleccionado no deben utilizarse como claves utilizadas por el Equipo de Usuario en el nodo de destino cuando el resultado de la verificación en el mensaje de respuesta de verificación recibido por la unidad receptora 134 indique que falla la verificación o que el RES calculado por el Equipo de Usuario es inconsistente con el XRES correspondiente al Vector de Autenticación seleccionado.

Las partes constituyentes del SGSN de esta realización se utilizan para implementar los pasos de la realización del método antedicho ilustrado en la Fig. 12. Los pasos se han descrito al detalle en la realización del método que se ilustra en la Fig. 12 y, por lo tanto, en el presente se omiten descripciones abundantes.

El SGSN de esta realización vuelve a seleccionar las CK e IK para que las utilice el nuevo nodo de destino, logrando así la separación de la clave del nodo de origen de la del nodo de destino.

La Fig. 14 es un diagrama de flujo de un método de separación de claves según una realización de la invención actual, siendo el método aplicable a un Equipo de Usuario en un escenario de entrega en el que una señalización de entrega pasa por una Red Central. Consulte la Fig. 14, el método incluye lo siguiente:

Paso 1401: durante la entrega de un Equipo de Usuario desde un nodo de origen a un nodo destino, recibir un mensaje de reconfiguración de la conexión de control de recursos de radio RRC enviado por el nodo de origen, incluyendo el mensaje de reconfiguración de la conexión RRC el RAND correspondiente al Vector de Autenticación seleccionado por un SGSN;

en un ejemplo, el mensaje de reconfiguración de la conexión RRC puede incluir además el AUTN correspondiente al Vector de Autenticación seleccionado por el SGSN para la verificación.

Paso 1402: generar las CK e IK según el RAND, y usar las CK e IK como claves utilizadas en el nodo de destino.

En un ejemplo, después de generar nuevas CK e IK de acuerdo con el RAND, el Equipo de Usuario puede verificar el AUTN de acuerdo con los parámetros en el AUTN y el RAND, y devolver un resultado de verificación al SGSN, de modo que el SGSN determine si la CK y la IK correspondientes al Vector de Autenticación seleccionado deben o no utilizarse como claves utilizadas por el Equipo de Usuario en el nodo de destino de acuerdo con el resultado de la verificación.

En donde, el resultado de la verificación podrá enviarse al SGSN mediante un mensaje de respuesta de verificación u otro mensaje como, por ejemplo, el mensaje de finalización de la reubicación, y la realización no se limita a ello. Si la verificación falla, el SGSN no utiliza la CK y la IK correspondientes al Vector de Autenticación seleccionado como claves utilizadas por el Equipo de Usuario en el nodo de destino.

En otro ejemplo, el UE puede calcular el RES según el RAND y devolver el RES calculado al SGSN, de modo que el SGSN determine si la CK y la IK correspondientes al Vector de Autenticación seleccionado deben o no utilizarse como claves utilizadas por el Equipo de Usuario en el nodo de destino, de acuerdo con el RES.

En donde, y de forma similar, el RES podrá enviarse al SGSN mediante un mensaje de respuesta de verificación u otro mensaje, y la realización no se limita a ello. Si el RES es inconsistente con el XRES correspondiente al Vector de Autenticación seleccionado por el SGSN, el SGSN no utiliza la CK y la IK correspondientes al Vector de Autenticación seleccionado como claves utilizadas por el Equipo de Usuario en el nodo de destino.

Con el método de esta realización, el UE puede derivar nuevas CK e IK según el RAND, y el SGSN vuelve a seleccionar las CK e IK utilizadas por el nuevo nodo de destino, logrando así la separación de la clave del nodo de origen de la del nodo de destino.

La Fig. 15 es un diagrama de bloques constitucionales de un Equipo de Usuario según una realización de la invención presente. Consulte la Fig. 15, el Equipo de Usuario incluye lo siguiente:

una unidad receptora 151, configurada para recibir el mensaje de reconfiguración de la conexión RRC enviado por un nodo de origen, cuando el Equipo de Usuario entrega desde el nodo de origen a un nodo destino, incluyendo el mensaje de reconfiguración de la conexión RRC un RAND correspondiente al Vector de Autenticación seleccionado por SGSN;

una unidad de generación 152, configurada para generar las CK e IK según el RAND en el mensaje de reconfiguración de la conexión RRC recibido por la unidad receptora 151, y para utilizar la CK y la IK como claves utilizadas en el nodo destino.

En un ejemplo, el mensaje de reconfiguración de la conexión RRC recibido por la unidad receptora 151 incluye además el AUTN correspondiente al Vector de Autenticación seleccionado por el SGSN, y el Equipo de Usuario también incluye lo siguiente:

una unidad verificadora 153, configurada para verificar el AUTN de acuerdo con los parámetros en el AUTN y el RAND en el mensaje de reconfiguración de la conexión RRC recibido por la unidad receptora 151;

una unidad emisora 154, configurada para enviar al SGSN un mensaje de respuesta de verificación que incluya el resultado de la verificación después de la verificación realizada por la unidad verificadora 153, de modo que el SGSN determine si la CK y la IK correspondientes al Vector de Autenticación seleccionado deben utilizarse o no como las claves utilizadas por el Equipo de Usuario en el nodo de destino en función del resultado de la verificación; si el resultado de la verificación indica que la verificación ha fallado, el SGSN no utiliza la CK y la IK correspondientes al Vector de Autenticación como claves utilizadas por el UE en el nodo de destino.

En otro ejemplo, el UE incluye además:

una unidad de cálculo 155, configurada para calcular el RES según el RAND en el mensaje de reconfiguración de la conexión RRC recibido por la unidad receptora 151;

la unidad emisora 154 está configurada además para enviar el RES calculado por la unidad de cálculo 155 al SGSN a través del mensaje de respuesta de verificación, de modo que el SGSN determina si la CK y la IK correspondientes al Vector de Autenticación seleccionado deben utilizarse o no como las claves utilizadas por el Equipo de Usuario en el nodo de destino de acuerdo con el RES; si el RES es inconsistente con el XRES correspondiente al Vector de Autenticación seleccionado por el SGSN, el SGSN no utiliza la CK y la IK correspondientes al Vector de Autenticación como claves utilizadas por el Equipo de Usuario en el nodo de destino.

Las partes constituyentes del UE de esta realización se utilizan para poner en práctica los pasos de la realización del método antedicho como se ilustra en la Fig. 14. Los pasos se han descrito al detalle en la realización del método que se ilustra en la Fig. 14 y, por lo tanto, en el presente se omiten descripciones redundantes.

El UE de esta realización puede derivar nuevas CK e IK según el RAND, y el SGSN vuelve a seleccionar la Clave de Cifrado y la Clave de Integridad utilizadas por el nuevo nodo de destino, logrando así la separación de la clave del nodo de origen de la del nodo de destino.

Para poder ver y entender mejor el método de separación de claves de esta realización, a continuación se incluyen las descripciones de este con referencia al flujo que se ilustra en las Fig. 16. Consulte la Fig. 16, el flujo incluye lo siguiente:

Paso 1601: un HNB de origen decide la entrega a un RNC de destino;

Paso 1602: el HNB de origen envía un mensaje de solicitud de reubicación a una GW de HNB;

Etapa 1603: la GW de HNB envía además el mensaje de solicitud de reubicación a un SGSN de una Red Central;

Paso 1604: si la estación base de origen de la entrega es HNB o la estación base de origen de la entrega es HNB y el nodo de destino de la entrega es RNC, el SGSN vuelve a seleccionar un nuevo AV a partir de una pluralidad de AV almacenados localmente y utiliza las CK e IK correspondientes a este AV como claves utilizadas por el UE en el HNB/RNC de destino.

En donde, si el SGSN solo tiene un Vector de Autenticación AV, el SGSN solicita un HSS para un grupo de Vectores de Autenticación AV, selecciona un AV de este y utiliza las CK e IK correspondientes a este AV como claves utilizadas por el UE en el HNB/RNC de destino.

En donde, el método para que el SGSN juzgue si la estación base de origen es o no un HNB puede ser la siguiente: si el nodo de origen es HNB, el HNB lleva la ID RNC de la GW de HNB en el mensaje de solicitud de reubicación enviado al SGSN y este puede juzgar que el mensaje de solicitud de reubicación se ha reenviado desde la GW de HNB (la GW de HNB se registrará en el SGSN cuando acceda a la red), por lo que el SGSN puede reconocer que la estación base de origen es HNB. Por supuesto, el SGSN puede juzgar si el Nodo B Residencial es o no HNB con otro método, por ejemplo, el SGSN puede juzgar si la estación base de origen es HNB asignando diferentes rangos de ID RNC a la GW de HNB y al RNC, y la realización no se limita a ello.

Paso 1605: el SGSN envía el mensaje de solicitud de reubicación al RNC de destino;

Paso 1606: la RNC de destino devuelve un mensaje de respuesta de solicitud de reubicación al SGSN;

Paso 1607: el SGSN envía a la GW de HNB un mensaje de comando de reubicación que lleva el RAND correspondiente al AV;

de forma opcional, el mensaje puede llevar el AUTN correspondiente al AV.

Paso 1608: la GW de HNB reenvía el mensaje de comando de reubicación que lleva el RAND al HNB de origen.

Paso 1609: el HNB de origen envía al UE el mensaje de reconfiguración de la conexión RRC con el RAND correspondiente al AV seleccionado por el SGSN;

Paso 1610: después de recibir el RAND, el UE genera nuevas CK e IK según el RAND;

en donde, si el mensaje anterior lleva el AUTN, el UE puede verificar el AUTN de acuerdo con los parámetros en el AUTN y el RAND; si la verificación falla, la información de verificación de falla se devuelve al SGSN y este no utiliza la CK y la IK correspondientes al AV como las claves utilizadas por el UE en el HNB/RNC de destino.

En donde, el UE puede calcular el RES con arreglo al RAND.

Paso 1611: tras verificar el AUTN o calcular el RES, el UE vuelve a enviar un mensaje de respuesta de verificación al SGSN para notificarle el resultado de la verificación y el RES calculado por el UE;

en donde, el mensaje de respuesta de verificación puede enviarse al SGSN como parte de otro mensaje de entrega, como el mensaje de finalización de la reubicación, y la realización no se limita a él.

Paso 1602: el SGSN compara el RES y el XRES correspondientes al AV y, si son diferentes entre sí, el SGSN no utiliza la CK y la IK correspondientes al AV como el par de claves utilizado por el UE en el HNB/RNC de destino;

Paso 1613: otro mensaje de entrega, es decir, el resto del procedimiento de entrega.

Con el método de esta realización, el SGSN puede notificar al RNC de destino de las CK e IK a través del procedimiento SMC, de modo que el UE utiliza nuevas CK e IK en la RNC de destino, logrando así la separación de la clave del HNB de origen de la de la RNC de destino.

Realización 3:

La Fig. 17 es un diagrama de flujo de una información relacionada con la seguridad que proporciona un método proporcionado por la realización. La realización es aplicable a un escenario de entrega en el que una señalización de entrega entre HNB termina en una GW de HNB y no existe una interfaz directa entre HNB. Consulte la Fig. 17, el método se aplica a la pasarela de Nodo B Residencial (GW de HNB), y este incluye lo siguiente:

Paso 1701: adquisición y almacenamiento de información relacionada con la seguridad, incluida una lista de algoritmos de cifrado y protección de la integridad permitidos por la Red Central y la Clave de Cifrado y la Clave de Integridad del plano de usuario actual;

en donde, existen diferentes métodos para que la GW de HNB adquiera la información relacionada con la seguridad en función de si el UE accede a la red desde el HNB o desde la RNC. A continuación se dan diferentes ejemplos.

Paso 1702: enviar la información relacionada con la seguridad a un nodo de destino, de modo que el nodo de destino seleccione el algoritmo y utilice claves de acuerdo con la información relacionada con la seguridad.

En el procedimiento convencional de la entrega de datos, el SGSN envía al RNC de destino la lista de algoritmos de cifrado y protección de la integridad permitidos por la Red Central y la Clave de Cifrado y la Clave de Integridad del plano de usuario actual, de modo que el RNC de destino realiza una selección para su uso. Si el SGSN de la Red Central no participa en la entrega del UE al HNB, según el estado de la técnica, el HNB de destino no puede adquirir la lista de algoritmos de cifrado y protección de la integridad permitidos por la Red Central y la Clave de Cifrado y la Clave de Integridad del plano de usuario actual.

La realización adquiere y guarda la información relacionada con la seguridad a través de la GW de HNB y la envía al nodo de destino como demanda, de modo que el nodo de destino selecciona el algoritmo y adquiere las claves del plano de usuario de acuerdo con esto, resolviendo así el problema anterior.

La Fig. 18 es un diagrama de flujo de un ejemplo de la realización. Consulte la Fig. 18; si un UE accede a la red desde HNB, el UE puede adquirir la información relacionada con la seguridad durante un procedimiento SMC (Comando de Modo de Seguridad). En cada SMC, la GW de HNB analiza un mensaje de comando del modo de seguridad enviado por el SGSN y adquiere y guarda la información relacionada con la seguridad (es decir, la información de cifrado y protección de la integridad) que se transmite en el mensaje de comando del modo de seguridad. La información relacionada con la seguridad incluye una lista de algoritmos de cifrado y protección de la integridad permitidos por una Red Central y una Clave de Cifrado y una Clave de Integridad de un plano de usuario actual. Consulte la Fig. 18, el flujo incluye lo siguiente:

Paso 1801: un SGSN envía a la GW de HNB un mensaje de comando de modo de seguridad que contiene información sobre cifrado y protección de la integridad, incluida una lista de algoritmos de cifrado y protección de la integridad permitidos por una Red Central y una Clave de Cifrado y una Clave de Integridad de un plano de usuario actual;

Paso 1802: la GW de HNB analiza el mensaje de comando del modo de seguridad enviado por el SGSN y adquiere y guarda la información de cifrado y protección de la integridad contenida en el mensaje;

Paso 1803: la GW de HNB reenvía el mensaje de comando del modo de seguridad al HNB;

Paso 1804: el HNB envía un mensaje de finalización del modo de seguridad a la GW de HNB;

Paso 1805: la GW de HNB reenvía el mensaje de finalización del modo de seguridad al SGSN.

De este modo, la GW de HNB adquiere la información relacionada con la seguridad en el procedimiento SMC y puede proporcionarse al HNB de destino para la selección del algoritmo y el uso de las claves del plano de usuario, resolviendo así el problema de que el HNB de destino no pueda adquirir la lista de algoritmos de cifrado y protección de la integridad permitidos por una Red Central y una Clave de Cifrado y una Clave de Integridad de un plano de usuario actual debido a que el SGSN no participa en la entrega del UE bajo el HNB.

La Fig. 19 es un diagrama de flujo de otro ejemplo de la realización. Consulte la Fig. 19, si un UE se conecta a una red desde un RNC, el UE puede adquirir la información relacionada con la seguridad durante el procedimiento de entrega de la RNC a un HNB. El escenario en el que una señalización de entrega entre los HNB termina en la GW de HNB no se producirá hasta que el UE entregue del RNC al HNB. En ese caso, durante el procedimiento de entrega del UE desde el RNC al HNB, el SGSN transmite la información de cifrado y protección de la integridad en un mensaje de solicitud de entrega enviado al HNB de destino, y la GW de HNB puede adquirir y guardar dicha información. Consulte la Fig. 19, el procedimiento incluye lo siguiente:

Paso 1901: un RNC de origen decide la entrega a un HNB de destino;

Paso 1902: el RNC de origen envía un mensaje de solicitud de reubicación a un SGSN;

Paso 1903: el SGSN envía un mensaje de solicitud de reubicación a una GW de HNB; en donde, el mensaje de solicitud de reubicación incluye información sobre cifrado y protección de la integridad que contiene una lista de algoritmos de cifrado y protección de la integridad permitidos por una Red Central y la Clave de Cifrado y la Clave de Integridad actuales.

Paso 1904: la GW de HNB analiza el mensaje de solicitud de reubicación enviado por el SGSN y adquiere y guarda la información de cifrado y protección de la integridad contenida en el mensaje;

Paso 1905: la GW de HNB envía un mensaje de solicitud de reubicación al HNB de destino;

Pasos 1906 a 1910: otro mensaje de la entrega, es decir, el resto del procedimiento de la entrega.

De este modo, la GW de HNB adquiere la información relacionada con la seguridad en el procedimiento de entrega desde el RNC al HNB y puede proporcionarse al HNB de destino para la selección del algoritmo y el uso de las claves del plano de usuario, resolviendo así el problema de que el HNB de destino no pueda adquirir la lista de algoritmos de cifrado y protección de la integridad permitidos por una Red Central y una Clave de Cifrado y una Clave de Integridad de un plano de usuario actual debido a que el SGSN no participa en la entrega del UE bajo el HNB.

La Fig. 20 es un diagrama de flujo de otro ejemplo de la realización. Como se muestra en la Fig. 20, después de que un UE accede desde un HNB, una GW de HNB puede adquirir información relacionada con la seguridad desde un SGSN a través de un mensaje específico. Consulte la Fig. 20, el flujo incluye lo siguiente:

Paso 2001: una GW de HNB envía un mensaje de solicitud de contexto de seguridad a un SGSN, a fin de solicitarle que envíe información relacionada con la seguridad a la GW de HNB; y

Paso 2002: el SGSN devuelve a la GW de HNB un mensaje de respuesta al contexto de seguridad que incluye información sobre cifrado y protección de la integridad y que incluye una lista de algoritmos de cifrado y protección de la integridad permitidos por una Red Central y una Clave de Cifrado y una Clave de Integridad actuales.

De este modo, la GW de HNB adquiere la información relacionada con la seguridad a través de un mensaje específico y puede proporcionarse al HNB de destino para la selección del algoritmo y el uso de las claves del plano de usuario, resolviendo así el problema de que el HNB de destino no pueda adquirir la lista de algoritmos de cifrado y protección de la integridad permitidos por una Red Central y una Clave de Cifrado y una Clave de Integridad de un plano de usuario actual debido a que el SGSN no participa en la entrega del UE bajo el HNB.

La Fig. 21 es un diagrama de bloques constitucionales de una GW de HNB proporcionado por la realización. Consulte la Fig. 21, la GW de HNB incluye lo siguiente:

una unidad de adquisición 211, configurada para adquirir y guardar información relacionada con la seguridad, incluida una lista de algoritmos de cifrado y protección de la integridad permitidos por una Red Central y una Clave de Cifrado y una Clave de Integridad de plano de usuario actual; y

una unidad emisora 212, configurada para enviar la información relacionada con la seguridad adquirida por la unidad de adquisición 211 a un nodo de destino, de modo que el nodo de destino seleccione el algoritmo y utilice claves de acuerdo con la información relacionada con la seguridad.

En un ejemplo, la unidad de adquisición 211 puede incluir lo siguiente:

un primer módulo de recepción 2111, configurado para recibir un mensaje de comando de modo de seguridad enviado por un SGSN, incluyendo el mensaje de comando de modo de seguridad la información relacionada con la seguridad;

un primer módulo de análisis 2112, configurado para analizar el mensaje de comando del modo de seguridad recibido por el primer módulo receptor 2111 y adquirir y guardar la información relacionada con la seguridad del mensaje de comando del modo de seguridad.

En otro ejemplo, la unidad de adquisición 211 puede incluir lo siguiente: un segundo módulo de recepción 2113, configurado para recibir el mensaje de solicitud de reubicación enviado por el SGSN, incluyendo el mensaje de solicitud de reubicación la información relacionada con la seguridad;

un segundo módulo de análisis 2114, configurado para analizar el mensaje de solicitud de reubicación recibido por el segundo módulo de recepción 2113 y adquirir y guardar la información relacionada con la seguridad del mensaje de solicitud de reubicación.

En otro ejemplo, la unidad de adquisición 211 puede incluir lo siguiente: un módulo de envío 2115, configurado para enviar un mensaje de solicitud de contexto de seguridad al SGSN, a fin de solicitar al SGSN que envíe la información relacionada con la seguridad a la pasarela de Nodo B Residencial;

un tercer módulo de recepción 2116, configurado para recibir un mensaje de respuesta al contexto de seguridad devuelto por el SGSN, incluyendo el mensaje de respuesta al contexto de seguridad la información relacionada con la seguridad;

un tercer módulo de análisis 2117, configurado para analizar el mensaje de respuesta al contexto de seguridad recibido por el tercer módulo de recepción 2116 y adquirir y guardar la información relacionada con la seguridad del mensaje de respuesta al contexto de seguridad.

Las partes constituyentes de la pasarela de Nodo B Residencial de esta realización se utilizan para implementar los pasos de la realización del método mencionado anteriormente. Los pasos se han descrito al detalle en la realización del método antedicha y, por lo tanto, en el presente se omiten descripciones redundantes.

Con la pasarela de Nodo B Residencial de esta realización, en el caso de que una señalización de entrega entre los HNB termine en la GW de HNB y no exista una interfaz directa entre los HNB, es posible adquirir la información relacionada con la seguridad a través de varios medios y proporcionar dicha información relacionada con la seguridad al nodo de destino, a fin de que el HNB de destino seleccione el algoritmo y utilice las claves del plano de usuario de acuerdo con este, resolviendo así el problema de que el HNB de destino no pueda adquirir la lista de algoritmos de cifrado y protección de la integridad permitidos por una Red Central y una Clave de Cifrado y una Clave de Integridad de un plano de usuario actual debido a que el SGSN no participa en la entrega del UE bajo el HNB.

Una persona experta en la materia apreciará que todos o parte de los pasos para la aplicación del método anterior pueden completarse mediante la instrucción de

hardware relevante a través de un programa que puede almacenarse en un medio de almacenamiento legible por ordenador y, al ejecutarse, el programa realiza los pasos que incluyen las realizaciones del método anterior. El medio de almacenaje puede incluir varios medios capaces de almacenar códigos de programa, como ROM, RAM, disco magnético y disco óptico.

Las realizaciones anteriores ofrecen descripciones aún más detalladas del objeto, soluciones técnicas y efectos beneficiosos de la invención presente.

REIVINDICACIONES

1. Un método de separación de claves aplicable a un nodo de soporte GPRS servidor SGSN, que comprende lo siguiente:

cuando un Equipo de Usuario hace una entrega desde un nodo de origen a un nodo de destino, o cuando el Equipo de Usuario se mueve del nodo de origen al nodo de destino en estado inactivo, determinar si el nodo de origen es o no un Nodo B Residencial (201); y
si el nodo de origen es el Nodo B Residencial HNB, activar un procedimiento de Autenticación y Acuerdo de Claves de acuerdo con la política del operador, a fin de actualizar la Clave de Cifrado y la Clave de Integridad (202),
en donde, cuando un mensaje de solicitud de reubicación enviado por el nodo de origen al SGSN lleva una identificación de Controlador de Red Radio, ID RNC, de una pasarela de HNB, GW de HNB, el SGSN determina que el nodo de origen es un HNB.

2. Un método de separación de claves aplicable a un nodo de soporte GPRS servidor SGSN, que comprende cuando un Equipo de Usuario entrega desde un nodo de origen a un nodo de destino, o cuando el Equipo de Usuario se desplace del nodo de origen al nodo de destino en estado inactivo, determinar si el nodo de origen es o no un Nodo B Residencial y determinar si el nodo de destino es o no un Controlador de Red Radio;
si el nodo de origen es un Nodo B Residencial y el nodo de destino es un Controlador de Red Radio, activar el procedimiento de Autenticación y Acuerdo de Claves de acuerdo con la política del operador,
en donde cuando un mensaje de solicitud de reubicación enviado por el nodo de origen al SGSN lleva una identificación de Controlador de Red Radio, ID RNC, de una pasarela de HNB, GW de HNB, el SGSN determina que el nodo de origen es un HNB.

3. El método según la reivindicación 1 o 2, en el que activar el procedimiento de Autenticación y Acuerdo de Claves de acuerdo con la política del operador comprende:

activar el procedimiento de Autenticación y Acuerdo de Claves después de que se haya completado el traspaso del Equipo de Usuario desde el nodo de origen al nodo de destino o se haya completado el movimiento del Equipo de Usuario desde el nodo de origen al nodo de destino en estado inactivo, o la pasarela de Nodo B Residencial del nodo de origen recibe un mensaje de liberación de interfaz IU.

4. El procedimiento según la reivindicación 1, que comprende además:

enviar la Clave de Cifrado y la Clave de Integridad al nodo de destino mediante un comando de modo de seguridad, de modo que el nodo de origen y el nodo de destino utilicen Claves de Cifrado y Claves de Integridad diferentes.

5. Un SGSN, que comprende:

una unidad determinante (31), configurada para determinar si un nodo de origen es o no un Nodo B Residencial, cuando un Equipo de Usuario entrega desde el nodo de origen a un nodo de destino, o cuando el Equipo de Usuario se mueve del nodo de origen al nodo de destino en estado inactivo; y
una unidad activadora (32), configurada para activar un Procedimiento de Autenticación y Acuerdo de Claves de acuerdo con la política del operador, cuando la unidad determinante determina que el nodo de origen es el Nodo B Residencial, con el fin de actualizar la Clave de Cifrado y la Clave de Integridad,
en donde cuando un mensaje de solicitud de reubicación enviado por el nodo de origen al SGSN lleva una identificación de Controlador de Red Radio, ID RNC, de una pasarela de HNB, GW de HNB, el SGSN determina que el nodo de origen es un HNB.

6. El SGSN de acuerdo con la reivindicación 5, en donde la unidad determinante se configura además para determinar si el nodo de destino es o no un Controlador de Red Radio, y la unidad activadora se configura específicamente para activar el procedimiento de Autenticación y Acuerdo de Claves de acuerdo con la política del operador cuando el nodo de origen es un Nodo B Residencial y el nodo de destino es un Controlador de Red de Radio.

7. El SGSN de acuerdo con la reivindicación 5 o 6, en donde la unidad activadora está configurada específicamente para activar el procedimiento de Autenticación y Acuerdo de Claves después de que se haya completado el traspaso del Equipo de Usuario desde el nodo de origen al nodo de destino, o se haya completado el movimiento del Equipo de Usuario desde el nodo de origen al nodo de destino en estado inactivo, o la pasarela Nodo B Residencial del nodo de origen recibe un mensaje de liberación de interfaz IU.

8. El SGSN, de acuerdo con la reivindicación 5, comprende además:

una unidad emisora, configurada para enviar la Clave de Cifrado y la Clave de Integridad actualizadas por la unidad activadora al nodo de destino mediante un comando de modo de seguridad, de modo que el nodo de origen y el nodo de destino utilicen Claves de Cifrado y Claves de Integridad diferentes.

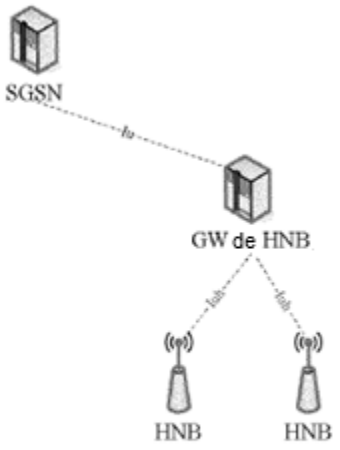

FIG. 1A

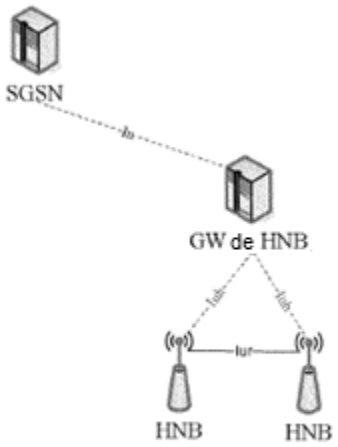

FIG. 1B

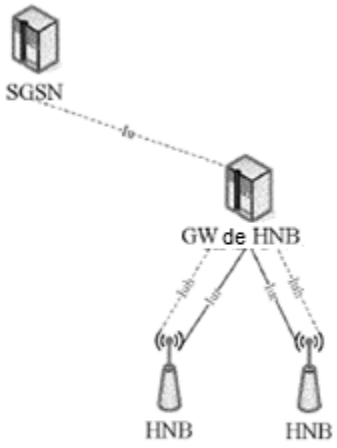

FIG. 1C

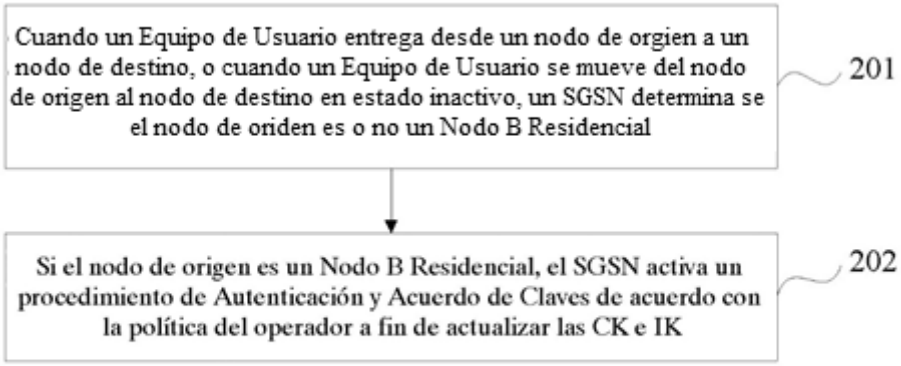

FIG. 2

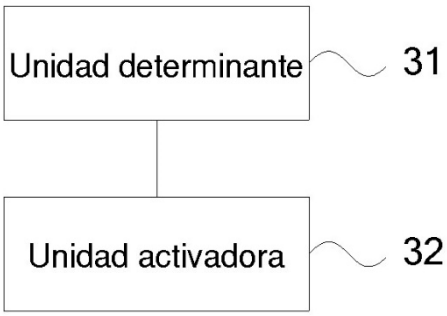

FIG. 3

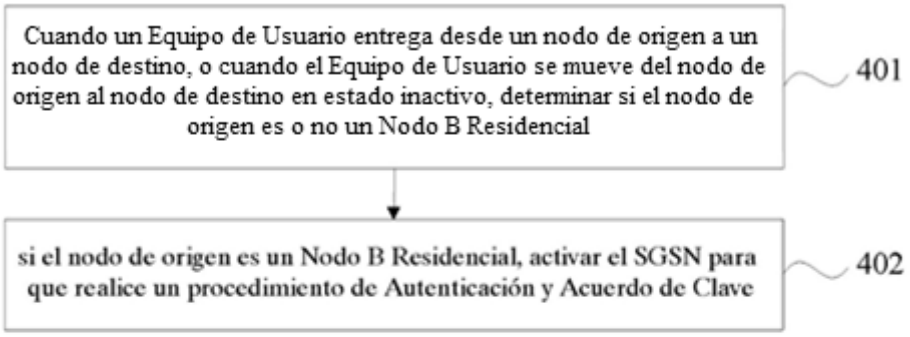

FIG. 4

FIG. 5

FIG. 6

FIG. 7

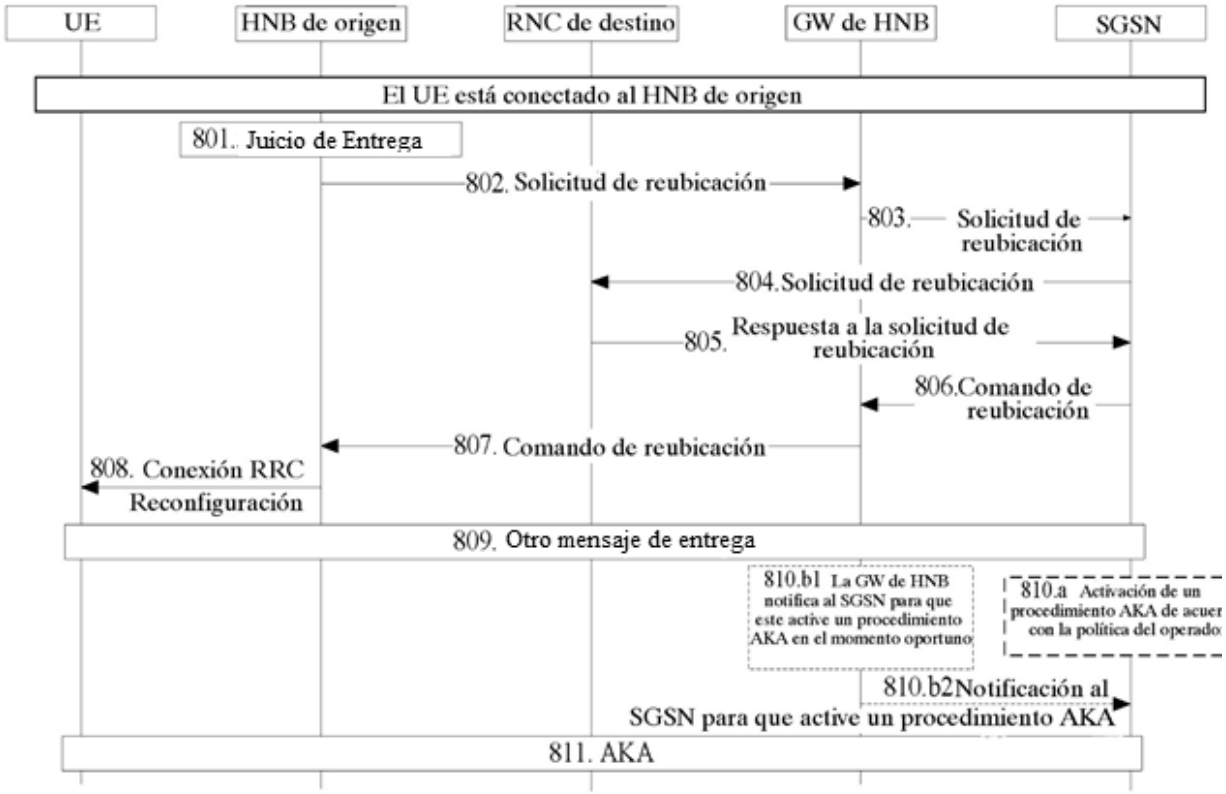
UE
HNB de origen
RNC de destino
GW de HNB
SGSN
El UE está conectado al HNB de origen
801. Juicio de Entrega
802. Solicitud de reubicación
803. Solicitud de reubicación
804. Solicitud de reubicación
805. Respuesta a la solicitud de reubicación
806. Comando de reubicación
807. Comando de reubicación
808. Conexión RRC Reconfiguración
809. Otro mensaje de entrega
810.b1 La GW de HNB notifica al SGSN para que este active un procedimiento AKA en el momento oportuno
810.a Activación de un procedimiento AKA de acuer con la política del operado
810.b2 Notificación al SGSN para que active un procedimiento AKA
811. AKA

FIG. 8

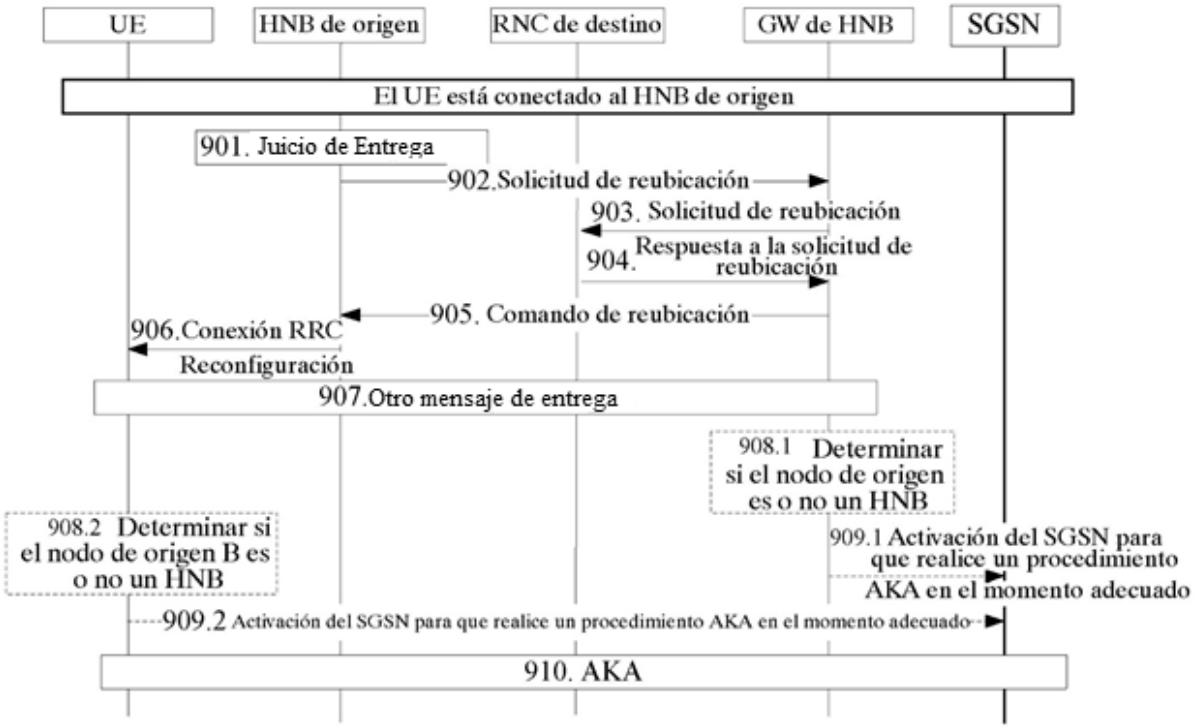
UE
HNB de origen
RNC de destino
GW de HNB
SGSN
El UE está conectado al HNB de origen
901. Juicio de Entrega
902. Solicitud de reubicación
903. Solicitud de reubicación
904. Respuesta a la solicitud de reubicación
905. Comando de reubicación
906. Conexión RRC Reconfiguración
907. Otro mensaje de entrega
908.1 Determinar si el nodo de origen es o no un HNB
908.2 Determinar si el nodo de origen B es o no un HNB
909.1 Activación del SGSN para que realice un procedimiento AKA en el momento adecuado
909.2 Activación del SGSN para que realice un procedimiento AKA en el momento adecuado
910. AKA

FIG. 9

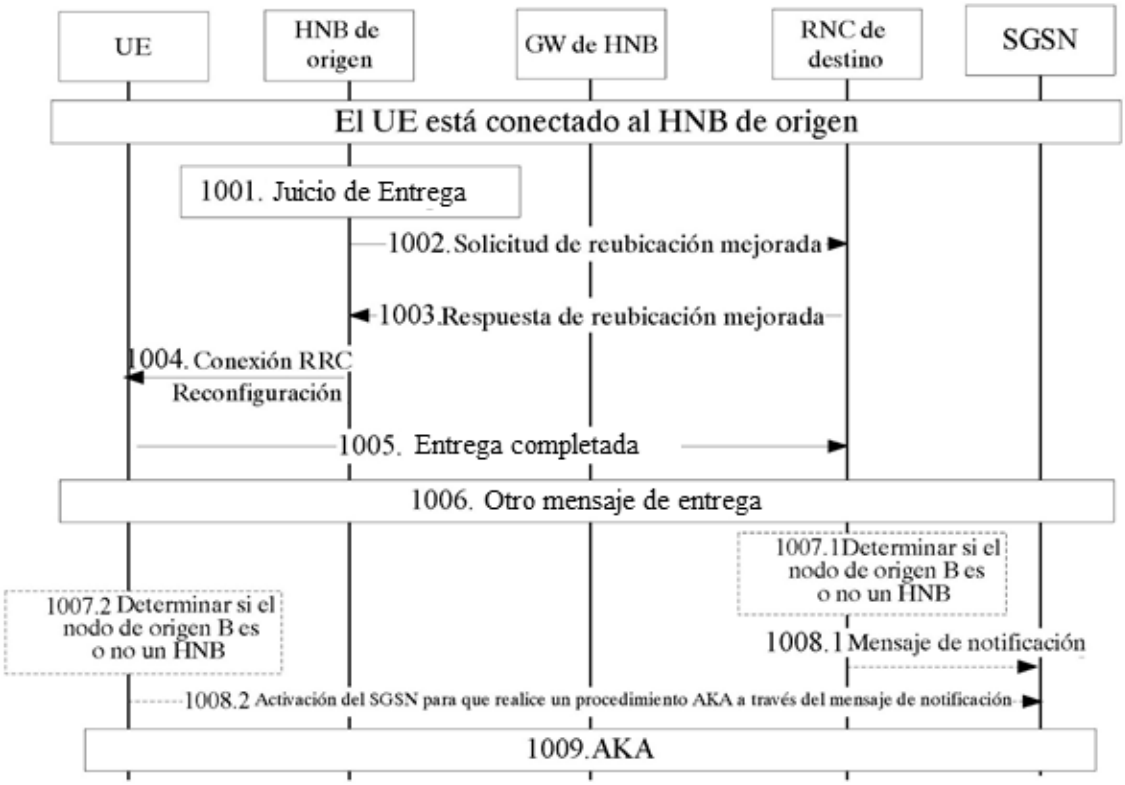
UE
HNB de origen
GW de HNB
RNC de destino
SGSN
El UE está conectado al HNB de origen
1001. Juicio de Entrega
1002. Solicitud de reubicación mejorada
1003. Respuesta de reubicación mejorada
1004. Conexión RRC Reconfiguración
1005. Entrega completada
1006. Otro mensaje de entrega
1007.1 Determinar si el nodo de origen B es o no un HNB
1007.2 Determinar si el nodo de origen B es o no un HNB
1008.1 Mensaje de notificación
1008.2 Activación del SGSN para que realice un procedimiento AKA a través del mensaje de notificación
1009. AKA

FIG. 10

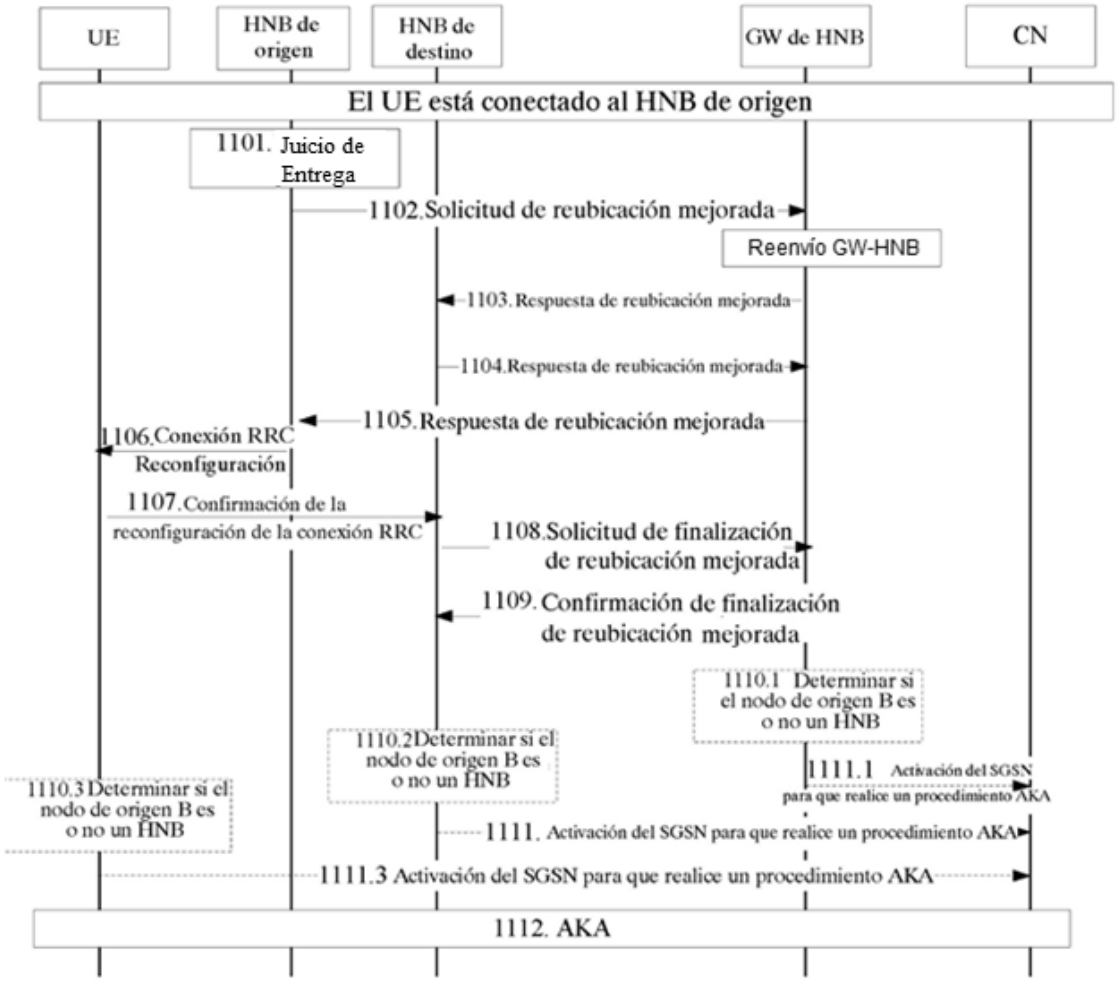
UE
HNB de origen
HNB de destino
GW de HNB
CN
El UE está conectado al HNB de origen
1101. Juicio de Entrega
1102. Solicitud de reubicación mejorada
Reenvío GW-HNB
1103. Respuesta de reubicación mejorada
1104. Respuesta de reubicación mejorada
1105. Respuesta de reubicación mejorada
1106. Conexión RRC Reconfiguración
1107. Confirmación de la reconfiguración de la conexión RRC
1108. Solicitud de finalización de reubicación mejorada
1109. Confirmación de finalización de reubicación mejorada
1110.1 Determinar si el nodo de origen B es o no un HNB
1110.2 Determinar si el nodo de origen B es o no un HNB
1111.1 Activación del SGSN para que realice un procedimiento AKA
1110.3 Determinar si el nodo de origen B es o no un HNB
1111. Activación del SGSN para que realice un procedimiento AKA
1111.3 Activación del SGSN para que realice un procedimiento AKA
1112. AKA

FIG. 11

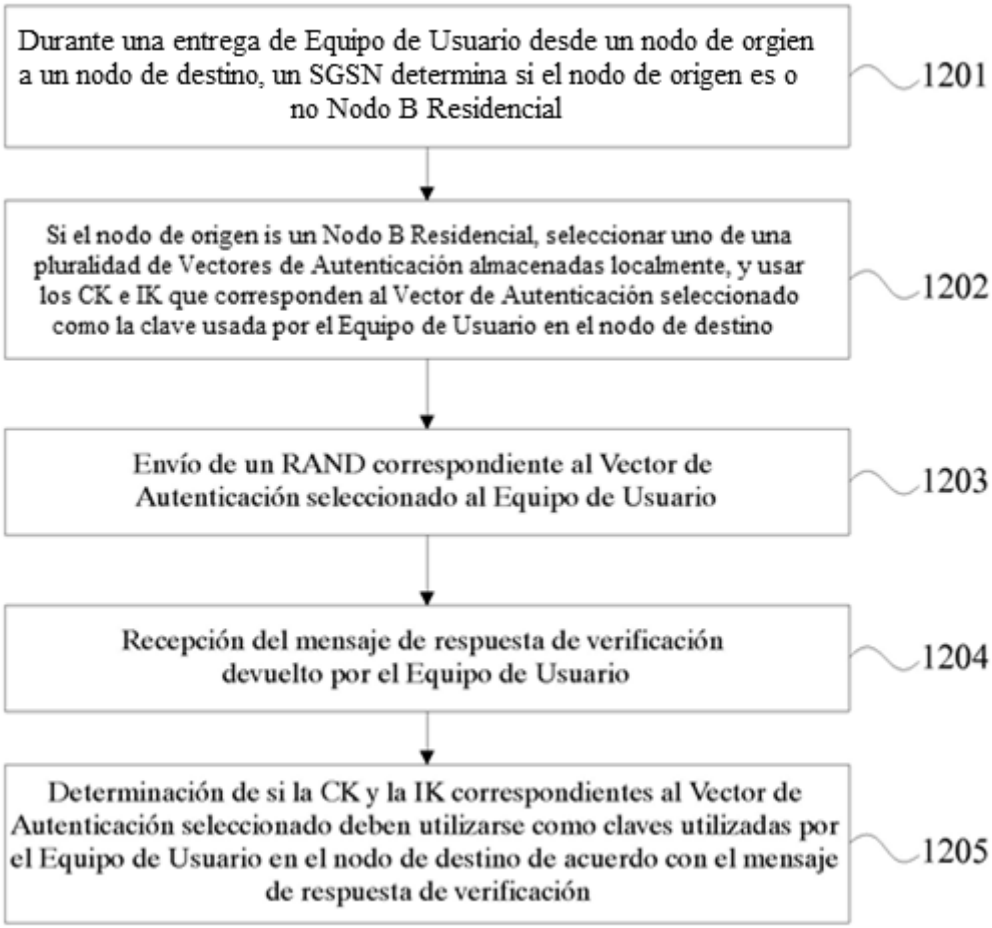
Durante una entrega de Equipo de Usuario desde un nodo de orgien a un nodo de destino, un SGSN determina si el nodo de origen es o no Nodo B Residencial
1201
Si el nodo de origen is un Nodo B Residencial, seleccionar uno de una pluralidad de Vectores de Autenticación almacenadas localmente, y usar los CK e IK que corresponden al Vector de Autenticación seleccionado como la clave usada por el Equipo de Usuario en el nodo de destino
1202
Envío de un RAND correspondiente al Vector de Autenticación seleccionado al Equipo de Usuario
1203
Recepción del mensaje de respuesta de verificación devuelto por el Equipo de Usuario
1204
Determinación de si la CK y la IK correspondientes al Vector de Autenticación seleccionado deben utilizarse como claves utilizadas por el Equipo de Usuario en el nodo de destino de acuerdo con el mensaje de respuesta de verificación
1205

FIG. 12

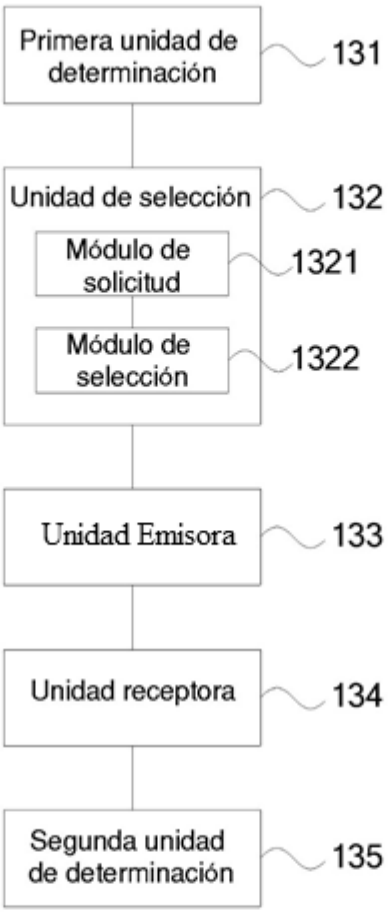
Primera unidad de determinación
131
Unidad de selección
132
Módulo de solicitud
1321
Módulo de selección
1322
Unidad Emisora
133
Unidad receptora
134
Segunda unidad de determinación
135

FIG. 13

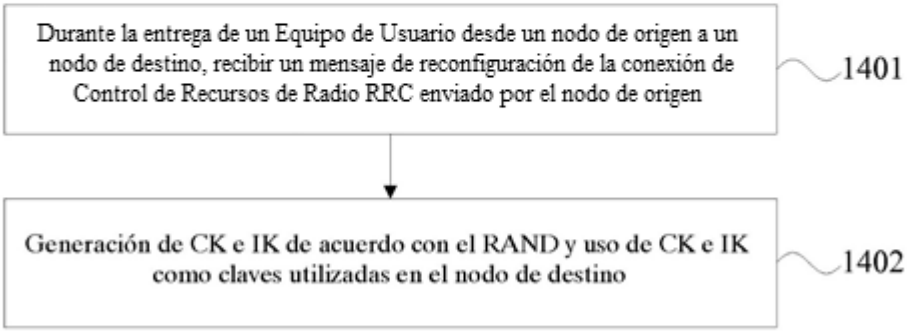
Durante la entrega de un Equipo de Usuario desde un nodo de origen a un nodo de destino, recibir un mensaje de reconfiguración de la conexión de Control de Recursos de Radio RRC enviado por el nodo de origen
1401
Generación de CK e IK de acuerdo con el RAND y uso de CK e IK como claves utilizadas en el nodo de destino
1402

FIG. 14

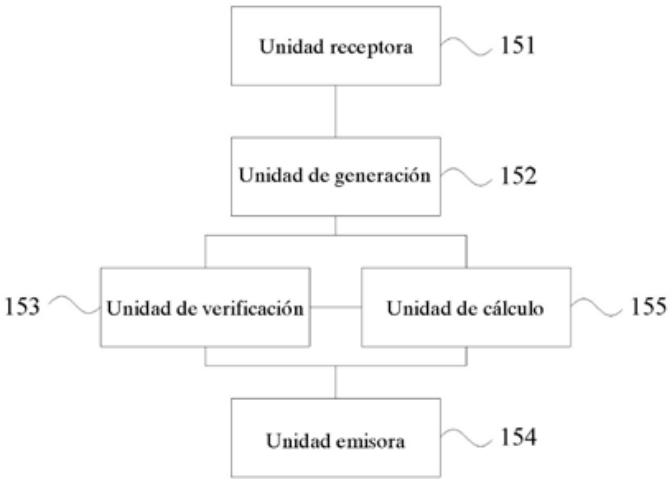
Unidad receptora
151
Unidad de generación
152
153
Unidad de verificación
Unidad de cálculo
155
Unidad emisora
154

FIG. 15

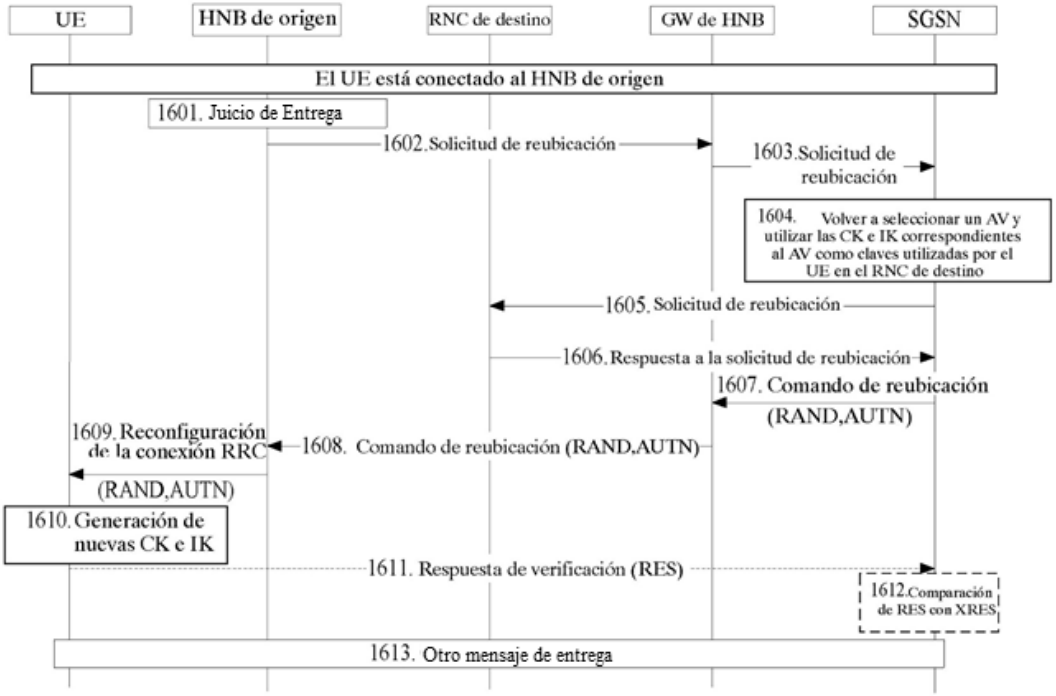
UE
HNB de origen
RNC de destino
GW de HNB
SGSN
El UE está conectado al HNB de origen
1601. Juicio de Entrega
1602. Solicitud de reubicación
1603. Solicitud de reubicación
1604. Volver a seleccionar un AV y utilizar las CK e IK correspondientes al AV como claves utilizadas por el UE en el RNC de destino
1605. Solicitud de reubicación
1606. Respuesta a la solicitud de reubicación
1607. Comando de reubicación (RAND,AUTN)
1608. Comando de reubicación (RAND,AUTN)
1609. Reconfiguración de la conexión RRC (RAND,AUTN)
1610. Generación de nuevas CK e IK
1611. Respuesta de verificación (RES)
1612. Comparación de RES con XRES
1613. Otro mensaje de entrega

FIG. 16

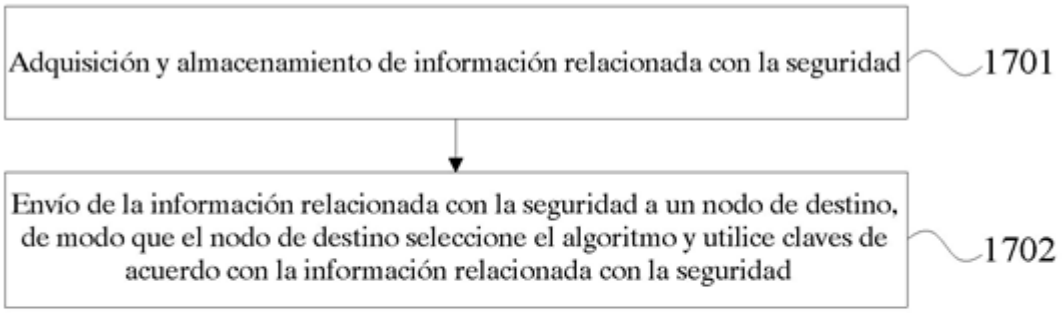
Adquisición y almacenamiento de información relacionada con la seguridad
1701
Envío de la información relacionada con la seguridad a un nodo de destino, de modo que el nodo de destino seleccione el algoritmo y utilice claves de acuerdo con la información relacionada con la seguridad
1702

FIG. 17

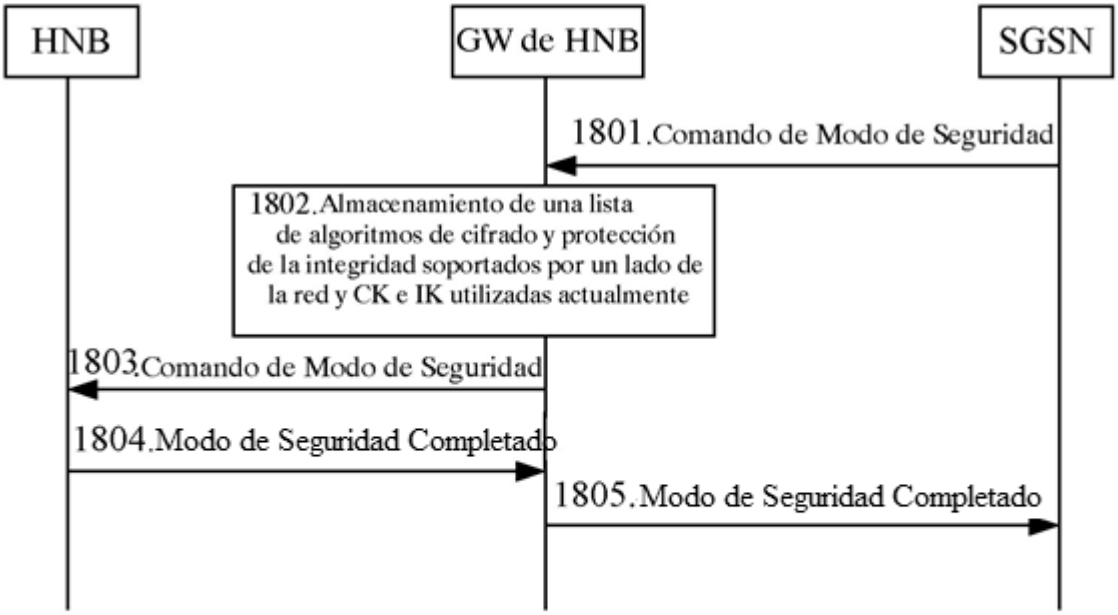
HNB
GW de HNB
SGSN
1801.Comando de Modo de Seguridad
1802.Almacenamiento de una lista de algoritmos de cifrado y protección de la integridad soportados por un lado de la red y CK e IK utilizadas actualmente
1803.Comando de Modo de Seguridad
1804.Modo de Seguridad Completado
1805.Modo de Seguridad Completado

FIG. 18

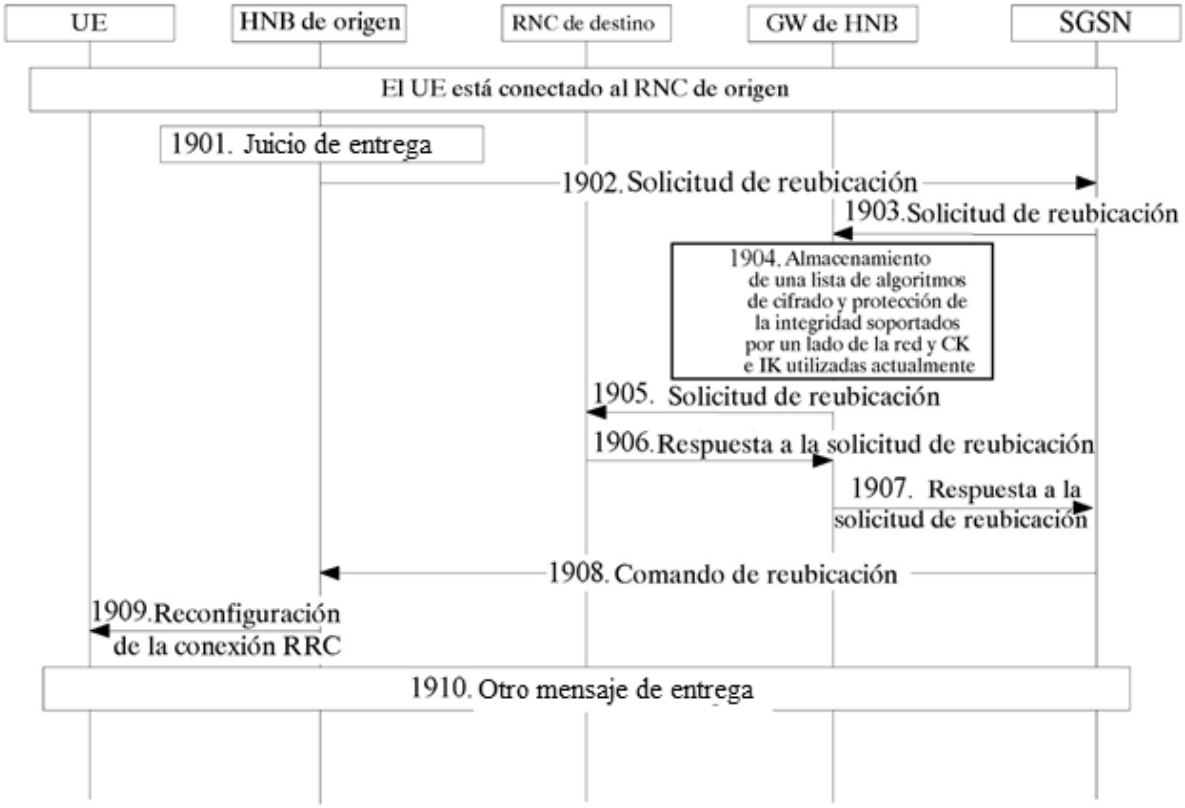
UE
HNB de origen
RNC de destino
GW de HNB
SGSN
El UE está conectado al RNC de origen
1901. Juicio de entrega
1902. Solicitud de reubicación
1903. Solicitud de reubicación
1904. Almacenamiento de una lista de algoritmos de cifrado y protección de la integridad soportados por un lado de la red y CK e IK utilizadas actualmente
1905. Solicitud de reubicación
1906. Respuesta a la solicitud de reubicación
1907. Respuesta a la solicitud de reubicación
1908. Comando de reubicación
1909. Reconfiguración de la conexión RRC
1910. Otro mensaje de entrega

FIG. 19

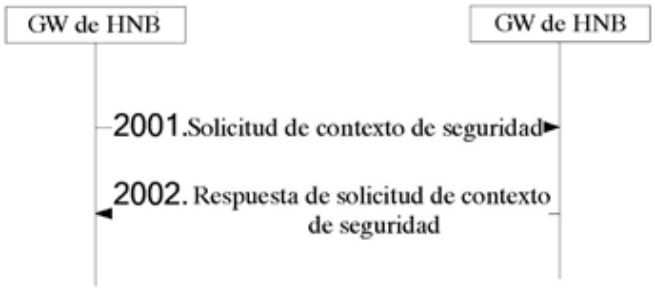
GW de HNB
GW de HNB
2001. Solicitud de contexto de seguridad
2002. Respuesta de solicitud de contexto de seguridad

FIG. 20

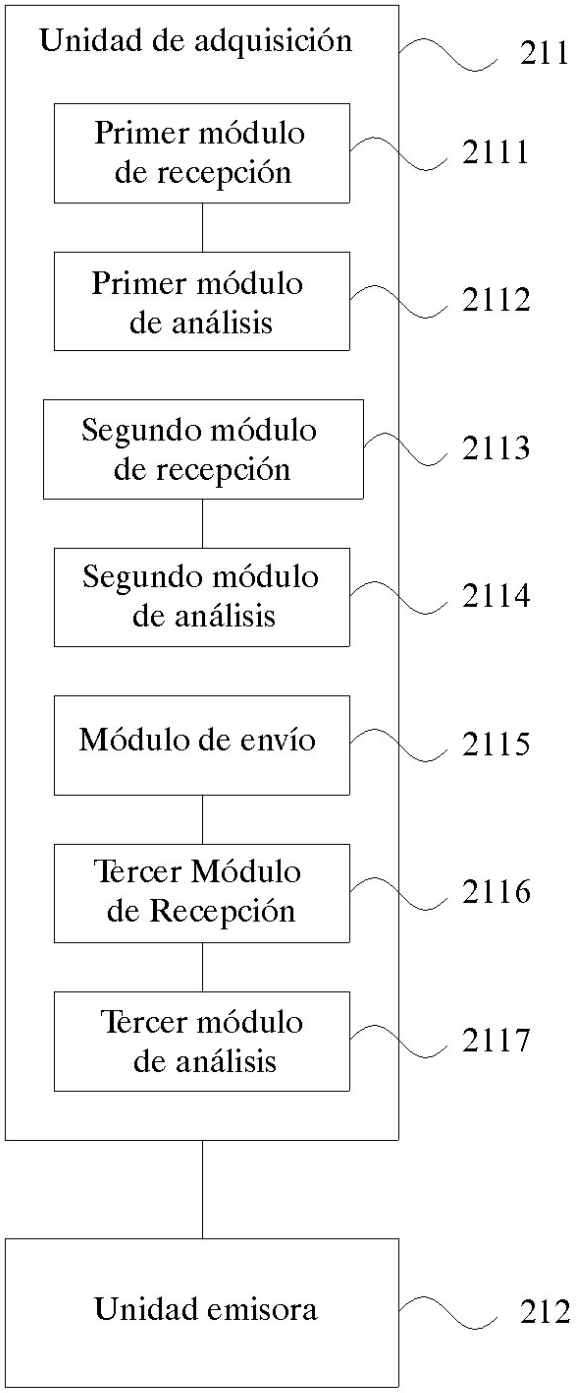
Unidad de adquisición
211
Primer módulo de recepción
2111
Primer módulo de análisis
2112
Segundo módulo de recepción
2113
Segundo módulo de análisis
2114
Módulo de envío
2115
Tercer Módulo de Recepción
2116
Tercer módulo de análisis
2117
Unidad emisora
212

FIG. 21