(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 436 552**

(51) Int. CI.:

H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.06.2010 E 10791589 (4)**

(97) Fecha y número de publicación de la concesión europea: **28.08.2013 EP 2416598**

(54) Título: **Método, dispositivo y sistema de derivación de clave**

(30) Prioridad:

26.06.2009 CN 200910148423

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.01.2014

(73) Titular/es:

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

(72) Inventor/es:

ZHANG, AIQIN;
CHEN, JING y
BI, XIAOYU

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método, dispositivo y sistema de derivación de clave

CAMPO DEL INVENTO

El presente invento se refiere al campo de las tecnologías de comunicaciones, y en particular, a un método, dispositivo y sistema de derivación de clave.

ANTECEDENTES DEL INVENTO

En un sistema de comunicación móvil, una red de acceso por radio incluye un sistema de comunicación móvil de segunda generación, un sistema de comunicación móvil de tercera generación, y un sistema de Evolución a Largo Plazo (LTE).

En una transferencia o traspaso de un Equipamiento de Usuario (UE) desde una red donde se sitúa originalmente el UE, en particular una red fuente o de origen, a una red objetivo, una clave de la red objetivo puede ser derivada a partir de una clave de la red fuente, evitando por ello el proceso de autenticación y negociación de clave, de manera que el UE y un lado de la red generan, a través del mismo parámetro y algoritmo de clave, la clave eventualmente utilizada en la red objetivo.

En una Red de Acceso por Radio Terrestre Universal (UTRAN), el proceso de autenticación y negociación de clave genera una Clave de Cifrado (CK) y una Clave de Integridad (IK); y en un UTRAN evolucionado (EUTRAN), el proceso de autentificación y generación de clave genera una clave raíz (Kasme).

Tomando la transferencia de un UE desde una EUTRAN a una UTRAN como un ejemplo, una estación base (BS) que sirve originalmente al UE en la EUTRAN (denominada como una BS fuente para abreviar en lo que sigue) inicia un proceso de transferencia de red; una Entidad de Gestión de Movilidad (MME) asociada con la BS fuente, en particular una MME fuente, deriva una clave CK' || IK' del UE en una red objetivo de acuerdo con una Función de Derivación de Clave (KDF), un parámetro de entrada, en particular una clave de raíz Kasme, y un valor COUNT de enlace descendente de Estrato Sin Acceso (NAS) en el contexto de seguridad actual, y envía la clave derivada a la UTRAN objetivo; la red objetivo decide un algoritmo de seguridad para el UE y devuelve el algoritmo de seguridad al UE; y el UE sincroniza la clave con un lado de la red objetivo de acuerdo con el algoritmo de seguridad.

3GPP TS 33. 401 v8.4.0 describe un procedimiento de transferencia desde la E-UTRAN a la UTRAN, el UE y la MME derivarán una clave CK' confidencialmente, y una clave de integridad IK' desde la K_{ASME} y el valor COUNT de enlace descendente de NAS del contexto de seguridad actual con la ayuda de una función de derivación de clave KDF de una sola dirección como se ha especificado en el Anexo A. Una MME proporcionará también al menos los 4 lsb del valor COUNT de enlace descendente de NAS a la eNB fuente, que entonces incluirá los bits al Comando de MobilityFromE-UTRAN al UE.

El documento EP2293609 describe un método para derivar claves cuando la Transferencia o Actualización del Área de Enrutamiento del Equipamiento de Usuario (UE) desde una Red de Acceso por Radio Terrestre Universal Evolucionada (E-UTRAN) a una Red de Acceso por Radio Terrestre Universal (UTRAN) o Sistema Global para Tasa de Comunicación Móvil/Datos Mejorados para Red de Acceso por Radio de Evolución de GSM (GERAN) ocurre, las claves para la UTRAN o la GERAN son derivadas por una Entidad de Gestión de Movilidad (MME) y/o el UE utilizando parámetros predefinidos. Los parámetros predefinidos incluyen una clave de raíz de la E-UTEAN y un valor de un Cómputo de Estrato Sin Acceso (NAS). Un sistema de derivación de claves para derivar las claves está descrito también.

En el proceso de transferencia anterior del UE desde la EUTRAN a la UTRAN, la transferencia del UE a la UTRAN puede fallar debido al fallo de la conexión de un enlace por radio de interfaz de aire, de manera que el UE vuelve a la EUTRAN e inicia un proceso de restablecimiento de enlace a la BS que sirve actualmente al UE, es decir, la BS donde se sitúa el UE actualmente, denominada como una BS actual para abreviar en lo que sigue, y decidir después realizar un transferencia, la BS inicia otro proceso de transferencia. En este caso, la derivación de clave en la MME en el segundo proceso de transferencia y la derivación de clave en la MME en el primer proceso de transferencia son ambas realizadas de acuerdo con la clave de raíz Kasme y el valor COUNT de enlace descendente de NAS actual, y por tanto la clave CK' || IK' calculada es la misma, lo que da como resultado que la clave obtenida durante la transferencia por múltiples Controladores de Red de Radio (RNC) en una red UMTS a través de un nodo de soporte GPRS de servicio objetivo (SGSN) es la misma. De esta manera, una vez que la clave utilizada en un RNC es obtenida, las claves en otros RNC puede ser derivadas consiguientemente, y la seguridad de red se encuentra en peligro.

RESUMEN DEL INVENTO

El presente invento está dirigido a un método, dispositivo y sistema de derivación de clave, para mejorar la seguridad de red.

Una realización del presente invento proporciona un método de derivación de clave, donde el método incluye en su

primera forma de implementación o puesta en práctica:

generar un valor aleatorio;

utilizar el valor aleatorio y una clave raíz como parámetros de entrada de una KDF para derivar una clave de un UE en una UTRAN objetivo; o

utilizar el valor aleatorio, un valor COUNT de enlace descendente de NAS actual, y la clave raíz como parámetros de entrada de la KDF para derivar la clave del UE en la UTRAN objetivo. Una realización del presente invento proporciona un método de derivación de clave, donde el método incluye:

recibir, por un UE, un mensaje de Comando de Transferencia;

utilizar un valor aleatorio y una clave raíz como parámetros de entrada de una KDF para derivar una clave del UE en una UTRAN objetivo si el mensaje de Comando de Transferencia incluye el valor aleatorio; y

utilizar el valor aleatorio, un valor COUNT de enlace descendente de NAS actual, y la clave raíz como parámetros de entrada de la KDF para derivar la clave del UE en la UTRAN objetivo si el mensaje de Comando de Transferencia incluye el valor aleatorio y el valor COUNT de enlace descendente de NAS actual.

Una realización del presente invento proporciona un método de derivación de clave, donde el método incluye:

obtener un nuevo valor COUNT de enlace descendente de NAS;

derivar una clave de un UE en una UTRAN objetivo de acuerdo con una KDF, una clave raíz, y el nuevo valor COUNT de enlace descendente de NAS;

guardar, por la MME, la clave después de la derivación de clave, y

enviar el nuevo valor COUNT de enlace descendente de NAS al UE, de manera que el UE derive la clave en la UTRAN objetivo,

en el que antes de obtener, por la MME, el nuevo valor COUNT de enlace descendente de NAS, el método comprende además:

determinar, por la MME, si la clave del UE en la UTRAN objetivo está guardada actualmente; en caso afirmativo, determinar además si un valor COUNT de enlace descendente de NAS correspondiente con la clave guardada actualmente del UE en la UTRAN objetivo es consistente con el valor COUNT de enlace descendente de NAS actual; y

si es consistente, realizar la operación de obtener el nuevo valor COUNT de enlace descendente de NAS.

Una realización del presente invento proporciona un método de derivación de clave donde el método incluye:

recibir, por un UE, un mensaje de Comando de Transferencia, en que el mensaje de Comando de Transferencia incluye un nuevo valor COUNT de enlace descendente de NAS; y

derivar una clave del UE en una UTRAN objetivo de acuerdo con una KDF, una clave raíz, y el nuevo valor COUNT de enlace descendente de NAS,

recibir, por el UE, un cierto valor que se añade al valor COUNT de enlace descendente de NAS actual en un segundo proceso de transferencia.

Una realización del presente invento proporciona un método de derivación de clave, donde el método incluye:

recibir un mensaje de Transferencia Requerida, en que el mensaje de Transferencia Requerida incluye un valor reciente de un UE;

utilizar el valor reciente del UE y una clave raíz como parámetros de entrada de una KDF para derivar una clave del UE en una UTRAN objetivo; o

utilizar el valor reciente del UE, un valor COUNT de enlace descendente NAS actual, y la clave raíz como parámetros de entrada de la KDF para derivar la clave del UE en la UTRAN objetivo.

Una realización del presente invento proporciona un método de derivación de clave, en el que el método incluye:

enviar, por un UE, un mensaje de Solicitud de Restablecimiento de Conexión de Control de Recurso de Radio (RRC), en que el mensaje de Solicitud de Restablecimiento de Conexión de RRC incluye un valor reciente del UE;

utilizar el valor reciente del UE y una clave raíz como parámetros de entrada de una KDF para derivar una clave del UE en una UTRAN objetivo cuando recibe un mensaje de Comando de Transferencia enviado por una BS; y

utilizar el valor reciente del UE, un valor COUNT de enlace descendente de NAS actual, y la clave raíz como parámetros de entrada de la KDF para derivar la clave del UE en una UTRAN objetivo si el mensaje de Comando de Transferencia incluye el valor COUNT de enlace descendente de NAS actual.

Una realización del presente invento proporciona una MME, donde la MME incluye:

una unidad generadora, configurada para generar un valor aleatorio; y

una unidad de derivación, configurada para utilizar una clave raíz y el valor aleatorio generado por la unidad generadora como parámetros de entrada de una KDF para derivar una clave de un UE en una UTRAN objetivo; o configurada para utilizar el valor aleatorio, un valor COUNT de enlace descendente de NAS actual, y la clave raíz como parámetros de entrada de la KDF para derivar la clave del UE en la UTRAN objetivo.

Una realización del presente invento proporciona un UE, en el que el UE incluye:

una unidad receptora de mensajes, configurada para recibir un mensaje de Comando de Transferencia;

una unidad de derivación de clave, configurada para utilizar un valor aleatorio y una clave raíz como parámetros de entrada de una KDF para derivar una clave del UE en una UTRAN objetivo si el mensaje de Comando de Transferencia recibido por la unidad receptora de mensajes incluye el valor aleatorio: y configurada para utilizar el valor aleatorio, un valor COUNT de enlace descendente de NAS actual, y la clave raíz como parámetros de entrada de la KDF para derivar la clave del UE en la UTRAN objetivo si el mensaje de Comando de Transferencia recibido por la unidad receptora de mensajes incluye el valor aleatorio y el valor COUNT de enlace descendente de NAS actual.

Una realización del presente invento proporciona una MME, en la que la MME incluye:

una unidad de obtención de valor de cómputo, configurada para obtener un nuevo valor COUNT de enlace descendente de NAS;

una segunda unidad de derivación, configurada para derivar una clave de un UE en una UTRAN objetivo de acuerdo con una KDF, una clave raíz, y el nuevo valor COUNT de enlace descendente de NAS obtenido por la unidad de obtención de valor de cómputo; una unidad de guardar, configurada para guardar la clave derivada por la segunda unidad de derivación; y

una unidad de envío de transferencia, configurada para enviar el nuevo valor OCUNT de enlace descendente de NAS obtenido por la unidad de obtención de valor de cómputo al UE, de manera que el UE deriva la clave en la UTRAN objetivo.

una unidad de determinación (34), configurada para determinar si la clave del UE en la UTRAN objetivo está guardada actualmente; en caso afirmativo, determinar además si un valor COUNT de enlace descendente de NAS correspondiente a la clave guardada actualmente del UE en la UTRAN objetivo es consistente con el valor COUNT de enlace descendente de NAS actual, en el que cuando un resultado de determinación de la unidad de determinación es que el valor COUNT de enlace descendente de NAS correspondiente a la clave guardada actualmente del UE en la UTRAN objetivo es consistente con el valor COUNT de enlace descendente de NAS, la unidad de obtención de valor COUNT obtiene el nuevo valor COUNT de enlace descendente de NAS.

Una realización del presente invento proporciona un UE, en el que el UE incluye:

una segunda unidad receptora de mensajes, configurada para recibir un valor COUNT de enlace descendente de Estrato Sin Acceso (NAS) desde una Entidad de Gestión de Movilidad (MME) en un primer proceso de transferencia;

una segunda unidad de derivación de clave, configurada para derivar una clave del UE en una UTRAN objetivo de acuerdo con una KDF, una clave raíz, y el nuevo valor COUNT de enlace descendente de NAS en el mensaje de Comando de Transferencia recibido por la segunda unidad receptora de mensajes;

la segunda unidad receptora de mensajes, configurada para recibir un cierto valor que se añade al valor COUNT de enlace descendente de NAS actual en un segundo proceso de transferencia.

Una realización del presente invento proporciona un método de derivación de clave, en el que el método incluye:

recibir, por una Entidad de Gestión de Movilidad (MME), un mensaje de Transferencia Requerida desde una BS;

derivar, por la MME, una clave de un Equipamiento de Usuario (UE) en una Red de Acceso por radio Terrestre Universal (UTRAN) objetivo de acuerdo con una Función de Derivación de Clave (KDF), una clave raíz, y un valor COUNT de enlace descendente de Estrato Sin Acceso (NAS) actual;

enviar, por la MME, el valor COUNT de enlace descendente de NAS actual al UE;

añadir, por la MME, un cierto valor al valor COUNT de enlace descendente de NAS actual.

Una realización del presente invento proporciona una MME, la MME incluye:

una unidad receptora de transferencia, configurada para recibir un mensaje de Transferencia Requerida desde una BS;

una segunda unidad de derivación, configurada para derivar una clave de un Equipamiento de Usuario (UE) en una Red de Acceso por Radio Terrestre Universal (UTRAN) de acuerdo con una Función de Derivación de Clave (KDF), una clave raíz, y un valor COUNT de enlace descendente de NAS actual;

una unidad de envío de transferencia, configurada para enviar el valor COUNT de enlace descendente de NAS actual al UE; y

una unidad de obtención de valor de cómputo, configurada para añadir un cierto valor al valor COUNT de enlace descendente de NAS actual.

Una realización del presente invento proporciona un sistema de comunicación, en que el sistema de comunicación incluye cualquiera de las MME anteriores.

El método, dispositivo y sistema de derivación de clave de acuerdo con las realizaciones del presente invento son aplicables al proceso de transferencia del UE desde la EUTRAN a la UTRAN. A partir del fallo de la primera transferencia a la segunda transferencia, se garantiza que la clave derivada de la MME fuente en el primer proceso de transferencia del UE es diferente de la clave derivada sobre la MME en el segundo proceso de transferencia del UE mediante el cambio de los parámetros de entrada utilizados en la derivación de clave, tal como generar el valor aleatorio, cambiar el valor COUNT de enlace descendente de NAS actual, y obtener el valor reciente del UE, de modo que se impida la situación de la técnica anterior que una vez que la clave utilizada en un RNC es obtenida, las claves en otros RNC pueden ser derivadas consecuentemente, mejorando por ello la seguridad de la red.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La fig. 1 es un diagrama de flujo de un método de derivación de clave de acuerdo con una realización del presente invento;

La fig. 2 es un diagrama de flujo de un método de derivación de clave de acuerdo con la Realización 1 de Método del presente invento;

La fig. 3 es un diagrama de flujo de un método de derivación de clave de acuerdo con la Realización 2 de Método del presente invento;

La fig. 4 es un diagrama de flujo de un método de derivación de clave de acuerdo con la Realización 3 de Método del presente invento;

La fig. 5 es un diagrama de flujo de un método de derivación de clave de acuerdo con la Realización 4 de Método del presente invento;

La fig. 6 es un diagrama de flujo de un método de derivación de clave de acuerdo con la Realización 5 de Método del presente invento;

La fig. 7 es un diagrama esquemático que ilustra una estructura lógica de una MME de acuerdo con la Realización 1 de Dispositivo del presente invento;

La fig. 8 es un diagrama esquemático que ilustra una estructura lógica de un UE de acuerdo con la Realización 2 de Dispositivo del presente invento;

La fig. 9 es un diagrama esquemático que ilustra una estructura lógica de una MME de acuerdo con la Realización 3 de Dispositivo del presente invento;

La fig. 10 es un diagrama esquemático que ilustra una estructura lógica de un UE de acuerdo con la Realización 4 de Dispositivo del presente invento;

La fig. 11 es un diagrama esquemático que ilustra una estructura lógica de una MME de acuerdo con la Realización 5 de Dispositivo del presente invento;

La fig. 12 es un diagrama esquemático que ilustra una estructura lógica de una BS de acuerdo con la Realización 6 de Dispositivo del presente invento;

La fig. 13 es un diagrama esquemático que ilustra una estructura lógica de un UE de acuerdo con la Realización 7 de Dispositivo del presente invento;

La fig. 14 es un diagrama esquemático que ilustra una estructura lógica de una MME de acuerdo con la Realización 8 de Dispositivo del presente invento;

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES

Las realizaciones del presente invento son aplicables al proceso de transferencia de un UE desde una EUTRAN a una UTRAN. El siguiente método es utilizado para mejorar la seguridad de la red en las realizaciones del presente invento: un valor COUNT de enlace descendente de NAS utilizado cuando la derivación de clave es realizada sobre una MME fuente durante un primer proceso de transferencia del UE es diferente del valor COUNT de enlace descendente de NAS utilizado cuando la derivación de clave es realizada sobre la MME durante un segundo proceso de transferencia del UE, de manera que las claves generadas durante cada proceso de transferencia del UE desde la EUTRAN a la UTRAN son diferentes, y las claves del UE utilizadas en el RNC y SGSN en la red objetivo son así diferentes. Por tanto, la situación en la técnica anterior de que una vez que la clave utilizada en un RNC es obtenida, las claves utilizadas en otros RNC pueden ser derivadas consecuentemente es evitada, mejorando por ello la seguridad de la red.

Una realización del presente invento proporciona un método de derivación de clave, donde el método incluye las siguientes operaciones:

Operación 10: una MME genera un valor aleatorio.

Operación 20: La MME utiliza el valor aleatorio y la clave raíz como parámetros de entrada de una KDF para derivar una clave de un UE en una UTRAN objetivo; o utiliza el valor aleatorio, un valor COUNT de enlace descendente de NAS actual, y la clave raíz como parámetros de entrada de la KDF para derivar la clave del UE en la UTRAN objetivo. Para una mejor comprensión, el método, dispositivo y sistema de derivación de clave de acuerdo con las realizaciones del presente invento son descritos después a través de un proceso de transferencia de red específico.

Realización 1 de Método

Se ha proporcionado un método de derivación de clave. Un escenario de aplicación de esta realización es un proceso de transferencia de un UE desde una EUTRAN a una UTRAN. Un diagrama de flujo del método de acuerdo con esta realización está mostrado en la fig. 2, que incluye las siguientes operaciones:

Operación 101: Una BS donde se sitúa un UE actualmente, a saber una BS actual, envía un mensaje de Transferencia Requerida a una MME asociada con la BS actual, en particular una MME actual.

Operación 102: La MME actual recibe el mensaje de Transferencia Requerida, genera un valor aleatorio, y utiliza el valor aleatorio y una clave raíz como parámetros de entrada de una KDF para derivar una clave del UE en una UTRAN objetivo.

Puede comprenderse que la MME actual puede generar un valor aleatorio en cualquier momento cuando recibe el mensaje de Transferencia Requerida. Cuando se genera el valor aleatorio, la MME actual puede generar aleatoriamente el valor aleatorio, es decir, un valor reciente de la MME a través de un módulo de generación interno de número aleatorio.

La descripción específica de una KDF es que la KDF = Función Hash (HMAC)-SHA-256(Clave, S), en que Clave es una función de entrada, y S=FC || P0 || L0 ||P1 || L1 || P2 || L2 || P3 || L3 ||… || Pn || Ln, donde || representa la concatenación, FC es utilizado para distinguir diferentes KDF, P es un código del parámetro de entrada, y L es la longitud del parámetro de entrada correspondiente a P. Cuando la KDF es empleada para derivar una clave CK' || IK', la CK' || IK'=KDF(KASME, S), y S= FC || P0 || L0, donde FC es específicamente 0x16, P0 es un valor COUNT de enlace descendente de NAS, y L0 es la longitud del valor COUNT de enlace descendente de NAS (tal como 0x00 0x04).

Cuando se deriva la clave en esta realización, la MME actual puede utilizar el valor reciente de la MME y la clave raíz como parámetros de entrada de la KDF para derivar la clave del UE en la UTRAN objetivo. En este caso, la clave CK' || IK'=KDF(Kasme, S), donde S=FC || valor reciente de la MME || longitud del valor reciente de la MME.

Operación 103: La MME actual envía un mensaje de Solicitud de Reubicación a un RNC objetivo a través de un SGSN objetivo, en que el mensaje de Solicitud de Reubicación incluye la clave del UE en la UTRAN objetivo calculada en la operación 102, un KSI correspondiente, y la información tal como una capacidad de seguridad de la UTRAN del UE o Red de Acceso por Radio GSM/EDGE (GERAN).

Operación 104: El RNC objetivo envía un mensaje de Respuesta de Reubicación de Reenvío a la MME a través del SGSN objetivo, en que el mensaje de Respuesta de Reubicación de Reenvío lleva un identificador de algoritmo (ID) seleccionado por el RNC objetivo de acuerdo con la capacidad de seguridad del UE.

Operación 105: La MME actual envía el valor aleatorio obtenido en la operación 102 al UE a través de un mensaje de Comando de Transferencia.

Puede comprenderse que la MME puede enviar el mensaje de Comando de Transferencia a la BS, en que el mensaje de Comando de Transferencia puede incluir el valor aleatorio generado, e incluir además información tal como el ID de algoritmo y el valor COUNT de enlace descendente de NAS actual; y la BS envía a continuación información tal como el valor aleatorio, el valor COUNT de enlace descendente de NAS actual, y el ID de algoritmo incluido en el mensaje de Comando de Transferencia al UE a través de un HO desde el mensaje de orden de EUTRAN.

Operación 106: El UE recibe el mensaje de Comando de Transferencia, deriva la clave de acuerdo con el valor aleatorio a través del método en la operación 102 anterior, alcanzando por ello la sincronización de la clave entre el UE y la red objetivo, y envía un mensaje de Completar HO al RNC objetivo para completar la transferencia de red. Puede comprenderse que el UE puede calcular la CK' o IK' específica de acuerdo con el ID de algoritmo.

Debería observarse que en el primer proceso de transferencia del UE a la UTRAN, la MME fuente puede aplicar el método de derivación de clave utilizado en la transferencia de red de esta realización, y después del fallo de la primera transferencia del UE, la MME puede aplicar también el método de derivación de clave de esta realización para derivar la clave en la segunda transferencia del UE.

En otra realización específica, cuando se realiza la derivación de clave en la operación 102, la MME puede utilizar el valor aleatorio, el valor COUNT de enlace descendente de NAS actual, y la clave raíz como los parámetros de entrada de la KDF para derivar la clave del UE en la UTRAN objetivo. En este caso, la clave CK' || IK'=KDF(Kasme, S), donde S=FC || P0 || L0 || valor reciente de la MME || longitud del valor reciente de la MME. A continuación, en la operación 105, la MME envía el mensaje de Comando de Transferencia que incluye el valor aleatorio y el valor COUNT de enlace descendente de NAS actual al UE, y solamente cuatro bits menos significativos del valor COUNT de enlace descendente de NAS actual pueden ser incluidos aquí. Por ello, en la operación 106, el UE deriva la clave de acuerdo con el valor aleatorio y el valor COUNT de enlace descendente de NAS actual utilizando el método en la operación 102.

En otras realizaciones específicas, en la primera transferencia del UE, la MME fuente puede guardar la clave después de derivar la clave, y cuando la primera transferencia del UE tiene éxito, la clave guardada puede ser borrada. La MME fuente recibe un mensaje de Completar Reubicación de Reenvío enviado por el SGSN objetivo después de que el UE envíe el mensaje de Completar HO, que indica que la primer transferencia ha tenido éxito. Después de recibir el mensaje de Transferencia Requerida, la MME determina si la clave del UE en la UTRAN objetivo es actualmente guardada; en caso afirmativo, la MME determina además si el valor COUNT de enlace descendente de NAS actual correspondiente a la clave guardada actualmente del UE en la UTRAN objetivo es consistente con el valor COUNT de enlace descendente de NAS actual; y si es consistente, la MME obtiene un valor aleatorio. Definitivamente, cuando la MME determina que la clave del UE en la UTRAN objetivo no es guardada actualmente, se obtiene un valor aleatorio utilizando el método de esta realización, y a continuación se realiza la derivación, y si el resultado de determinación de consistencia anterior es inconsistente, la derivación es realizada utilizando el método de derivación actual.

Puede comprenderse que en la segunda transferencia del UE después de que la primera transferencia del UE falle y antes de que la MME reciba el mensaje de Transferencia Requerida otra vez, un proceso NAS puede ser realizado, y el valor COUNT de enlace descendente de NAS cambia, de manera que cuando el resultado de la determinación anterior es inconsistente, la MME puede utilizar el valor COUNT de enlace descendente de NAS actual para derivar la clave, y la clave derivada de esta manera es diferente de la clave derivada en la primera transferencia; si el resultado de la determinación es positivo, se obtiene un valor aleatorio.

En la realización del presente invento, el método de derivación de clave utilizado en la transferencia del UE desde la EUTRAN a la UTRAN es que: cuando recibe el mensaje de Transferencia Requerida, la MME genera un valor aleatorio, y deriva la clave del UE en la UTRAN objetivo de acuerdo con la KDF, la clave raíz, y el valor aleatorio. En este caso, la clave derivada en el segundo proceso de transferencia después del fallo de la primera transferencia del UE es ciertamente diferente de la clave derivada en el primer proceso de transferencia, evitando por ello la situación en la técnica anterior y mejorando la seguridad de la red.

Realización 2 de Método

Se ha proporcionado un método de transferencia de red. Un escenario de aplicación de esta realización es que en el proceso de transferencia de un UE desde una EUTRAN a una UTRAN, después de que una primera transferencia del UE falle, el UE vuelve a una EUTRAN original y selecciona una SGSN para una segunda transferencia. Un diagrama de flujo del método de acuerdo con esta realización está mostrado en la fig. 3, que incluye los siguientes operaciones:

Operación 201: El UE envía un mensaje de Solicitud de Restablecimiento de Conexión RRC a una BS fuente, y realiza un proceso de restablecimiento de conexión RRC.

Puede comprenderse que después de que la primera transferencia falle, el UE puede volver a una celda diferente bajo la BS fuente, o volver a la misma celda bajo la BS fuente, o volver a una BS diferente de la BS fuente. En esta realización, un ejemplo del UE que vuelve a la misma celda bajo la BS fuente es utilizado para ilustración.

Operación 202: Después de que la conexión RRC es restablecida, la BS fuente envía un Mensaje de Transferencia Requerida a una MME fuente.

Operación 203: La MME fuente recibe el mensaje de Transferencia Requerida, y obtiene un nuevo Valor COUNT de enlace descendente de NAS actual, en el que el nuevo valor COUNT de enlace descendente de NAS es diferente del Valor COUNT de enlace Descendente de NAS actual.

Cuando se obtiene el nuevo valor COUNT de enlace descendente de NAS, la MME fuente puede obtener el nuevo valor COUNT de enlace descendente de NAS de la siguiente manera: añadiendo un cierto valor al valor COUNT de enlace descendente de NAS actual, tal como añadiendo 1; o

enviando un mensaje de NAS, tal como un mensaje de Comando de Modo de Seguridad (SMC) de NAS, al UE, de manera que al valor COUNT de enlace descendente de NAS actualmente guardado se le añade 1, y el valor COUNT de enlace descendente de NAS después de que el mensaje de NAS sea enviado es utilizado como el nuevo valor COUNT de enlace descendente de NAS.

Operación 204: La MME fuente deriva la clave del UE en una UTRAN objetivo de acuerdo con una KDF, una clave raíz, y el nuevo valor COUNT de enlace descendente de NAS.

La clave derivada por la MME fuente CK' || IK'=KDF(Kasme, S), donde S=FC || nuevo valor COUNT de enlace descendente de NAS || longitud del nuevo valor COUNT de enlace descendente de NAS.

Operación 205: La MME fuente envía un mensaje de Solicitud de Reubicación a un RNC objetivo a través de la SGSN objetivo, en que el mensaje de Solicitud de Reubicación incluye la clave del UE en la UTRAN objetivo calculada en el operación 204.

Operación 206: El RNC objetivo envía un mensaje de Respuesta de Reubicación de Reenvío a la MME fuente a través del SGSN objetivo, en el que el mensaje de Respuesta de Reubicación de Reenvío lleva un ID de algoritmo seleccionado por el RNC objetivo de acuerdo con una capacidad de seguridad del UE.

Operación 207: La MME fuente envía el nuevo valor COUNT de enlace descendente de NAS al UE a través de un mensaje de Comando de Transferencia, en el que solamente 4 bits menos significativos del nuevo valor COUNT de enlace descendente de NAS pueden ser enviados al UE.

Puede comprenderse que la MME puede enviar el mensaje de Comando de Transferencia a la BS, en el que el mensaje de Comando de Transferencia puede incluir el nuevo valor COUNT de enlace descendente de NAS, y puede incluir también información tal como un ID de algoritmo; y la BS envía a continuación el nuevo valor COUNT de enlace descendente de NAS al UE a través de un HO desde el mensaje de comando de EUTRAN.

Operación 208: el UE recibe el mensaje de Comando de Transferencia, deriva la clave de acuerdo con la KDF, la clave raíz, y el nuevo valor COUNT de enlace descendente de NAS utilizando el método en la operación 204 anterior, consiguiendo por tanto la sincronización de la clave entre el UE y la red objetivo, y envía un mensaje de Completar HO al RNC objetivo para completar la transferencia de la red.

En otras realizaciones específicas, en el primer proceso de transferencia del UE, la MME fuente puede guardar la clave después de la derivación de clave, y cuando recibe un mensaje de Completar Reubicación de Reenvío enviado por el SGSN objetivo, la MME fuente puede borrar la clave guardada. Por tanto, antes de realizar la operación 203, la MME fuente determina si la clave del UE en la UTRAN objetivo está guardada actualmente; en caso afirmativo, determina además si el valor de COUNT de enlace descendente de NAS correspondiente a la clave guardada del UE en la UTRAN objetivo es consistente con el valor COUNT de enlace descendente de NAS actual; y si es consistente, realiza la operación 203 para obtener el nuevo valor COUNT de enlace descendente de NAS. Definitivamente, cuando la MME fuente determina que la clave del UE en la UTRAN objetivo no está guardada actualmente, la MME puede realizar la operación 203 para obtener el nuevo valor COUNT de enlace descendente de NAS; y si el resultado de determinación de consistencia anterior es inconsistente, la MME realiza la derivación de acuerdo con el método de derivación actual.

Puede comprenderse que en la segunda transferencia del UE después de que la primera transferencia del UE falle y antes de que la MME fuente reciba el mensaje de Transferencia Requerida otra vez, puede ser realizado un proceso de NAS, y el valor COUNT de enlace descendente de NAS cambia, de manera que cuando el resultado de la determinación anterior es inconsistente, la MME fuente puede utilizar el valor COUNT de enlace descendente de NAS actual para derivar la clave, y la clave derivada de esta manera es diferente de la clave derivada en la primera transferencia; si el resultado de determinación es positivo, la derivación de clave es realizada después de que se obtenga el nuevo valor COUNT de enlace descendente de NAS.

En una realización del presente invento, dos máquinas de estado son establecidas en la MME fuente, respectivamente para la derivación de clave incapaz de utilizar el valor COUNT de enlace descendente de NAS guardado y la derivación de clave capaz de utilizar el valor COUNT de enlace descendente de NAS guardado, y son indicadas respectivamente por Estado 0 y Estado 1. Cuando la MME fuente recibe el mensaje de Transferencia Requerida, se establece el Estado

0; y cuando la MME va a través de un cierto proceso interno y satisface una condición preestablecida, se establece el Estado 1, es decir, la derivación de clave puede ser realizada, en que la condición preestablecida incluye: la MME recibe un mensaje de Completar Reubicación de Reenvío, al valor COUNT de enlace descendente de NAS actual se le añade un cierto valor, y la MME entrega un mensaje de NAS. Por ejemplo, después de que la MME reciba al mensaje de Transferencia Requerida y entregue el mensaje de NAS, se puede realizar la derivación de clave.

En la realización del presente invento, en el proceso de transferencia del UE desde la EUTRAN a la UTRAN después de que falle la primera transferencia, el método de derivación de clave en la segunda transferencia de red es que, después de recibir el mensaje de Transferencia Requerida, la MME fuente obtiene el nuevo valor COUNT de enlace descendente de NAS diferente del valor COUNT de enlace descendente de NAS actual, y deriva la clave del UE en la UTRAN objetivo de acuerdo con la KDF, la clave raíz, y el nuevo valor COUNT de enlace descendente de NAS. De esta manera, la clave derivada en el segundo proceso de transferencia es ciertamente diferente de la clave derivada en el primer proceso de transferencia, evitando por ello la situación de la técnica anterior y mejorando la seguridad de red.

Realización 3 de Método

Se ha proporcionado un método de derivación de clave. Un escenario de aplicación de esta realización es que en el proceso de transferencia de un UE desde una EUTRAN a una UTRAN, después de que falle una primera transferencia del UE, el UE vuelve a la EUTRAN original y selecciona un SGSN para una segunda transferencia. Un diagrama de flujo del método está mostrado en la fig. 4, que incluye los siguientes operaciones:

Operación 301: El UE envía un mensaje de Solicitud de Restablecimiento de Conexión en RRC a una BS donde se sitúa el UE actualmente, en particular una BS actual, para realizar un proceso de restablecimiento de conexión de RRC.

Puede comprenderse que después de que falle la primera transferencia, el UE puede volver a una celda diferente bajo una BS fuente, o volver a la misma celda bajo la BS fuente, o volver a una BS diferente de la BS fuente.

Operación 302: Después de que la conexión RRC sea restablecida, la BS actual envía un mensaje de Completar Restablecimiento de Conexión de RRC a una MME asociada con la BS actual, en particular una MME actual.

Puede comprenderse que el mensaje de Completar Restablecimiento de Conexión de RRC puede ser un mensaje de Notificar HO, o puede ser un mensaje de Conmutar Trayecto. Específicamente, si el UE vuelve a la celda diferente bajo la BS fuente, la BS actual, en particular la BS fuente, puede enviar el mensaje de Notificar HO a la MME actual para indicar que el restablecimiento de conexión ha sido completado; si el UE vuelve a la BS diferente de la BS fuente, la BS actual puede enviar el mensaje de Conmutar Trayecto a la MME actual.

Operación 303: La MME actual recibe el mensaje de Completar Restablecimiento de Conexión de RRC enviado por la BS actual, y obtiene un nuevo valor COUNT de enlace descendente de NAS, en que el nuevo valor COUNT de enlace descendente de NAS es diferente de un valor COUNT de enlace descendente de NAS actual.

El método de obtención es el mismo que el descrito en la operación 203 de la Realización 2 de Método, y los detalles no son descritos aquí otra vez.

Operación 304: La BS actual determina realizar la segunda transferencia y envía un mensaje de Transferencia Requerida a la MME actual.

Operación 305: Después de recibir el mensaje de Transferencia Requerida, la MME actual deriva la clave del UE en la UTRAN de acuerdo con una KDF, una clave raíz, y el nuevo valor COUNT de enlace descendente de NAS obtenido en la operación 303, y envía la clave derivada a un RNC objetivo.

Después de que la clave es enviada al RNC objetivo, el método de transferencia de red es el mismo que el método de la Realización 2 de Método después de la operación 205, y los detalles no son descritos aquí otra vez. Además, la operación 303 y la operación 304 en esta realización pueden ser realizadas al mismo tiempo, pero son realizadas preferiblemente en secuencia, y por tanto, el proceso de transferencia de red puede no ser afectado, lo que ahorra tiempo a la transferencia de red.

El método de derivación de clave en la realización del presente invento es que, durante la transferencia del UE desde la EUTRAN a la UTRAN, después de que falle la primera transferencia y antes de la segunda transferencia del UE, la MME obtiene el nuevo valor COUNT de enlace descendente de NAS diferente del valor COUNT de enlace descendente de NAS actual, de manera que la MME recibe el mensaje de Transferencia Requerida, la clave derivada y calculada del UE en la UTRAN es ciertamente diferente de la clave derivada en el primer proceso de transferencia, evitando por ello la situación de la técnica anterior y mejorando la seguridad de red.

Además, debido a que la obtención del nuevo valor COUNT de enlace descendente de NAS es realizada antes de la segunda transferencia, la transferencia de red puede no ser afectada, y comparado con la Realización 1 de Método, el tiempo de transferencia de red es reducido.

Realización 4 de Método

Se ha proporcionado un método de derivación de clave. Un escenario de aplicación de esta realización es que en el proceso de transferencia de un UE desde una EUTRAN a una UTRAN, después de que falle la primera transferencia del UE, el UE vuelve a la EUTRAN original para una segunda transferencia. Un diagrama de flujo del método está mostrado en la fig. 5, que incluye los siguientes operaciones:

Operación 401: El UE envía un mensaje de Solicitud de Restablecimiento de Conexión de RRC a una BS donde el UE se sitúa actualmente, en particular una BS actual, en que el mensaje de Solicitud de Restablecimiento de Conexión de RRC puede incluir repuesto de 2 bits para llevar un valor reciente del UE, en particular un valor aleatorio.

Operación 402: Después de recibir el mensaje de Solicitud de Restablecimiento de Conexión de RRC, la BS actual determina realizar la segunda transferencia del UE y envía, a través de un mensaje de Transferencia Requerida, el valor reciente del UE a la MME asociada con la BS actual, en particular la MME actual, para derivar la clave del UE en la UTRAN objetivo.

Operación 403: Después de recibir el mensaje de Transferencia Requerida, la MME utiliza el valor reciente del UE incluido en el mensaje de Transferencia Requerida y una clave raíz como parámetros de entrada de una KDF para derivar la clave del UE en la UTRAN objetivo.

Cuando se deriva la clave, la MME actual puede utilizar el valor reciente del UE y la clave raíz como parámetros de entrada de la KDF para derivar la clave del UE en la UTRAN objetivo, y en este caso, la clave CK'|| IK'=KDF(Kasme, S), donde S=FC || valor reciente del UE || longitud del valor reciente del UE.

Operación 404: La MME actual envía un mensaje de Solicitud de Reubicación a un RNC objetivo a través de un SGSN objetivo, en que el mensaje de Solicitud de Reubicación incluye la clave del UE en la UTRAN objetivo calculada en la operación 403.

Operación 405: El RNC objetivo envía un mensaje de Respuesta de Reubicación de Reenvío a la MME actual a través de la SGSN objetivo, en que el mensaje de Respuesta de Reubicación de Reenvío lleva un ID de algoritmo seleccionado por el RNC objetivo de acuerdo con una capacidad de seguridad del UE.

Operación 406: La MME actual envía un mensaje de Comando de Transferencia a la BS, en que el mensaje de Comando de Transferencia puede incluir el valor COUNT de enlace descendente de NAS actual, y puede incluir además información tal como un ID de algoritmo; y la BS a continuación envía el mensaje de Comando de Transferencia al UE, en que el mensaje de Comando de Transferencia puede incluir el valor COUNT de enlace descendente de NAS actual.

Operación 407: El UE recibe el mensaje de Comando de Transferencia, y deriva la clave de acuerdo con el valor reciente del UE a través del método en la operación 403 anterior, consiguiendo por tanto la sincronización de la clave entre el UE y la red objetivo.

En otra realización específica, en la operación 403, la MME puede utilizar el valor reciente del UE, el valor COUNT de enlace descendente de NAS actual, y la clave raíz como parámetros de entrada de la KDF para derivar la clave del UE en la UTRAN objetivo. En este caso, la clave CK'|| IK'=KDF(Kasme, S), donde S=FC || P0 || L0 || valor reciente del UE || longitud del valor reciente del UE, de manera que el mensaje de Comando de Transferencia enviado por el UE en la operación 406 debe incluir valor COUNT de enlace descendente de NAS actual, y puede incluir los cuatro bits menos significativos; y en la operación 407, el UE puede derivar la clave de acuerdo con el valor reciente del UE y el valor COUNT de enlace descendente de NAS actual utilizando el método en la operación 403.

Puede comprenderse que el proceso subsiguiente es similar a la técnica anterior, y los detalles no son descritos aquí otra vez.

En otras realizaciones específicas, en el primer proceso de transferencia del UE, la MME puede guardar la clave después de la derivación de clave, y cuando recibe un mensaje de Completar Reubicación de Reenvío enviado por el SGSN objetivo, la MME fuente puede borrar la clave guardada. Por ello, después de recibir el mensaje de Transferencia Requerida, la MME actual determina si la clave del UE en la UTRAN objetivo está guardada actualmente; en caso afirmativo, determina además si el valor COUNT de enlace descendente de NAS correspondiente a la clave guardada actualmente del UE en la UTRAN objetivo es consistente con el valor COUNT de enlace descendente de NAS actual; y si es consistente, la derivación de clave se realiza de acuerdo con el método de esta realización. En definitiva, cuando la MME determina que la clave del UE en la UTRAN objetivo no está guardada actualmente, la derivación es realizada de acuerdo con el método de esta realización, y si el resultado de determinación de consistencia anterior es inconsistente, la derivación de clave es realizada de acuerdo con el método de derivación de la técnica anterior.

Puede comprenderse que en la segunda transferencia del UE después de que falle la primera transferencia del UE, antes de que la MME reciba de nuevo el mensaje de Transferencia Requerida, puede ser realizado un proceso de NAS, y el valor COUNT de enlace descendente de NAS cambia, de manera que cuando el resultado de la determinación anterior es inconsistente, la MME puede utilizar el valor COUNT de enlace descendente de NAS actual para derivar la clave, y la clave derivada de esta manera es diferente de la clave derivada de la primera transferencia; si el resultado de determinación es positivo, la derivación de clave es realizada de acuerdo con el método de esta realización.

El método de derivación de clave en la realización del presente invento es que, en el proceso de transferencia del UE desde la EUTRAN a la UTRAN, cuando el UE realiza la segunda transferencia después de que falle la primera transferencia, el UE calcula un valor reciente, y envía el valor reciente a la MME actual a través de la BS actual; después de recibir el mensaje de Transferencia Requerida, la MME deriva la clave del UE en la UTRAN objetivo de acuerdo con el valor reciente del UE, la KDF, la clave raíz, y el valor COUNT de enlace descendente de NAS actual incluido en el mensaje de Transferencia Requerida. De esta manera, la clave derivada en el segundo proceso de transferencia es diferente de la clave derivada en el primer proceso de transferencia, evitando por ello la situación de la técnica anterior y mejorando la seguridad de red.

Realización 5 de Método

Se ha proporcionado un método de derivación de clave. Un escenario de aplicación de esta realización es que en el proceso de transferencia de un UE desde una EUTRAN a una UTRAN, una BS en la EUTRAN original del UE, en particular una BS fuente, inicia un transferencia de red. Un diagrama de flujo del método está mostrado en la fig. 6, que incluye los siguientes operaciones.

Operación 501: La BS fuente envía un mensaje de Transferencia Requerida a una MME fuente.

Operación 502: La MME fuente deriva CK' || IK' de acuerdo con una KDF, una clave raíz Kasme, y un valor COUNT de enlace descendente de NAS en un contexto de seguridad actual.

Operación 503: La MME fuente envía un mensaje de Solicitud de Reubicación a un RNC objetivo a través de un SGSN objetivo, en que el mensaje de Solicitud de Reubicación incluye CK' || IK', KSI, e información tal como una capacidad de seguridad de la UTRAN/GERAN del UE.

Operación 504: El RNC objetivo envía un mensaje de Respuesta de Reubicación de Reenvío a una MME fuente a través del SGSN objetivo, en que el mensaje de Respuesta de Reubicación de Reenvío lleva un ID de algoritmo de la capacidad de seguridad del UE.

Operación 505: La MME fuente completa un proceso de preparación de transferencia, y envía un mensaje de Comando de Transferencia al UE a través de la BS fuente, en que el mensaje de Comando de Transferencia lleva el valor COUNT de enlace descendente de NAS actual y el ID de algoritmo de la capacidad de seguridad.

Operación 506: La MME cambia el valor COUNT de enlace descendente de NAS actual, por ejemplo, añadiendo un cierto valor al valor COUNT de enlace descendente de NAS actual, tal como añadiendo 1, y guarda el valor COUNT de enlace descendente de NAS cambiado; el valor COUNT de enlace descendente de NAS cambiado es utilizado para derivar la clave del UE en la UTRAN objetivo.

Operación 507: después de recibir el mensaje de Comando de Transferencia, el UE deriva y calcula la clave CK' || IK' de acuerdo con la KDF y el valor COUNT de enlace descendente de NAS que está incluido en el mensaje de Comando de Transferencia, de manera que la clave del UE y la red objetivo es sincronizada, y el mensaje de Completar HO es enviado al RNC objetivo.

Puede comprenderse que en el primer proceso de transferencia en esta realización, después de que la MME fuente envíe el mensaje de Comando de Transferencia, el valor COUNT de enlace descendente de NAS es cambiado, de manera que después de que falle la primera transferencia del UE, el valor COUNT de enlace descendente de NAS guardado en la operación 506 y utilizado por la MME para la derivación de clave en la segunda transferencia es ciertamente diferente del valor COUNT de enlace descendente de NAS utilizado en la primera transferencia, y por tanto las claves derivadas y calculadas en los dos transferencias son diferentes, lo que consigue el propósito de mejorar la seguridad de red.

Realización 1 de Dispositivo

Se ha proporcionado una MME. Un diagrama estructural esquemático de la MME está mostrado en la fig. 7, que incluye una unidad generadora 10, una unidad de derivación 11, y una unidad de envío 12.

La unidad generadora 10 está configurada para generar un valor aleatorio.

La unidad de derivación 11 está configurada para utilizar una clave raíz y el valor aleatorio que es generado por la unidad generadora 10 como parámetros de entrada de una KDF para derivar una clave de un UE en una UTRAN objetivo.

La unidad de envío 12 está configurada para enviar el valor aleatorio generado por la unidad generadora 10 al UE, de manera que el UE deriva la clave en la UTRAN objetivo de acuerdo con el valor aleatorio.

La unidad de derivación 11 está configurada además para utilizar un valor COUNT de enlace descendente de NAS actual, la clave raíz, y el valor aleatorio generado por la unidad generadora 10 como los parámetros de entrada de la KDF para derivar la clave del UE en la UTRAN objetivo; y la unidad de envío 12 está configurada para enviar el valor COUNT de enlace descendente de NAS actual y el valor aleatorio generado por la unidad generadora 10 al UE, de manera que el

UE deriva la clave en la UTRAN objetivo de acuerdo con el valor aleatorio y el valor COUNT de enlace descendente de NAS actual.

En esta realización, la unidad generadora 10 de la MME genera un valor aleatorio, y la unidad de derivación 11 deriva la clave de acuerdo con el valor aleatorio, de manera que en el proceso de transferencia del UE desde la EUTRAN a la UTRAN, después de que falle la primera transferencia, la clave derivada por la MME en el segundo proceso de transferencia es ciertamente diferente de la clave derivada en el primer proceso de transferencia, evitando por ello la situación de la técnica anterior y mejorando la seguridad de red.

Realización 2 de Dispositivo

Se ha proporcionado un UE. Un diagrama estructural esquemático del UE está mostrado en la fig. 8, que incluye una unidad receptora de mensaje 20 y una unidad de derivación de clave 21.

La unidad receptora de mensaje 20 está configurada para recibir un mensaje de Comando de Transferencia.

La unidad de derivación de clave 21 está configurada para utilizar un valor aleatorio y una clave raíz como parámetros de entrada de una KDF para derivar la clave del UE en una UTRAN objetivo si el mensaje de Comando de Transferencia recibido por la unidad receptora de mensaje 20 incluye el valor aleatorio; y configurada para utilizar el valor aleatorio, un valor COUNT de enlace descendente de NAS actual, y la clave raíz como parámetros de entrada de la KDF para derivar la clave del UE en la UTRAN objetivo si el mensaje de Comando de Transferencia recibido por la unidad receptora de mensaje 20 incluye el valor aleatorio y el valor COUNT de enlace descendente de NAS actual.

Realización 3 de Dispositivo

Se ha proporcionado una MME. Un diagrama estructural esquemático de la MME está mostrado en la fig. 9, que incluye una unidad de obtención de valor de cómputo 31, una segunda unidad de derivación 32 y una unidad de envío de transferencia 33.

La unidad de obtención de valor de cómputo 31 está configurada para obtener un nuevo valor COUNT de enlace descendente de NAS.

Cuando se obtiene el nuevo valor COUNT de enlace descendente de NAS, un mensaje NAS puede ser enviado a un UE, tal como un mensaje SMC de NAS, de manera que al valor COUNT de enlace descendente de NAS guardado actualmente se le puede añadir 1, y el valor COUNT de enlace descendente de NAS después de que el mensaje NAS sea enviado puede ser utilizado como el nuevo valor COUNT de enlace descendente de NAS. Un cierto valor, tal como 1, puede ser añadido al valor COUNT de enlace descendente de NAS actual.

La segunda unidad de derivación 32 está configurada para derivar una clave del UE en una UTRAN objetivo de acuerdo con una KDF, una clave raíz y el nuevo valor COUNT de enlace descendente de NAS que es obtenido por la unidad de obtención de valor de cómputo 31.

La unidad de envío de transferencia 33 está configurada para enviar el nuevo valor COUNT de enlace descendente de NAS obtenido por la unidad de obtención de valor de cómputo 31 al UE a través de una BS donde el UE se sitúa actualmente, de manera que el UE deriva la clave en la UTRAN objetivo.

Puede comprenderse que en otras realizaciones específicas, la MME puede incluir además una unidad de determinación 34, configurada para determinar si la clave del UE en la UTRAN objetivo está guardada actualmente; y en caso afirmativo, determinar además si el valor COUNT de enlace descendente de NAS correspondiente a la clave guardada actualmente del UE en la UTRAN objetivo es consistente con el valor COUNT de enlace descendente de NAS actual.

Cuando el resultado de la determinación de la unidad de determinación 34 es que el valor COUNT de enlace descendente de NAS correspondiente con la clave guardada actualmente del UE en la UTRAN es consistente con el valor COUNT de enlace descendente de NAS actual, la unidad de obtención de valor de cómputo 31 obtiene el nuevo valor COUNT de enlace descendente de NAS.

La unidad de obtención de valor de cómputo 31 en la MME de acuerdo con la realización del presente invento obtiene el nuevo valor COUNT de enlace descendente de NAS diferente del valor COUNT de enlace descendente de NAS actual; y finalmente la segunda unidad de derivación 32 deriva la clave del UE en la UTRAN objetivo de acuerdo con la KDF, la clave raíz, y el nuevo valor COUNT de enlace descendente de NAS, y la unidad de envío de transferencia 33 envía el nuevo valor COUNT de enlace descendente de NAS al UE. De esta manera, en el proceso de transferencia del UE desde la EUTRAN a la UTRAN, después de que falle la primera transferencia, la clave derivada por la MME en el segundo proceso de transferencia es ciertamente diferente de la clave derivada en el primer proceso de transferencia, evitando por ello la situación de la técnica anterior y mejorando la seguridad de red.

Además, puede comprenderse que después de que falle la primera transferencia del UE, durante la segunda transferencia del UE, antes de que la MME reciba el mensaje de Transferencia Requerida otra vez, puede ser realizado un proceso NAS, y el valor COUNT de enlace descendente de NAS cambia por ello. La MME incluye además la unidad

de determinación 34 para la determinación de consistencia. Si el resultado de la determinación de consistencia es inconsistente, el valor COUNT de enlace descendente de NAS actual puede ser utilizado para derivar la clave; si el resultado de la determinación de consistencia es positivo, la clave es derivada después de que la unidad de obtención de valor de cómputo 31 obtenga el nuevo valor COUNT de enlace descendente de NAS. Por ello, la obtención del nuevo valor COUNT de enlace descendente de NAS es reducida cuando el resultado de determinación de consistencia es inconsistente, guardando por ello la carga de la MME.

Realización 4 de Dispositivo

Se ha proporcionado un UE. Un diagrama estructural esquemático del UE está mostrado en la fig. 10, que incluye una segunda unidad receptora de mensaje 40 y una segunda unidad de derivación de clave 41.

La segunda unidad receptora de mensaje 40 está configurada para recibir un mensaje de Comando de Transferencia, en el que el mensaje de Comando de Transferencia incluye un nuevo valor COUNT de enlace descendente de NAS.

La segunda unidad de derivación de clave 41 está configurada para derivar una clave del UE en una UTRAN objetivo de acuerdo con una KDF, una clave raíz, y el nuevo valor COUNT de enlace descendente de NAS en el mensaje de Comando de Transferencia recibido por la segunda unidad receptora de mensaje 40.

Realización 5 de Dispositivo

Se ha proporcionado una MME. Un diagrama estructural esquemático de la MME está mostrado en la fig. 11, que incluye una unidad receptora de transferencia 50 y una tercera unidad de derivación 51.

La unidad receptora de transferencia 50 está configurada para recibir un mensaje de Transferencia Requerida, en que el mensaje de Transferencia Requerida incluye un valor reciente de un UE.

La tercera unidad de derivación 51 está configurada para utilizar una clave raíz y el valor reciente del UE en el mensaje de Transferencia Requerida recibido por la unidad receptora de transferencia 50 como parámetros de entrada de una KDF para derivar la clave del UE en una UTRAN objetivo, o utilizar un valor COUNT de enlace descendente de NAS actual, la clave raíz, y el valor reciente del UE en el mensaje de Transferencia Requerida recibido por la unidad receptora de transferencia 50 como parámetros de entrada de la KDF para derivar la clave del UE en la UTRAN objetivo.

En esta realización, después de que la unidad receptora de transferencia 50 de la MME reciba el mensaje de Transferencia Requerida, la tercera unidad de derivación 51 deriva la clave de acuerdo con el valor reciente del UE incluido en el mensaje de Transferencia Requerida, de manera que en el proceso de transferencia del UE desde la EUTRAN a la UTRAN, después de que falle la primera transferencia, la clave derivada por la MME en el segundo proceso de transferencia es ciertamente diferente de la clave derivada en el primer proceso de transferencia, evitando por ello la situación de la técnica anterior y mejorando la seguridad de red.

Realización 6 de Dispositivo

Se ha proporcionado una BS. Un diagrama estructural esquemático de la BS está mostrado en la fig. 12, que incluye una unidad receptora de restablecimiento 60 y una unidad de envío y derivación 61.

La unidad receptora de restablecimiento 60 está configurada para recibir un mensaje de Solicitud de Restablecimiento de Conexión de RRC, en el que el mensaje de Restablecimiento de Conexión de RRC incluye un valor reciente de un UE.

La unidad de envío y derivación 61 está configurada para enviar el valor reciente del UE incluido en el mensaje de Solicitud de Restablecimiento de Conexión RRC recibido por la unidad receptora de restablecimiento 60 a una MME a través de un mensaje de Transferencia Requerida cuando es determinada una segunda transferencia del UE, de modo que facilite a la MME derivar la clave del UE en la UTRAN objetivo.

Realización 7 de Dispositivo

Se ha proporcionado un UE. Un diagrama estructural esquemático del UE está mostrado en la fig. 13, que incluye una unidad de envío de restablecimiento 71 y una tercera unidad de derivación de clave 72.

La unidad de envío de restablecimiento 71 está configurada para enviar un mensaje de Solicitud de Restablecimiento de Conexión de RRC, en que el mensaje de Solicitud de Restablecimiento de Conexión de RRC incluye un valor reciente de un UE.

La tercera unidad de derivación de clave 72 está configurada para utilizar el valor reciente del UE y una clave raíz como parámetros de entrada de una KDF para derivar la clave del UE en una UTRAN objetivo cuando recibe un mensaje de Comando de Transferencia, y para utilizar el valor reciente del UE, un valor COUNT de enlace descendente de NAS actual, y la clave raíz como parámetros de entrada de la KDF para derivar la clave del UE en la UTRAN objetivo si el mensaje de Comando de Transferencia incluye el valor COUNT de enlace descendente de NAS actual.

Realización 8 de Dispositivo

Se ha proporcionado una MME. Un diagrama estructural esquemático de la MME está mostrado en la fig. 14, que incluye una unidad receptora de mensaje 81 y una unidad de cambio de valor de cómputo 81.

La unidad receptora de mensaje 81 está configurada para recibir un mensaje de Respuesta de Reubicación de Reenvío enviada por un SGSN objetivo.

La unidad de cambio de valor de cómputo 82 está configurada para cambiar un valor COUNT de enlace descendente de NAS actual y guardar el valor COUNT de enlace descendente de NAS cambiado después de enviar un mensaje de Comando de Transferencia a un UE, en que el valor COUNT de enlace descendente de NAS cambiado es utilizado para derivar una clave del UE en una UTRAN objetivo.

Puede comprenderse que: después de que la unidad receptora de mensaje 81 en la MME reciba el mensaje de Respuesta de Reubicación de Reenvío enviado por el SGSN en la red objetivo, que indica que la red objetivo ha realizado la reubicación para el UE, la transferencia puede ser realizada. En este caso, después de que la unidad de cambio de valor de cómputo 82 envíe el mensaje de Comando de Transferencia, el valor COUNT de enlace descendente de NAS actual es cambiado.

Por ello, después de que la primera transferencia del UE falle, durante una segunda transferencia, la MME utiliza el valor COUNT de enlace descendente de NAS guardado en la MME para derivar la clave, que garantiza que el valor COUNT de enlace descendente de NAS es diferente del valor COUNT de enlace descendente de NAS utilizado en la primera transferencia, de manera que las claves derivadas y calculadas en los dos transferencias son diferentes. Por tanto, se consigue el propósito de mejorar la seguridad de red.

Realización del Sistema

Se ha proporcionado un sistema de comunicación, que incluye una MME. La MME es similar a cualquiera de las MME en las Realizaciones 1, 3, 5 y 8 de Dispositivo, y el método de derivación de clave de acuerdo con las realizaciones anteriores puede ser realizado.

Puede comprenderse que el sistema de comunicación incluye además otros dispositivos tales como un UE y una BS, y la seguridad de red puede ser mejorada a través de la comunicación entre el UE y la BS.

El método, dispositivo, y sistema de derivación de clave de acuerdo con las realizaciones del presente invento son aplicables al proceso de transferencia del UE desde la EUTRAN a la UTRAN. A partir del fallo de la primera transferencia a la segunda transferencia, se garantiza que la clave derivada en la MME fuente en el primer proceso de transferencia del UE es diferente de la clave derivada en la MME en el segundo proceso de transferencia del UE cambiando los parámetros de entrada utilizados en la derivación de clave por la MME, tales como generar el valor aleatorio, cambiar el valor COUNT de enlace descendente de NAS actual, y obtener el valor reciente del UE, de modo que impidan la situación de la técnica anterior en la que una vez que se obtiene la clave utilizada en un RNC, las claves en otros RNC pueden ser derivadas consecuentemente, mejorando por ello la seguridad de red.

Personas expertas en la técnica deben comprender que la totalidad o parte de los operaciones del método de acuerdo con las realizaciones del presente invento pueden ser implementadas por un hardware relevante de instrucción de programa. El programa puede ser almacenado en un medio de almacenamiento legible por ordenador, tal como una Memoria Solo de Lectura (ROM), una Memoria de Acceso Aleatorio (RAM), un disco magnético, o un disco óptico.

El método, dispositivo, y sistema de derivación de clave están descritos en detalle antes. El principio y la implementación del presente invento están descritos aquí a través de los ejemplos específicos. La descripción acerca de las realizaciones del presente invento es simplemente proporcionada para facilitar la comprensión del método y las ideas principales del presente invento. Las personas expertas en la técnica pueden hacer variaciones y modificaciones al presente invento en términos de las implementaciones específicas y los marcos de aplicación de acuerdo con las ideas del presente invento. Por lo tanto, la especificación no será construida como un límite al presente invento.

REIVINDICACIONES

1.- Un método de derivación de clave, que comprende:

obtener (203) por una Entidad de Gestión de Movilidad, MME, un valor COUNT de enlace descendente de Estrato Sin Acceso, NAS;

derivar (204), por la MME, una clave de un Equipamiento de Usuario, UE, en una Red de Acceso por Radio Terrestre Universal, UTRAN, de acuerdo con una Función de Derivación de Clave, KDF, una clave raíz, y el nuevo valor COUNT de enlace descendente de NAS;

guardar, mediante la MME, la clave después de la derivación de clave, y

enviar (207), por la MME, el nuevo valor COUNT de enlace descendente de NAS al UE.

en el que antes de obtener, por la MME, el nuevo valor COUNT de enlace descendente de NAS, el método comprende además:

determinar, por la MME, si la clave del UE en la UTRAN objetivo está actualmente guardada; en caso afirmativo, determinar además si un valor COUNT de enlace descendente de NAS correspondiente a la clave guardada actualmente del UE en la UTRAN objetivo es consistente con el valor COUNT de enlace descendente de NAS actual; y

si es consistente, realizar la operación de obtener el nuevo valor COUNT de enlace descendente de NAS.

2.- El método según la reivindicación 1, en el que la obtención, por la MME, del valor COUNT de enlace descendente de NAS comprende:

añadir, por la MME, un cierto valor a un valor COUNT de enlace descendente de NAS actual.

3.- El método según la reivindicación 2, en el que el cierto valor es 1.

4.- El método según la reivindicación 1, en el que la obtención por la MME del nuevo valor COUNT de enlace descendente de NAS comprende:

enviar, mediante la MME, un mensaje de NAS al UE, y utilizar un valor COUNT de enlace descendente de NAS después de que el mensaje NAS sea enviado como el nuevo valor COUNT de enlace descendente de NAS.

5.- El método según la reivindicación 1, en el que el envío, por la MME, del nuevo valor COUNT de enlace descendente de NAS al UE comprende:

enviar, mediante la MME, cuatro bits menos significativos del nuevo valor COUNT de enlace descendente de NAS al UE.

6.- Una Entidad de Gestión de Movilidad, MME, que comprende:

una unidad de valor de cómputo (31), configurada para obtener un nuevo valor COUNT de enlace descendente, de Estrato si Acceso, NAS;

una segunda unidad de derivación (32), configurada para derivar una clave de un Equipamiento de Usuario, UE, en una Red de Acceso por Radio Terrestre Universal, UTRAN, de acuerdo con una Función de Derivación de Clave, KDF, una clave de raíz, y el nuevo valor COUNT de enlace descendente de NAS que es obtenido por la unidad de obtención de valor de cómputo;

una unidad para guardar, configurada para guardar la clave derivada por la segunda unidad de derivación (32);

una unidad de envío de transferencia (33), configurada para enviar el nuevo valor COUNT de enlace descendente de NAS obtenido por la unidad de obtención de valor de cómputo a la UE; y

una unidad de determinación (34), configurada para determinar si la clave del UE en la UTRAN objetivo está guardada actualmente; en caso afirmativo, determinar además si un valor COUNT de enlace descendente de NAS correspondiente con la clave actualmente guardada del UE en la UTRAN objetivo es consistente con el valor COUNT de enlace descendente de NAS actual, en el que

cuando un resultado de determinación de la unidad de determinación es que el valor COUNT de enlace descendente de NAS correspondiente a la clave guardada actualmente del UE en la UTRAN objetivo es consistente con el valor de COUNT de enlace descendente de NAS actual, la unidad de obtención del valor de cómputo obtiene el nuevo valor COUNT de enlace descendente de NAS.

7.- La MME según la reivindicación 6, en la que

la unidad de obtención de valor de cómputo (31) está configurada para obtener el nuevo valor COUNT de enlace descendente de NAS añadiendo un cierto valor al valor COUNT de enlace descendente de NAS actual.

8.- La MME según la reivindicación 7, en la que el cierto valor es 1.

9.- Un método de derivación de clave, que comprende:

recibir (501), por una Entidad de Gestión de Movilidad, MME, un mensaje de Transferencia Requerida desde una Estación Base BS;

derivar (502), por la MME, una clave de un Equipamiento de Usuario, UE, en una Red de Acceso por Radio Terrestre Universal, UTRAN, de acuerdo con una Función de Derivación de Clave, KDF, una clave raíz, y un valor COUNT de enlace descendente de Estrato Sin Acceso, NAS;

enviar (505), mediante la MME, el valor COUNT de enlace descendente de NAS actual al UE;

añadir (506), mediante la MME, un cierto valor al valor COUNT de enlace descendente de NAS actual.

10.- El método según la reivindicación 9, en la que la derivación (502), por la MME, de una clave de un Equipamiento de Usuario, UE, en una Red de Acceso por Radio Terrestre Universal, UTRAN, de acuerdo con una Función de Derivación de Clave, KDF, una clave raíz, y un valor COUNT de enlace descendente de Estrato Sin Acceso, NAS, actual comprende:

derivar (502), mediante la MME, la clave del UE en la UTRAN de acuerdo con la KDF, la clave raíz, y el valor COUNT de enlace descendente de NAS actual en un contexto de seguridad actual.

11.- El método según la reivindicación 9, o la reivindicación 10, en el que el cierto valor es 1.

12.- El método según la reivindicación 9, en el que el envío, mediante la MME, del valor COUNT de enlace descendente de NAS al UE comprende:

enviar, mediante la MME, un mensaje de Comando de Transferencia que lleva el valor COUNT de enlace descendente de NAS al UE.

13.- El método según la reivindicación 9, en el que el envío, mediante la MME, del valor COUNT de enlace descendente de NAS actual al UE comprende:

enviar, mediante la MME, los cuatro bits menos significativos del valor COUNT de enlace descendente de NAS actual al UE.

14.- Un método de derivación de clave, que comprende:

recibir (507) por un Equipamiento de Usuario, UE, un valor COUNT de enlace descendente de Estrato Sin Acceso, NAS, desde una Entidad de Gestión de Movilidad, MME, en un primer proceso de transferencia; y

derivar (507), por el UE, una clave del UE en una Red de Acceso por Radio Terrestre Universal, UTRAN, de acuerdo con una Función de Derivación de Clave, KDF, una clave raíz, y un valor COUNT de enlace descendente de NAS actual en el primer proceso de transferencia;

recibir por el UE, un nuevo valor COUNT de enlace descendente de NAS obtenido por la MME añadiendo un cierto valor al valor COUNT de enlace descendente de NAS actual en un segundo proceso de transferencia.

15.- El método según la reivindicación 14, en el que el cierto valor es 1.

16.- El método según la reivindicación 14, en el que la recepción, por el UE de un valor COUNT de enlace descendente de Estrato Sin Acceso, NAS, actual comprende: recibir, por el UE un mensaje de Comando de Transferencia enviado por la MME, en el que el mensaje de Comando de Transferencia comprende el valor COUNT de enlace descendente de Estrato Sin Acceso, NAS.

17.- Una Entidad de Gestión de Movilidad, MME, que comprende:

una unidad receptora de transferencia, configurada para recibir un mensaje de Transferencia Requerida desde una Estación Base, BS;

una segunda unidad de derivación (32), configurada para derivar una clave de un Equipamiento de Usuario, UE, en una Red de Acceso por Radio Terrestre Universal, UTRAN, de acuerdo con una Función de Derivación de Clave (KDF), una clave raíz, y un valor COUNT de enlace descendente de NAS;

una unidad de envío de transferencia (33), configurada para enviar el valor COUNT de enlace descendente de NAS

actual al UE; y

una unidad de obtención de valor de cómputo (31), configurada para añadir un cierto valor al valor COUNT de enlace descendente de NAS actual.

18.- La MME según la reivindicación 17, en la que el cierto valor es 1.

19.- La MME según la reivindicación 17, en la que la unidad de envío de transferencia (33) está configurada para enviar un mensaje de Comando de Transferencia que lleva el valor COUNT de enlace descendente de NAS al UE.

20.- Un Equipamiento De Usuario, UE, que comprende:

una segunda unidad receptora de mensaje (40) configurada para recibir un valor COUNT de enlace descendente de Estrato Sin Acceso, NAS, desde una Entidad de Gestión de Movilidad, MME, en un primer proceso de transferencia; y

una segunda unidad de derivación de clave (41) configurada para derivar una clave del UE en una Red de Acceso por Radio Terrestre Universal, UTRAN, de acuerdo con una Función de Derivación de Clave, KDF, una clave raíz, y el valor COUNT de enlace descendente de NAS actual en el mensaje de Comando de Transferencia recibido por la segunda unidad receptora de mensaje en el primer proceso de transferencia;

la segunda unidad receptora de mensaje (40), configurada para recibir un nuevo valor COUNT de enlace descendente de NAS obtenido por la MME añadiendo un cierto valor al valor COUNT de enlace descendente de NAS actual en un segundo proceso de transferencia.

21.- El UE según la reivindicación 20, en el que el cierto valor es 1.

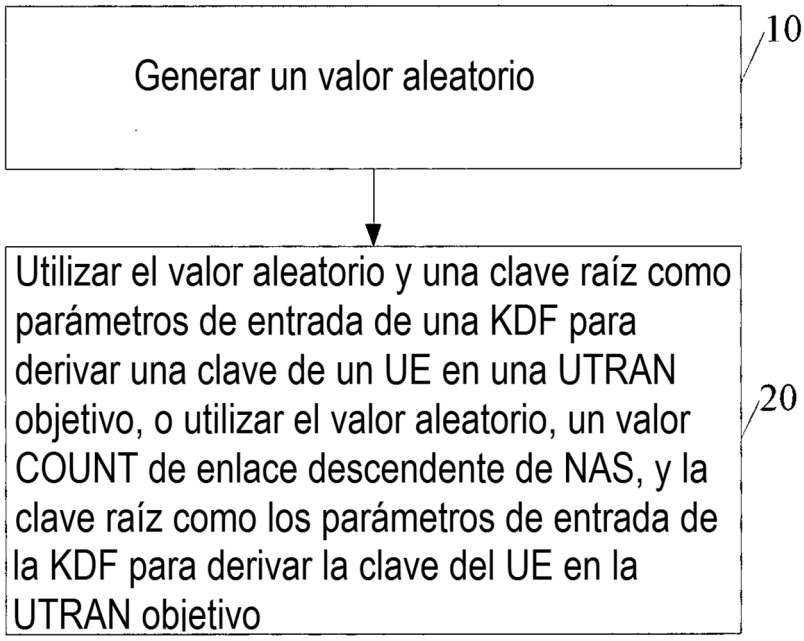
Generar un valor aleatorio
10
Utilizar el valor aleatorio y una clave raíz como parámetros de entrada de una KDF para derivar una clave de un UE en una UTRAN objetivo, o utilizar el valor aleatorio, un valor COUNT de enlace descendente de NAS, y la clave raíz como los parámetros de entrada de la KDF para derivar la clave del UE en la UTRAN objetivo
20

FIG. 1

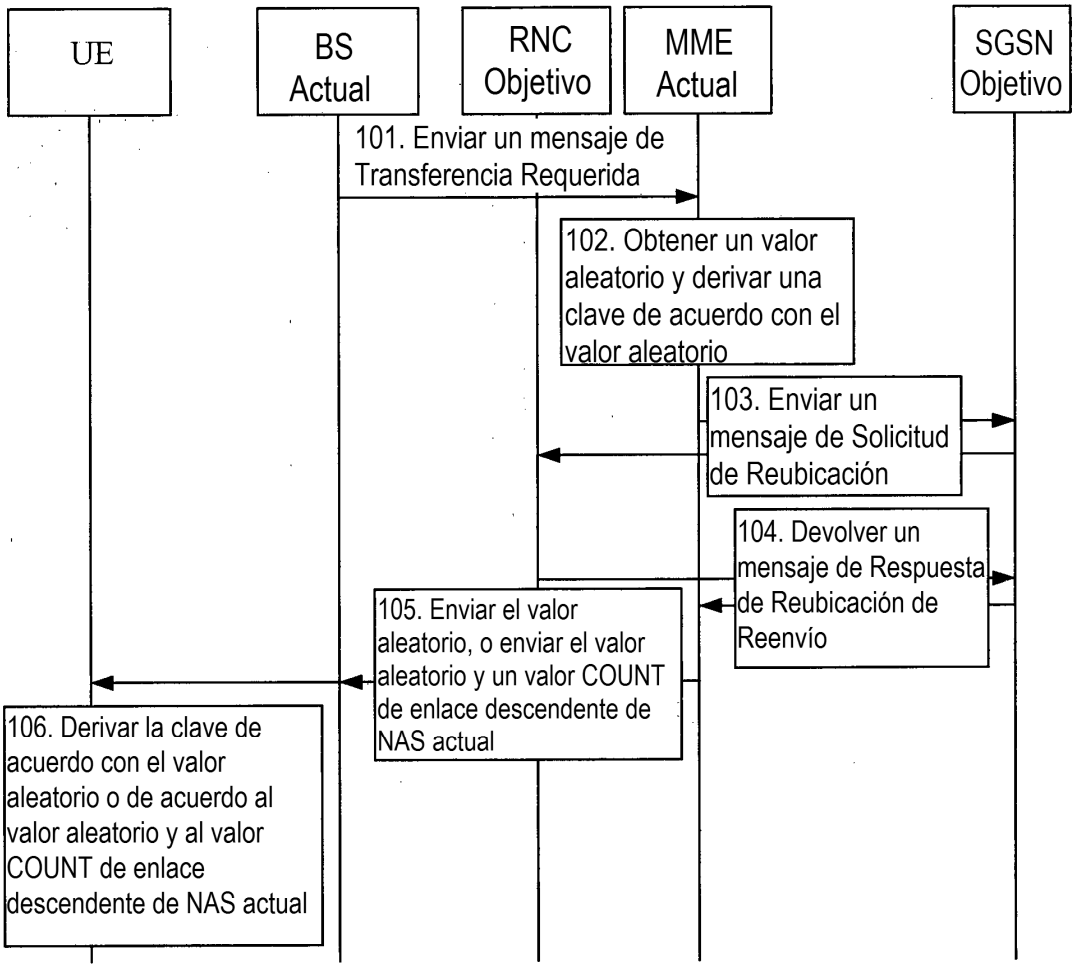
UE
BS Actual
RNC Objetivo
MME Actual
SGSN Objetivo
101. Enviar un mensaje de Transferencia Requerida
102. Obtener un valor aleatorio y derivar una clave de acuerdo con el valor aleatorio
103. Enviar un mensaje de Solicitud de Reubicación
104. Devolver un mensaje de Respuesta de Reubicación de Reenvío
105. Enviar el valor aleatorio, o enviar el valor aleatorio y un valor COUNT de enlace descendente de NAS actual
106. Derivar la clave de acuerdo con el valor aleatorio o de acuerdo al valor aleatorio y al valor COUNT de enlace descendente de NAS actual

FIG. 2

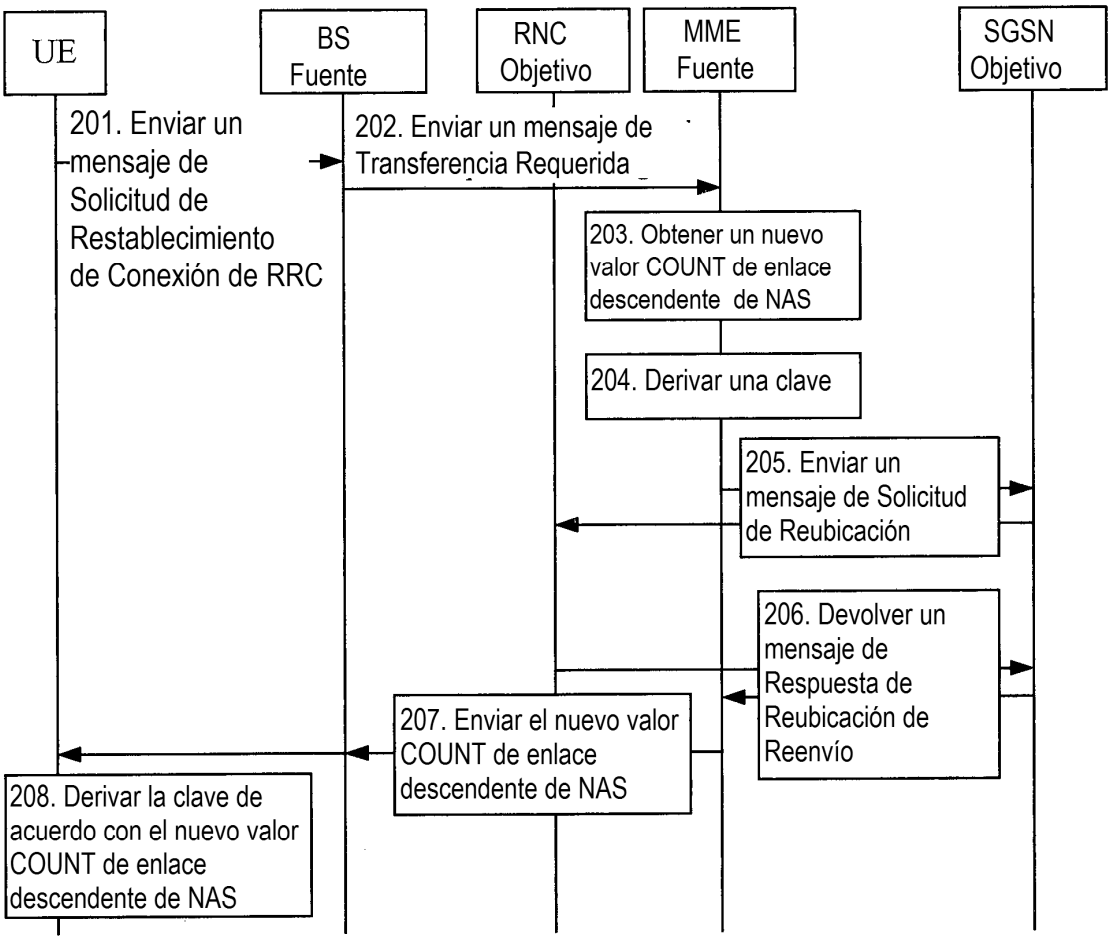
UE
BS Fuente
RNC Objetivo
MME Fuente
SGSN Objetivo
201. Enviar un mensaje de Solicitud de Restablecimiento de Conexión de RRC
202. Enviar un mensaje de Transferencia Requerida
203. Obtener un nuevo valor COUNT de enlace descendente de NAS
204. Derivar una clave
205. Enviar un mensaje de Solicitud de Reubicación
206. Devolver un mensaje de Respuesta de Reubicación de Reenvío
207. Enviar el nuevo valor COUNT de enlace descendente de NAS
208. Derivar la clave de acuerdo con el nuevo valor COUNT de enlace descendente de NAS

FIG. 3

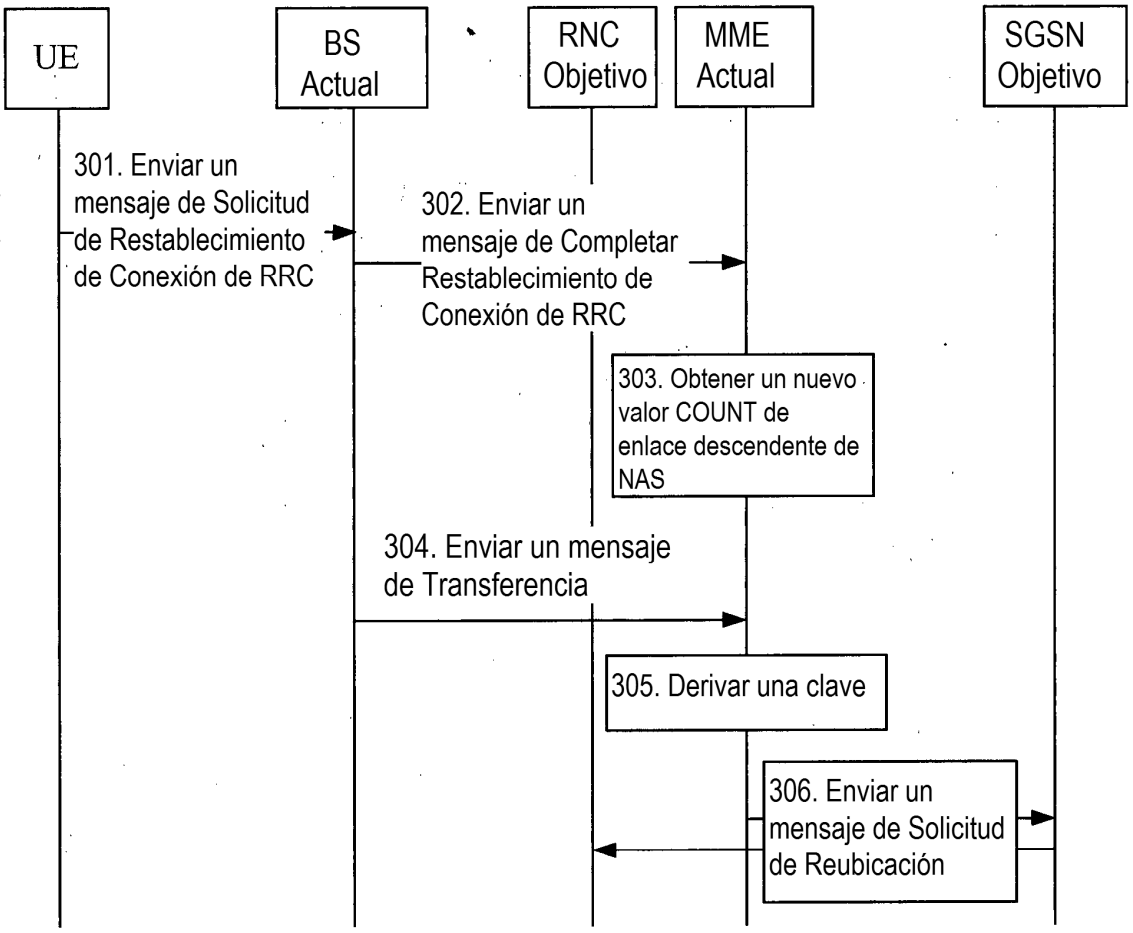
UE
BS Actual
RNC Objetivo
MME Actual
SGSN Objetivo
301. Enviar un mensaje de Solicitud de Restablecimiento de Conexión de RRC
302. Enviar un mensaje de Completar Restablecimiento de Conexión de RRC
303. Obtener un nuevo valor COUNT de enlace descendente de NAS
304. Enviar un mensaje de Transferencia
305. Derivar una clave
306. Enviar un mensaje de Solicitud de Reubicación

FIG. 4

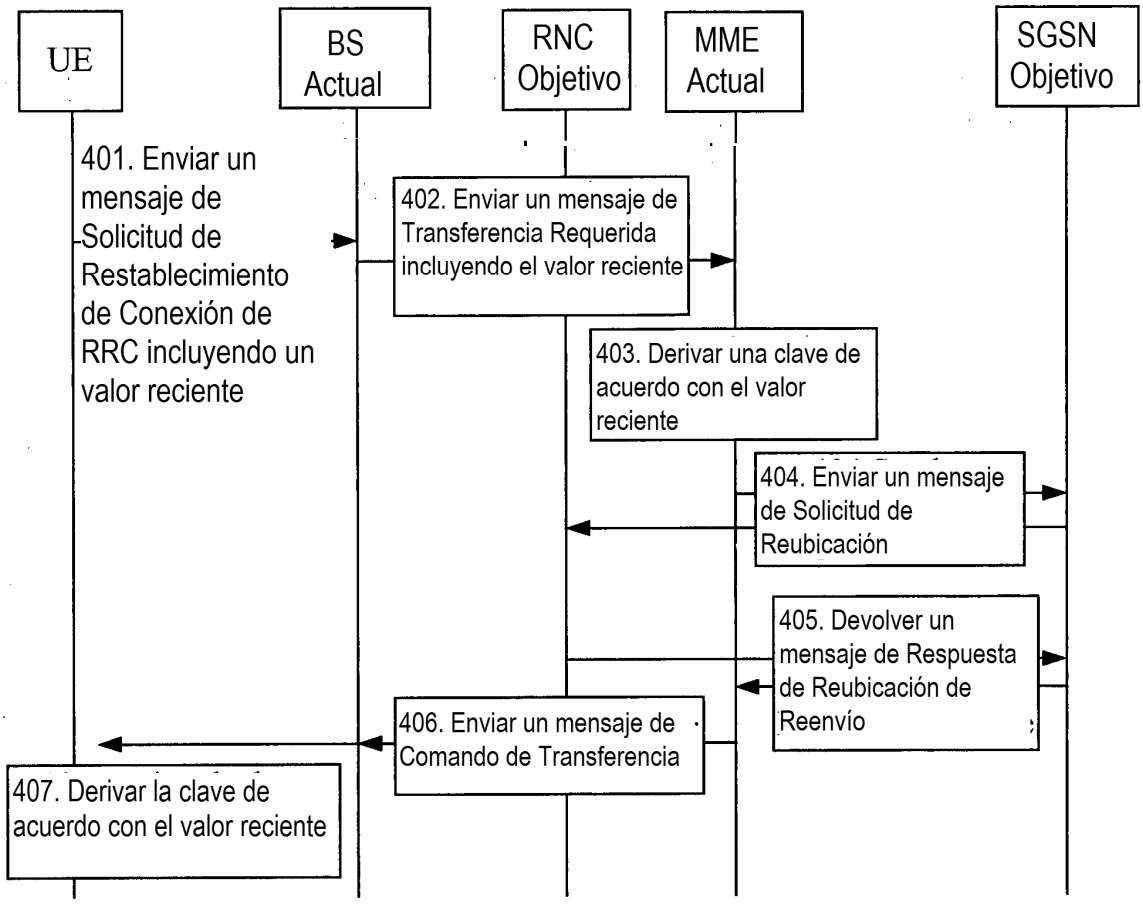
UE
BS Actual
RNC Objetivo
MME Actual
SGSN Objetivo
401. Enviar un mensaje de Solicitud de Restablecimiento de Conexión de RRC incluyendo un valor reciente
402. Enviar un mensaje de Transferencia Requerida incluyendo el valor reciente
403. Derivar una clave de acuerdo con el valor reciente
404. Enviar un mensaje de Solicitud de Reubicación
405. Devolver un mensaje de Respuesta de Reubicación de Reenvío
406. Enviar un mensaje de Comando de Transferencia
407. Derivar la clave de acuerdo con el valor reciente

FIG. 5

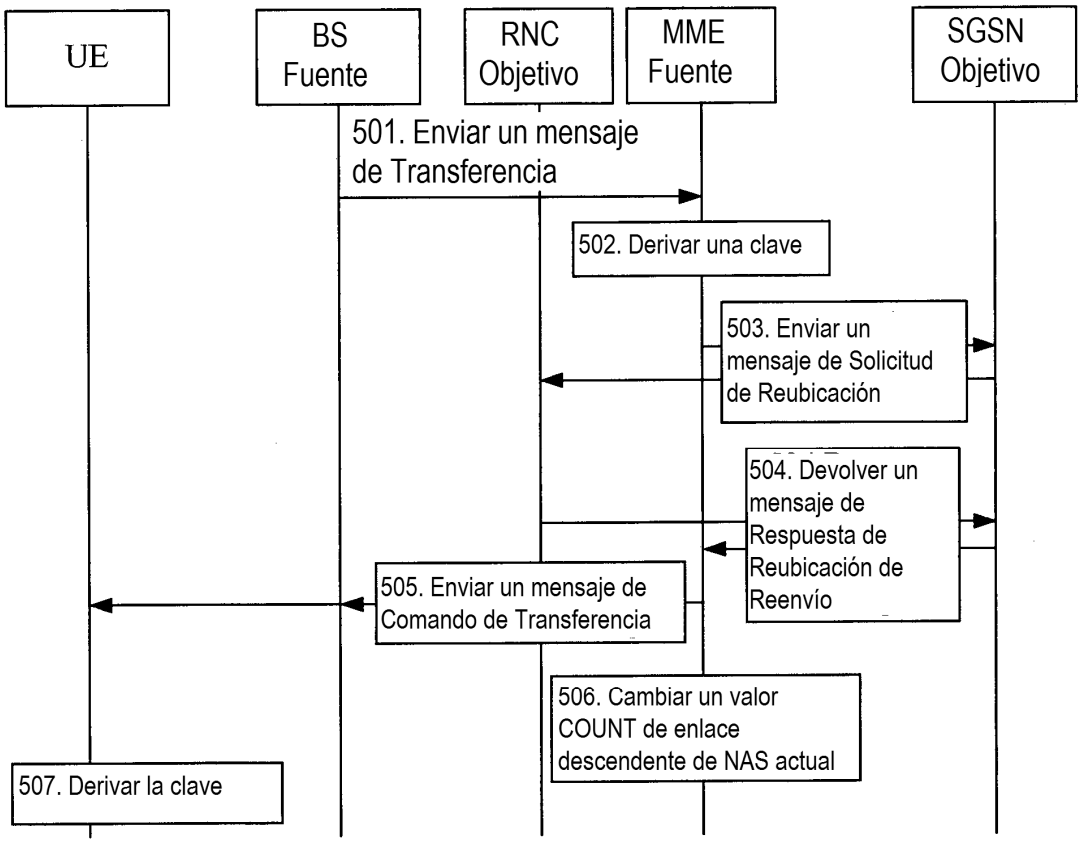
UE
BS Fuente
RNC Objetivo
MME Fuente
SGSN Objetivo
501. Enviar un mensaje de Transferencia
502. Derivar una clave
503. Enviar un mensaje de Solicitud de Reubicación
504. Devolver un mensaje de Respuesta de Reubicación de Reenvío
505. Enviar un mensaje de Comando de Transferencia
506. Cambiar un valor COUNT de enlace descendente de NAS actual
507. Derivar la clave

FIG. 6

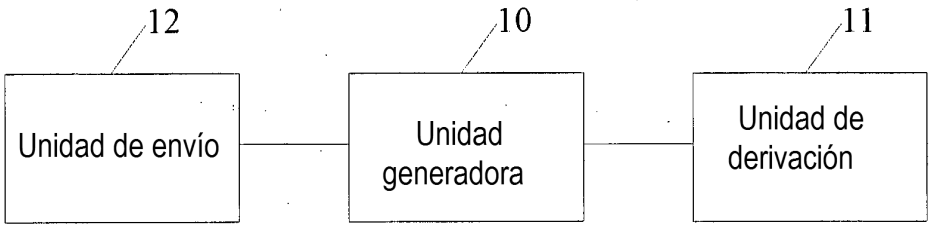

FIG. 7

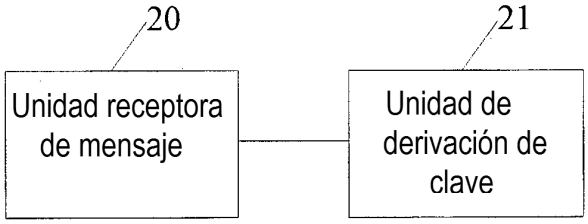

FIG. 8

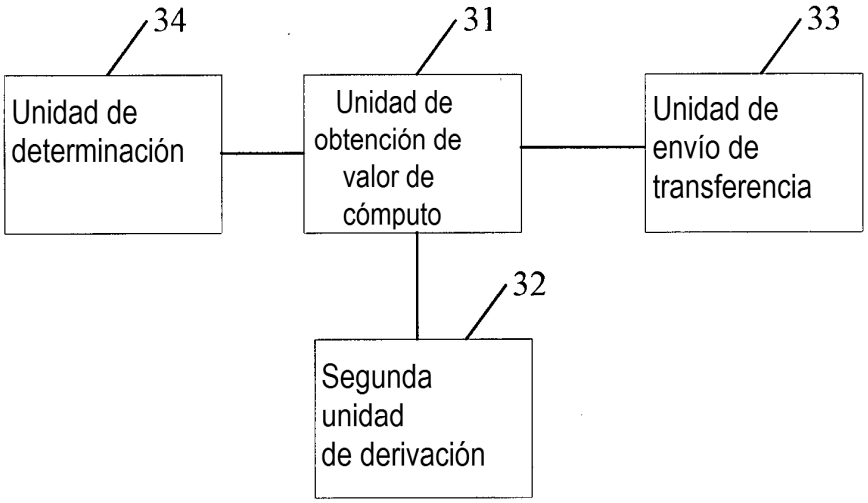

FIG. 9

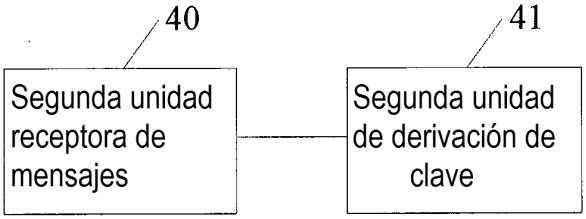

FIG. 10

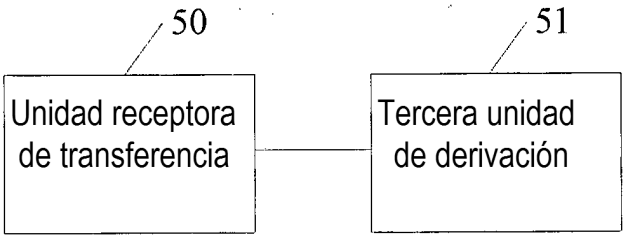

FIG. 11

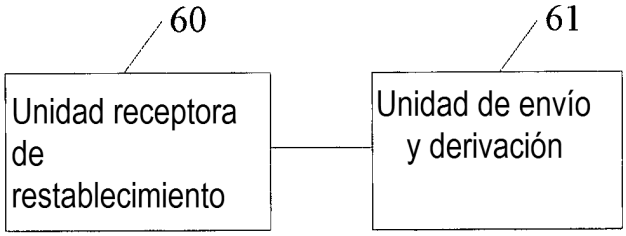

FIG. 12

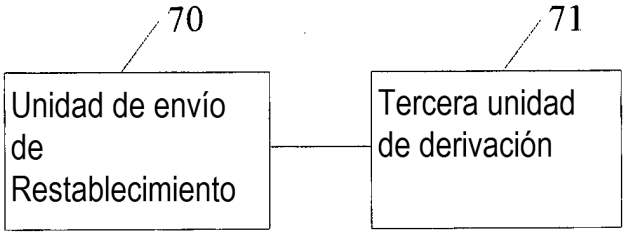

FIG. 13

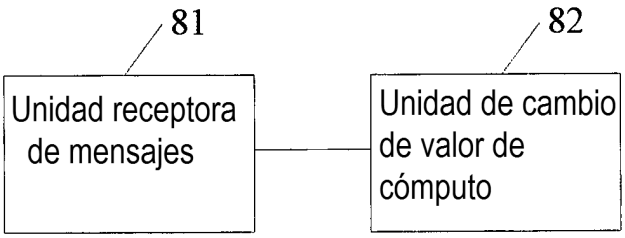

FIG. 14