(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 764 438**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04W 36/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.01.2018 PCT/EP2018/052162**

(87) Fecha y número de publicación internacional: **02.08.2018 WO18138355**

(96) Fecha de presentación y número de la solicitud europea: **29.01.2018 E 18703269 (3)**

(97) Fecha y número de publicación de la concesión europea: **25.09.2019 EP 3485669**

(54) Título: **Métodos y aparatos para reestablecer una conexión de Control de Recuso de Radio (RRC)**

(30) Prioridad:

30.01.2017 US 201762451866 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.06.2020

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

LEHTOVIRTA, VESA;
WIFVESSON, MONICA y
NAKARMI, PRAJWOL KUMAR

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Métodos y aparatos para restablecer una conexión de Control de Recuso de Radio (RRC)

Campo técnico

La invención se refiere a métodos, Equipo de Usuario, NodeB fuente, NodeB objetivo, Entidad de Gestión de Movilidad y programas informáticos para restablecer una conexión de Control de Recurso de Radio.

Antecedentes

Las optimizaciones de Internet Celular de las Cosas (CIoT) de Plano de Control (CP) (también conocida como Datos Sobre Estrato de No Acceso (NAS) (DoNAS)) es una solución para transportar datos sobre NAS según se especifica en la especificación técnica TS 23.401 V14.2.0 del Proyecto Partnership de 3ª Generación (3GPP), cláusula 5.3.4B (y otras especificaciones, p. ej., TS 24.301 V14.2.0). Las características de seguridad están especificadas en TS 33.401 V14.1.0, cláusula 8.2. El impacto de seguridad de la solución básica es muy limitado. El propósito de la característica de DoNAS es enviar datos sobre señalización de NAS sin establecer portadoras de radio de datos (DRBs) y sin establecer seguridad de Estrato de Acceso (AS). La intención es ahorrar señalización. La Fig. 1, que corresponde a la Figura 5.3.4B.2-1 de TS 23.401 V14.2.0, ilustra el principio de los DoNAS.

El artículo de trabajo contenido en el documento R3-161324 de 3GPP busca incrementos de movilidad para CIoT de CP. Los traspasos no están soportados para CIoT de CP, pero un Equipo de Usuario (UE) puede moverse en cualquier caso, causando un fallo del enlace de radio (RLF) cuando el UE está en modo conectado (es decir, tiene conexión de Control de Recurso de Radio (RRC) con un NodeB evolucionado (eNB)). Esto ha presentado el problema de qué hacer en ese caso. Puesto que la seguridad de AS no está soportada para la característica de CIoT de CP, los mecanismos existentes para RLF no pueden ser usados de forma segura como tales. En otras palabras, no es aceptable desde el punto de vista de la seguridad usar el mecanismo de gestión de RLF existente en el CIoT de CP.

La Capa de RRC está en los sistemas de LTE (Evolución de Largo Plazo) actuales, véase p. ej., 3GPP TS 36.331 V14.1.0, especificada como que incluye un elemento de información (IE) denominado ShortMAC-I que se usa para identificación del UE, por ejemplo, durante procedimientos de Restablecimiento de Conexión de RRC. El cálculo del ShortMAC-I incluye lo siguiente como entrada:

- Clave de integridad de RRC: CADENA DE BITS (TAMAÑO (128))

- Identidad de la célula objetivo: CADENA DE BITS (TAMAÑO (28))

- Identidad de célula física de la célula fuente: NÚMERO ENTERO (0, ..., 503)

- C-RNTI (Identificador Temporal de Red de Radio de la Célula) del UE en la célula fuente: CADENA DE BITS (TAMAÑO (16))

La función usada está especificada en TS 33.401 V14.1.0.

La Capa de RRC está en los sistemas de LTE especificada como que incluye un elemento de información (IE) denominado ShortResumeMAC-I que se utiliza para identificación del UE, por ejemplo, durante procedimientos de Reanudación de Conexión de RRC. El cálculo del ShortResumeMAC-I incluye lo siguiente como entrada:

- Clave de integridad de RRC: CADENA DE BITS (TAMAÑO (128))

- Identidad de la célula objetivo: CADENA DE BITS (TAMAÑO (28))

- Identidad de célula física de la célula fuente: NÚMERO ENTERO (0, ..., 503)

- C-RNTI del UE en la célula fuente: CADENA DE BITS (TAMAÑO (16))

- Constante de reanudación.

Obsérvese que el cálculo de ShortResumeMAC-I incluye adicionalmente una constante de reanudación, la cual permite la diferenciación de ShortMAC-I respecto a ResumeShortMAC-I. La función = usada está especificada en TS 33.401 V14.1.0.

Ghizlande Orhanou et al.: “EPS Confidentiality and Integrity mechanisms Algorithmic Approach”, IJCSI Diario Internacional de temas de informática, vol. 7, núm. 4, describe señalización de RRC y de NAS. También se describe una clave de integridad K_{NASint} para tráfico de NAS.

Compendio

Un objeto de la invención consiste en habilitar una señalización reducida durante el restablecimiento de una

conexión de control de recurso de radio.

Otro objeto de la invención consiste en habilitar autenticación de un eNB objetivo por parte del UE durante restablecimiento de conexión de RRC.

La invención está definida en las reivindicaciones independientes. Las características adicionales de la invención se proporcionan en las reivindicaciones dependientes. Las realizaciones y/o los ejemplos divulgados en la descripción que sigue que no estén cubiertos por las reivindicaciones anexas, se consideran que no forman parte de la presente invención, sino que constituyen ejemplos útiles para la comprensión de la invención.

Según un primer aspecto de la invención, se presenta un método para el restablecimiento de una conexión de Control de Recurso de Radio (RRC) entre un Equipo de Usuario (UE) y un NodeB evolucionado objetivo (eNB objetivo). El método se lleva a cabo por medio del UE y comprende:

recibir un mensaje de Restablecimiento de Conexión de RRC desde el eNB objetivo, incluyendo el mensaje de Restablecimiento de Conexión de RRC una señal de muestra de autenticación de enlace descendente (DL) que ha sido generada por una Entidad de Gestión de Movilidad (MME) y que ha tenido una clave de integridad de Estrato de No Acceso (NAS) como entrada, y

autenticar la señal de muestra de autenticación de DL recibida.

Con ello se consigue, inter alia, que el UE esté habilitado para autenticar un eNB durante el restablecimiento de conexión de RRC, tal como el restablecimiento de conexión de RRC para optimización de IoT de EPS CP, con la ayuda de una clave de integridad de NAS. De ese modo, no se necesita que se cree ninguna clave de Estrato de Acceso (AS), lo que es muy beneficioso, por ejemplo debido a que las claves de NAS deben ser generadas de todos modos, mientras que las claves de AS tendrían que ser generadas solamente para ser usadas en restablecimiento de conexión de RRC.

El método puede comprender también una etapa de cálculo de una señal de muestra de autenticación de enlace ascendente (UL) con la clave de integridad de NAS como entrada, y el envío de una solicitud de restablecimiento de conexión de RRC que incluya la señal de muestra de autenticación de UL, al eNB objetivo. La señal de muestra de autenticación de UL puede ser calculada, en ese caso, con una identidad de la célula objetivo como entrada. La identidad de la célula objetivo puede estar incluida, en el último caso, en la solicitud de restablecimiento de conexión de RRC. La señal de muestra de autenticación de DL puede, en una forma de realización del método, haber sido calculada por la MME con una identidad de la célula objetivo como entrada.

Un segundo aspecto se refiere a un método para el restablecimiento de una conexión de RRC entre un UE y un eNB objetivo, y se lleva a cabo por medio del eNB objetivo. El método comprende:

recibir, desde una MME, un mensaje que incluye una señal de muestra de autenticación de DL que ha sido generada por la MME, en donde la señal de muestra de autenticación de DL ha sido generada con una clave de integridad de NAS como entrada, y

enviar un mensaje de Restablecimiento de Conexión de RRC al UE, incluyendo el mensaje de Restablecimiento de Conexión de RRC la señal de muestra de autenticación de DL.

En una realización del segundo aspecto, el método comprende recibir desde el UE, una solicitud de restablecimiento de conexión de RRC que incluye una señal de muestra de autenticación de UL, en donde la señal de muestra de autenticación de UL ha sido calculada por el UE con la clave de integridad de NAS como entrada. La señal de muestra de autenticación de UL puede entonces haber sido calculada por el UE con una identidad de la célula objetivo como entrada.

En una realización del segundo aspecto, la señal de muestra de autenticación de DL ha sido calculada por la MME con una identidad de la célula objetivo como entrada.

Un tercer aspecto se refiere a un método para restablecer una conexión de RRC entre un UE y un eNB objetivo, y se lleva a cabo por medio de una MME. El método comprende:

generar una señal de muestra de autenticación de DL con una clave de integridad de NAS como entrada, y

enviar un mensaje que incluya la señal de muestra de autenticación de DL generada, al eNB objetivo.

En una realización del tercer aspecto, la generación de la señal de muestra de autenticación de DL se realiza con una identidad de la célula objetivo como entrada (adicionalmente a la clave de integridad de NAS).

El método según el tercer aspecto puede comprender:

recibir una señal de muestra de autenticación de UL desde el eNB objetivo, habiendo sido generada dicha señal de muestra de autenticación de UL por parte del UE con la clave de integridad de NAS como entrada, y

verificar la señal de muestra de autenticación de UL.

La señal de muestra de autenticación de UL puede haber sido generada por el UE con una identidad de la célula objetivo como entrada.

Un cuarto aspecto de la invención se refiere a un UE para el restablecimiento de una conexión de RRC entre el UE y un eNB objetivo. El UE comprende:

un procesador, y un producto de programa informático que almacena instrucciones que, cuando se ejecutan por medio del procesador, hacen que el UE:

reciba un mensaje de Restablecimiento de Conexión de RRC desde el eNB objetivo, incluyendo el mensaje de Restablecimiento de Conexión de RRC una señal de muestra de autenticación de DL que ha sido generada por una MME y que ha tenido una clave de integridad de NAS como entrada, y

autentique la señal de muestra de autenticación de DL recibida.

En una realización del UE, la señal de muestra de autenticación de DL ha sido calculada por la MME con una identidad de la célula objetivo como entrada.

Un quinto aspecto se refiere a un eNB objetivo para el restablecimiento de una conexión de RRC entre un UE y el eNB objetivo. El eNB objetivo comprende:

un procesador, y

un producto de programa informático que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el eNB:

reciba, desde una MME, un mensaje que incluye una señal de muestra de autenticación de DL que ha sido generada por la MME, en donde la señal de muestra de autenticación de DL ha sido generada con una clave de integridad de NAS como entrada, y

envíe un mensaje de Restablecimiento de Conexión de RRC al UE, incluyendo el mensaje de Restablecimiento de Conexión de RRC la señal de muestra de autenticación de DL.

La señal de muestra de autenticación de DL ha sido calculada, en una realización del eNB objetivo, por medio de la MME con una identidad de la célula objetivo como entrada.

Un sexto aspecto se refiere a un eNB fuente para restablecer una conexión de RRC entre un UE y un eNB objetivo. El eNB fuente comprende:

un procesador, y

un producto de programa informático que almacena instrucciones que, cuando se ejecutan por medio del procesador, hacen que el eNB fuente:

obtenga una señal de muestra de autenticación de DL que ha sido generada con una clave de integridad de Estrato de No Acceso como entrada, y

envíe un mensaje de respuesta al eNB objetivo, incluyendo el mensaje de respuesta la señal de muestra de autenticación de DL obtenida.

Un séptimo aspecto se refiere a una MME para el restablecimiento de una conexión de RRC entre un UE y un eNB objetivo. La MME comprende:

un procesador, y

un producto de programa informático que almacena instrucciones que, cuando se ejecutan por medio del procesador, hacen que la MME:

genere una señal de muestra de autenticación de DL con una clave de integridad de NAS como entrada, y

envíe un mensaje que incluye la señal de muestra de autenticación de DL generada hasta el eNB objetivo.

Un octavo aspecto se refiere a un programa informático para el restablecimiento de una conexión de RRC entre un UE y un eNB objetivo. El programa informático comprende un código de programa informático que, cuando se ejecuta en el eNB objetivo, hace que el eNB:

reciba, desde una MME, un mensaje que incluye una señal de muestra de autenticación de DL que ha sido generada por la MME, en donde la señal de muestra de autenticación de DL ha sido generada con una clave de

integridad de NAS como entrada, y

envíe un mensaje de Restablecimiento de Conexión de RRC al UE, incluyendo el mensaje de Restablecimiento de Conexión de RRC la señal de muestra de autenticación de DL.

Un noveno aspecto se refiere a un programa informático para el restablecimiento de una conexión de RRC entre un UE y un eNB objetivo. El programa informático comprende un código de programa informático que, cuando se ejecuta en una MME, provoca que la MME:

genere una señal de muestra de autenticación de DL con una clave de integridad de NAS como entrada, y

envíe un mensaje que incluye la señal de muestra de autenticación de DL generada al eNB objetivo.

En general, todos los términos usados en la lista detallada de realizaciones han de ser interpretados conforme a su significado ordinario en el campo de la técnica, a menos que se defina explícitamente otra cosa en la presente descripción. Todas las referencias a “un/uno/el elemento, aparato, componente, medio, etapa, etc.”, han de ser interpretados abiertamente como referidos a al menos una instancia del elemento, aparato, componente, medio, etapa, etc., a menos que se defina explícitamente otra cosa. Las etapas de cualquiera de los métodos descritos en la presente memoria no tienen que ser realizadas en el orden exacto que se describe, a menos que se defina así explícitamente.

Breve descripción de los dibujos

Ahora se va a describir la invención, a título de ejemplo, con referencia a los dibujos que se acompañan, en los que:

La Figura 1 muestra esquemáticamente señalización del principio de DoNAS;

La Figura 2 ilustra esquemáticamente un entorno en el que pueden ser aplicadas las realizaciones presentadas en la presente descripción;

La Figura 3a muestra esquemáticamente señalización conforme a una parte de una realización presentada en la presente descripción;

La Figura 3b muestra esquemáticamente señalización conforme a una parte de una realización presentada en la presente descripción y que se inicia en la Figura 3a;

Loa Figura 4a muestra esquemáticamente señalización conforme a una parte de una realización presentada en la presente descripción;

La Figura 4b muestra esquemáticamente señalización conforme a una parte de una realización presentada en la presente descripción y que se inicia en la Figura 4a;

La Figura 5 muestra esquemáticamente señalización conforme a una realización presentada en la presente memoria;

La Figura 6 muestra esquemáticamente señalización conforme a una realización presentada en la presente descripción;

Las Figuras 7A-7D son diagramas de flujo que ilustran métodos conforme a realizaciones presentadas en la presente descripción;

Las Figuras 8-11 son diagramas esquemáticos que ilustran algunos componentes de entidades presentadas en la presente memoria, y

Las Figuras 12-15 son diagramas esquemáticos que muestran módulos funcionales de realizaciones presentadas en la presente descripción.

Descripción detallada

Ahora se va a describir la invención de forma más detallada en lo que sigue, con referencia a los dibujos que se acompañan, en los que se han mostrado algunas realizaciones de la invención. Esta invención puede ser materializada, sin embargo, de muchas formas diferentes y no debe ser entendida como limitada a las realizaciones que se exponen en la presente descripción, por el contrario, estas realizaciones se proporcionan a título de ejemplo de modo que esta descripción sea rigurosa y completa, y pueda transmitir por completo el alcance de la invención a los expertos en la materia. Los números iguales se refieren a elementos iguales a través de la descripción.

El restablecimiento de conexión de Control de Recurso de Radio (RRC) y los procedimientos de suspensión/reanudación de conexión de RRC son soluciones existentes, que podrían ser candidatos para gestionar un fallo de radio enlace en caso de un caso de optimización Internet Celular de las Cosas (CIoT) de Plano de Control (CP). Ambas soluciones existentes citadas usan una señal de muestra de autenticación del Equipo de Usuario (UE)

según se ha descrito en los antecedentes, para mostrar a un NodeB evolucionado (eNB) que un UE 1 genuino desea restablecer o reanudar una conexión de RRC. Adicionalmente, se usan mensajes de RRC protegidos en cuanto a integridad en la dirección de enlace descendente (DL) para mostrar al UE 1 que éste se encuentra conectado a un eNB genuino. Sin embargo, esas soluciones están basadas en la existencia de seguridad de Estrato de Acceso (AS) (especialmente, seguridad de RRC), pero la seguridad de AS y la seguridad de RRC no existen o no se usan para las optimizaciones de CIoT de CP. Por lo tanto, el restablecimiento de conexión de RRC y los procedimientos de suspensión/reanudación de conexión de RRC como tales, no son aceptables en cuanto a seguridad para ser usados en la gestión de movilidad en el CIoT de CP.

Una solución descrita en S3-161717 de contribución de 3GPP propone que una señal de muestra de autenticación podría estar basada en una nueva clave de integridad de RRC (denominada KeNB-RRC) que puede ser deducida tanto por el UE 1 como por la Entidad 4 de Gestión de Movilidad (MME), sin establecer seguridad de AS (incluyendo seguridad de RRC) entre el UE 1 y el eNB 2 fuente a través de un procedimiento de Comando de Modo de Seguridad (SMC) de AS , y la señal de muestra podría ser usada entre el UE 1 y el eNB 3 objetivo. Sin embargo, la solución descrita en S3-161717 de contribución de 3GPP está intentando resolver el problema de cómo mostrar al eNB que un UE 1 genuino desea restablecer una conexión de RRC. El problema de cómo mostrar al UE 1 que está conectado a un eNB genuino, no está contemplado.

En ausencia de seguridad de AS, y por consiguiente la ausencia de protección de integridad de mensajes de RRC de DL desde el eNB hasta el UE, en el contexto de movilidad de CIoT de CP, no existe actualmente ninguna manera de mostrar al UE que está conectado a un eNB genuino. Para mitigar ese problema, se ha presentado el uso de una señal de muestra de autenticación en la dirección de DL desde la red hasta el UE. La señal de muestra de autenticación puede ser generada y enviada por la MME, por el eNB fuente o por el eNB objetivo. La señal de muestra de autenticación de DL puede ser calculada usando las claves de NAS o de AS (aunque esto último no está dentro del alcance de las reivindicaciones la presente solicitud), dependiendo de la entidad que la esté enviando. Se han identificado los casos siguientes:

Una señal de muestra de autenticación de DL se envía siempre al UE a través del eNB objetivo.

Las cuatro variantes de soluciones que siguen muestran cómo se puede conseguir esto.

1a. La señal de muestra de autenticación de DL se envía desde el eNB fuente a través del eNB objetivo hasta el UE y se comprueba por medio del UE con una clave de AS. Alternativamente, el eNB objetivo calcula la señal de muestra con claves de KrrC_int recibidas desde el eNB fuente. Esta variante no está dentro del alcance de las reivindicaciones de la presente solicitud.

1b. La señal de muestra de autenticación de DL se envía desde la MME a través del eNB fuente y del eNB objetivo, hasta el UE y se comprueba por medio del UE con una clave de NAS.

2a. La señal de muestra de autenticación de DL se envía desde la MME en un mensaje de Acuse de Recibo de Conmutación de Ruta a través del eNB objetivo hasta el UE, y el UE comprueba la señal de muestra de autenticación de DL con una clave de NAS.

2b. La señal de muestra de autenticación de DL se envía desde la MME en un nuevo mensaje a través del eNB objetivo hasta el UE y el UE comprueba la señal de muestra con una clave de NAS.

Cuando una comprobación realizada por el UE que está conectado a un eNB genuino esté basada en una señal de muestra de autenticación de DL, no existe ninguna necesidad de establecer claves de AS en absoluto. Con ello, se puede evitar la generación de claves de AS, lo que resulta beneficioso, puesto que las claves de AS podrían, en su caso, tener que ser generadas solamente a los efectos del restablecimiento de la conexión de RRC y no ser usadas para nada más. Las claves de NAS podrían sin embargo ser utilizables para otros problemas de seguridad distintos de autenticar solamente el eNB. De manera más precisa, las claves de NAS han sido creadas en cualquier caso, puesto que existe un contexto de seguridad de NAS para un UE que envía datos a través de la NAS.

Cuando el UE experimenta un fallo de enlace de radio (RLF) durante una conexión de CIoT de CP (DoNAS), el UE trata de restablecer la conexión de RRC con otro eNB, véase la Figura 2.

La señal de muestra de autenticación de la red para su uso en CIoT de CP (indicada como MAC CIoT DL) es una señal de muestra que podrá ser usada para autenticación de la red, es decir, para mostrar al UE 1 que está conectado a un eNB 3 objetivo genuino.

La MAC CIoT DL puede, según aspectos de la invención reivindicada, ser calculada con lo siguiente como entrada:

- Clave de integridad de NAS (NAS-int., p. ej., K_{NASint}). En otras variantes, aunque no se reivindican en esta solicitud, también puede ser una clave de integridad de AS o una clave deducida a partir de la clave de NAS-int o de integridad de AS (Krrc_int) o una clave deducida a partir de una cualquiera de esas claves. NAS-int está indicada, en muchas instancias a través del texto que sigue, como Key-MAC CIoT DL. El uso de una clave de NAS o de AS depende de si MAC CIoT DL es calculada por la MME 4 o por un eNB. Tras claves alternativas fuera del alcance de

las reivindicaciones de la presente solicitud, son claves raíz para el NAS-int, p. ej., KASME en LTE y KAUSF, KSEAF y KAMF en sistemas de Nueva Radio.

- Identidad de la célula objetivo (ID de célula)

- Identidad de célula física de la célula fuente

- C-RNTI del UE en la célula fuente.

- constante (la constante permite la diferenciación de MAC CIoT de la ShortResumeMAC-I y de la ShortMAC-I o una MAC definida de otras formas).

- posiblemente una entrada al cálculo de MAC CIoT DL es una señal de muestra de autenticación de enlace ascendente, UL, denominada en la presente como MAC CIoT UL (enlace ascendente).

- un parámetro de refresco.

La entrada usada para el cálculo de la MAC CIoT DL será indicada como Input-MAC CIoT DL. La identidad de la célula objetivo puede, de ese modo, formar parte de la Input-MAC CIoT DL, pero la clave de integridad de NAS puede estar separada de la Input-MAC-CIoT DL recibida por el UE, dado que típicamente éste tiene ya la clave de integridad de NAS y ha usado la misma para el cálculo de la MAC CIoT UL.

La función usada para el cálculo de la MAC CIoT DL (indicada como Fun-MAC CIoT DL) puede ser la misma usada en el Anexo B.2 de TS 33.401 para restablecimiento de RRC y reanudación de RRC, es decir, un algoritmo de integridad en forma de un algoritmo de integridad NAS de 128 bits, el cual puede ser 128-EIA1, 128-EIA2 y 128-EIA3.

La variante 1a ha sido ilustrada en las Figuras 3a y 3b, en donde MAC CIoT DL se envía desde el eNB fuente y se comprueba por medio del UE con una clave de AS (no comprendida dentro del alcance de las reivindicaciones de la solicitud) o mediante una clave de NAS.

Esta variante está basada en una negociación de algoritmo de AS a través del protocolo de NAS y la posterior comprobación de la señal de muestra de enlace ascendente denominada MAC CIoT UL en el eNB fuente. La variante comprende un mecanismo donde el eNB fuente, tras haber comprobado la MAC CIoT UL, genera una señal de muestra de enlace descendente denominada MAC CIoT DL. El eNB fuente envía la MAC CIoT DL al eNB objetivo en un mensaje de respuesta de contexto de UE X2. El eNB objetivo envía la MAC CIoT DL además al UE en un mensaje de RRC para comprobación de autenticación. Si la comprobación de la MAC CIoT DL tiene éxito, el UE sabe que está conectado a un eNB auténtico, y no a un eNB falso.

Las etapas 1 a 15 están definidas en las especificaciones de 3GPP actuales. El UE establece una conexión de RRC y envía datos a través de NAS, los cuales son reenviados desde MME a Puerta de Acceso de Servidor (S-GW)/Puerta de Acceso de Red de Datos por Paquetes (P-GW). En la etapa 15 ocurre un RLF. El RLF también puede ocurrir antes de que el UE haya recibido datos de DL.

Etapa 16. El UE inicia una conexión de RRC enviando un mensaje de Acceso Aleatorio a un eNB objetivo.

Etapa 17. El eNB objetivo responde con una Respuesta de Acceso Aleatorio al UE.

Etapa 18. El UE genera una señal de muestra de autenticación, MAC CIoT UL. La señal de muestra puede ser calculada de la forma siguiente: señal de muestra = f(PCI fuente, C-RNTI fuente, ID de Célula objetivo, clave de NAS, entrada de repetición), donde la clave de NAS es la actual clave de integridad de NAS, p. ej. K_{NASint}, o es un derivado de la misma. f = función. Sin embargo, con respecto a esta variante 1a particular, la señal de muestra podría en cambio ser deducida por medio de una clave de AS en vez de la clave de NAS. La clave de AS puede ser una clave de integridad de AS, tal como K_{RRCint}.

Etapa 19. El UE envía un mensaje de restablecimiento de conexión de RRC al eNB objetivo, p. ej., para optimización de EPS (Sistema de Paquetes Evolucionado) de IoT de CP. El mensaje incluye la MAC CIoT UL.

Etapa 20. El eNB objetivo envía un mensaje de solicitud de contexto de UE X2 al eNB fuente. El mensaje incluye la MAC CIoT UL.

Etapa 21. El eNB fuente comprueba si la MAC CIoT UL es auténtica.

Etapa 22. Si la autenticación tiene éxito, el eNB fuente genera MAC CIoT DL según se ha descrito con anterioridad usando Input-MAC CIoT DL y la Key-MAC CIoT DL, y el procesamiento continúa en la etapa 23. Si la autenticación falla, el eNB fuente envía una respuesta de contexto de UE X2 indicando el fallo. El fallo activará el eNB objetivo para que libere la conexión de RRC (no representada).

Etapa 23. El eNB fuente envía una respuesta de contexto de UE X2 al eNB objetivo. El mensaje incluye la MAC

CIoT DL. El mensaje puede incluir además Input-MAC CIoT DL.

Etapa 24. El eNB objetivo envía un mensaje de restablecimiento de conexión de RRC al UE. El mensaje incluye la MAC CIoT DL. El mensaje puede incluir además Input-MAC CIoT DL.

Etapa 25. Tras la recepción del mensaje de restablecimiento de conexión de RRC, el UE autentica la MAC CIoT DL usando Input-MAC CIoT DL y la Key-MAC CIoT DL según se ha descrito con anterioridad.

Etapa 26A. Si la autenticación de MAC CIoT DL tiene éxito:

26A.1 El UE envía un mensaje de Restablecimiento de Conexión de RRC Completado, que opcionalmente contiende PDU de datos NAS, al eNB objetivo.

26A.2-26A.5. Estas etapas son procedimientos normales de conmutación de ruta y de modificación de portadora.

26A.6. El eNB objetivo dice ahora al eNB fuente que libere el contexto de UE enviando un mansaje X2 denominado Liberación de Contexto de UE.

Si la autenticación de la MAC CIoT DL de la etapa 25 falla, el UE puede realizar acciones tales como no enviar mensajes adicionales o hacer transición al modo RRC_CONNECTED para autenticar la red, etc.

La variante 1b ha sido ilustrada en las Figuras 4a-4b, en donde la MAC CIoT DL se envía desde la MME hasta el eNB fuente y desde el eNB fuente hasta el eNB objetivo y desde el eNB objetivo hasta el UE y a continuación se comprueba por medio del UE con una clave de NAS.

Éste es un ejemplo aplicable a una situación en la que ocurra un RLF, p. ej., durante el envío de datos NAS para optimizaciones de CIoT de CP.

Las etapas 1 a 18 son según están definidas en las especificaciones actuales de 3GPP.

Etapa 19. El UE envía un mensaje de RRC al eNB objetivo que incluye la MAC CIoT UL. El mensaje de RRC puede ser una solicitud de restablecimiento de conexión de RRC, una solicitud de reanudación de RRC o algún otro mensaje de RRC.

Etapa 20. El eNB objetivo envía un mensaje X2 al eNB fuente que incluye la MAC CIoT UL. El mensaje X2 puede ser un mensaje de extracción de contexto X2.

Etapa 21. El eNB fuente envía un mensaje S1 a la MME que incluye la MAC CIoT UL y la Input-MAC CIoT UL.

Etapa 22. Tras la recepción de la MAC CIoT UL y de la Input-MAC CIoT UL, la MME verifica la MAC CIoT UL llevando a cabo el mismo cálculo que realizó el UE, y comparándola con la MAC CIoT UL recibida. Si la verificación tiene éxito, la MME genera MAC CIoT DL según se ha descrito con anterioridad, usando la Input-MAC CIoT DL y la Key-MAC CIoT DL y continúa el procesamiento en la etapa 23, en donde la MME envía un mensaje S1 indicando el éxito al eNB fuente y que incluye la MAC CIoT DL. Si la verificación no ha tenido éxito, la MME envía un mensaje S1 indicando el error al eNB fuente. El eNB fuente envía a continuación una respuesta de contexto de UE X2 indicando el fallo. El fallo activará el eNB objetivo para liberar la conexión de RRC (no representada).

Etapa 23. La MME envía un mensaje de respuesta de Comprobación S1 al eNB fuente indicando el éxito. El mensaje incluye la MAC CIoT DL. El mensaje puede incluir además Input-MAC CIoT DL.

Etapa 24. El eNB fuente envía una respuesta de contexto de UE al eNB objetivo. El mensaje incluye la MAC CIoT DL. El mensaje puede incluir además Input-MAC CIoT DL.

Etapa 25. El eNB objetivo envía un mensaje de restablecimiento de conexión de RRC al UE. El mensaje incluye la MAC CIoT DL. El mensaje puede incluir además Input-MAC CIoT DL.

Etapa 26. Tras la recepción del mensaje de restablecimiento de conexión de RRC, el UE autentica la MAC CIoT DL usando Input-MAC CIoT DL y la Key-MAC CIoT DL según se ha descrito con anterioridad.

Etapa 27A. Si la autenticación de la MAC CIoT DL ha tenido éxito:

27A.1. El UE envía un mensaje de Restablecimiento de Conexión de RRC Completado, que opcionalmente contiene PDU de datos NAS, al eNB objetivo.

27A.2-27A.5. Estas etapas son procedimientos normales de conmutación de ruta y de modificación de portadora.

27A.6. El eNB objetivo dice ahora al eNB fuente que libere el contexto de UE enviando un mensaje X2 denominado Liberación de Contexto de UE.

Si la autenticación de la MAC CIoT DL en la etapa 25 falla, entonces el UE puede realizar acciones tales como no

enviar mensajes adicionales o hacer transición al modo RRC_CONNECTED para autenticar la red, etc.

La variante 2a ha sido ilustrada en la Figura 5, en donde la MAC CIoT DL se envía desde la MME al eNB objetivo en un mensaje de Acuse de Recibo de Solicitud de Conmutación de Ruta S1AP. La MAC CIoT DL se envía desde el eNB objetivo hasta el UE.

Esta variante se basa en un mensaje S1AP existente denominado Acuse de Recibo de Solicitud de Conmutación de Ruta que se envía desde la MME hasta el eNB objetivo. El Acuse de Recibo de Solicitud de Conmutación de Ruta se modifica para que sea capaz de portar la MAC CIoT DL y la Input-MAC CIoT DL. Resultará obvio para los expertos en la materia que el orden de las etapas, los mensajes y los campos podrá ser alterado; los mensajes combinados; los campos situados en diferentes mensajes, etc., para conseguir el mismo efecto.

Las etapas 1-17 son las mismas que las descritas con anterioridad en relación con la Figura 3a.

Las etapas 18-19 son también iguales que las descritas con anterioridad en relación con la Figura 3a, pero éstas se han mostrado también en la Figura 5 para la integridad del procedimiento de Restablecimiento de Conexión de RRC.

Etapa 20. El eNB objetivo solicita al eNB fuente que envíe el contexto del UE. Un mensaje X2 existente denominado Recuperar Solicitud de Contexto de UE puede ser adaptado según sea necesario (p. ej., usando ReestabUE-Identity en vez de ResumeIdentity).

Etapa 21. El eNB fuente envía el contexto del UE al eNB objetivo. Un mensaje X2 existente denominado Recuperar Respuesta de Contexto de UE puede ser adaptado según sea necesario.

Etapa 22. El eNB objetivo envía un mensaje de Restablecimiento de Conexión de RRC al UE.

Etapa 23. El UE envía un mensaje de Restablecimiento de Conexión de RRC Completado, que opcionalmente contiene PDU (Unidad de Datos de Protocolo) de datos NAS, al eNB objetivo.

Etapa 24. El eNB objetivo envía una Solicitud de Conmutación de Ruta a la MME. En la Solicitud de Conmutación de Ruta, el eNB objetivo incluye MAC CIoT UL e Input-MAC CIoT UL. Según se ha comentado con anterioridad, la Input-MAC CIoT UL puede incluir la identidad de la célula objetivo. El eNB objetivo recibió la MAC CIoT UL en la Etapa 19. La Input-MAC CIoT UL puede incluir información que el eNB objetivo recibió en la etapa 19 y/o en la etapa 21, y/o información propia del eNB objetivo. La Solicitud de Conmutación de Ruta puede contener la información del UE que permite que la MME identifique el contexto del UE en la MME. Esa información del UE se denomina en la actualidad “ID de MME UE S1AP Fuente”, que el eNB objetivo está capacitado para proporcionar por el eNB a partir de la información que éste recibió en la etapa 23.

Etapa 25. La MME autentica la MAC CIoT UL, p. ej., usando la Input-MAC CIoT UL y la Key-MAC CIoT UL como entrada a la Fun-MAC CIoT UL. La Key-MAC CIoT UL es, una realización, igual que la Key-MAC CIoT DL, es decir, la clave de integridad de NAS que puede ser deducida separadamente por la MME y por el UE, respectivamente, en base a KASME, como conocen los expertos en la materia.

En lo que sigue, por motivos de simplicidad, solamente se van a describir con detalle las etapas relevantes para la presente solución, las cuales son, en caso de que la autenticación en la etapa 25 tenga éxito:

Etapa 26. La MME genera MAC CIoT DL según se ha descrito con anterioridad, usando la Input-MAC CIoT DL y la Key-MAC CIoT DL. Algunos elementos de la Input-MAC CIoT DL, al igual que la identificad de la célula (ID de célula) objetivo, pueden ser obtenidos a partir de la Input-MAC CIoT UL.

Etapa 27. La MME envía un mensaje S1, mensaje de Acuse de Recibo de Solicitud de Conmutación de Ruta, indicando éxito al eNB objetivo, y el mensaje de Acuse de Recibo de Solicitud de Conmutación de Ruta está adaptado para que incluya MAC CIoT DL e Input-MAC CIoT DL.

Etapa 28. El eNB objetivo sabe ahora que la MAC CIoT UL enviada por el UE y mencionada en etapas anteriores, es auténtica. El eNB objetivo envía la MAC CIoT DL y la Input-MAC CIoT DL al UE en un mensaje de RRC, por ejemplo poniéndolas en el campo de DedicatedInfoNAS del mensaje de DLInformationTransfer del procedimiento de Transferencia de Información de DL de RRC. Se puede introducir también una nueva clase de procedimiento de RRC para este propósito particular de transporte de la MAC CIoT DL hasta el UE, p. ej., Confirmación de Restablecimiento de RRC.

Etapa 29. El UE autentica la MAC CIoT DL usando la Input-MAC CIoT DL y la Key-MAC CIoT DL como entrada a la Fun-MAC CIoT DL.

Si la autenticación de la MAC CIoT DL en la etapa 27 falla, entonces el UE puede realizar acciones tales como no enviar mensajes adicionales o hacer transición al modo de RRC_CONNECTED para autenticar la red, etc.

La variante 2b ha sido ilustrada en la Figura 6, en donde la MAC CIoT DL se envía desde la MME hasta el eNB objetivo en un nuevo mensaje S1AP y desde el eNB objetivo hasta el UE.

Esta variante se basa en un nuevo mensaje S1AP (indicado como Comprobar Solicitud de MAC) que se envía desde el eNB objetivo hasta la MME. El mensaje de Comprobar Solicitud de MAC está capacitado para transportar la MAC CIoT UL y la Input-MAC CIoT UL. De forma similar, nuevos mensajes S1AP, indicados como Comprobar Acuse de Recibo de MAC y Comprobar Fallo de MAC, que se envían desde la MME hasta el eNB objetivo, son usados para indicar respectivamente que la MAC CIoT UL era auténtica o no era auténtica. El nuevo mensaje S1AP de Comprobar Acuse de Recibo de MAC porta la MAC CIoT DL y la Input-MAC CIoT DL desde la MME hasta el eNB objetivo. El eNB objetivo incluye la MAC CIoT DL y la Input-MAC CIoT DL para el UE en un mensaje de Restablecimiento de Conexión de RRC. Resultará obvio para un experto en la materia apreciar que el orden de las etapas, ,mensajes, campos, podrá ser alterado; los mensajes combinados; los campos situados en diferentes mensajes, etc., para conseguir los mismos efectos.

Las etapas 1-17 son iguales que las discutidas con anterioridad en relación con la Figura 3.

Las etapas 18-19 son también iguales que las discutidas con anterioridad, pero han sido ilustradas por razones de integridad del procedimiento de Restablecimiento de Conexión de RRC.

Etapa 20. El eNB objetivo solicita al eNB fuente que envíe el contexto del UE. Un mensaje X2 existente denominado Recuperar Solicitud de Contexto de UE puede ser adaptado según sea necesario, p. ej., usando ReestabUE-Identitiy en vez de ResumeIdentity.

Etapa 21. El eNB fuente envía el contexto del UE al eNB objetivo. Un mensaje X2 existente denominado Recuperar Respuesta de Contexto de UE puede ser adaptado según sea necesario. El contexto del UE dice al eNB objetivo la MME correspondiente en la que el UE está registrado.

Etapa 22. El eNB objetivo envía un mensaje en forma de Comprobar Solicitud de MAC a la MME identificada en la etapa 21. En el mensaje de Comprobar Solicitud de MAC, el eNB objetivo incluye MAC CIoT UL e Input-MAC CIoT UL. El eNB objetivo recibió la MAC CIoT UL en la etapa 19. La Input-MAC CIoT UL puede incluir información que el eNB objetivo recibió en la etapa 19 y/o en la etapa 21 y/o la información propia del eNB objetivo. Tal información incluida en la Input-MAC CIoT UL puede ser la identidad de la célula objetivo, que ha sido por tanto usada como entrada junto con al menos la clave de integridad de NAS para generar la señal de muestra MAC CIoT UL de autenticación de UL. El mensaje de Comprobar Solicitud de MAC puede contener también información del UE que permita que la MME identifique el contexto del UE en la MME. Esa información del UE puede ser, por ejemplo, el ID de MME UE S1AP que el eNB objetivo recibió desde el eNB fuente en la etapa 21.

Etapa 23. La MME autentica la MAC CIoT UL usando la Input-MAC CIoT UL y la Key-MAC CIoT UL (p. ej., la misma clave de integridad de NAS usada como Key-MAC CIoT DL) como entrada a la Fun-MAC CIoT UL. En otras palabras, el resultado de la Fun-MAC CIoT UL se compara con la MAC CIoT UL recibida para una verificación de la MAC CIoT UL recibida.

En lo que sigue, por motivos de simplicidad, solamente se describen con más detalle las etapas relevantes para esta variante, las cuales son, si la autenticación de la etapa 23 ha tenido éxito:

Etapa 24. La MME genera MAC CIoT DL según se ha descrito con anterioridad, usando la Input-MAC CIoT DL y la Key-MAC CIoT DL. Algunos elementos de la Input-MAC CIoT DL, como la identidad de la célula objetivo, pueden ser obtenidos a partir de la Input-MAC CIoT UL. La MME envía un mensaje S1 (mensaje de Comprobar Acuse de Recibo de MAC) indicando el éxito al eNB objetivo e incluye MAC CIoT DL e Input-MAC CIoT DL.

Etapa 25. La MME envía un mensaje de Comprobar Acuse de Recibo de Solicitud de MAC al eNB objetivo. El mensaje incluye la MAC CIoT DL, y opcionalmente también la Input-MAC CIoT DL. El eNB objetivo sabe ahora que la MAC CIoT UL mencionada en las etapas anteriores, es auténtica.

Etapa 26. El eNB objetivo envía un mensaje de Restablecimiento de Conexión de RRC al UE. Este mensaje incluye la MAC CIoT DL y puede incluir la Input-MAC CIoT DL.

Etapa 27. El UE autentica la MAC CIoT DL usando la Input-CIoT DL y la Key-MAC CIoT DL como entrada a la Fun-MAC CIoT DL.

Etapa 28. Si la autenticación de la MAC CIoT DL en la etapa 27 tiene éxito, entonces el UE envía un mensaje de Restablecimiento de Conexión de RRC Completado, que opcionalmente contiene la PDU de datos NAS al eNB objetivo.

Si la autenticación de la MAC CIoT DL en la etapa 27 falla, entonces el UE puede realizar algunas acciones tales como no enviar mensajes adicionales o hacer una transición al modo de RRC_CONNECTED para autenticar la red, etc.

Un método, según una realización, para el restablecimiento de una conexión de RRC entre un UE y un eNB objetivo, se presenta con referencia a la Figura 7A. El método se lleva a cabo por medio del UE 1 y comprende recibir S100 un mensaje de Restablecimiento de Conexión de RRC desde un eNB 3 objetivo, p. ej., para optimización de ÌoT de

CP, incluyendo el mensaje de Restablecimiento de Conexión de RRC una señal de muestra de autenticación de DL que ha sido generada por la MME 4 y que ha tenido una clave de integridad de NAS como entrada, y autenticar S110 la señal de muestra de autenticación de DL recibida.

El mensaje de Restablecimiento de Conexión de RRC que incluye la señal de muestra de autenticación de DL puede también incluir opcionalmente una Input-MAC CIoT DL y la señal de muestra de autenticación de DL recibida puede ser autenticada usando la Input-MAC CIoT DL recibida y la clave de integridad de NAS.

El mensaje de RRC puede ser un mensaje de Transferencia de Información de DL de RRC que incluya MAC CIoT DL y opcionalmente Input-MAC CIoT DL, y la MAC CIoT DL recibida puede ser autenticada usando Input-MAC CIoT DL y Key-MAC CIoT DL.

En una etapa S80 opcional anterior a S100, el UE calcula una señal de muestra de autenticación de UL (mencionada como AT de UL en la Figura 7A) con la clave de integridad de NAS como entrada, y en una etapa S90 opcional envía una solicitud de restablecimiento de conexión de RRC que incluye la señal de muestra de autenticación de UL al eNB 3 objetivo. La señal de muestra de autenticación de UL puede ser calculada con la identidad de la célula objetivo como entrada, y la identidad de la célula objetivo puede estar incluida en la solicitud de restablecimiento de conexión de RRC, p. ej., como parte de una Input-MAC UL.

Un método, según una realización, para restablecer una conexión de RRC entre un UE y un eNB objetivo, p. ej. para optimización de IoT de CP, ha sido ilustrado con referencia a la Figura 7B. El método se lleva a cabo por medio del eNB 3 objetivo y comprende recibir S300, desde la MME 4, un mensaje que incluye una señal de muestra de autenticación de DL que ha sido generada por la MME, en donde la señal de muestra de autenticación de DL ha sido generada con una clave de integridad de Estrato de No Acceso como entrada, y enviar S310 un mensaje de Restablecimiento de Conexión de RRC al UE 1, incluyendo el mensaje de Restablecimiento de Conexión de RRC la señal de muestra de autenticación de DL.

En una etapa S280 opcional, anterior a la S300, el eNB objetivo recibe desde el UE 1, una solicitud de restablecimiento de conexión de RRC que incluye una señal de muestra de autenticación de UL, en donde la señal de muestra de autenticación de UL ha sido calculada por el UE 1 con la clave de integridad de NAS como entrada. La señal de muestra de autenticación de UL, en una realización junto con la Input-MAC CIoT UL que incluye la identidad de la célula objetivo. En una etapa S290 opcional, anterior a la S300, el eNB objetivo envía/reenvía la señal de muestra de autenticación de UL a la MME 4, opcionalmente con la Input-MAC CIoT UL que incluye la identidad de la célula objetivo.

El mensaje de Restablecimiento de Conexión de RRC enviado puede incluir una Input-MAC CIoT DL.

El mensaje recibido puede ser un mensaje de Acuse de Recibo de Solicitud de Conmutación de Ruta que incluye Input-MAC CIoT DL.

El mensaje recibido puede ser un mensaje de Comprobar Acuse de Recibo de MAC que incluye una Input-MAC CIoT DL.

Un método, según una realización, para restablecer una conexión de RRC entre un UE y un eNB objetivo, p. ej., para optimización de IoT de CP, ha sido presentado con referencia a la Figura 7C. El método se lleva a cabo en un eNB 2 fuente y comprende obtener S200 una señal de muestra de autenticación de DL que ha sido generada con una clave de integridad de NAS como entrada, y enviar S210 un mensaje de respuesta a un eNB 3 objetivo, incluyendo el mensaje de respuesta la señal de muestra de autenticación de DL obtenida.

La obtención S200 puede comprender generar la señal de muestra de autenticación de DL, o recibir un mensaje de Comprobar respuesta de S1 desde una MME 4, incluyendo el mensaje de Comprobar respuesta S1 recibido la señal de muestra de autenticación de DL y opcionalmente también la Input-MAC CIoT DL.

El mensaje de respuesta puede ser un mensaje de respuesta de contexto de UE X2.

Un método, según una realización, para restablecer una conexión de RRC entre un UE y un eNB objetivo, p. ej., para optimización de IoT de CP, ha sido presentado con referencia a la Figura 7D. El método se lleva a cabo por medio de la MME 4 y comprende generar S400 una señal de muestra de autenticación de DL con una clave de integridad de NAS como entrada, y enviar S410 un mensaje que incluye la señal de muestra de autenticación de DL generada al eNB 3 objetivo. La señal de muestra de autenticación de DL puede ser generada también con la identidad de la célula objetivo como entrada.

En una etapa S380 opcional, anterior a la S400, la MME recibe una señal de muestra de autenticación de UL desde el eNB 3 objetivo, habiendo sido dicha señal de muestra de autenticación de UL generada por el UE 1 con la clave de integridad de NAS como entrada, y en una etapa S390 opcional verifica la señal de muestra de autenticación de UL, p. ej., calculando una segunda señal de muestra de autenticación de UL de la misma manera que lo hizo el UE (p. ej., con la clave de integridad de NAS y con la identidad de la célula objetivo como entrada) y comparando a continuación la segunda señal de muestra de autenticación de UL con la recibida desde el eNB objetivo.

El mensaje puede ser un mensaje de Acuse de Recibo de Solicitud de Conmutación de Ruta e incluye Input-MAC CIoT DL.

El mensaje puede ser un mensaje de Comprobar Acuse de Recibo de MAC que incluye Input-MAC CIoT DL.

Un UE 1 según una realización, para restablecer una conexión de RRC entre el UE 1 y el eNB 3 objetivo, ha sido presentado con referencia a la Figura 8. El UE 1 comprende un procesador 10 y un producto de programa informático. El producto de programa informático almacena instrucciones que, cuando son ejecutadas por el procesador, provocan que el UE reciba un mensaje de Restablecimiento de Conexión de RRC desde un eNB 3 objetivo, incluyendo el mensaje de Restablecimiento de Conexión de RRC una señal de muestra de autenticación de DL que ha sido generada por la MME 4 y que ha tenido una clave de integridad de NAS como entrada, y que autentique la señal de muestra de autenticación de DL recibida.

El mensaje de Restablecimiento de Conexión de RRC puede incluir opcionalmente Input-MAC CIoT DL, y la señal de muestra de autenticación de DL recibida puede ser autenticada usando Input-MAC CIoT DL y la clave de integridad de NAS.

Un eNB fuente, según una realización, para restablecer una conexión de RRC entre un UE 1 y un eNB 3 objetivo, se ha presentado con referencia a la Figura 9. El eNB 2 fuente comprende un procesador 20 y un producto de programa informático. El producto de programa informático almacena instrucciones que, cuando son ejecutadas por el procesador, provocan que el eNB fuente obtenga una señal de muestra de autenticación de DL que ha sido generada con una clave de integridad de NAS como entrada, y envíe un mensaje de respuesta al eNB 3 objetivo, incluyendo el mensaje de respuesta la señal de muestra de autenticación de DL obtenida.

El mensaje de respuesta puede ser un mensaje de respuesta de Contexto de UE X2.

Un eNB objetivo, según una realización, para restablecer una conexión de RRC entre un UE 1 y un eNB 3 objetivo, ha sido presentado con referencia a la Figura 10. El eNB 3 objetivo comprende un procesador 30 y un producto de programa informático. El producto de programa informático almacena instrucciones que, cuando son ejecutadas por el procesador, provocan que el eNB objetivo reciba desde la MME 4, un mensaje que incluye una señal de muestra de autenticación de DL que ha sido generada por la MME 4, en donde la señal de muestra de autenticación de DL ha sido generada con una clave de integridad de NAS como entrada, y envíe un mensaje de Restablecimiento de Conexión de RRC a un UE 1, incluyendo el mensaje de Restablecimiento de Conexión de RRC la señal de muestra de autenticación de DL. La señal de muestra de autenticación de DL ha sido calculada, en una realización, por medio de la MME 4 con una identidad de la célula objetivo como entrada.

El mensaje de Restablecimiento de Conexión de RRC enviado incluye opcionalmente Input-MAC CIoT DL, la cual puede incluir la identidad de la célula objetivo.

El mensaje recibido puede ser un mensaje de Acuse de Recibo de Solicitud de Conmutación de Ruta que incluya la Input-MAC CIoT DL.

El mensaje recibido puede ser un mensaje de Comprobar Acuse de Recibo de MAC que incluya Input-MAC CIoT DL.

Una MME, según una realización, para restablecer una conexión de RRC entre un UE 1 y un eNB 3 objetivo, ha sido presentada con referencia a la Figura 11. La MME 4 comprende un procesador 40 y un producto de programa informático. El producto de programa informático almacena instrucciones que, cuando son ejecutadas por el procesador, provocan que la MME genere una señal de muestra de autenticación de DL con una clave de integridad de NAS como entrada, y envíe un mensaje que incluye la señal de muestra de autenticación de DL generada al eNB 3 objetivo.

El mensaje puede ser un mensaje de Acuse de Recibo de Solicitud de Conmutación de Ruta, incluyendo el mensaje una Input-MAC CIoT DL.

El mensaje puede ser un mensaje de Comprobar Acuse de Recibo de MAC, incluyendo el mensaje la Input-MAC CIoT DL.

La Figura 8 es un diagrama esquemático que muestra algunos componentes del UE 1. El procesador 10 puede ser proporcionado con el uso de cualquier combinación de una o más de entre una unidad central de proceso, CPU, apropiada, un multiprocesador, microcontrolador, procesador de señal digital, DSP, circuito integrado específico de la aplicación, etc., capacitados para ejecutar instrucciones de software de un programa informático 14 almacenado en una memoria. La memoria puede ser considerada, por lo tanto, como que es el, o forma parte del, producto 12 de programa informático. El procesador 10 puede estar configurado para ejecutar métodos descritos en la presente memoria con referencia a la Figura 7A.

La memoria puede ser cualquier combinación de memoria de lectura y escritura, RAM, y de memoria de sólo lectura, ROM. La memoria puede comprender también almacenaje persistente, la cual puede ser, por ejemplo, una sola o

una combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada remotamente.

Un segundo producto 13 de programa informático en forma de memoria de datos puede ser proporcionado también, p. ej., para lectura y/o almacenaje de datos durante la ejecución de instrucciones de software en el procesador 10. La memoria de datos puede ser cualquier combinación de memoria de lectura y escritura, RAM, y de memoria de sólo lectura, ROM, y también puede comprender almacenaje persistente, la cual puede ser, por ejemplo, una sola o una combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada remotamente. La memoria de datos puede contener, p. ej., otras instrucciones 15 de software, para mejorar la funcionalidad para el UE 1.

El UE 1 puede comprender además una interfaz 11 de entrada/salida (E/S) que incluya, p. ej., una interfaz de usuario. El UE 1 puede comprender además un receptor configurado para recibir señalización desde otros nodos, y un transmisor configurado para transmitir señalización a otros nodos (no representados). Otros componentes del UE 1 han sido omitidos con el fin de no oscurecer los conceptos que se presentan en la presente memoria.

La Figura 12 es un diagrama esquemático que muestra bloques funcionales del UE 1. Los módulos pueden ser implementados como únicamente instrucciones de software tal como un programa informático que se ejecuta en el servidor caché, o como únicamente hardware, tal como circuitos integrados específicos de la aplicación, matrices de puerta programable en campo, componentes lógicos discretos, transceptores, etc., o como una combinación de los mismos. En una realización alternativa, algunos de los bloques funcionales pueden ser implementados mediante software y otros mediante hardware. Los módulos corresponden a las etapas de los métodos ilustrados en la Figura 7A, comprendiendo una unidad 60 de gestor de determinación y una unidad 61 de gestor de comunicación. En las realizaciones en las que uno o más de los módulos están implementados por un programa informático, se comprenderá que esos módulos no correspondan necesariamente a módulos de proceso, sino que pueden estar escritos a modo instrucciones conforme a un lenguaje de programación en el que éstos podrían estar implementados, dado que algunos lenguajes de programación no contienen típicamente módulos de proceso.

El gestor 60 de determinación está destinado a habilitar el restablecimiento de una conexión de RRC entre un UE y un eNB objetivo. Este módulo corresponde a la etapa de comprobación S110 de la Figura 7A, es decir, la autenticación de la señal de muestra de autenticación de DL recibida. Este módulo puede estar implementado, p. ej., por el procesador 10 de la Figura 8, cuando ejecuta el programa informático.

El gestor 61 de comunicación está destinado a habilitar el restablecimiento de una conexión de RRC entre un UE y un eNB objetivo. Este módulo corresponde a la etapa de recepción S100 de la Figura 7A. Este módulo puede estar implementado, p. ej., por el procesador 10 de la Figura 12, cuando ejecuta el programa informático.

La Figura 9 es un diagrama esquemático que muestra algunos componentes del eNB 2 fuente. El procesador 20 puede ser proporcionado usando cualquier combinación de una o más de entre una unidad central de proceso, CPU, adecuada, un multiprocesador, microcontrolador, procesador de señal digital, DSP, circuito integrado específico de la aplicación, etc., capacitado para ejecutar instrucciones de software de un programa informático 24 almacenado en una memoria. La memoria puede ser considerada, por lo tanto, como que es el, o como que forma parte del, producto 22 de programa informático. El procesador 20 puede estar configurado para ejecutar métodos descritos en la presente memoria con referencia a la Figura 7B.

La memoria puede ser cualquier combinación de memoria de lectura y escritura, RAM, y de memoria de sólo lectura, ROM. La memoria puede también comprender almacenaje persistente, la cual puede ser, por ejemplo, una sola o una combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada remotamente.

Un segundo producto 23 de programa informático en forma de memoria de datos puede ser también proporcionado, p. ej., para la lectura y/o el almacenaje de datos durante la ejecución de instrucciones de software en el procesador 20. La memoria de datos puede ser cualquier combinación de memoria de lectura y escritura, RAM, y de memoria de sólo lectura, ROM, y también puede comprender almacenaje persistente, la cual puede ser, por ejemplo, una sola o una combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada remotamente. La memoria de datos puede, p. ej., mantener otras instrucciones 25 de software, para mejorar la funcionalidad para el eNB 2 fuente.

El eNB 2 fuente puede comprender además una interfaz 21 de entrada/salida (E/S) que incluya, p. ej., una interfaz de usuario. El eNB 2 fuente puede comprender además un receptor configurado para recibir señalización desde otros nodos, y un transmisor configurado para transmitir señalización a otros nodos (no representados). Otros componentes del eNB 2 fuente han sido omitidos con el fin de no oscurecer los conceptos presentados en la presente memoria.

La Figura 13 es un diagrama esquemático que muestra bloques funcionales del eNB 2 fuente. Los módulos pueden ser implementados como únicamente instrucciones de software tal como un programa informático que se ejecuta en el servidor caché, o como únicamente hardware, tal como los circuitos integrados específicos de la aplicación, matrices de puerta programable en campo, componentes lógicos discretos, transceptores, etc., o como una

combinación de los mismos. En una realización alternativa, algunos de los bloques funcionales puede ser implementados mediante software y otros mediante hardware. Los módulos corresponden a las etapas de los métodos ilustrados en la Figura 7C, comprendiendo una unidad 70 de gestor de determinación y una unidad 71 de gestor de comunicación. En las realizaciones en las que uno o más de los módulos se han implementado mediante un programa informático, se podrá comprender que esos módulos no correspondan necesariamente a módulos de proceso, sino que pueden estar escritos a modo de instrucciones conforme a un lenguaje de programación en el que éstos puedan ser implementados, dado que algunos lenguajes de programación no contienen típicamente módulos de proceso.

El gestor 70 de determinación está destinado a habilitar el restablecimiento de una conexión de RRC entre un UE y un eNB objetivo. Este módulo corresponde a la etapa de obtención S200 de la Figura 7C. Este módulo puede ser implementado, p. ej., mediante el procesador 20 de la Figura 9, cuando ejecuta el programa informático.

El gestor 71 de comunicación está destinado a habilitar el restablecimiento de una conexión de RRC entre un UE y un eNB objetivo. Este módulo corresponde a la etapa de envío S210 de la Figura 7C. Este módulo puede ser implementado, p. ej., mediante el procesador 20 de la Figura 13, cuando ejecuta el programa informático.

La Figura 10 es un diagrama esquemático que muestra algunos componentes del eNB 3 objetivo. El procesador 30 puede ser proporcionado usando cualquier combinación de uno o más de entre una unidad central de proceso, CPU, adecuada, un multiprocesador, microcontrolador, procesador de señal digital, DSP, circuito integrado específico de la aplicación, etc., capaz de ejecutar instrucciones de software de un programa informático 34 almacenado en una memoria. La memoria puede ser, por tanto, considerada como que es el, o forma parte del, producto 32 de programa informático. El procesador 30 puede estar configurado para ejecutar métodos descritos en la presente memoria con referencia a la Figura 7C.

La memoria puede ser cualquier combinación de memoria de lectura y escritura, RAM, y de memoria de sólo lectura, ROM. La memoria puede también comprender almacenaje persistente, la cual puede ser, por ejemplo, una sola o una combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada remotamente.

Un segundo producto 33 de programa informático en forma de una memoria de datos, puede ser también proporcionado, p. ej., para lectura y/o almacenaje de datos durante la ejecución de instrucciones de software en el procesador 30. La memoria de datos puede ser cualquier combinación de memoria de lectura y escritura, RAM, y de memoria de sólo lectura, ROM, y también puede comprender almacenaje persistente, la cual puede ser, por ejemplo, una sola o una combinación de memoria magnética, memoria óptica, memoria de estado sólido, o incluso memoria montada remotamente. La memoria de datos puede contener, por ejemplo, otras instrucciones 35 de software, para mejorar la funcionalidad para el eNB 3 objetivo.

El eNB 3 objetivo puede comprender además una interfaz 31 de entrada/salida (E/S) que incluya, p. ej., una interfaz de usuario. El eNB 3 objetivo puede comprender además un receptor configurado para recibir señalización desde otros nodos, y un transmisor configurado para transmitir señalización a otros nodos (no representados). Otros componentes del eNB 3 objetivo han sido omitidos con el fin de no oscurecer los conceptos presentados en la presente memoria.

La Figura 14 es un diagrama esquemático que muestra bloques funcionales del eNB 3 objetivo. Los módulos pueden ser implementados como únicamente instrucciones de software tal como un programa informático que se ejecute en el servidor caché, o como únicamente hardware, tal como circuitos integrados específicos de la aplicación, matrices de puerta programable en campo, componentes lógicos discretos, transceptores, etc., o como una combinación de los mismos. En una realización alternativa, algunos de los bloques funcionales pueden ser implementados mediante software y otros mediante hardware. Los módulos corresponden a las etapas de los métodos ilustrados en la Figura 7B, comprendiendo una unidad 80 de gestor de determinación y una unidad 81 de gestor de comunicación. En las realizaciones en las que uno o más de los módulos estén implementados por un programa informático, se comprenderá que esos módulos no correspondan necesariamente a módulos de proceso, sino que pueden estar escritos a modo de instrucciones conforme a un lenguaje de programación en el que éstos podrían estar implementados, dado que algunos lenguajes de programación no contienen típicamente módulos de proceso.

El gestor 81 de comunicación está destinado a habilitar el restablecimiento de una conexión de RRC entre un UE y un eNB objetivo. Este módulo corresponde a la etapa de recepción S300 y a la etapa de envío 310 de la Figura 7B. Este módulo puede ser implementado, p. ej., mediante el procesador 30 de la Figura 10, cuando ejecuta el programa informático.

La Figura 11 es un diagrama esquemático que muestra algunos componentes de la MME 4. El procesador 40 puede ser proporcionado usando cualquier combinación de una o más de entre una unidad central de proceso, CPU, adecuada, un multiprocesador, microcontrolador, procesador de señal digital, DSP, circuito integrado específico de la aplicación, etc., capacitado para ejecutar instrucciones de software de un programa informático 44 almacenado en una memoria. La memoria puede ser considerada, por lo tanto, como que es el, o forma parte del, producto 42 de programa informático. El procesador 40 puede estar configurado para ejecutar métodos descritos en la presente

memoria con referencia a la Figura 7D.

La memoria puede ser cualquier combinación de memoria de lectura y escritura, RAM, y de memoria de sólo lectura, ROM. La memoria puede comprender también almacenaje persistente, la cual puede ser, por ejemplo, una sola o una combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso una memoria montada remotamente.

Un segundo producto 43 de programa informático en forma de una memoria de datos puede ser proporcionado también, p. ej., para lectura y/o almacenaje de datos durante la ejecución de instrucciones de software en el procesador 40. La memoria de datos puede ser cualquier combinación de memoria de lectura y escritura, RAM, y de memoria de sólo lectura, ROM, y puede comprender también almacenaje persistente, la cual puede ser, por ejemplo, una sola o una combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso una memoria montada remotamente. La memoria de datos puede contener, p. ej., otras instrucciones 45 de software, para mejorar la funcionalidad para la MME 4.

La MME 4 puede comprender además una interfaz 41 de entrada/salida (E/S) que incluya, p. ej., una interfaz de usuario. La MME 4 puede comprender además un receptor configurado para recibir señalización desde otros nodos, y un transmisor configurado para transmitir señalización a otros nodos (no representados). Otros componentes de la MME 4 han sido omitidos con el fin de no oscurecer los conceptos presentados en la presente memoria.

La Figura 15 es un diagrama esquemático que muestra bloques funcionales de la MME 4. Los módulos pueden ser implementados como ´únicamente instrucciones de software tal como un programa informático que se ejecuta en el servidor caché, o como únicamente hardware, tal como circuitos integrados específicos de la aplicación, matrices de puerta programable en campo, componentes lógicos discretos, transceptores, et., o como una combinación de los mismos. En una realización alternativa, algunos de los bloques funcionales pueden ser implementados por medio de software y otros por medio de hardware. Los módulos corresponden a las etapas de los métodos ilustrados en la Figura 7D, comprendiendo una unidad 90 de gestor de determinación y una unidad 91 de gestor de comunicación. En las realizaciones en las que uno o más de los módulos estén implementados por un programa informático, se comprenderá que esos módulos no correspondan necesariamente a módulos de proceso, sino que pueden estar escritos a modo de instrucciones conforme a un lenguaje de programación en el que éstos podrían estar implementados, puesto que algunos lenguajes de programación no contienen típicamente módulos de proceso.

El gestor 90 de determinación está destinado a habilitar el restablecimiento de una conexión de RRC entre un UE y un eNB objetivo. Este módulo corresponde a la etapa de generación 400 de la Figura 7D. Este módulo puede ser implementado, p. ej., por el procesador 40 de la Figura 11, cuando ejecuta el programa informático.

El gestor 91 de comunicación está destinado a habilitar el restablecimiento de una conexión de RRC entre un UE y un eNB objetivo. Este módulo corresponde a la etapa de envío S410 de la Figura 7D. Este módulo puede ser implementado, p. ej., por el procesador 40 de la Figura 11, cuando ejecuta el programa informático.

La invención ha sido principalmente descrita en lo que antecede con referencia a unas pocas realizaciones. Sin embargo, como podrán apreciar fácilmente los expertos en la materia, otras realizaciones distintas de las descritas con anterioridad son igualmente posibles dentro del alcance de la invención. El alcance de la invención está definido las reivindicaciones anexas.

REIVINDICACIONES

1. Un método para restablecer una conexión de Control de Recurso de Radio, RRC, entre un Equipo de Usuario (1), UE, y un NodeB evolucionado (3) objetivo, eNB objetivo, siendo el método llevado a cabo por el UE (1), y comprendiendo:

recibir (S100) un mensaje de Restablecimiento de Conexión de RRC desde el eNB (3) objetivo, incluyendo el mensaje de Restablecimiento de Conexión de RRC una señal de muestra de autenticación de enlace descendente, DL, que ha sido generada por una Entidad (4) de Gestión de Movilidad y que ha tenido una clave de integridad de Estrato de No Acceso como entrada, y

autenticar (S110) la señal de muestra de autenticación de DL recibida.

2. El método según la reivindicación 1, que comprende calcular una señal de muestra de autenticación de enlace ascendente, UL, con la clave de integridad de Estrato de No Acceso como entrada, y enviar una solicitud de restablecimiento de conexión de RRC que incluya la señal de muestra de autenticación de UL al eNB (3) objetivo.

3. El método según la reivindicación 2, en donde la señal de muestra de autenticación de UL se calcula con una identidad de la célula objetivo como entrada.

4. El método según la reivindicación 3, que incluye la identidad de la célula objetivo en la solicitud de restablecimiento de conexión de RRC.

5. El método según la reivindicación 1, en donde la señal de muestra de autenticación de DL ha sido calculada por la Entidad (4) de Gestión de Movilidad con una identidad de la célula objetivo como entrada.

6. Un método para restablecer una conexión de Control de Recurso de Radio, RRC, entre un Equipo de Usuario (1), UE, y un NodeB evolucionado (3) objetivo, eNB objetivo, siendo el método llevado a cabo por el eNB (3) objetivo y comprendiendo:

recibir (S300), desde una Entidad (4) de Gestión de Movilidad, MME, un mensaje que incluye una señal de muestra de autenticación de enlace descendente, DL, que ha sido generada por la MME (4), en donde la señal de muestra de autenticación de DL ha sido generada con una clave de integridad de Estrato de No Acceso como entrada, y

enviar (S310) un mensaje de Restablecimiento de Conexión de RRC al UE (1), incluyendo el mensaje de Restablecimiento de Conexión de RRC la señal de muestra de autenticación de DL.

7. El método según la reivindicación 6, que comprende recibir desde el UE (1) una solicitud de restablecimiento de conexión de RRC que incluye una señal de muestra de autenticación de enlace ascendente, UL, en donde la señal de muestra de autenticación de UL ha sido calculada por el UE (1) con la clave de integridad de Estrato de No Acceso como entrada.

8. El método según la reivindicación 7, en donde la señal de muestra de autenticación de UL ha sido calculada por el UE (1) con una identidad de la célula objetivo como entrada.

9. El método según la reivindicación 6, en donde la señal de muestra de autenticación de DL ha sido calculada por la MME (4) con una identidad de la célula objetivo como entrada.

10. Un método para restablecer una conexión de Control de Recurso de Radio, RRC, entre un Equipo de Usuario (1), UE, y un NodeB evolucionado (3) objetivo, eNB objetivo, siendo el método llevado a cabo por una Entidad (4) de Gestión de Movilidad, MME, y comprendiendo:

generar (S400) una señal de muestra de autenticación de enlace descendente, DL, con una clave de integridad de Estrato de No Acceso como entrada, y

enviar (S410) un mensaje que incluya la señal de muestra de autenticación de DL generada al eNB (3) objetivo.

11. El método según la reivindicación 10, que comprende generar la señal de muestra de autenticación de DL con una identidad de la célula objetivo como entrada.

12. El método según la reivindicación 10, que comprende:

recibir una señal de muestra de autenticación de enlace ascendente, UL, desde el eNB objetivo, habiendo sido dicha señal de muestra de autenticación de UL generada por el UE (1) con la clave de integridad de Estrato de No Acceso como entrada, y

verificar la señal de muestra de autenticación de UL.

13. El método según la reivindicación 12, en donde la señal de muestra de autenticación de UL ha sido generada por el UE (1) con una identidad de la célula objetivo como entrada.

14. Un Equipo de Usuario (1), UE, para restablecer una conexión de Control de Recurso de Radio, RRC, entre el UE (1) y un NodeB evolucionado (3) objetivo, eNB objetivo, comprendiendo el UE (1):

un procesador (10), y

un producto (12, 13) de programa informático que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el UE:

reciba un mensaje de Restablecimiento de Conexión de RRC desde el eNB (3) objetivo, incluyendo el mensaje de Restablecimiento de Conexión de RRC una señal de muestra de autenticación de enlace descendente, DL, que ha sido generada por una Entidad (4) de Gestión de Movilidad y que ha tenido una clave de integridad de Estrato de No Acceso como entrada, y

autentique la señal de muestra de autenticación de DL recibida.

15. El UE según la reivindicación 14, en donde la señal de muestra de autenticación de DL ha sido calculada por la Entidad (4) de Gestión de Movilidad con una identidad de la célula objetivo como entrada.

16. Un NodeB evolucionado (3) objetivo, eNB objetivo, para restablecer una conexión de Control de Recurso de Radio, RRC, entre un Equipo de Usuario (1), UE, y el eNB objetivo, comprendiendo el eNB (3) objetivo:

un procesador (30), y

un producto (32, 33) de programa informático que almacena instrucciones que, cuando son ejecutadas por el procesador, provocan que el eNB objetivo:

reciba, desde una Entidad (4) de Gestión de Movilidad, MME, un mensaje que incluye una señal de muestra de autenticación de enlace descendente, DL, que ha sido generada por la MME (4),, en donde la señal de muestra de autenticación de DL ha sido generada con una clave de integridad de Estrato de No Acceso como entrada, y

envíe un mensaje de Restablecimiento de Conexión de RRC al UE (1), incluyendo el mensaje de Restablecimiento de Conexión de RRC la señal de muestra de autenticación de DL.

17. El eNB (3) objetivo según la reivindicación 16, en donde la señal de muestra de autenticación de DL ha sido calculada por la MME (4) con una identidad de la célula objetivo como entrada.

18. Un NodeB evolucionado (2) fuente, eNB fuente, para restablecer una comunicación de Control de Recurso de Radio, RRC, entre un Equipo de Usuario (1), UE, y un eNB (3) objetivo, comprendiendo el eNB (2) fuente:

un procesador (20), y

un producto (22, 23) de programa informático que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el eNB fuente:

obtenga una señal de muestra de autenticación de enlace descendente, DL, que ha sido generada con una clave de integridad de Estrato de No Acceso como entrada, y

envíe un mensaje de respuesta al eNB (3) objetivo, incluyendo el mensaje de respuesta la señal de muestra de autenticación de DL obtenida.

19. Una Entidad (4) de Gestión de Movilidad, MME, para restablecer una conexión de Control de Recurso de Radio, RRC, entre un Equipo de Usuario (1), UE, y un NodeB evolucionado (3) objetivo, eNB objetivo, comprendiendo la MME (4):

un procesador (40), y

un producto (42, 43) de programa informático que almacena instrucciones que, cuando son ejecutadas por el procesador, provocan que la MME:

genere una señal de muestra de autenticación de enlace descendente, DL, con una clave de integridad de Estrato de No Acceso como entrada, y

envíe un mensaje que incluye la señal de muestra de autenticación de DL generada al eNB (3) objetivo.

20. Un programa informático (14, 15) para restablecer una conexión de Control de Recurso de Radio, RRC, entre un Equipo de Usuario (1), UE, y un NodeB evolucionado (3) objetivo, eNB objetivo, comprendiendo el programa informático un código de programa informático que, cuando se ejecuta en el UE (1), provoca que el UE:

reciba (S100) un mensaje de Restablecimiento de Conexión de RRC desde el eNB (3) objetivo, incluyendo el mensaje de Restablecimiento de Conexión de RRC una señal de muestra de autenticación de enlace descendente,

DL, que ha sido generada por una Entidad (4) de Gestión de Movilidad y que ha tenido una clave de integridad de Estrato de No Acceso como entrada, y

autentique (S110) la señal de muestra de autenticación de DL recibida.

21. Un programa informático (34, 35) para restablecer una conexión de Control de Recurso de Radio, RRC, entre un Equipo de Usuario (1), UE, y un NodeB evolucionado (3) objetivo, eNB objetivo, comprendiendo el programa informático un código de programa informático que, cuando se ejecuta en el eNB (3) objetivo, provoca que el eNB objetivo:

reciba, desde una Entidad (4) de Gestión de Movilidad, MME, un mensaje que incluye una señal de muestra de autenticación de enlace descendente, DL, que ha sido generada por la MME (4), en donde la señal de muestra de autenticación de DL ha sido generada con una clave de integridad de Estrato de No Acceso como entrada, y

envíe un mensaje de Restablecimiento de Conexión de RRC al UE (1), incluyendo el mensaje de Restablecimiento de Conexión de RRC la señal de muestra de autenticación de DL.

22. Un programa informático (44, 45) para restablecer una conexión de Control de Recurso de Radio, RRC, entre un Equipo de Usuario (1), UE, y un NodeB evolucionado (3) objetivo, eNB objetivo, comprendiendo el programa informático un código de programa informático que, cuando se ejecuta en una Entidad (4) de Gestión de Movilidad, MME, provoca que la MME (4):

genere una señal de muestra de autenticación de enlace descendente, DL, con una clave de integridad de Estrato de No Acceso como entrada, y

envíe un mensaje que incluye la señal de muestra de autenticación de DL generada al eNB (3) objetivo.

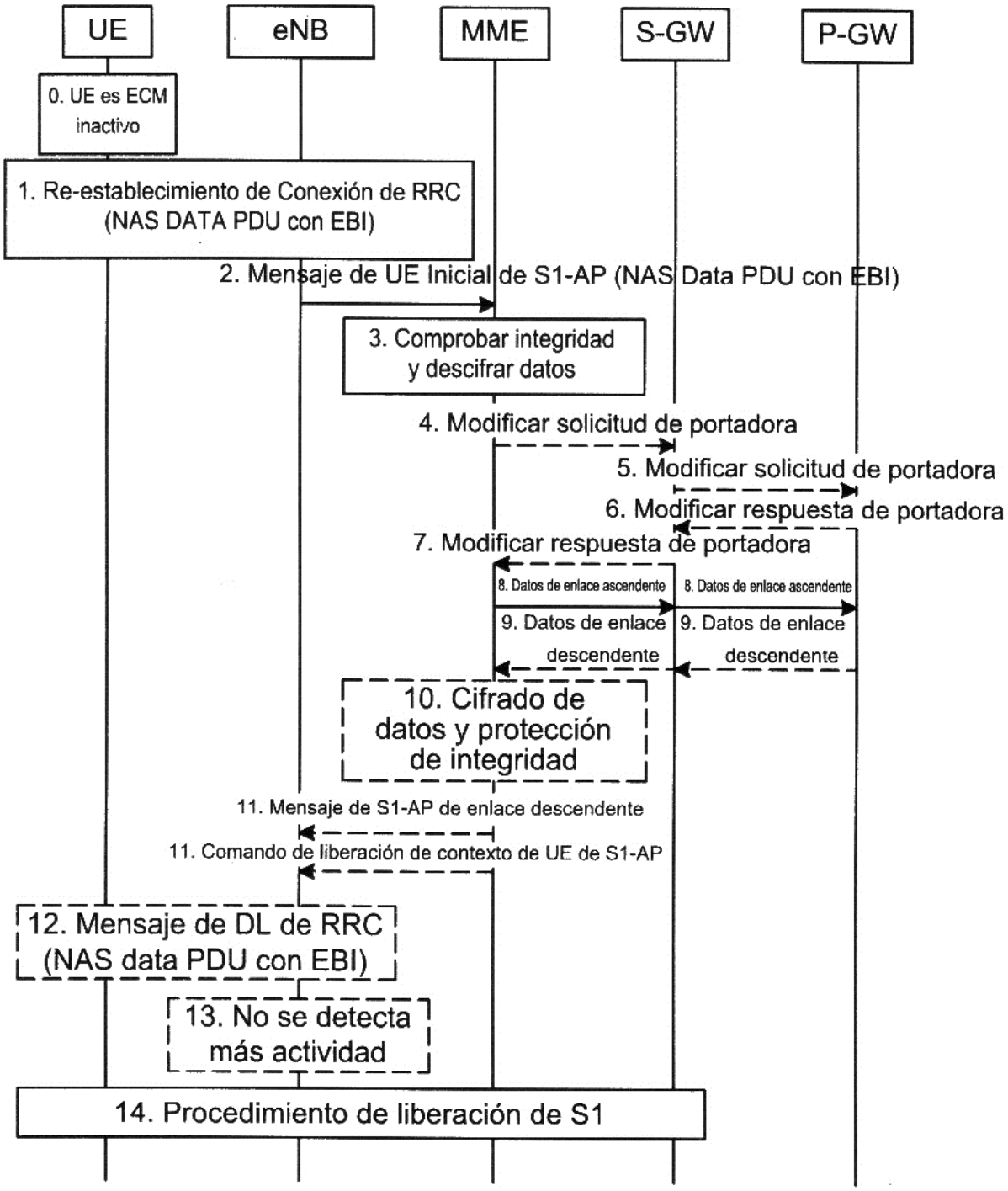
UE
eNB
MME
S-GW
P-GW
0. UE es ECM inactivo
1. Re-establecimiento de Conexión de RRC (NAS DATA PDU con EBI)
2. Mensaje de UE Inicial de S1-AP (NAS Data PDU con EBI)
3. Comprobar integridad y descifrar datos
4. Modificar solicitud de portadora
5. Modificar solicitud de portadora
6. Modificar respuesta de portadora
7. Modificar respuesta de portadora
8. Datos de enlace ascendente
8. Datos de enlace ascendente
9. Datos de enlace descendente
9. Datos de enlace descendente
10. Cifrado de datos y protección de integridad
11. Mensaje de S1-AP de enlace descendente
11. Comando de liberación de contexto de UE de S1-AP
12. Mensaje de DL de RRC (NAS data PDU con EBI)
13. No se detecta más actividad
14. Procedimiento de liberación de S1

Fig. 1

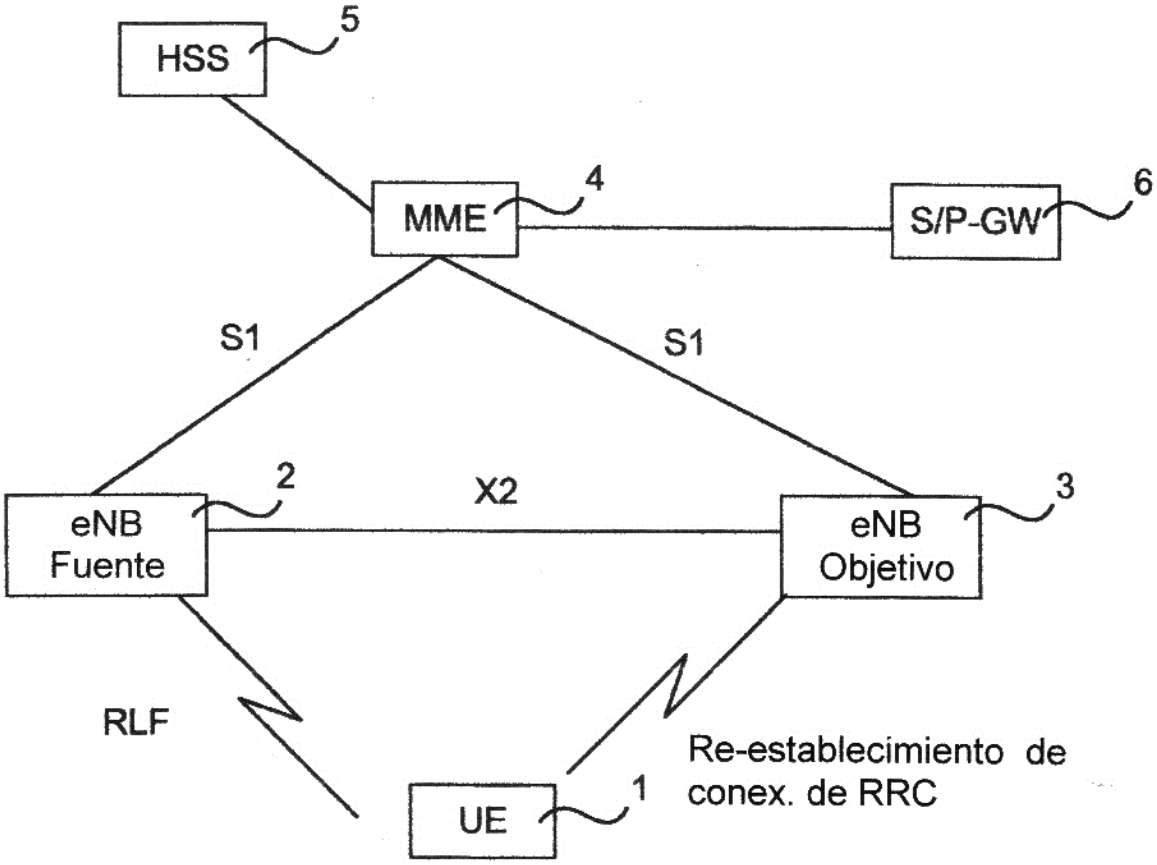
HSS
5
MME
4
S/P-GW
6
S1
S1
eNB
Fuente
2
X2
eNB
Objetivo
3
RLF
Re-establecimiento de
conex. de RRC
UE
1

Fig. 2

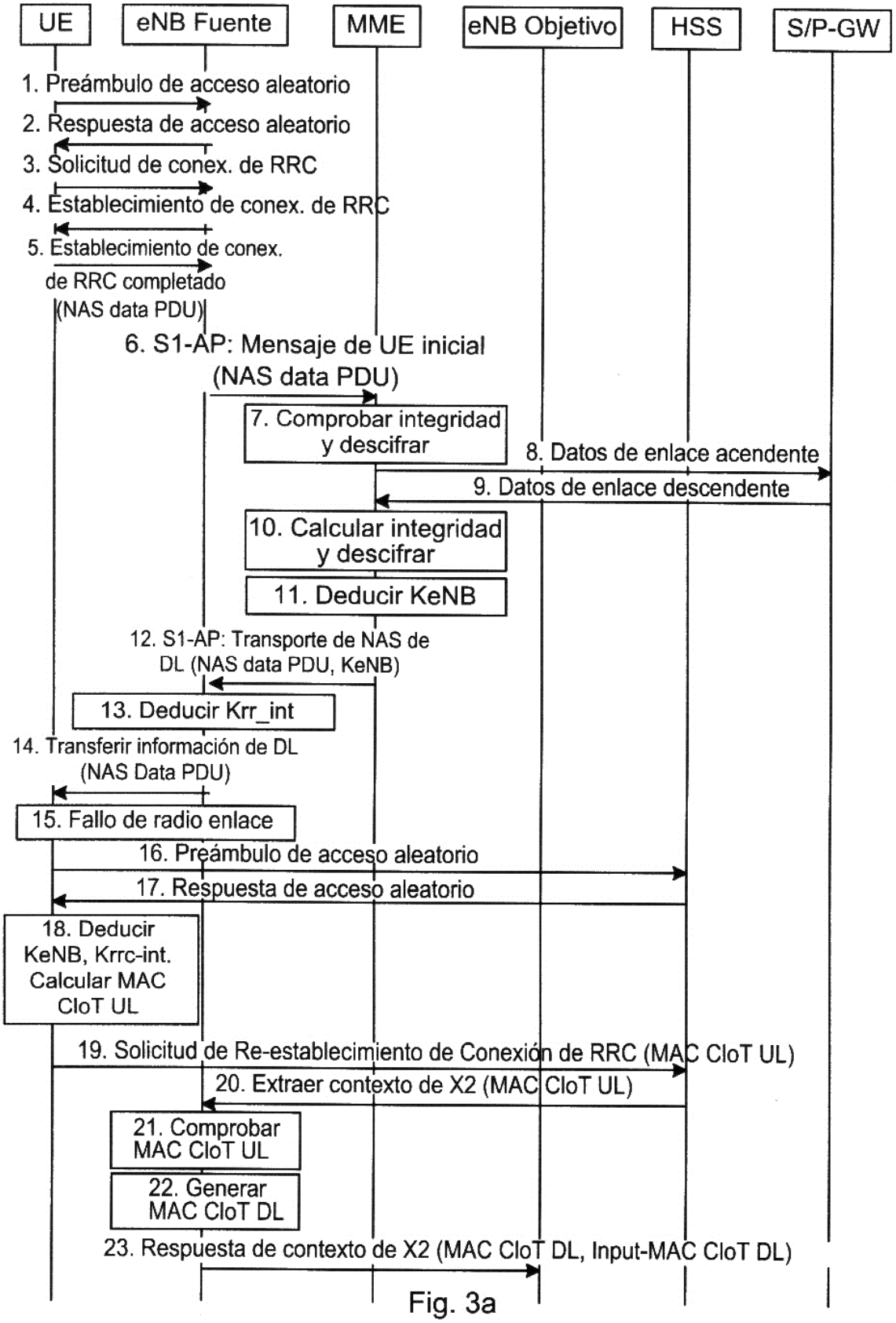
UE
eNB Fuente
MME
eNB Objetivo
HSS
S/P-GW
1. Preámbulo de acceso aleatorio
2. Respuesta de acceso aleatorio
3. Solicitud de conex. de RRC
4. Establecimiento de conex. de RRC
5. Establecimiento de conex. de RRC completado (NAS data PDU)
6. S1-AP: Mensaje de UE inicial (NAS data PDU)
7. Comprobar integridad y descifrar
8. Datos de enlace acendente
9. Datos de enlace descendente
10. Calcular integridad y descifrar
11. Deducir KeNB
12. S1-AP: Transporte de NAS de DL (NAS data PDU, KeNB)
13. Deducir Krr_int
14. Transferir información de DL (NAS Data PDU)
15. Fallo de radio enlace
16. Preámbulo de acceso aleatorio
17. Respuesta de acceso aleatorio
18. Deducir KeNB, Krrc-int. Calcular MAC CIoT UL
19. Solicitud de Re-establecimiento de Conexión de RRC (MAC CIoT UL)
20. Extraer contexto de X2 (MAC CIoT UL)
21. Comprobar MAC CIoT UL
22. Generar MAC CIoT DL
23. Respuesta de contexto de X2 (MAC CIoT DL, Input-MAC CIoT DL)

Fig. 3a

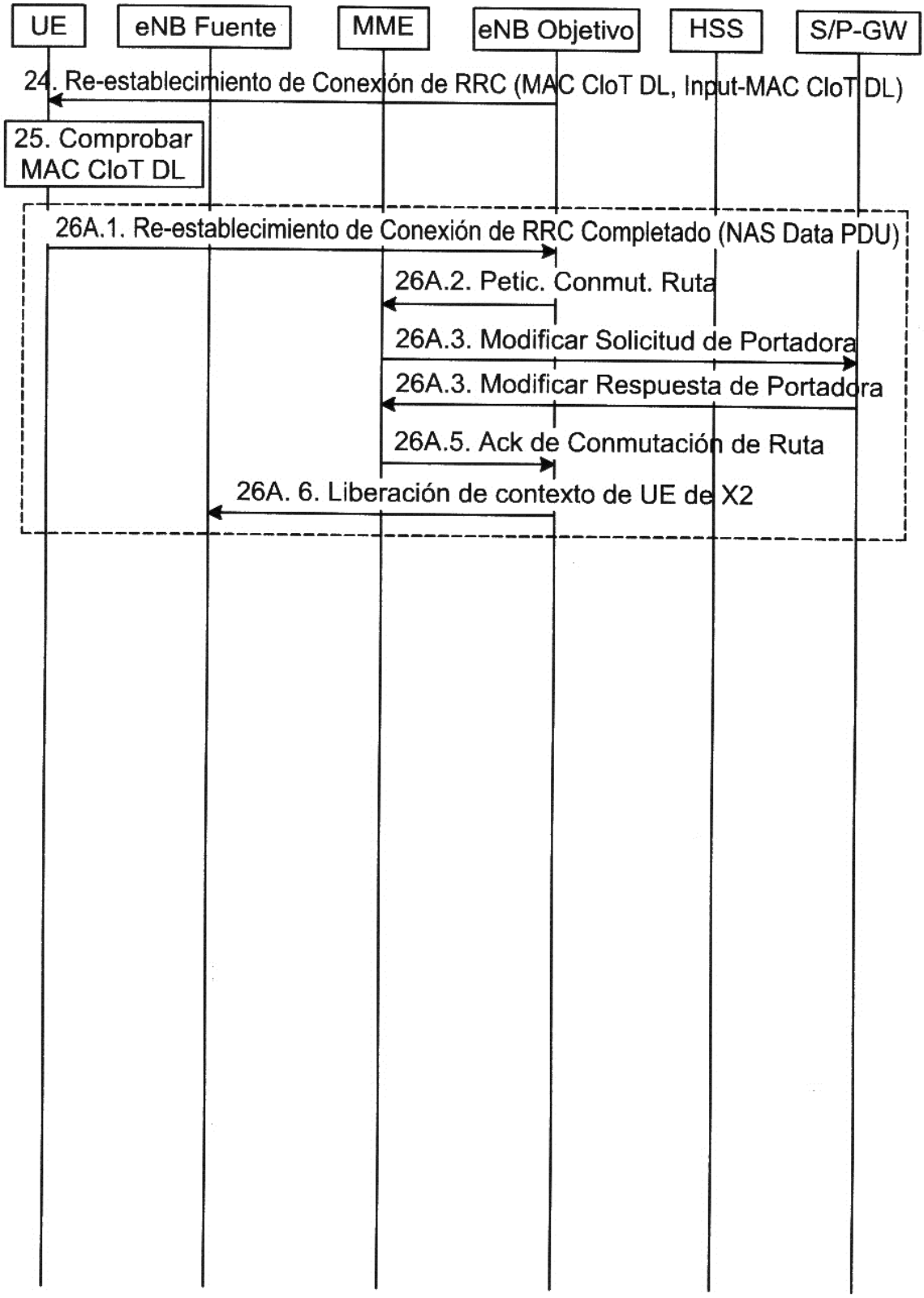
UE
eNB Fuente
MME
eNB Objetivo
HSS
S/P-GW
24. Re-establecimiento de Conexión de RRC (MAC CIoT DL, Input-MAC CIoT DL)
25. Comprobar MAC CIoT DL
26A.1. Re-establecimiento de Conexión de RRC Completado (NAS Data PDU)
26A.2. Petic. Conmut. Ruta
26A.3. Modificar Solicitud de Portadora
26A.3. Modificar Respuesta de Portadora
26A.5. Ack de Conmutación de Ruta
26A. 6. Liberación de contexto de UE de X2

Fig. 3b

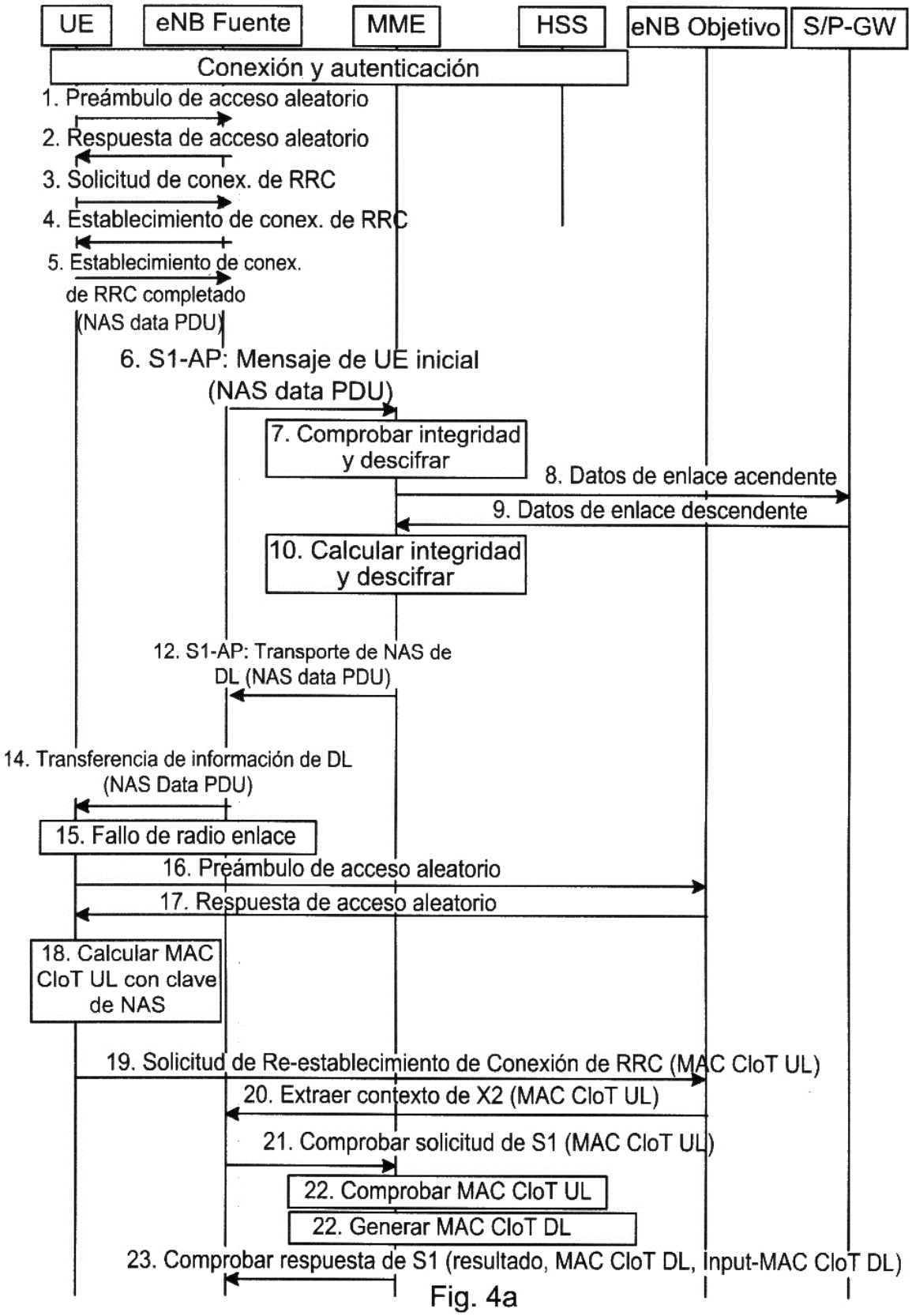
UE
eNB Fuente
MME
HSS
eNB Objetivo
S/P-GW
Conexión y autenticación
1. Preámbulo de acceso aleatorio
2. Respuesta de acceso aleatorio
3. Solicitud de conex. de RRC
4. Establecimiento de conex. de RRC
5. Establecimiento de conex. de RRC completado (NAS data PDU)
6. S1-AP: Mensaje de UE inicial (NAS data PDU)
7. Comprobar integridad y descifrar
8. Datos de enlace acendente
9. Datos de enlace descendente
10. Calcular integridad y descifrar
12. S1-AP: Transporte de NAS de DL (NAS data PDU)
14. Transferencia de información de DL (NAS Data PDU)
15. Fallo de radio enlace
16. Preámbulo de acceso aleatorio
17. Respuesta de acceso aleatorio
18. Calcular MAC CIoT UL con clave de NAS
19. Solicitud de Re-establecimiento de Conexión de RRC (MAC CIoT UL)
20. Extraer contexto de X2 (MAC CIoT UL)
21. Comprobar solicitud de S1 (MAC CIoT UL)
22. Comprobar MAC CIoT UL
22. Generar MAC CIoT DL
23. Comprobar respuesta de S1 (resultado, MAC CIoT DL, Input-MAC CIoT DL)

Fig. 4a

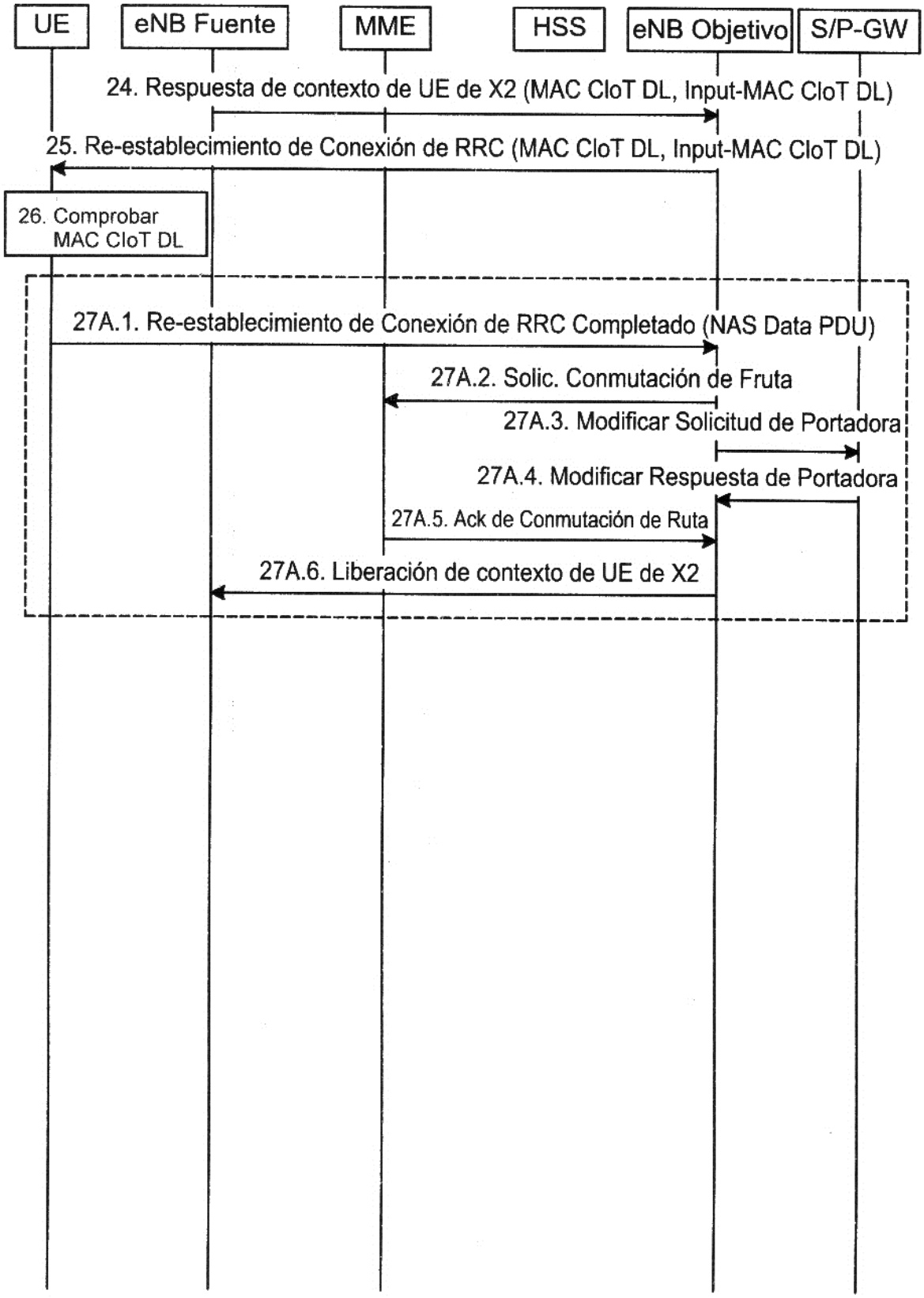
UE
eNB Fuente
MME
HSS
eNB Objetivo
S/P-GW
24. Respuesta de contexto de UE de X2 (MAC CIoT DL, Input-MAC CIoT DL)
25. Re-establecimiento de Conexión de RRC (MAC CIoT DL, Input-MAC CIoT DL)
26. Comprobar MAC CIoT DL
27A.1. Re-establecimiento de Conexión de RRC Completado (NAS Data PDU)
27A.2. Solic. Conmutación de Fruta
27A.3. Modificar Solicitud de Portadora
27A.4. Modificar Respuesta de Portadora
27A.5. Ack de Conmutación de Ruta
27A.6. Liberación de contexto de UE de X2

Fig. 4b

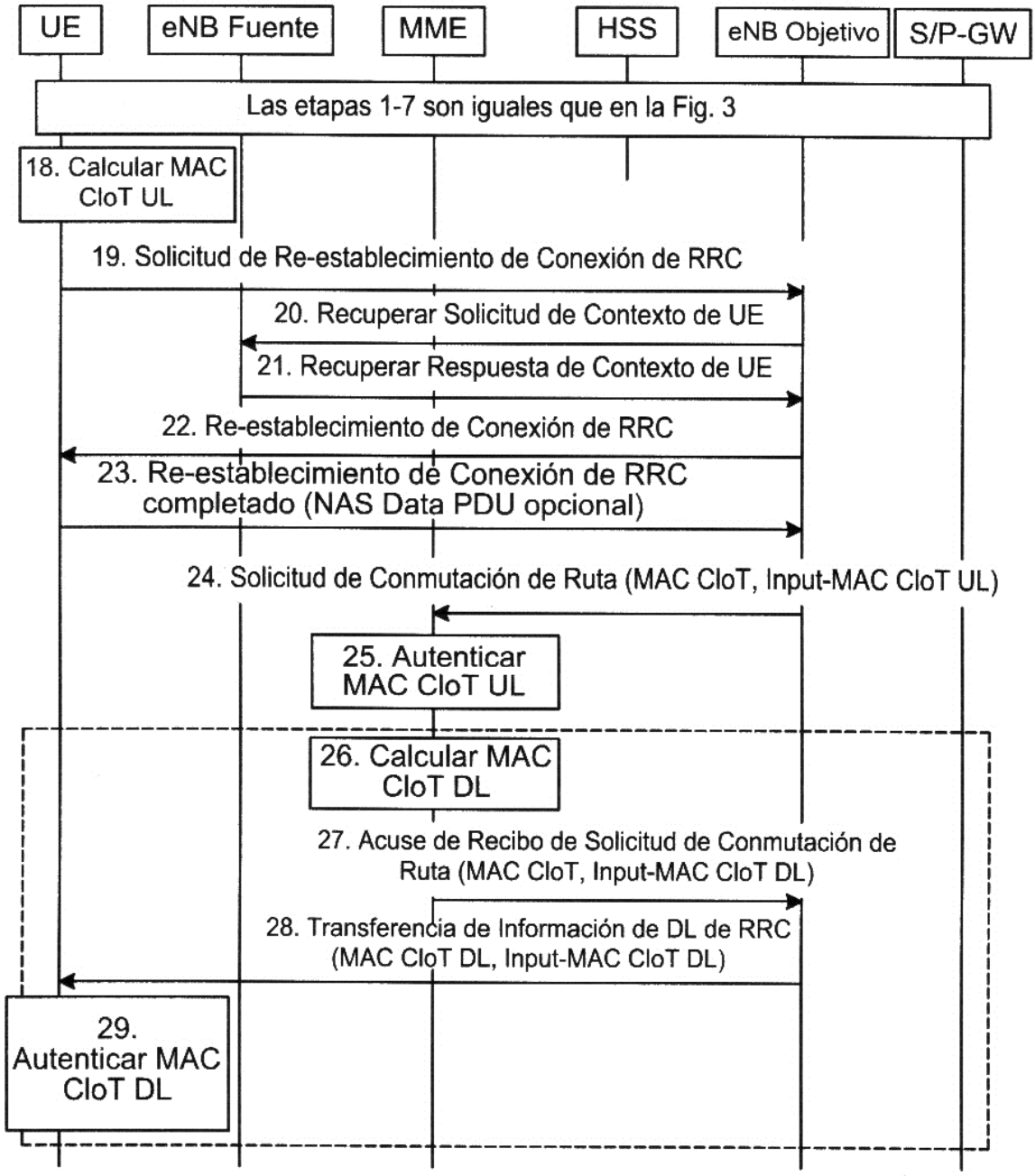
UE
eNB Fuente
MME
HSS
eNB Objetivo
S/P-GW
Las etapas 1-7 son iguales que en la Fig. 3
18. Calcular MAC CIoT UL
19. Solicitud de Re-establecimiento de Conexión de RRC
20. Recuperar Solicitud de Contexto de UE
21. Recuperar Respuesta de Contexto de UE
22. Re-establecimiento de Conexión de RRC
23. Re-establecimiento de Conexión de RRC completado (NAS Data PDU opcional)
24. Solicitud de Conmutación de Ruta (MAC CIoT, Input-MAC CIoT UL)
25. Autenticar MAC CIoT UL
26. Calcular MAC CIoT DL
27. Acuse de Recibo de Solicitud de Conmutación de Ruta (MAC CIoT, Input-MAC CIoT DL)
28. Transferencia de Información de DL de RRC (MAC CIoT DL, Input-MAC CIoT DL)
29. Autenticar MAC CIoT DL

Fig. 5

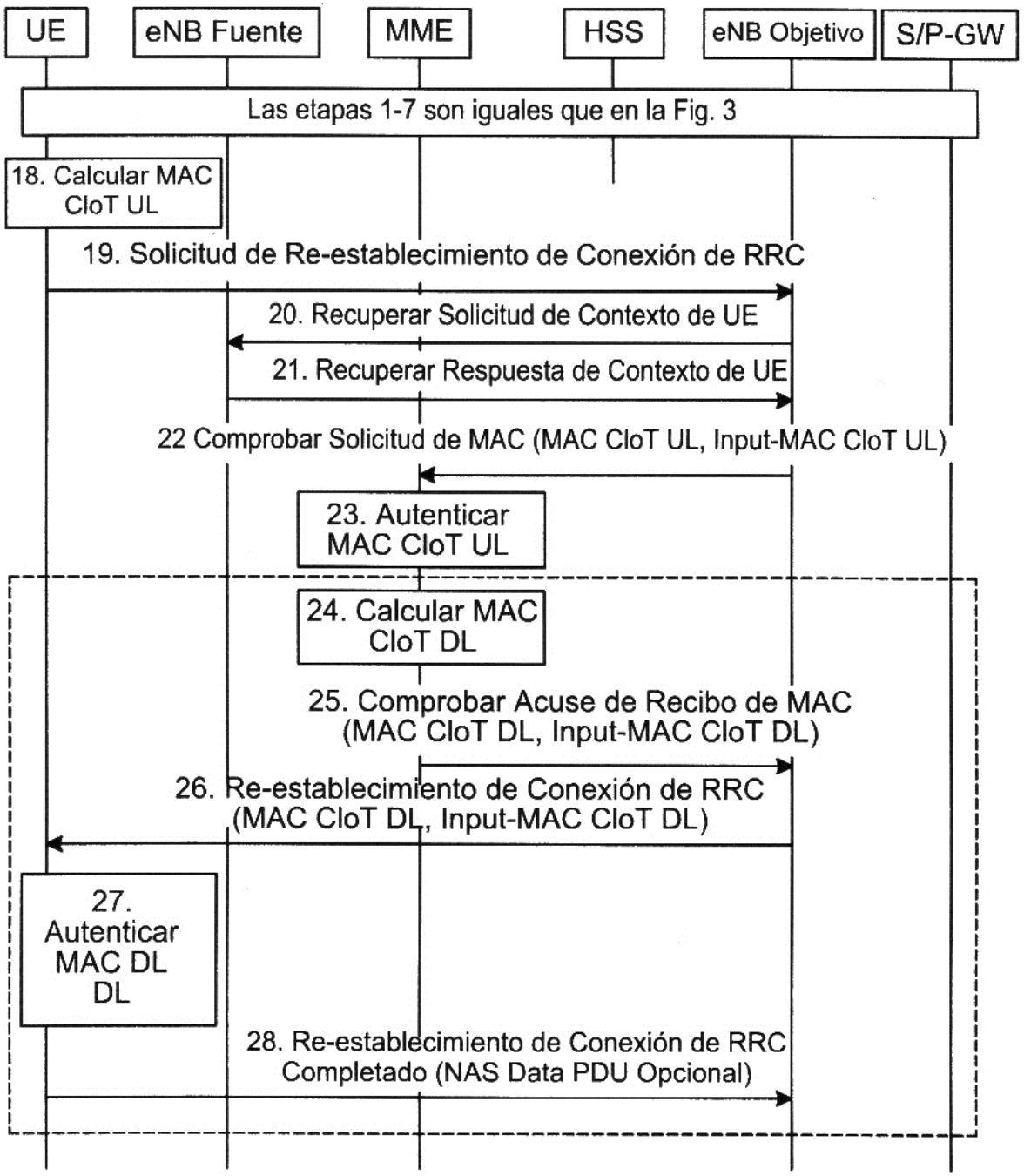
UE
eNB Fuente
MME
HSS
eNB Objetivo
S/P-GW
Las etapas 1-7 son iguales que en la Fig. 3
18. Calcular MAC CIoT UL
19. Solicitud de Re-establecimiento de Conexión de RRC
20. Recuperar Solicitud de Contexto de UE
21. Recuperar Respuesta de Contexto de UE
22 Comprobar Solicitud de MAC (MAC CIoT UL, Input-MAC CIoT UL)
23. Autenticar MAC CIoT UL
24. Calcular MAC CIoT DL
25. Comprobar Acuse de Recibo de MAC (MAC CIoT DL, Input-MAC CIoT DL)
26. Re-establecimiento de Conexión de RRC (MAC CIoT DL, Input-MAC CIoT DL)
27. Autenticar MAC DL DL
28. Re-establecimiento de Conexión de RRC Completado (NAS Data PDU Opcional)

Fig. 6

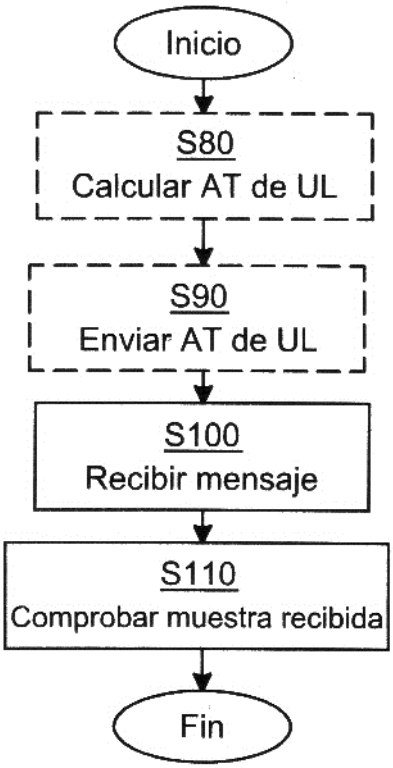

Fig. 7A

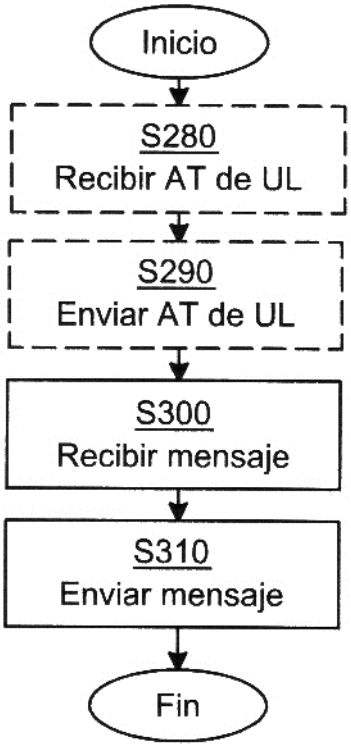

Fig. 7B

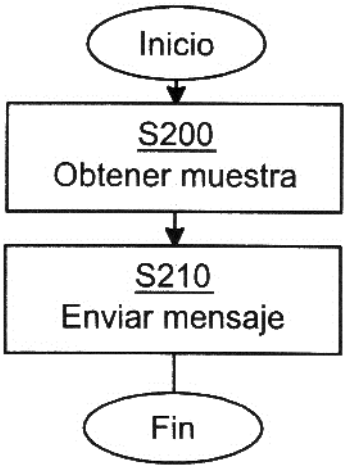

Fig. 7C

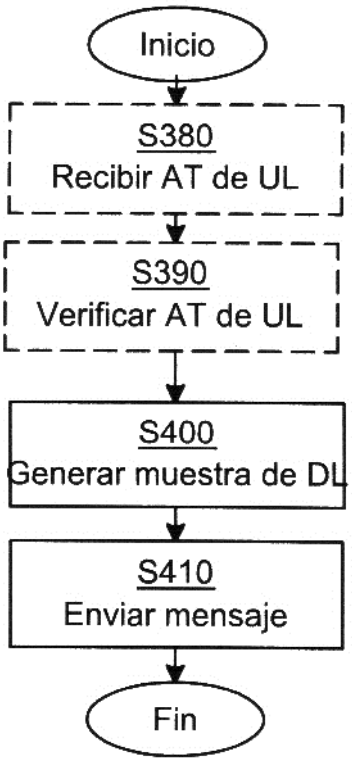

Fig. 7D

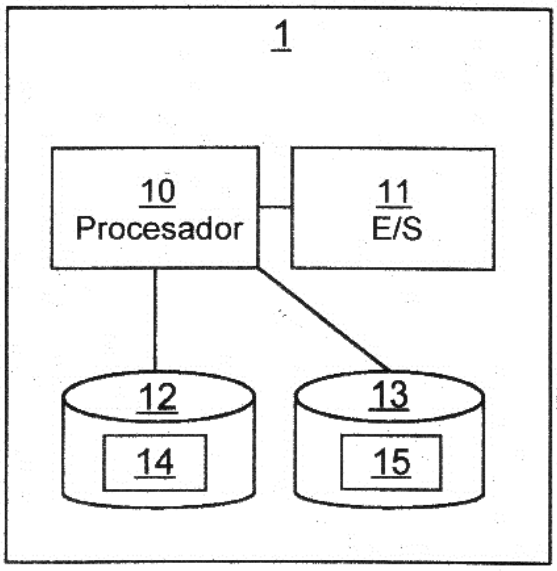

Fig. 8

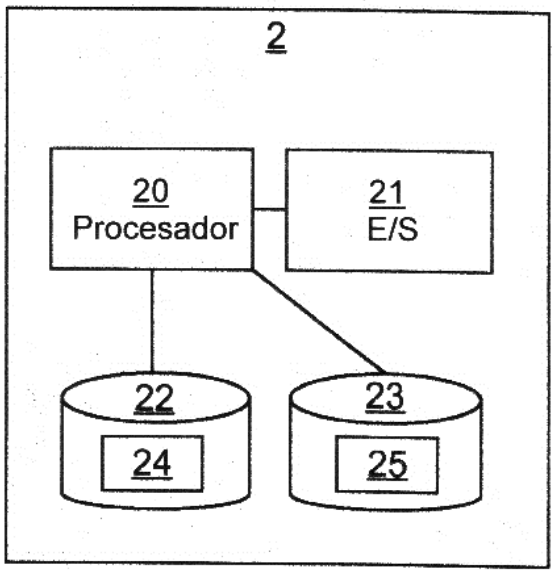

Fig. 9

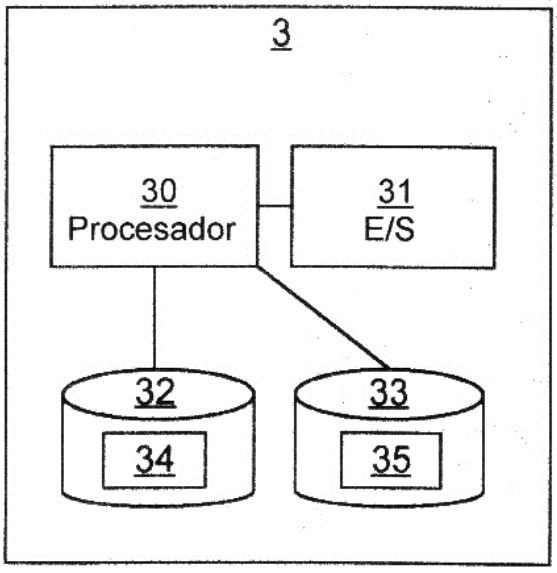

Fig. 10

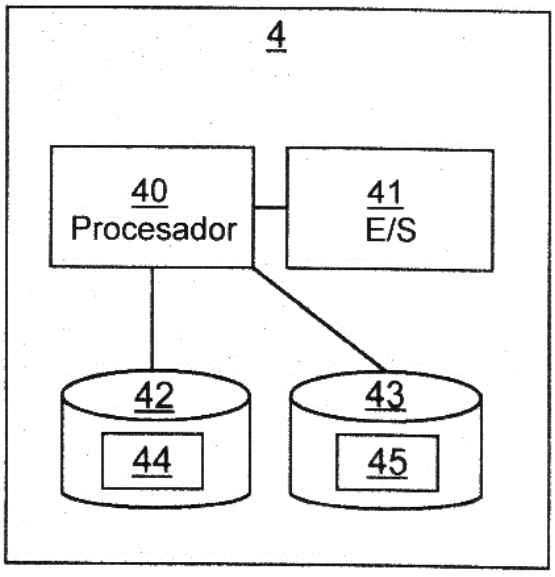

Fig. 11

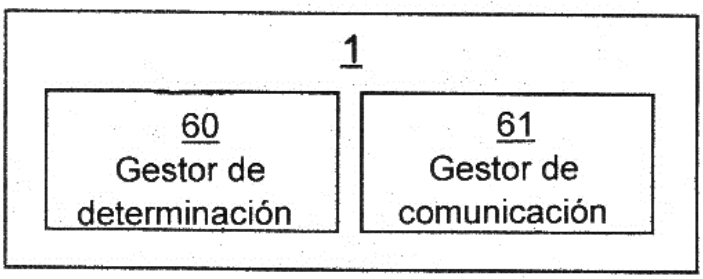

Fig. 12

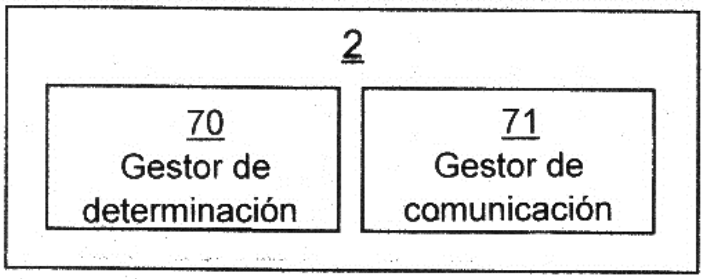

Fig. 13

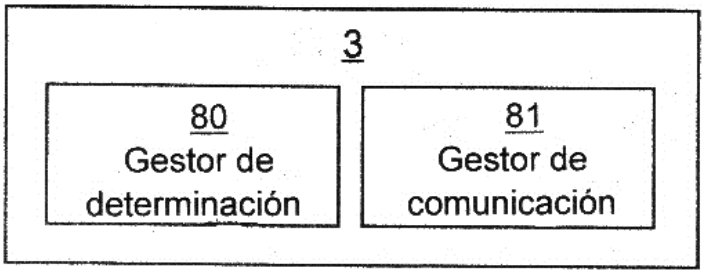

Fig. 14

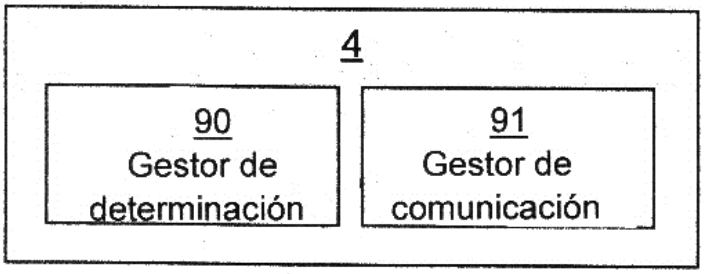

Fig. 15