(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 784 977**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04W 76/19 (2008.01)
H04W 4/70 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.01.2018 PCT/EP2018/051748**

(87) Fecha y número de publicación internacional: **02.08.2018 WO18138163**

(96) Fecha de presentación y número de la solicitud europea: **24.01.2018 E 18701745 (4)**

(97) Fecha y número de publicación de la concesión europea: **22.01.2020 EP 3479613**

(54) Título: **Restablecimiento de una conexión del control de los recursos de radio**

(30) Prioridad:

25.01.2017 US 201762450152 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.10.2020

(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

Restablecimiento de una conexión del control de los recursos de radio

CAMPO TÉCNICO

La invención hace referencia a métodos para restablecer una conexión del control de los recursos de radio entre un equipo de usuario y un Nodo B evolucionado de destino. Asimismo, se dan a conocer nodos de red en forma de entidades de gestión de la movilidad, nodos B evolucionados de origen y nodos B evolucionados de destino, así como programas informáticos y un producto de programa informático de los mismos.

ANTECEDENTES

Las optimizaciones de la Internet de las cosas desde celular (CIoT – Cellular Internet of Things, en inglés) mediante el plano de control (CP – Control Plane, en inglés) (también llamado Datos sobre estrato de no acceso (NAS) (DoNAS – Data over Non-Access Stratum, en inglés)) es una solución para transportar datos a través del NAS tal como se especifica en la especificación técnica TS 23.401 V14.2.0, apartado 5.3.4B del Proyecto de asociación de 3ra generación (3GPP – 3rd Generation Partnership Project, en inglés) (y en otras especificaciones, por ejemplo, el documento TS 24.301 V14.2.0). Las características de seguridad se especifican en el documento TS 33.401 V14.1.0, apartado 8.2. El impacto en seguridad de la solución básica es muy limitado. El propósito de la función DoNAS es enviar datos por medio de señalización del NAS sin establecer portadores de datos de radio (DRB – Data Radio Bearers, en inglés) y sin establecer la seguridad del Estrato de acceso (AS – Access Stratum, en inglés). La intención es ahorrar señalización. La figura 1, que corresponde a la figura 5.3.4B.2-1 del documento TS 23.401 V14.2.0, ilustra el principio.

El elemento de trabajo en el documento R3-161324 del 3GPP analiza las mejoras de movilidad para CP CIoT. Los traspasos no son compatibles con CP CIoT, pero un equipo de usuario (UE – User Equipment, en inglés) puede moverse de todos modos, causando un fallo del enlace de radio (RLF – Radio Link Failure, en inglés) cuando el UE está en modo conectado, es decir, tiene una conexión del Control de recursos de radio (RRC – Radio Resource Control, en inglés) con un Nodo B evolucionado (eNB – Evolved Node B, en inglés). Esto ha planteado el problema de qué hacer en tal caso. Puesto que la seguridad del AS no es compatible con la función CP CIoT, los mecanismos existentes para el RLF no se pueden utilizar de manera segura tal como están. En otras palabras, no es aceptable en términos de seguridad utilizar el mecanismo de manejo del RLF existente en la CP CIoT.

La capa de RRC está especificada en los sistemas LTE (Evolución a largo plazo – Long Term Evolution, en inglés), véase, por ejemplo, el documento TS 36.331 V14.1.0 del 3GPP, como que incluye un elemento de información (IE – Information Element, en inglés) llamado ShortMAC-I que se utiliza para la identificación del UE, por ejemplo, durante los procedimientos de restablecimiento de la conexión del RRC. El cálculo del ShortMAC-I incluye lo siguiente como entrada:

- Clave de integridad del RRC: SECUENCIA DE BITS (TAMAÑO (128))
- Identidad de la celda de destino: SECUENCIA DE BITS (TAMAÑO (28))
- Identidad de celda física de la celda de origen: entero (0 ... 503)
- C-RNTI (Identificador temporal de la red de radio celular – Cell Radio Network Temporary Identifier, en inglés) del UE en la celda de origen: SECUENCIA DE BITS (TAMAÑO (16))

La función utilizada está especificada en el documento TS 33.401 V14.1.0.

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

- Clave de integridad del RRC: SECUENCIA DE BITS (TAMAÑO (128))
- Identidad de la celda de destino: SECUENCIA DE BITS (TAMAÑO (28))
- Identidad de celda física de la celda de origen: ENTERO (0 ... 503)
- C-RNTI del UE en la celda de origen: SECUENCIA DE BITS (TAMAÑO (16))
- Constante de reanudación

Cabe señalar que el cálculo de ShortResumeMAC-I incluye, adicionalmente, una constante de reanudación, que permite la diferenciación de ShortMAC-I de ResumeShortMAC-I. La función utilizada está especificada en el documento TS 33.401 V14.1.0. El documento US-2009/258631-A1 da a conocer una característica en un sistema de telecomunicaciones, que está relacionada con el traspaso, más específicamente, con la señalización de control del traspaso. Las realizaciones del sistema comprenden nodos tales como una entidad de gestión de la movilidad (MME – Mobility Management, Entity, en inglés), un equipo de usuario (UE), un eNB de destino y un eNB de origen. El documento está relacionado con el encadenamiento de tokens de autorización para un UE durante el traspaso.

El documento S3-162089 (antiguo S3-161717) del 3GPP con el título “Security of RRC Connection re-establishment

of NB-IoT for CP solution" da a conocer una solución en la que una entidad de gestión de la movilidad (MME) proporciona una clave $K_{eNB-RRC}$ a un AS de equipo de usuario.

El documento EP-2426996-A1 da a conocer un método de recuperación de servicio en el que se recibe una solicitud de restablecimiento del RRC o un mensaje de actualización de celda desde un UE.

COMPENDIO

Un objeto de la invención es permitir una menor señalización y/o una menor potencia de procesamiento durante el restablecimiento de una conexión del control de los recursos de radio.

De acuerdo con un primer aspecto de la invención, se presenta un método para restablecer una conexión del Control de los recursos de radio (RRC) entre un Equipo de usuario (UE) y un Nodo B evolucionado (eNB de destino). El método es llevado a cabo por el eNB de destino y comprende recibir una solicitud de restablecimiento de la conexión del RRC del UE, en el que la solicitud de restablecimiento de la conexión del RRC incluye un token de autenticación generado con una clave de integridad del estrato de no acceso (NAS) y la identidad de una celda de destino como entrada; enviar un mensaje de verificación a una entidad de gestión de la movilidad (MME), en el que el mensaje de verificación incluye el token de autenticación recibido; y recibir una respuesta de la MME, de verificación del token de autenticación. De este modo, se consigue, por ejemplo, que no sea necesario generar claves del estrato de acceso (AS).

De acuerdo con un segundo aspecto, se presenta un método para restablecer una conexión del RRC entre un UE y un eNB de destino. El método es llevado a cabo por una MME y comprende recibir un mensaje de verificación del eNB de destino, en el que el mensaje de verificación incluye un token de autenticación generado en el UE con una clave de integridad del NAS y la identidad de una celda de destino como entrada; verificar el token de autenticación recibido; y enviar al eNB de destino un mensaje de respuesta de verificación, que verifica el token de autenticación recibido.

Un tercer hace referencia a un eNB de destino para restablecer una conexión del RRC entre un UE y el eNB de destino. El eNB de destino comprende un procesador; y un producto de programa informático que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el eNB de destino reciba una solicitud de restablecimiento de la conexión del RRC del UE, en el que la solicitud de restablecimiento de conexión del RRC incluye un token de autenticación generado con una clave de integridad del NAS y la identidad de una celda de destino como entrada; envíe un mensaje de verificación a una MME, en el que el mensaje de verificación incluye el token de autenticación recibido; y reciba una respuesta de la MME, de verificación del token de autenticación.

En una realización del tercer aspecto, el mensaje de verificación es una solicitud de verificación de MAC, y la respuesta es un acuse de recibo de verificación de MAC o un fallo de verificación de MAC. En dicha realización, la solicitud de verificación de MAC puede incluir el MAC-CIoT como dicho token de autenticación, y/o el Input-MAC-CIoT.

En otra realización del tercer aspecto, el mensaje de verificación es una solicitud de cambio de ruta, y la respuesta es un acuse de recibo de solicitud de cambio de ruta o un fallo de solicitud de cambio de ruta. En dicha realización, la solicitud de cambio de ruta puede incluir el MAC-CIoT como dicho token de autenticación y/o el Input-MAC-CIoT.

Un cuarto aspecto hace referencia a un eNB de origen para restablecer una conexión del RRC entre un UE y un eNB de destino. El eNB de origen comprende un procesador; y un producto de programa informático que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el eNB de origen: reciba un mensaje X2 del eNB de destino, en el que el mensaje incluye un token de autenticación generado por el UE con una clave de integridad del NAS como entrada; envíe una solicitud de verificación a una MME para verificar el token de autenticación recibido, incluyendo dicha solicitud de verificación el token de autenticación; reciba una respuesta de verificación de la MME, verificando el token de autenticación recibido; y envíe un mensaje de fallo de contexto del UE al eNB de destino.

Un quinto aspecto hace referencia a una MME para restablecer una conexión del RRC entre un UE y un eNB de destino. La MME comprende un procesador; y un producto de programa informático que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que la MME: reciba un mensaje de verificación del eNB de destino, en el que el mensaje de verificación incluye un token de autenticación generado en el UE con una clave de integridad del NAS y una identidad de la celda de destino como entrada; verifique el token de autenticación recibido; y envíe al eNB de destino un mensaje de respuesta de verificación que verifica el token de autenticación recibido.

En una realización del quinto aspecto, recibir el mensaje de verificación es recibir una solicitud de cambio de ruta del eNB de destino, y enviar el mensaje de respuesta de verificación es enviar un acuse de recibo de solicitud de cambio de ruta al eNB de destino (3) o se envía un Fallo de solicitud de cambio de ruta al eNB de destino.

En otra realización del quinto aspecto, recibir el mensaje de verificación es recibir una solicitud de verificación de

MAC del eNB de destino, y enviar el mensaje de respuesta de verificación es enviar un acuse de recibo de verificación de MAC o un fallo de verificación de MAC al eNB de destino. En dicha realización, la solicitud de verificación de MAC puede incluir el MAC-CIoT como dicho token de autenticación, y/o el Input-MAC-CIoT.

Un sexto aspecto hace referencia a un programa informático para restablecer una conexión del RRC entre un UE y un eNB de destino. El programa informático comprende un código de programa informático que, cuando es ejecutado en el eNB de destino, hace que el eNB de destino:

reciba una solicitud de restablecimiento de la conexión del RRC del UE, en el que la solicitud de restablecimiento de la conexión del RRC incluye un token de autenticación generado con una clave de integridad del NAS y la identidad de una celda de destino como entrada;

envíe un mensaje de verificación a una MME, en el que el mensaje de verificación incluye el token de autenticación recibido; y

reciba una respuesta de la MME, de verificación del token de autenticación.

Un séptimo aspecto de la invención hace referencia a un programa informático para restablecer una conexión del RRC entre un UE y un eNB de destino. El programa informático comprende un código de programa informático que, cuando es ejecutado en una MME, hace que la MME:

reciba un mensaje de verificación del eNB de destino, en el que el mensaje de verificación incluye un token de autenticación generado en el UE con una clave de integridad del NAS y una identidad de la celda de destino como entrada;

verifique el token de autenticación recibido; y

envíe al eNB de destino un mensaje de respuesta de verificación, verificando el token de autenticación recibido.

Un octavo aspecto hace referencia a un método para restablecer una conexión del RRC entre un UE y un eNB de destino. El UE lleva a cabo este método y comprende:

– generar un token de autenticación con una clave de integridad del NAS y la identidad de una celda de destino como entrada,

– enviar un primer mensaje de restablecimiento de la conexión del RRC al eNB de destino, en el que el primer mensaje de restablecimiento de la conexión del RRC incluye el token de autenticación y

– recibir un segundo mensaje de restablecimiento de la conexión del RRC del eNB de destino.

La identidad de la celda de destino puede estar incluida también, en una realización del primer, segundo, tercer y quinto aspecto, en el mensaje de verificación. En caso de que la identidad de la celda de destino esté incluida en el mensaje de verificación, la verificación puede ser llevada a cabo, en las realizaciones del segundo y quinto aspecto, comparando el token de autenticación recibido con un token de autenticación calculado por la MME con la clave de integridad del RRC y la identidad de la celda de destino como entrada.

En la totalidad de los ocho aspectos anteriores, el restablecimiento para la conexión del RRC puede ser para optimizaciones de la Internet de las cosas mediante el plano de control.

En general, todos los términos utilizados en la lista detallada deben ser interpretados de acuerdo con su significado ordinario en el campo técnico, a menos que se defina explícitamente lo contrario en este documento. Todas las referencias a “un / el elemento, aparato, componente, medio, paso, etc.” deben ser interpretadas de manera abierta, como refiriéndose, al menos, a una instancia del elemento, aparato, componente, medio, paso, etc., a menos que se indique explícitamente lo contrario. Los pasos de cualquier método dado a conocer en el presente documento no tienen que ser llevados a cabo en el orden exacto dado a conocer, a menos que se indique explícitamente.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La invención se describe a continuación, a modo de ejemplo, con referencia a los dibujos adjuntos, en los que:

La figura 1 muestra esquemáticamente la señalización del principio de DoNAS;
la figura 2 ilustra esquemáticamente un entorno en el que se pueden aplicar las realizaciones presentadas en este documento;
la figura 3a muestra esquemáticamente la señalización de acuerdo con una realización presentada en este documento;

la figura 3b muestra esquemáticamente la señalización de acuerdo con la realización presentada junto con la figura 3a;
la figura 4 muestra esquemáticamente la señalización de acuerdo con una realización presentada en este documento;
la figura 5 muestra esquemáticamente la señalización de acuerdo con una realización presentada en este documento;
las figuras 6A a 6D son diagramas de flujo que ilustran métodos de acuerdo con las realizaciones presentadas en este documento;
las figuras 7 a 9 son diagramas esquemáticos que ilustran algunos componentes de entidades presentadas en este documento; y
las figuras 10 a 12 son diagramas esquemáticos que muestran módulos funcionales de realizaciones presentadas en este documento.

DESCRIPCIÓN DETALLADA

La invención se describirá a continuación de manera más completa con referencia a los dibujos adjuntos, en los que se muestran ciertas realizaciones de la invención. No obstante, esta invención puede ser llevada a cabo en muchas formas diferentes, y no debe ser interpretada como limitada a las realizaciones expuestas en el presente documento; por el contrario, estas realizaciones son proporcionadas a modo de ejemplo, para que esta invención sea exhaustiva y completa, y transmita de manera completa el alcance de la invención a los expertos en la técnica. Números iguales se refieren a elementos similares en toda la descripción.

En primer lugar, el restablecimiento de la conexión del control de recursos de radio (RRC) y los procedimientos de suspensión / reanudación de la conexión del RRC son soluciones existentes, que podrían ser candidatas para manejar el fallo del enlace de radio en el caso de optimizaciones en caso de una internet de las cosas celular mediante el plano de control (CP) (CIoT). Ambas soluciones existentes utilizan un token de autenticación del equipo de usuario (UE) tal como se ha descrito en los antecedentes para mostrarle a un NodoB (eNB) evolucionado que un UE genuino desea restablecer o reanudar una conexión del RRC. No obstante, esas soluciones se basan en la existencia de seguridad del estrato de acceso (AS) (especialmente seguridad del RRC), pero la seguridad del AS y la seguridad del RRC no existen o no se utilizan para las optimizaciones de la CP CIoT. Por lo tanto, el restablecimiento de la conexión del RRC y los procedimientos de suspensión / reanudación de la conexión del RRC tal como están, no son aceptables en términos de seguridad para ser utilizados para manejar la movilidad en la CP CIoT.

En segundo lugar, una solución descrita en la contribución del 3GPP S3-161717 propone que un token de autenticación esté basado en una nueva clave de integridad del RRC (llamada KeNB-RRC) que puede ser obtenida a partir tanto del UE como de una entidad de gestión de la movilidad (MME), sin configurar la seguridad del AS (incluida la seguridad del RRC) entre el UE y el eNB de origen por medio del procedimiento de Comando de modo de seguridad (SMC – Security Mode Command, en inglés) del AS, y el token se utilizaría entre el UE y el eNB de destino. No obstante, sin el procedimiento SMC del AS soportado con el caso de CP CIoT, el UE y los eNB no pueden ponerse de acuerdo sobre un algoritmo de integridad común, que se utilizaría para el cálculo y la verificación de tokens. Por lo tanto, la solución descrita en la contribución del 3GPP S3-161717 parece no ser adecuada para manejar la movilidad en la CP CIoT.

En lugar de utilizar claves del AS, una clave de integridad del estrato de no acceso (NAS) se utiliza de acuerdo con las realizaciones de la invención para garantizar el restablecimiento del RRC para la CP CIoT, por ejemplo, el restablecimiento del RRC entre un UE y un eNB de destino en un escenario de CP CIoT. En particular, un token de autenticación generado por un UE se calcula utilizando la clave de integridad del NAS. El token de autenticación del UE se envía a una MME para su verificación. Se identifican los siguientes casos y algunos de ellos están dentro del alcance de la invención reivindicada de esta aplicación, mientras que otros pueden estar dentro del alcance de otras aplicaciones:

El token de autenticación es enviado desde el UE a un eNB de destino. Existen las siguientes soluciones variantes de lo que puede suceder a continuación:

1. el token de autenticación es enviado desde el eNB de destino a un eNB de origen

    1a. el token de autenticación es verificado por el eNB de origen con una clave del AS (no obstante, esta realización forma parte de otra aplicación PCT / EP2017 / 078012);

    1b. el token de autenticación es enviado desde el eNB de origen a la MME y la MME lo verifica con una clave del NAS, por ejemplo, una clave de integridad del NAS;

2. el token de autenticación es enviado desde el eNB de destino a la MME

    2a. en un mensaje de cambio de ruta, y la MME verifica el token con una clave del NAS, por ejemplo, una

clave de integridad del NAS, como en las reivindicaciones de esta solicitud;

2b. en algún otro mensaje, antes de que tenga lugar una búsqueda de contexto o un cambio de ruta, y la MME verifica el token con una clave del NAS, por ejemplo, una clave de integridad del NAS, como en las reivindicaciones de esta solicitud.

Cuando el cálculo del token de autenticación se basa en claves del NAS, no hay necesidad de establecer claves del AS, en absoluto. Por lo tanto, se puede evitar la generación de claves del AS únicamente para su utilización en el RRC.

Cuando el UE experimenta un fallo del enlace de radio (RLF) durante la conexión de la CP CIoT (DoNAS), el UE intenta restablecer la conexión del RRC a otro eNB, véase la figura 2.

El token de autenticación del UE para utilizar en la CP CIoT (denominado MAC-CIoT) es un token que se utilizará para la autenticación del UE, es decir, para determinar que existe un UE genuino.

El MAC-CIoT se puede calcular con lo siguiente como entrada:

– Key-MAC-CIoT: clave de integridad del NAS (NAS-int), indicada con KNASint en 33.401 V14.1.0, o una clave obtenida a partir del NAS-int o una clave obtenida a partir de una clave raíz KASME o cualquier otra clave raíz, por ejemplo, en una red 5G o una red futura, tal como KAUSF, KSEAF y KAMF
– Identidad de la celda de destino
– Identidad de celda física de la celda de origen
– C-RNTI del UE en la constante de la celda de origen (la constante permite la diferenciación del MAC-CIoT con respecto al ShortResumeMAC-I y al ShortMAC -I).

En una realización, el token de autenticación puede ser calculado, al menos, con la identidad de la celda de destino y la clave de integridad del NAS como entrada. Cabe señalar que la clave Key-MAC-CIoT / NAS dentro del alcance de las reivindicaciones de esta solicitud es la clave de integridad del NAS.

La entrada utilizada para el cálculo del MAC-CIoT se denominará Input-MAC-CIoT.

La función utilizada para el del MAC-CIoT (denominada Fun-MAC-CIoT) podría ser la misma utilizada en el Anexo B.2 del documento TS 33.401 para el restablecimiento del RRC y la reanudación del RRC, es decir, un algoritmo de integridad del NAS de 128 bits, que puede ser 128-EIA1, 128-EIA2 y 128-EIA3.

Con referencia a la figura 2, cuando la MME 4 ha autenticado el UE 1 y se ha establecido la seguridad entre la MME y el UE, ambos conocen la Fun-MAC-CIoT y tienen o pueden obtener la Key-MAC-CIoT a partir del anterior.

Se puede enviar un token MAC-CIoT desde el UE al eNB 3 de destino.

Existen las siguientes soluciones variantes de lo que puede suceder a continuación:

1. El token MAC-CIoT es enviado desde el eNB 3 de destino al eNB 2 de origen

1a. el token MAC-CIoT es verificado con la clave del AS (no forma parte de la invención reivindicada de esta solicitud);

1b. el token MAC-CIoT es enviado desde el eNB 2 de origen a la MME 4, y es verificado por la MME 4 con una clave del NAS.

2. El token MAC-CIoT es enviado desde el eNB 3 de destino a la MME 4

2a. en el mensaje de cambio de ruta, y la MME 4 verifica el token con la clave del NAS;

2b. en algún otro mensaje, antes de que tenga lugar la búsqueda de contexto o el cambio de ruta, y la MME 4 verifica el token con la clave del NAS3.

Variante 1b: el MAC-CIoT es enviado desde el eNB de destino al eNB de origen y desde el eNB de origen a la MME, y es verificado por la MME con la clave del NAS, véanse las figuras 3a y 3b. El orden de los pasos, mensajes, campos puede ser alterado; se pueden combinar mensajes; se pueden poner campos en diferentes mensajes, etc. para conseguir el mismo efecto.

Este es un ejemplo, aplicable a una situación en la que se envían datos del NAS para optimizaciones de CP CIoT y se produce un RLF, por ejemplo, durante el envío de los datos del NAS.

Los pasos 1 a 15 de la figura 3a no son nuevos como tales, ya que se describen en las especificaciones actuales del 3GPP. El UE establece la conexión del RRC y envía datos a través del NAS, que son reenviados desde la MME, a la pasarela de servicio (S-GW – Serving Gateway, en inglés) / pasarela de la red de datos en paquetes (P-GW - Packet Data Network-Gateway, en inglés). El fallo del enlace de radio se produce (en el paso 15). El RLF también se puede producir antes de que el UE haya recibido datos de enlace descendente (DL – DownLink, en inglés).

Paso 16. El UE inicia la conexión del RRC enviando un mensaje de acceso aleatorio al eNB de destino.

Paso 17. El eNB de destino responde con una respuesta de acceso aleatorio al UE.

Paso 18. El UE genera un token de autenticación, MAC-CIoT. El token se puede calcular de la siguiente manera:

$$\text{token} = f(\text{PCI de origen, C-RNTI de origen, Cell-ID de destino, clave de NAS, entrada de reproducción})$$

donde la clave del NAS es la clave actual de integridad del NAS o una derivada de la misma. f = función.

Paso 19. El UE envía un mensaje del RRC al eNB de destino incluyendo el MAC-CIoT. El mensaje del RRC puede ser, por ejemplo, una solicitud de restablecimiento de la conexión del RRC (tal como se ilustra en la figura 3a), una solicitud de reanudación del RRC o algún otro mensaje del RRC. En las reivindicaciones de la presente solicitud, el mensaje del RRC es la solicitud de restablecimiento de la conexión del RRC.

Paso 20. El eNB de destino envía un mensaje X2 al eNB de origen que incluye el MAC-CIoT y el Input-MAC-CIoT si es necesario. El mensaje X2 puede ser, por ejemplo, un mensaje de búsqueda de contexto X2.

Paso 21. El eNB de origen envía un mensaje S1 a la MME que incluye el MAC-CIoT y el Input-MAC-CIoT.

Paso 22. Tras la recepción del MAC-CIoT y del Input-MAC-CIoT, la MME verifica el MAC-CIoT realizando el mismo cálculo que el UE realizó en el paso 18, y comparándolo con el MAC-CIoT recibido. Si la verificación tiene éxito, la MME envía un mensaje S1 que indica éxito al eNB de origen. Si la verificación no tiene éxito, la MME envía un mensaje S1 que indica un error al eNB de origen.

Paso 23. Tras la recepción del mensaje S1 de la MME, el eNB de origen verifica el código de resultado en el mensaje.

Paso 24 ilustrado en la figura 3b: Si la autenticación en el paso 23 tiene éxito:

24.A.1. El eNB de origen envía la respuesta de contexto al UE.
24.A.2. y 24.A.3. El eNB de destino ejecuta el resto de la conexión del RRC con el UE, incluidos, por ejemplo, una configuración de restablecimiento de la conexión del RRC desde el eNB de destino al UE y un mensaje de configuración de conexión del RRC completada desde el UE al eNB de destino.
24.A.4. a 24.A.7. Procedimientos de cambio de ruta y de modificación de portador, que, en este documento, comprenden una solicitud de cambio de ruta del eNB de destino a la MME, una solicitud de cambio de portador del eNB de destino a la S/P-GW, una respuesta de modificación de portador de la S/P-GW al eNB de destino, y un acuse de recibo de cambio de ruta de la MME al eNB de destino.
24.A.8. El eNB de destino, a continuación, indica al eNB de origen que libere el contexto del UE enviando un mensaje X2 llamado liberación de contexto del UE.
Si la autenticación en el paso 23 falla:
24.B.1. El eNB de origen envía un mensaje de fallo de búsqueda de contexto del UE al eNB de destino. El eNB de destino, por lo tanto, sabe que el MAC-CIoT mencionado en los pasos anteriores no es auténtico.
24.B.2. El eNB de destino desencadena la liberación de la conexión del RRC con el UE enviando la liberación de la conexión del RRC al UE.

Variante 2a: el MAC-CIoT es enviado desde el eNB de destino a la MME en un mensaje de solicitud de cambio de ruta de SIAP. La MME autentica el MAC-CIoT. Esto se ilustra en la figura 4.

Esta variante 2a se basa en un mensaje SIAP existente llamado Solicitud de cambio de ruta que es enviado desde el eNB de destino a la MME. La solicitud de cambio de ruta se modifica para poder contener el MAC-CIoT y el Input-MAC-CIoT. Los mensajes de SIAP existentes llamados Acuse de recibo de solicitud de cambio de ruta y Fallo de cambio de ruta que se envían desde la MME al eNB de destino se utilizan, respectivamente, para indicar que el MAC-CIoT era auténtico o no auténtico. Una realización a modo de ejemplo, de hacer esto se muestra en la figura 4 y los pasos se describen a continuación. El orden de los pasos, mensajes y campos puede ser modificado; se pueden combinar mensajes; se pueden poner campos en diferentes mensajes, etc. para conseguir el mismo efecto.

Los pasos 1 a 17 son los mismos que los descritos anteriormente en relación con la figura 3a.

Los pasos 18 a 19 también son los mismos que los descritos anteriormente en relación con la figura 3a, pero también se muestran en la figura 4 para la integridad del procedimiento de restablecimiento de la conexión del RRC.

Paso 20. El eNB de destino solicita al eNB de origen que envíe el contexto del UE. El mensaje X2 existente llamado Recuperar solicitud de contexto de UE podría ser adaptado según sea necesario (por ejemplo, utilizando ReestabUE-Identity en lugar de Resumeldentity).

Paso 21. El eNB de origen envía el contexto del UE al eNB de destino. El mensaje X2 existente llamado Recuperar respuesta de contexto del UE podría ser adaptado según sea necesario.

Paso 22. El eNB de destino envía un mensaje de restablecimiento de la conexión del RRC al UE.

Paso 23. El UE envía el mensaje de restablecimiento de la conexión del RRC completada que, opcionalmente, contiene una PDU (Unidad de datos de protocolo – Protocol Data Unit, en inglés) de datos del NAS al eNB de destino.

Paso 24. El eNB de destino envía la solicitud de cambio de ruta a la MME. En la solicitud de cambio de ruta, el eNB de destino incluye el MAC-CIoT y el Input-MAC-CIoT. El Input MAC-CIoT puede estar encriptado, pero no tiene que estar encriptado en todas las realizaciones. El eNB de destino recibió el MAC-CIoT en el paso 19. El Input-MAC-CIoT puede incluir información que el eNB de destino recibió en el paso 19 y/o el paso 21, y/o la propia información del eNB de destino. La solicitud de cambio de ruta contiene la información del UE que le permite a la MME identificar el contexto del UE en la MME. La información de esa UE se denomina hoy en día “ID de SIAP del UE de la MME de origen”, que el eNB de destino puede proporcionar a partir de la información que recibió en el paso 23.

Paso 25. La MME autentica el MAC-CIoT utilizando el Input-MAC-CIoT y la Key-MAC-CIoT como entrada a la Fun-MAC-CIoT.

Paso 26. Si la autenticación en el paso 25 tiene éxito:

26.A.1. La MME envía un mensaje de confirmación de solicitud de cambio de ruta al eNB de destino. El eNB de destino sabe que el MAC-CIoT mencionado en los pasos anteriores es auténtico.
26.A.2. a 26.A.3. La MME desencadena la modificación del portador, por ejemplo, enviando una solicitud de modificación de portador a la S/P-GW y recibiendo una respuesta de modificación de portador de la S/P-GW.
26.A.4. El eNB de destino, a continuación, indica al eNB de origen que libere el contexto del UE enviando un mensaje X2 llamado Liberación de contexto del UE.

Si la autenticación falla en el paso 25, siguen los pasos 26.B.1 y 26.B.2:

26.B.1. La MME envía un mensaje de fallo de solicitud de cambio de ruta al eNB de destino. El eNB de destino, por lo tanto, sabe que el MAC-CIoT mencionado en los pasos anteriores de esta variante no es auténtico.
26.B.2. El eNB de destino desencadena la liberación de la conexión del RRC con el UE enviando la liberación de la conexión del RRC al UE.

Variante 2b: el MAC-CIoT es enviado desde el eNB de destino a la MME en un nuevo mensaje de SIAP. La MME autentica el MAC-CIoT. Esto se ilustra en la figura 5.

Esta variante se basa en un nuevo mensaje de SIAP (denominado Solicitud de verificación de MAC) que es enviado desde el eNB de destino a la MME. El mensaje CheckMACReq puede contener el MAC-CIoT y el Input-MAC-CIoT.

De manera similar, los nuevos mensajes de SIAP, indicados con verificar acuse de recibo de MAC y verificar fallo de MAC, que se envían desde la MME al eNB de destino se utilizan para indicar, respectivamente, que el MAC-CIoT era auténtico o no auténtico. Una realización, a modo de ejemplo, de hacer esto, se muestra en la figura 5 y los pasos se describen a continuación. El orden de los pasos, mensajes, campos pueden ser alterados; se pueden combinar mensajes; se pueden poner campos en diferentes mensajes, etc. para conseguir el mismo efecto.

Los pasos 1 a 17 son los mismos que se explicaron anteriormente en relación con la figura 3.

Los pasos 18 a 19 también son los mismos que se explicaron anteriormente en relación con la figura 3, pero también se muestran en la figura 5 para completar el procedimiento de restablecimiento de la conexión del RRC.

Paso 20. El eNB de destino solicita al eNB de origen que envíe el contexto del UE. El mensaje X2 existente llamado Recuperación de solicitud de contexto del UE podría ser adaptado según sea necesario (por ejemplo, utilizando ReestabUE-Identity en lugar de Resumeldentity).

Paso 21. El eNB de origen envía el contexto del UE al eNB de destino. El mensaje X2 existente llamado Recuperación de respuesta de contexto del UE podría ser adaptado según sea necesario. El contexto de dicho UE indica al eNB de destino la MME correspondiente en la que está registrado el UE.

Paso 22. El eNB de destino envía la solicitud de verificación de MAC a la MME identificada en el paso 21. En la solicitud de verificación de MAC, el eNB de destino incluye el MAC-CIoT y el Input-MAC-CIoT. El eNB de destino recibió dicho MAC-CIoT en el paso 19. El Input-MAC-CIoT podría incluir información que el eNB de destino recibió en el paso 19 y/o el paso 21, y/o la propia información del eNB de destino. La solicitud de verificación de MAC también puede contener información del UE que le permite a la MME identificar el contexto de la UE en la MME. La información de ese UE podría ser, por ejemplo, la ID de SIAP del UE de la MME que el eNB de destino recibió del eNB de origen en el paso 21.

Paso 23. La MME autentica el MAC-CIoT utilizando el Input-MAC-CIoT y la Key-MAC-CIoT como entrada a la Fun-MAC-CIoT.

Paso 24.
Si la autenticación en el paso 23 tiene éxito:

24.A.1. La MME envía un mensaje de confirmación de solicitud de verificación de MAC al eNB de destino. El eNB de destino, ahora, sabe que el MAC-CIoT mencionado en los pasos anteriores es auténtico.
24.A.2. a 24.A.3. El eNB de destino envía un mensaje de restablecimiento de la conexión del RRC al UE y el UE envía un mensaje de restablecimiento de la conexión del RRC completado que, opcionalmente, contiene una PDU de datos del NAS al eNB de destino.
24.A.4. a 26.A.7. Estos pasos son procedimientos normales de cambio de ruta y modificación de portador.
26.A.8. El eNB de destino, a continuación, indica al eNB de origen que libere el contexto del UE enviando un mensaje X2 llamado Liberación de contexto del UE.

Si la autenticación en el paso 23 falla:

24.B.1. La MME envía el mensaje de verificación de fallo de MAC al eNB de destino. El eNB de destino sabe que el MAC-CIoT mencionado en los pasos anteriores no es auténtico.
24.B.2. El eNB de destino indica al UE que la solicitud del UE se rechaza enviando el mensaje de restablecimiento de la conexión del RRC al UE. Un método, de acuerdo con una realización, para restablecer una conexión del RRC, por ejemplo, para la optimización del EPS (Sistema de paquetes evolucionado – Evolved Packet System, en inglés) de la CP IoT, entre un UE y un eNB de destino se presenta con referencia a la figura 6A. El método se lleva a cabo en un eNB 3 de destino y comprende recibir, ilustrado con un paso S200, un mensaje del RRC de un UE 1, en el que el mensaje del RRC incluye un token de autenticación generado con una clave de integridad de la NAS como entrada. En un segundo paso S210, el eNB de destino envía un mensaje de verificación a una MME, en el que el mensaje de verificación incluye el token de autenticación recibido. En un tercer paso S220, el eNB de destino recibe una respuesta de la MME, verificando la respuesta el token de autenticación.

Alternativas a la clave de integridad del NAS, pueden ser otras claves del NAS, tal como una clave obtenida a partir de la clave de integridad de la NAS. Alternativamente, aunque no esté cubierto por las afirmaciones de esta solicitud, puede existir una clave obtenida a partir de una clave del NAS raíz, tal como KASME, y en un entorno 5G, por ejemplo, KAMF, KAUSF y KSEAF.

El mensaje del RRC es en las reivindicaciones una solicitud de restablecimiento de la conexión del RRC, pero en otras realizaciones puede ser una solicitud de reanudación del RRC.

El mensaje de verificación puede ser una solicitud de verificación de MAC, y la respuesta puede ser un acuse de recibo de verificación de MAC o un fallo de verificación de MAC. La solicitud de verificación de MAC puede incluir el MAC-CIoT y/o el Input-MAC-CIoT.

El mensaje de verificación puede ser una solicitud de cambio de ruta, y la respuesta puede ser un acuse de recibo de solicitud de cambio de ruta o un fallo de solicitud de cambio de ruta. La solicitud de cambio de ruta puede incluir el MAC-CIoT y/o el Input-MAC-CIoT.

Un método, de acuerdo con una realización, para restablecer una conexión del RRC, por ejemplo, para la optimización del EPS de CP IoT, entre un UE y un eNB de destino se presenta con referencia a la figura 6B. El método se lleva a cabo en un eNB 2 de origen y comprende recibir S300 un mensaje X2 desde el eNB 3 de destino, en el que el mensaje incluye un token de autenticación generado por un UE 1 con una clave de integridad del NAS como entrada; enviar S310 una solicitud de verificación a una MME 4, para verificar el token de autenticación recibido, incluyendo dicha solicitud de verificación el token de autenticación; recibir S320 una respuesta de

verificación de la MME, cuya respuesta de verificación indica una verificación del token de autenticación recibido; y enviar S330 un mensaje de fallo de contexto del UE al eNB de destino.

Un método, de acuerdo con una realización, para restablecer una conexión del RRC, por ejemplo, para la optimización del EPS de CP IoT, entre un UE y un eNB de destino se presenta con referencia a la figura 6C. El método lo lleva a cabo una MME 4 y comprende recibir un mensaje de verificación S400 del eNB de destino, en el que el mensaje de verificación incluye un token de autenticación generado en el UE 1 con una clave de integridad del NAS como entrada, verificar S410 el token de autenticación recibido y enviar S420 al eNB de destino un mensaje de respuesta de verificación, verificando el token de autenticación recibido.

La recepción S410 de un mensaje de verificación puede ser llevada a cabo recibiendo una solicitud de cambio de ruta de un eNB 3 de destino, y el envío de un mensaje de respuesta de verificación puede ser llevado a cabo enviando un acuse de recibo de solicitud de cambio de ruta al eNB de destino o enviando un fallo de solicitud de cambio de ruta al eNB de destino.

La recepción S410 de un mensaje de verificación puede ser llevada a cabo alternativamente recibiendo una solicitud de verificación de MAC de un eNB 3 de destino, y el envío de un mensaje de respuesta de verificación puede ser llevado a cabo enviando un acuse de recibo de verificación de MAC o un fallo de verificación de MAC al eNB de destino. La solicitud de verificación de MAC puede incluir el MAC-CIoT y/o el Input-MAC-CIoT.

Un método, de acuerdo con una realización, para restablecer una conexión del RRC, por ejemplo, para la optimización del EPS de la CP IoT, entre un UE y un eNB de destino se presenta con referencia a la figura 6D. El método es llevado a cabo por el UE 1 y comprende generar S500 un token de autenticación con una clave de integridad del estrato de no acceso como entrada. El token de autenticación en una realización también se calcula en base a otros parámetros, tal como se ha descrito anteriormente. Otra entrada para el cálculo del parámetro de autenticación es la identidad de la celda de destino. El método también comprende enviar S510 un primer mensaje de restablecimiento de la conexión del RRC al eNB 3 de destino, en el que el primer mensaje de restablecimiento de la conexión del RRC incluye el token de autenticación, y recibir S520 un segundo mensaje de restablecimiento de la conexión del RRC desde el eNB de destino.

Un eNB de destino, de acuerdo con una realización, para restablecer una conexión del RRC entre un UE y un eNB 3 de destino, se presenta con referencia a la figura 8. El eNB de destino comprende un procesador 30 y un producto de programa informático 32, 33 que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el eNB de destino reciba una solicitud de restablecimiento de la conexión del RRC del UE 1, en el que la solicitud de restablecimiento de la conexión del RRC incluye un token de autenticación generado con una clave de integridad del NAS como entrada, envíe un mensaje de verificación a una MME, en el que el mensaje de verificación incluye el token de autenticación recibido; y reciba una respuesta de la MME, de verificación del token de autenticación.

Se puede hacer que el eNB de destino envíe un mensaje X2 a un eNB 2 de origen, en el que el mensaje X2 incluye el token de autenticación recibido, y reciba un fallo de contexto del UE desde el eNB de origen.

Un eNB 2 de origen, de acuerdo con una realización, para restablecer una conexión del RRC entre un UE y un eNB 3 de destino, se presenta con referencia a la figura 7. El eNB de origen comprende un procesador 20 y un producto de programa informático 22, 23 que almacenan instrucciones que, cuando son ejecutadas por el procesador, hacen que el eNB de origen reciba un mensaje X2 del eNB 3 de destino, en el que el mensaje incluye un token de autenticación generado por un UE 1 con una clave de integridad del NAS como entrada; envíe una solicitud de verificación a una MME 4, para verificar el token de autenticación recibido, incluyendo dicha solicitud de verificación el token de autenticación; reciba una respuesta de verificación de la MME, verificando el token de autenticación recibido; y envíe un mensaje de fallo de contexto del UE al eNB de destino.

Una MME, de acuerdo con una realización, para restablecer una conexión del RRC entre un UE y un eNB de destino se presenta con referencia a la figura 9. La MME 4 comprende un procesador 40 y un producto de programa informático 42, 43 que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que la MME reciba un mensaje de verificación del eNB de destino (3), en el que el mensaje de verificación incluye un token de autenticación generado en un UE 1 con una clave de integridad del NAS como entrada; verifique el token de autenticación recibido; y envíe al eNB de destino (3) un mensaje de respuesta de verificación, verificando el token de autenticación recibido.

La recepción de un mensaje de verificación puede ser llevada a cabo recibiendo una solicitud de cambio de ruta de un eNB 3 de destino, y el envío de un mensaje de respuesta de verificación puede ser llevado a cabo enviando un acuse de recibo de solicitud de cambio de ruta al eNB o enviando un fallo de solicitud de cambio de ruta al eNB de destino.

La recepción de un mensaje de verificación puede ser llevada a cabo como recibir una solicitud de verificación de

MAC desde un eNB 3 de destino, y el envío de un mensaje de respuesta de verificación puede ser llevada a cabo como enviar un acuse de recibo de verificación de MAC o un fallo de verificación de MAC al eNB de destino.

Un eNB de destino, de acuerdo con una realización, para restablecer una conexión del RRC entre un UE y un eNB de destino, se presenta con referencia a la figura 11. El eNB de destino comprende un gestor de la comunicación 81 y un gestor de la determinación 80. El gestor de la comunicación 81 está destinado a recibir una solicitud de restablecimiento de la conexión del RRC del UE 1, en el que la solicitud de restablecimiento de la conexión del RRC incluye un token de autenticación generado con una clave de integridad del NAS como entrada; enviar un mensaje de verificación a una MME, en el que el mensaje de verificación incluye el token de autenticación recibido; y recibir una respuesta de la MME, de verificación del token de autenticación.

Un eNB de origen, de acuerdo con una realización, para restablecer una conexión del RRC entre un UE y un eNB de destino, se presenta con referencia a la figura 10. El eNB de origen comprende un gestor de la comunicación 71 para recibir un mensaje X2 del eNB 3 de destino, en el que el mensaje X2 incluye un token de autenticación generado por el UE 1 con una clave de integridad del NAS como entrada; enviar una solicitud de verificación a una MME 4, para verificar el token de autenticación recibido, incluyendo dicha solicitud de verificación el token de autenticación; recibir una respuesta de verificación de la MME, verificando el token de autenticación recibido; y enviar un mensaje de fallo de contexto del UE al eNB de destino.

Una MME, de acuerdo con una realización, para restablecer una conexión del RRC entre un UE y un eNB de destino se presenta con referencia a la figura 12. La MME 4 comprende un gestor de la comunicación 91 y un gestor de la determinación 90. El gestor de la comunicación 91 está destinado a recibir un mensaje de verificación del eNB de destino, en el que el mensaje de verificación incluye un token de autenticación generado en el UE 1 con una clave de integridad del NAS como entrada, y para enviar al eNB de destino un mensaje de respuesta de verificación, verificando el token de autenticación recibido. El gestor de la determinación 90 está destinado a verificar el token de autenticación recibido.

Un programa informático 34, 35, de acuerdo con una realización, para restablecer una conexión del RRC entre un UE y un eNB de destino, se presenta en la figura 8. El programa informático 34, 35 comprende un código de programa informático que, cuando es ejecutado en un eNB 3 de destino, hace que el eNB de destino reciba una solicitud de restablecimiento de la conexión del RRC del UE 1, en el que la solicitud de restablecimiento de la conexión del RRC incluye un token de autenticación generado con una clave de integridad del NAS como entrada; envíe un mensaje de verificación a una MME, en el que el mensaje de verificación incluye el token de autenticación recibido; y reciba una respuesta de la MME, de verificación del token de autenticación.

Un programa informático 24, 25, de acuerdo con una realización, para restablecer una conexión del RRC entre un UE y un eNB de destino, se presenta en la figura 7. El programa informático 24, 25 comprende un código de programa informático que, cuando es ejecutado en un eNB 2 de origen, hace que el eNB de origen reciba un mensaje X2 del eNB 3 de destino, en el que el mensaje X2 incluye un token de autenticación generado por un UE 1 con una clave de integridad del NAS como entrada; envíe una solicitud de verificación a una MME 4, para verificar el token de autenticación recibido, en el que la solicitud de verificación incluye el token de autenticación recibido; reciba una respuesta de verificación de la MME, verificando el token de autenticación recibido; y envíe un mensaje de fallo de contexto del UE al eNB de destino.

Un programa informático 44, 45, de acuerdo con una realización, para restablecer una conexión del RRC entre un UE y un eNB de destino, se presenta en la figura 9. El programa informático 44, 45 comprende el código del programa informático que, cuando es ejecutado en una MME, hace que la MME 4 reciba un mensaje de verificación del eNB de destino, en el que el mensaje de verificación incluye un token de autenticación generado en un UE 1 con una clave de integridad del NAS como entrada, verifique el token de autenticación recibido, y envíe al eNB de destino un mensaje de respuesta de verificación, verificando el token de autenticación recibido.

Asimismo, se presenta un producto de programa informático, tal como el ilustrado en diferentes formas con los signos de referencia 22, 23, 32, 33, 42, 43. El producto de programa informático comprende un programa informático y un medio de almacenamiento legible por ordenador en el que están almacenados uno o varios de los programas informáticos descritos en las figuras 7 a 9.

La figura 7 es un diagrama esquemático que muestra algunos componentes del eNB 2 de origen. El procesador 20 puede ser proporcionado utilizando cualquier combinación de uno o varios de una unidad de procesamiento central, CPU, un multiprocesador, un microcontrolador, un procesador de señal digital, DSP, un circuito integrado específico para una aplicación, etc. adecuados, capaz de ejecutar instrucciones de software de un programa informático 24 almacenado en una memoria. Por lo tanto, se puede considerar que la memoria es o forma parte del producto de programa informático 22. El procesador 20 puede ser configurado para ejecutar métodos descritos en este documento con referencia a la figura 6B.

La memoria puede ser cualquier combinación de memoria de lectura y escritura, RAM, y memoria de solo lectura,

ROM. La memoria también puede comprender un almacenamiento persistente, que, por ejemplo, puede ser cualquiera o una combinación de una memoria magnética, una memoria óptica, una memoria de estado sólido o, incluso, una memoria montada de manera remota.

Se puede proporcionar también un segundo producto de programa informático 23 en forma de memoria de datos, por ejemplo, para leer y/o almacenar datos durante la ejecución de instrucciones de software en el procesador 20. La memoria de datos puede ser cualquier combinación de una memoria de lectura y escritura, RAM y una memoria de solo lectura, ROM, y también puede comprender un almacenamiento persistente, que, por ejemplo, puede ser cualquiera o una combinación de una memoria magnética, una memoria óptica, una memoria de estado sólido o, incluso, una memoria montada de manera remota. La memoria de datos puede contener, por ejemplo, otras instrucciones de software 25 para mejorar la funcionalidad del eNB 2 de origen.

El eNB 2 de origen puede comprender, además, una interfaz de entrada / salida (E/S) 21 que incluye, por ejemplo, una interfaz de usuario. El eNB 2 de origen puede comprender, además, un receptor, configurado para recibir señalización de otros nodos, y un transmisor, configurado para transmitir señalización a otros nodos (no ilustrados). Otros componentes del eNB 2 de origen se han omitido para no oscurecer los conceptos presentados en el presente documento.

La figura 10 es un diagrama esquemático que muestra bloques funcionales del eNB 2 de origen. Los módulos pueden ser implementados como solo instrucciones de software, como un programa informático que es ejecutado en el servidor de la memoria oculta o como solo hardware, tal como circuitos integrados específicos para una aplicación, matrices de puertas programables 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 los pasos en los métodos ilustrados en la figura 6B, que comprenden una unidad de gestión de la determinación 70 y una unidad de gestión de la comunicación 71. En las realizaciones en las que uno o varios de los módulos son implementados por un programa informático, se comprenderá que estos módulos no corresponden necesariamente a los módulos de proceso, sino que pueden estar escritos como instrucciones de acuerdo con un lenguaje de programación en el que estarían implementados, puesto que algunos lenguajes de programación no suelen contener módulos de proceso.

El gestor de la comunicación 71 está destinado a permitir el restablecimiento de una conexión del RRC entre un UE y un eNB de destino. Este módulo corresponde al paso de recepción S300, el paso de envío S310, al paso de recepción S320 y al paso de envío S330 de la figura 6B. Este módulo puede ser implementado, por ejemplo, mediante el procesador 20 de la figura 7, cuando se ejecuta el programa informático.

La figura 8 es un diagrama esquemático que muestra algunos componentes del eNB 3. El procesador 30 puede ser proporcionado utilizando cualquier combinación de uno o varios de una unidad de procesamiento central, CPU, un multiprocesador, un microcontrolador, un procesador de señal digital, DSP, un circuito integrado específico para una aplicación, etc. adecuados, capaz de ejecutar instrucciones de software de un programa informático 34 almacenado en una memoria. Por lo tanto, se puede considerar que la memoria es o forma parte del producto de programa informático 32. El procesador 30 puede estar configurado para ejecutar los métodos descritos en este documento con referencia a la figura 6A.

La memoria puede ser cualquier combinación de una memoria de lectura y escritura, RAM, y una memoria de solo lectura, ROM. La memoria también puede comprender un almacenamiento persistente, que, por ejemplo, puede ser cualquiera o una combinación de una memoria magnética, una memoria óptica, una memoria de estado sólido o, incluso, una memoria montada de manera remota.

Asimismo, se puede proporcionar un segundo producto de programa informático 33 en forma de memoria de datos, por ejemplo, para leer y/o almacenar datos durante la ejecución de instrucciones de software en el procesador 20. La memoria de datos puede ser cualquier combinación de una memoria de lectura y escritura, RAM y una memoria de solo lectura, ROM, y también puede comprender un almacenamiento persistente, que, por ejemplo, puede ser cualquiera o una combinación de una memoria magnética, una memoria óptica, una memoria de estado sólido o, incluso, una memoria montada de manera remota. La memoria de datos puede contener, por ejemplo, otras instrucciones de software 35 para mejorar la funcionalidad del eNB 3 de destino.

El eNB 3 de destino puede comprender, además, una interfaz de entrada / salida (E/S) 31 que incluye, por ejemplo, una interfaz de usuario. El eNB 3 de destino puede comprender, además, un receptor, configurado para recibir señalización de otros nodos, y un transmisor, configurado para transmitir señalización a otros nodos (no ilustrados). Otros componentes del eNB 3 de destino se han omitido para no oscurecer los conceptos presentados en el presente documento.

La figura 11 es un diagrama esquemático que muestra bloques funcionales del eNB 3. Los módulos pueden estar implementados solo como instrucciones de software, como un programa informático que es ejecutado en el servidor de la memoria oculta o solo como hardware, tal como circuitos integrados específicos para una aplicación, matrices

de puertas programables en campo, componentes lógicos discretos, transceptores, etc. o como una combinación de los mismos. En una realización alternativa, algunos de los bloques funcionales pueden estar implementados mediante software y otros mediante hardware. Los módulos corresponden a los pasos de los métodos ilustrados en la figura 6A, que comprenden una unidad de gestión de la determinación 80 y una unidad de gestión de la comunicación 81. En las realizaciones en las que uno o varios de los módulos están implementados mediante un programa informático, se comprenderá que estos módulos no se corresponden necesariamente con los módulos de proceso, sino que pueden estar escritos como instrucciones de acuerdo con un lenguaje de programación en el que se implementarían, puesto que algunos lenguajes de programación no suelen contener módulos de proceso.

El gestor de la comunicación 81 está destinado a permitir el restablecimiento de una conexión del RRC entre un UE y un eNB de destino. Este módulo corresponde al paso de recepción S200, al paso de envío 210, al paso de recepción 220 de la figura 6A. Este módulo puede estar implementado, por ejemplo, mediante el procesador 30 de la figura 8, cuando se ejecuta el programa informático, o como hardware en forma de un ASIC.

La figura 9 es un diagrama esquemático que muestra algunos componentes de la MME 4. El procesador 40 puede ser proporcionado utilizando cualquier combinación de uno o varios de una unidad de procesamiento central, CPU, un multiprocesador, un microcontrolador, un procesador de señal digital, DSP, un circuito integrado específico para una aplicación, etc. adecuados, capaz de ejecutar instrucciones de software de un programa informático 44 almacenado en una memoria. Por lo tanto, se puede considerar que la memoria es o forma parte del producto del programa informático 42. El procesador 40 puede estar configurado para ejecutar los métodos descritos en este documento con referencia a la figura 6C.

La memoria puede ser cualquier combinación de una memoria de lectura y escritura, RAM, y una memoria de solo lectura, ROM. La memoria también puede comprender un almacenamiento persistente, que, por ejemplo, puede ser cualquiera o una combinación de una memoria magnética, una memoria óptica, una memoria de estado sólido o, incluso, una memoria montada de manera remota.

Asimismo, se puede proporcionar un segundo producto de programa informático 43 en forma de memoria de datos, por ejemplo, para leer y/o almacenar datos durante la ejecución de instrucciones de software en el procesador 40. La memoria de datos puede ser cualquier combinación de una memoria de lectura y escritura, RAM y una memoria de solo lectura, ROM, y también puede comprender un almacenamiento persistente, que, por ejemplo, puede ser cualquiera o una combinación de una memoria magnética, una memoria óptica, una memoria de estado sólido o, incluso, una memoria montada de manera remota. La memoria de datos puede contener, por ejemplo, otras instrucciones de software 45 para mejorar la funcionalidad de la MME 4.

La MME 4 puede comprender, además, una interfaz de entrada / salida (E/S) 41 que incluye, por ejemplo, una interfaz de usuario. La MME 4 puede comprender, además, un receptor, configurado para recibir señalización de otros nodos, y un transmisor, configurado para transmitir señalización a otros nodos (no ilustrados). Otros componentes de la MME 4 se han omitido para no oscurecer los conceptos presentados en el presente documento.

La figura 12 es un diagrama esquemático que muestra bloques funcionales de la MME 4. Los módulos pueden estar implementados como solo instrucciones de software, como un programa informático que se ejecuta en el servidor de la memoria oculta o como solo hardware, tal como circuitos integrados específicos para una aplicación, matrices de puertas programables en campo, componentes lógicos discretos, transceptores, etc. o como una combinación de los mismos. En una realización alternativa, algunos de los bloques funcionales pueden estar implementados mediante software y otros mediante hardware. Los módulos corresponden a los pasos de los métodos ilustrados en la figura 6C, que comprenden una unidad de gestión de la determinación 90 y una unidad de gestión de la comunicación 91. En las realizaciones en las que uno o varios de los módulos están implementados mediante un programa informático, se comprenderá que estos módulos no corresponden necesariamente a los módulos de proceso, sino que pueden estar escritos como instrucciones de acuerdo con un lenguaje de programación en el que se implementarían, puesto que algunos lenguajes de programación no contienen, habitualmente módulos de proceso.

El gestor de la determinación 90 está destinado a permitir el restablecimiento de una conexión del RRC entre un UE y un eNB de destino. Este módulo corresponde al paso de verificación 410 de la figura 6C. Este módulo puede estar implementado, por ejemplo, mediante el procesador 40 de la figura 9, cuando se ejecuta el programa informático.

El gestor de la comunicación 91 está destinado a permitir el restablecimiento de una conexión del RRC entre un UE y un eNB de destino. Este módulo corresponde al paso de recepción S400 y al paso de envío S420 de la figura 6C. Este módulo puede estar implementado, por ejemplo, mediante el procesador 40 de la figura 9, cuando se ejecuta el programa informático.

La invención se ha descrito anteriormente, principalmente, con referencia a algunas realizaciones. No obstante, tal como puede apreciar fácilmente un experto en la materia, otras formas de realización distintas de las descritas anteriormente son igualmente posibles dentro del alcance de la invención, tal como está definida en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para el restablecimiento de una conexión del control de los recursos de radio, RRC, entre un equipo de usuario (1), UE, y un Nodo B (3) evolucionado, eNB de destino,
siendo llevado a cabo el método por el eNB de destino (3) y comprendiendo:

recibir (S200) una solicitud de restablecimiento de la conexión del RRC del UE (1), en el que la solicitud de restablecimiento de la conexión del RRC incluye un token de autenticación generado con una clave de integridad del estrato de no acceso y la identidad de una celda de destino como entrada;
enviar (S210) un mensaje de verificación a una entidad de gestión de la movilidad (4), MME, en el que el mensaje de verificación incluye el token de autenticación recibido; y
recibir (S220) una respuesta de la MME, de verificación del token de autenticación.

2. El método de acuerdo con la reivindicación 1, que incluye la identidad de la celda de destino en el mensaje de verificación.

3. Un método para el restablecimiento de una conexión del control de los recursos de radio, RRC, entre un equipo de usuario (1), UE, y un Nodo B evolucionado (3), eNB de destino,
estando llevado a cabo el método por una entidad de gestión de la movilidad (4), MME, y que comprende:

recibir (S400) un mensaje de verificación del eNB de destino (3), en el que el mensaje de verificación incluye un token de autenticación generado en el UE (1) con una clave de integridad del estrato de no acceso y la identidad de una celda de destino como entrada;
verificar (S410) el token de autenticación recibido; y
enviar (S420) al eNB de destino (3) un mensaje de respuesta de verificación, verificando el token de autenticación recibido.

4. El método de acuerdo con la reivindicación 3, en el que el mensaje de verificación incluye la identidad de la celda de destino.

5. El método de acuerdo con la reivindicación 4, en el que la verificación es llevada a cabo comparando el token de autenticación recibido con un token de autenticación calculado por la MME, con la clave de integridad del estrato de no acceso y la identidad de la celda de destino como entrada.

6. Un Nodo B evolucionado (3), eNB, para el restablecimiento de una conexión del control de los recursos de radio, RRC, entre un equipo de usuario (1), UE, y el eNB de destino (3), comprendiendo el eNB de destino:

un procesador (30); y
un producto de programa informático (32, 33), que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el eNB de destino:

reciba una solicitud de restablecimiento de la conexión del RRC del UE (1), en donde la solicitud de restablecimiento de la conexión del RRC incluye un token de autenticación generado con una clave de integridad del estrato de no acceso y la identidad de una celda de destino como entrada;
envíe un mensaje de verificación a una entidad de gestión de la movilidad (4), MME, en el que el mensaje de verificación incluye el token de autenticación recibido; y
reciba una respuesta de la MME, de verificación del token de autenticación.

7. El eNB (3) de destino de acuerdo con la reivindicación 6, en el que el mensaje de verificación es una solicitud de verificación de MAC, y la respuesta es un acuse de recibo de verificación de MAC o un mensaje de fallo de verificación de MAC.

8. El eNB de destino (3) de acuerdo con la reivindicación 7, en el que la solicitud de verificación de MAC incluye el MAC-CIoT como dicho token de autenticación y/o el Input-MAC-CIoT.

9. El eNB de destino (3) de acuerdo con la reivindicación 6, en el que el mensaje de verificación es una solicitud de cambio de ruta, y la respuesta es un acuse de recibo de solicitud de cambio de ruta o un fallo de solicitud de cambio de ruta.

10. El eNB (3) de destino de acuerdo con la reivindicación 9, en el que la solicitud de cambio de ruta incluye el MAC-CIoT como dicho token de autenticación, y/o el Input-MAC-CIoT.

11. El eNB (3) de destino de acuerdo con la reivindicación 6, incluida la identidad de la celda de destino en el mensaje de verificación.

12. Un NodoB (2) evolucionado de origen, eNB de origen, para restablecer una conexión del control de los recursos de radio, RRC, entre el equipo de usuario (1), UE y un eNB de destino (3), comprendiendo el eNB (4) de origen:

un procesador (20);
un producto de programa informático (22, 23), que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el eNB de origen (4):

reciba un mensaje X2 del eNB de destino (3), en el que el mensaje incluye un token de autenticación generado por el UE (1) con una clave de integridad del estrato de no acceso como entrada;
envíe una solicitud de verificación a una entidad de gestión de la movilidad (4), MME, para verificar el token de autenticación recibido, incluyendo dicha solicitud de verificación el token de autenticación;
reciba una respuesta de verificación de la MME (4), verificando el token de autenticación recibido; y
envíe un mensaje de fallo de contexto del UE al eNB de destino (3).

13. Una entidad de gestión de la movilidad (4), MME, para restablecer una conexión del control de los recursos de radio, RRC, entre un equipo de usuario (1), UE y un eNB (3) de destino, comprendiendo la MME (4):

un procesador (40); y
un producto de programa informático (42, 43) que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que la MME:

reciba un mensaje de verificación del eNB de destino (3), en el que el mensaje de verificación incluye un token de autenticación generado en el UE (1) con una clave de integridad del estrato de no acceso y la identidad de una celda de destino como entrada;
verifique el token de autenticación recibido; y
envíe al eNB de destino (3) un mensaje de respuesta de verificación, verificando el token de autenticación recibido.

14. La MME (4) de acuerdo con la reivindicación 13, en la que recibir el mensaje de verificación es recibir una solicitud de cambio de ruta del eNB de destino (3), y enviar el mensaje de respuesta de verificación es enviar un acuse de recibo de solicitud de cambio de ruta al eNB de destino (3) o enviar un fallo de solicitud de cambio de ruta al eNB de destino (3).

15. La MME (4) de acuerdo con la reivindicación 13, en la que recibir el mensaje de verificación es recibir una solicitud de verificación de MAC del eNB de destino (3), y enviar el mensaje de respuesta de verificación es enviar un acuse de recibo de verificación de MAC o un fallo de verificación de MAC al eNB de destino (3).

16. La MME (4) de acuerdo con la reivindicación 15, en la que la solicitud de verificación de MAC incluye el MAC-CIoT como dicho token de autenticación y/o el Input-MAC-CIoT.

17. La MME de acuerdo con la reivindicación 13, en el que el mensaje de verificación incluye la identidad de la celda de destino.

18. La MME de acuerdo con la reivindicación 17, en la que la verificación es llevada a cabo comparando la el token de autenticación recibido con un token de autenticación calculado por la MME con la clave de integridad del estrato de no acceso y la identidad de la celda de destino como entrada.

19. Un programa informático (34, 35) para restablecer una conexión del control de los recursos de radio, RRC, entre un equipo de usuario (1), UE y un Nodo B (3) de destino, eNB de destino, comprendiendo el programa informático el código del programa informático que, cuando es ejecutado en el eNB de destino (3), hace que el eNB de destino:

reciba una solicitud de restablecimiento de la conexión del RRC del UE (1), en el que la solicitud de restablecimiento de la conexión del RRC incluye un token de autenticación generado con una clave de integridad del estrato de no acceso y la identidad de una celda de destino como entrada;
envíe un mensaje de verificación a una entidad de gestión de la movilidad (4), MME, en el que el mensaje de verificación incluye el token de autenticación recibido; y
reciba una respuesta de la MME, de verificación del token de autenticación.

20. Un programa informático (44, 45) para restablecer una conexión del control de los recursos de radio, RRC, entre un equipo de usuario (1), UE, y un Nodo B evolucionado (3), eNB de destino, comprendiendo el programa informático el código del programa informático que, cuando es ejecutado en una entidad de gestión de la movilidad (4), MME, hace que la MME (4):

reciba un mensaje de verificación del eNB de destino (3), en el que el mensaje de verificación incluye un token de autenticación generado en el UE (1) con una clave de integridad del estrato de no acceso y la

identidad de una celda de destino como entrada;
verifique el token de autenticación recibido; y
envíe al eNB de destino (3) un mensaje de respuesta de verificación, verificando el token de autenticación recibido.

21. Un método para restablecer una conexión del control de los recursos de radio, RRC, entre un equipo de usuario (1), UE y un Nodo B evolucionado (3) de destino), eNB de destino, estando llevado a cabo el método por el UE (1) y comprendiendo:

– generar un token de autenticación con una clave de integridad del estrato de no acceso y la identidad de una celda de destino como entrada,
– enviar un primer mensaje de restablecimiento de la conexión del RRC al eNB de destino (3), en el que el primer mensaje de restablecimiento de la conexión del RRC incluye el token de autenticación, y
– recibir un segundo mensaje de restablecimiento de la conexión del RRC del eNB de destino (3).

22. El método de acuerdo con la reivindicación 21, en el que el restablecimiento de la conexión del RRC está destinado a las optimizaciones de la Internet de las cosas mediante el plano de control.

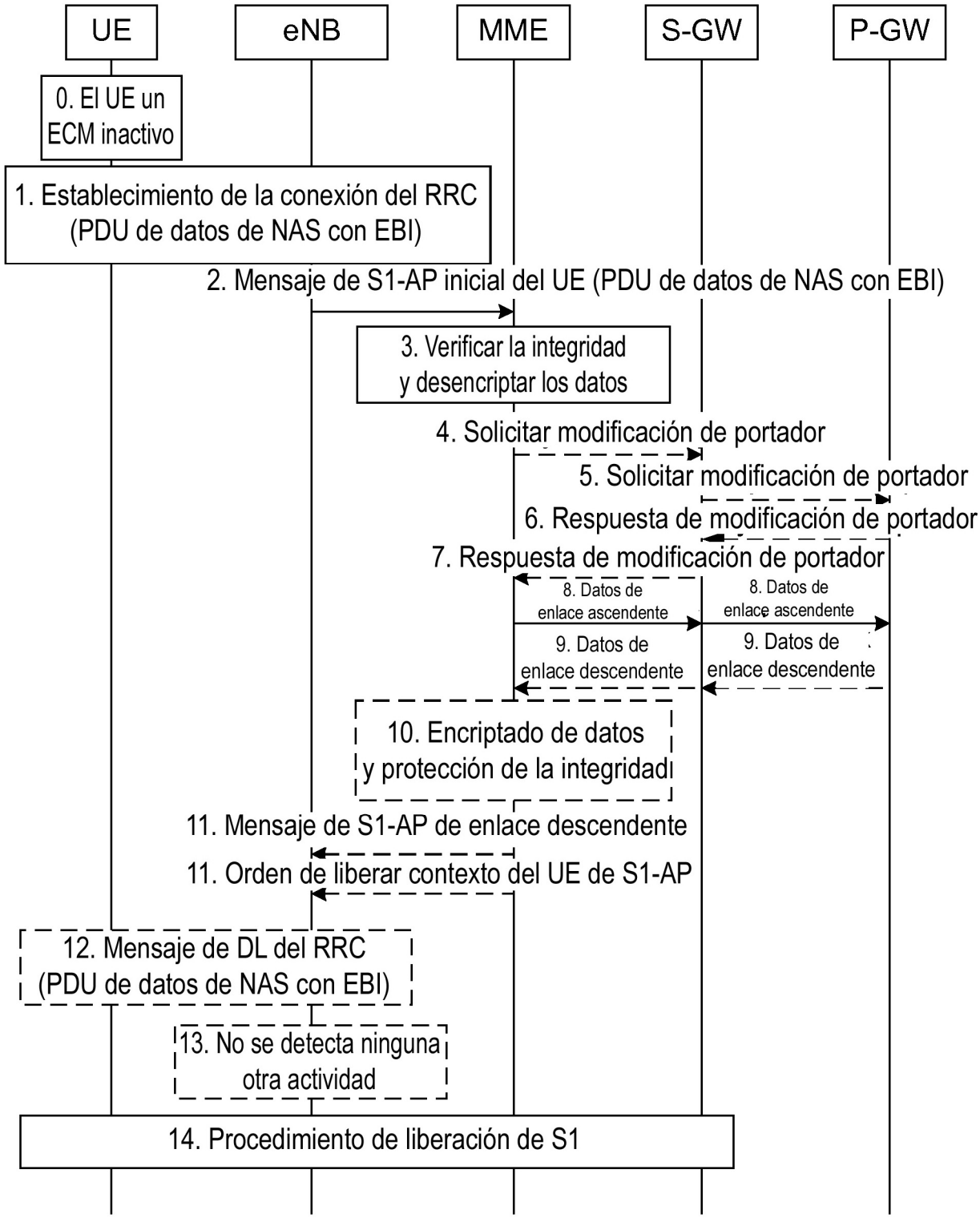

Fig. 1 (técnica anterior)

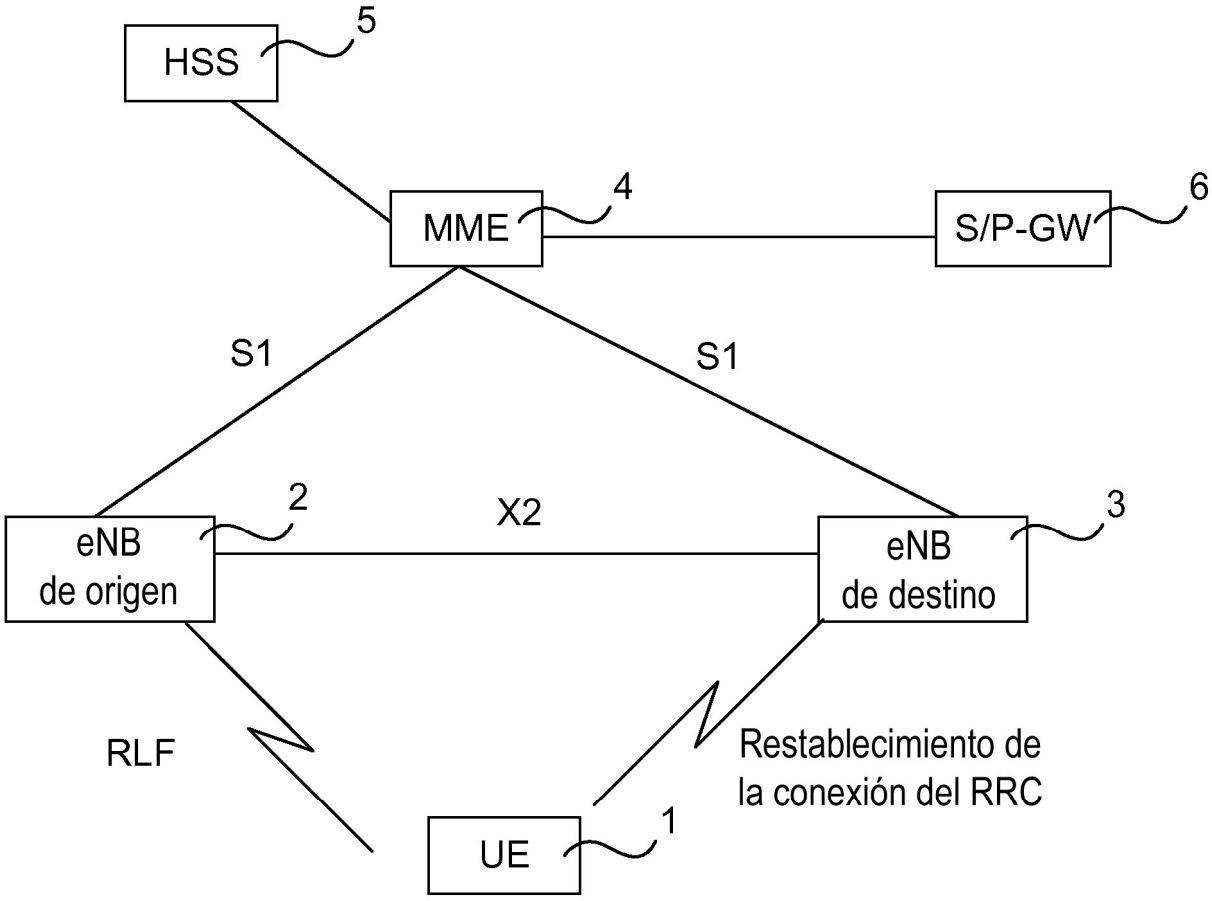
HSS
5
MME
4
S/P-GW
6
S1
S1
eNB
de origen
2
X2
eNB
de destino
3
RLF
Restablecimiento de
la conexión del RRC
UE
1

Fig. 2

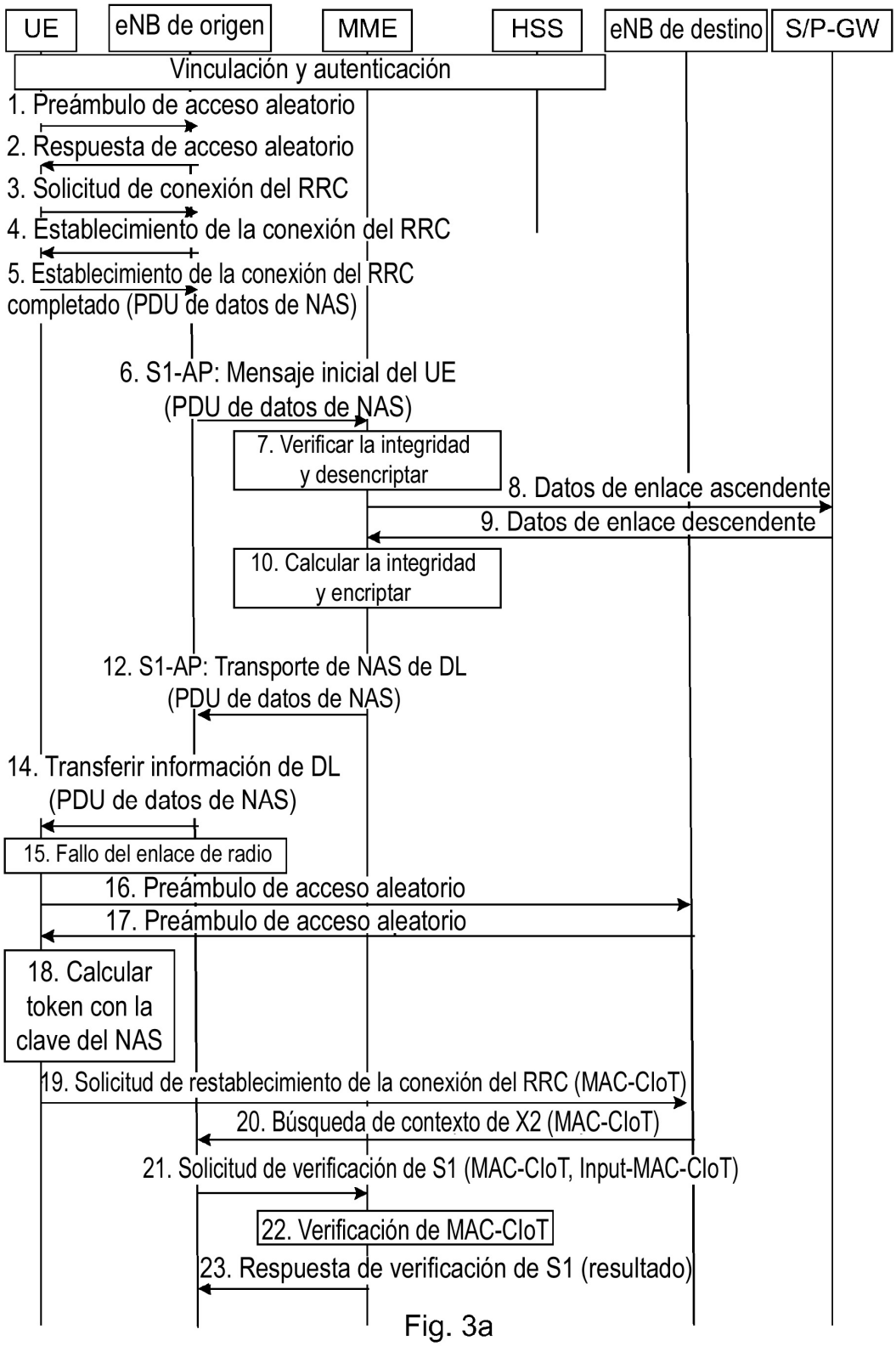
UE
eNB de origen
MME
HSS
eNB de destino
S/P-GW
Vinculación y autenticación
1. Preámbulo de acceso aleatorio
2. Respuesta de acceso aleatorio
3. Solicitud de conexión del RRC
4. Establecimiento de la conexión del RRC
5. Establecimiento de la conexión del RRC completado (PDU de datos de NAS)
6. S1-AP: Mensaje inicial del UE (PDU de datos de NAS)
7. Verificar la integridad y desencriptar
8. Datos de enlace ascendente
9. Datos de enlace descendente
10. Calcular la integridad y encriptar
12. S1-AP: Transporte de NAS de DL (PDU de datos de NAS)
14. Transferir información de DL (PDU de datos de NAS)
15. Fallo del enlace de radio
16. Preámbulo de acceso aleatorio
17. Preámbulo de acceso aleatorio
18. Calcular token con la clave del NAS
19. Solicitud de restablecimiento de la conexión del RRC (MAC-CIoT)
20. Búsqueda de contexto de X2 (MAC-CIoT)
21. Solicitud de verificación de S1 (MAC-CIoT, Input-MAC-CIoT)
22. Verificación de MAC-CIoT
23. Respuesta de verificación de S1 (resultado)

Fig. 3a

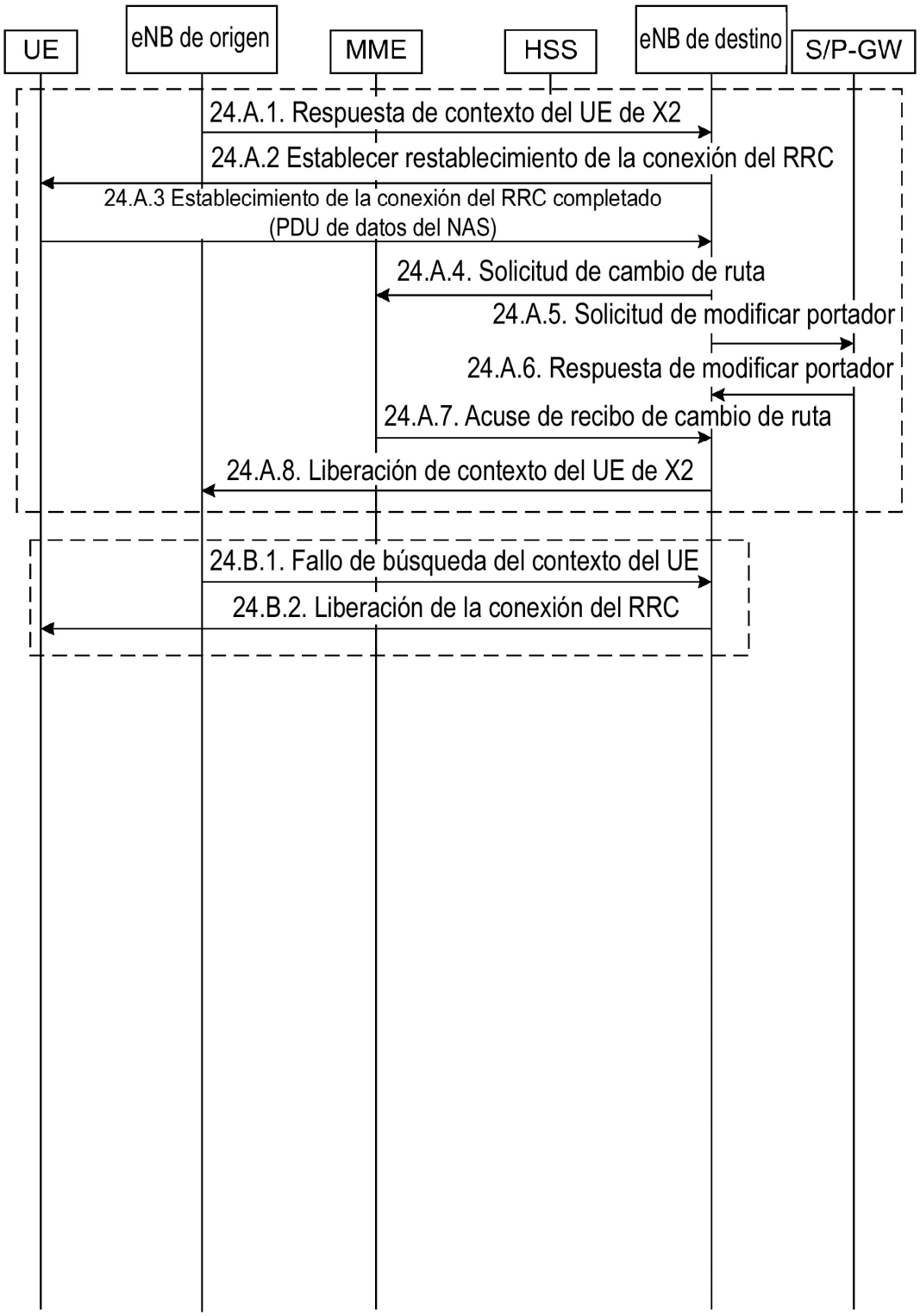
UE
eNB de origen
MME
HSS
eNB de destino
S/P-GW
24.A.1. Respuesta de contexto del UE de X2
24.A.2 Establecer restablecimiento de la conexión del RRC
24.A.3 Establecimiento de la conexión del RRC completado
(PDU de datos del NAS)
24.A.4. Solicitud de cambio de ruta
24.A.5. Solicitud de modificar portador
24.A.6. Respuesta de modificar portador
24.A.7. Acuse de recibo de cambio de ruta
24.A.8. Liberación de contexto del UE de X2
24.B.1. Fallo de búsqueda del contexto del UE
24.B.2. Liberación de la conexión del RRC

Fig. 3b

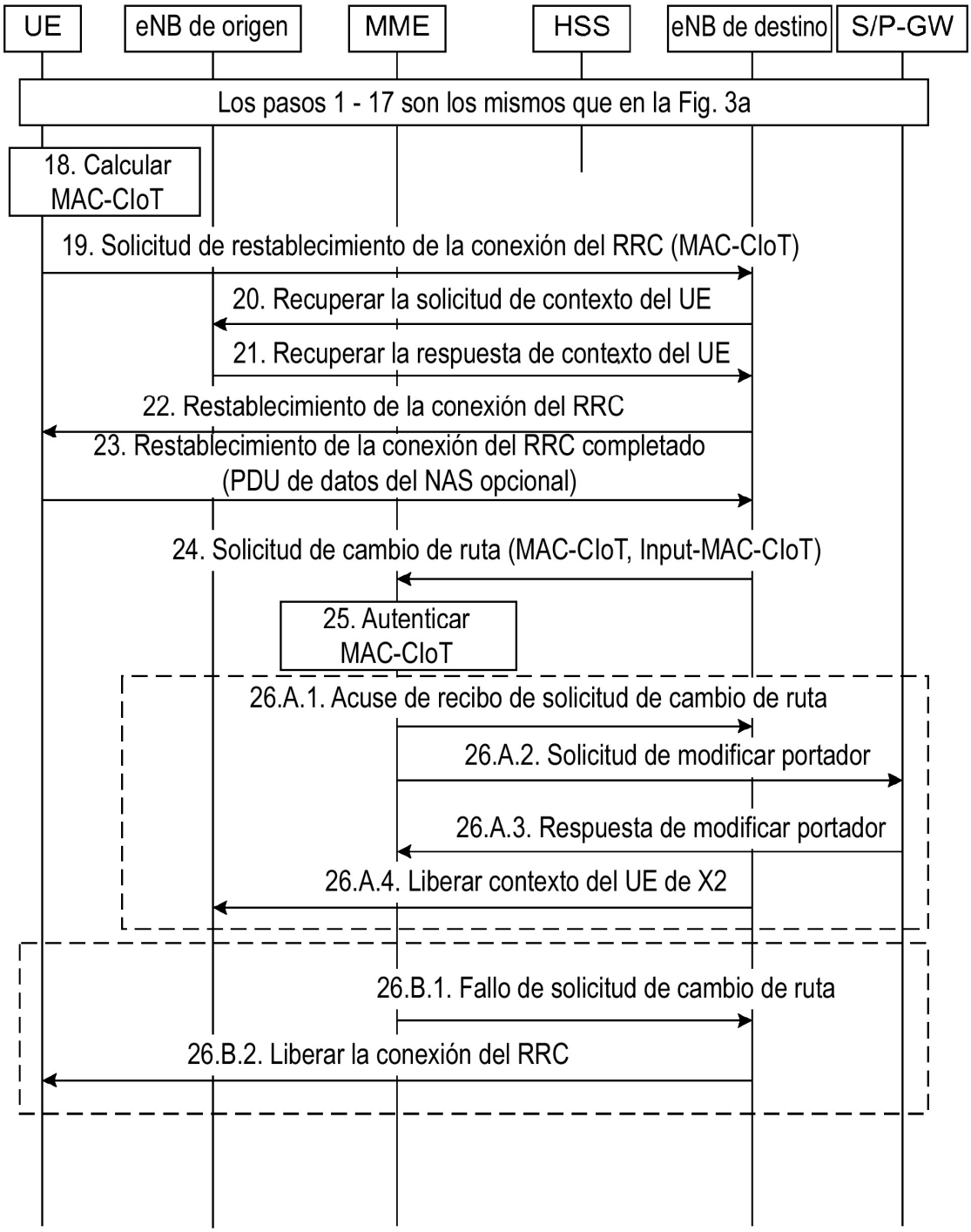
UE
eNB de origen
MME
HSS
eNB de destino
S/P-GW
Los pasos 1 - 17 son los mismos que en la Fig. 3a
18. Calcular MAC-CIoT
19. Solicitud de restablecimiento de la conexión del RRC (MAC-CIoT)
20. Recuperar la solicitud de contexto del UE
21. Recuperar la respuesta de contexto del UE
22. Restablecimiento de la conexión del RRC
23. Restablecimiento de la conexión del RRC completado (PDU de datos del NAS opcional)
24. Solicitud de cambio de ruta (MAC-CIoT, Input-MAC-CIoT)
25. Autenticar MAC-CIoT
26.A.1. Acuse de recibo de solicitud de cambio de ruta
26.A.2. Solicitud de modificar portador
26.A.3. Respuesta de modificar portador
26.A.4. Liberar contexto del UE de X2
26.B.1. Fallo de solicitud de cambio de ruta
26.B.2. Liberar la conexión del RRC

Fig. 4

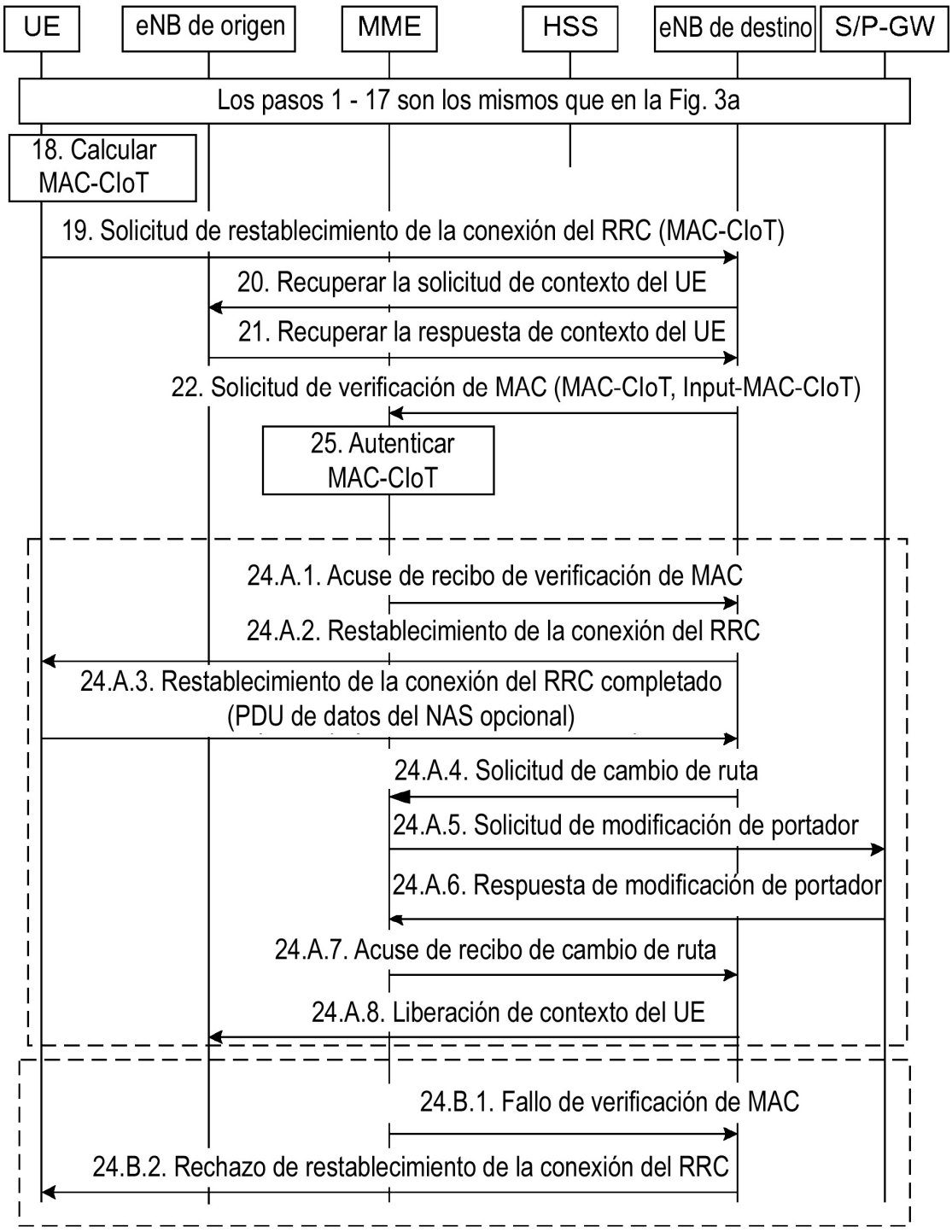
UE
eNB de origen
MME
HSS
eNB de destino
S/P-GW
Los pasos 1 - 17 son los mismos que en la Fig. 3a
18. Calcular MAC-CIoT
19. Solicitud de restablecimiento de la conexión del RRC (MAC-CIoT)
20. Recuperar la solicitud de contexto del UE
21. Recuperar la respuesta de contexto del UE
22. Solicitud de verificación de MAC (MAC-CIoT, Input-MAC-CIoT)
25. Autenticar MAC-CIoT
24.A.1. Acuse de recibo de verificación de MAC
24.A.2. Restablecimiento de la conexión del RRC
24.A.3. Restablecimiento de la conexión del RRC completado (PDU de datos del NAS opcional)
24.A.4. Solicitud de cambio de ruta
24.A.5. Solicitud de modificación de portador
24.A.6. Respuesta de modificación de portador
24.A.7. Acuse de recibo de cambio de ruta
24.A.8. Liberación de contexto del UE
24.B.1. Fallo de verificación de MAC
24.B.2. Rechazo de restablecimiento de la conexión del RRC

Fig. 5

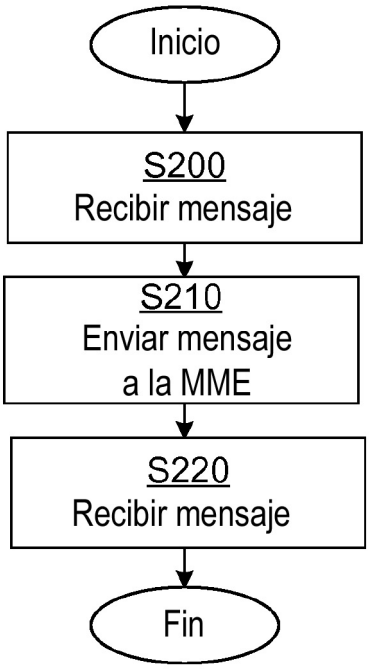

Fig. 6A

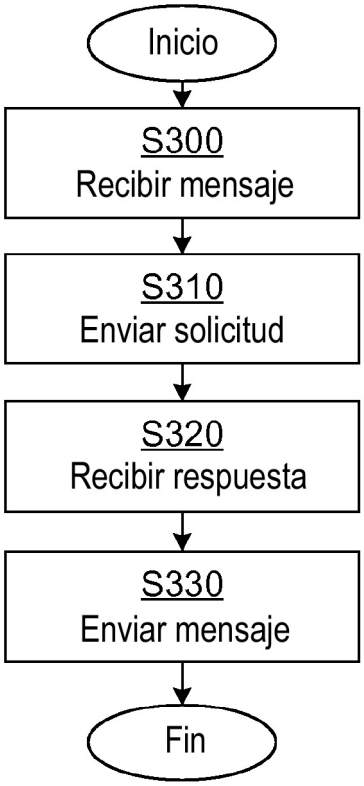

Fig. 6B

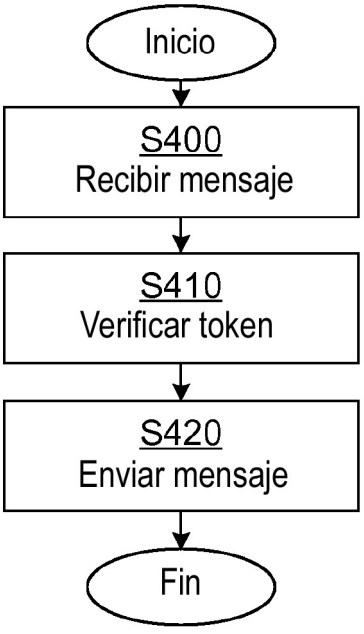

Fig. 6C

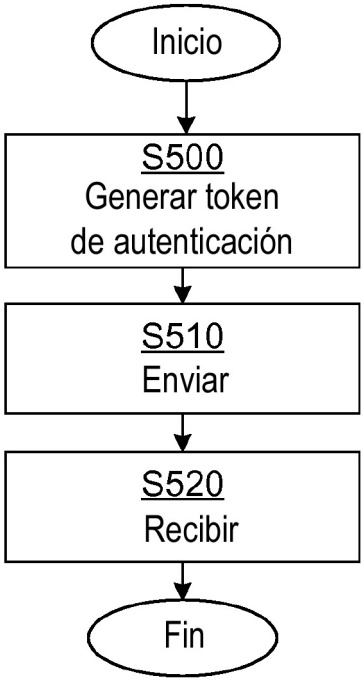

Fig. 6D

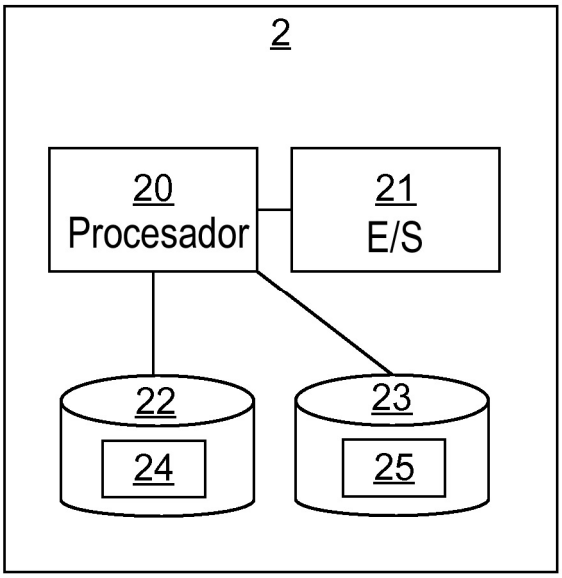

Fig. 7

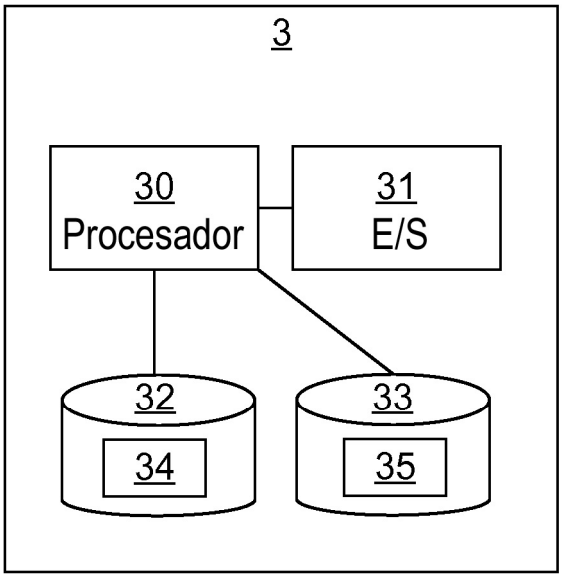

Fig. 8

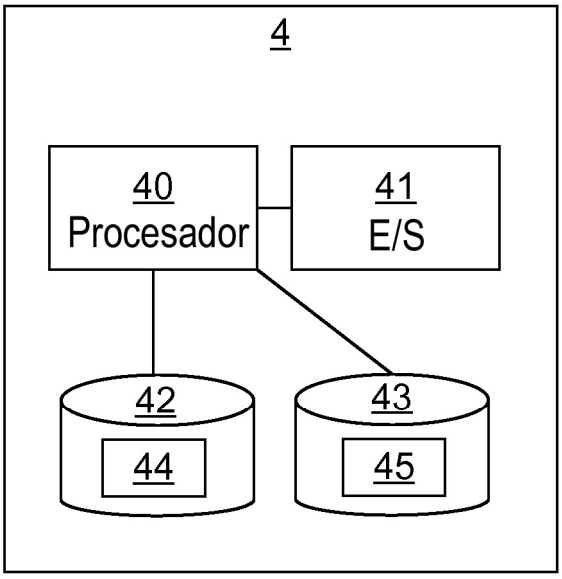

Fig. 9

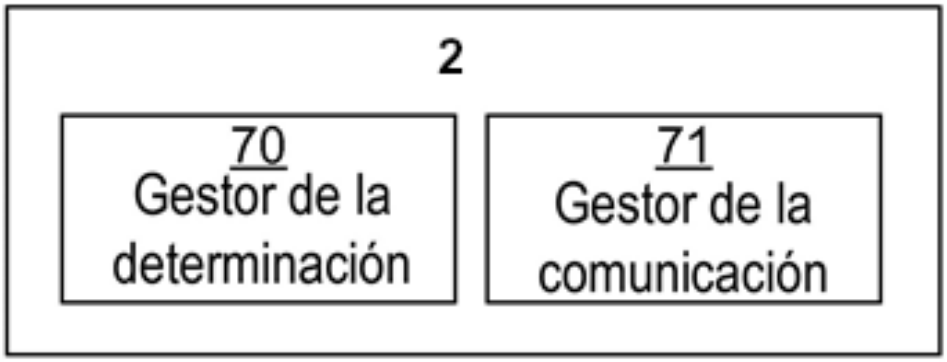

Fig. 10

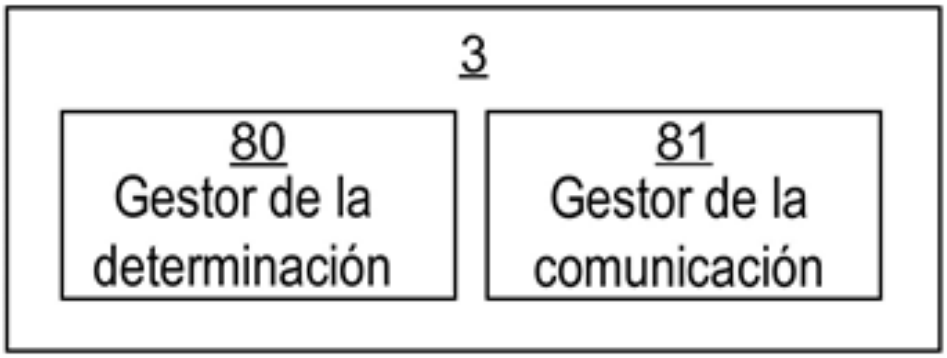

Fig. 11

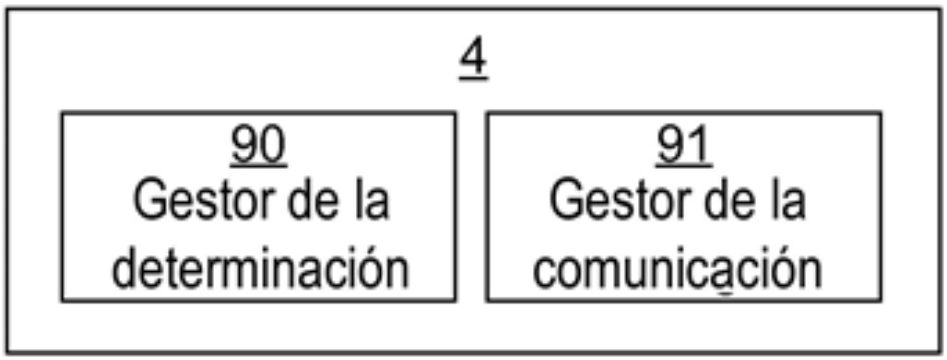

Fig. 12