(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 755 803**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 76/28 (2008.01)
H04W 52/02 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **04.08.2016 PCT/SE2016/050738**

(87) Fecha y número de publicación internacional: **23.03.2017 WO17048170**

(96) Fecha de presentación y número de la solicitud europea: **04.08.2016 E 16754335 (4)**

(97) Fecha y número de publicación de la concesión europea: **09.10.2019 EP 3351031**

(54) Título: **Nodos de acceso radioeléctrico y dispositivos terminales en una red de comunicación**

(30) Prioridad:

14.09.2015 US 201562218166 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.04.2020

(73) Titular/es:

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

(72) Inventor/es:

OHLSSON, OSCAR;
NORRMAN, KARL;
STATTIN, MAGNUS y
SCHLIWA-BERTLING, PAUL

(74) Agente/Representante:

MARTÍN BADAJOZ, Irene

DESCRIPCIÓN

Nodos de acceso radioeléctrico y dispositivos terminales en una red de comunicación

Campo técnico

La divulgación se refiere a nodos de acceso radioeléctrico y a dispositivos terminales en una red de comunicación.

Antecedentes

En un sistema radioeléctrico celular típico, los terminales radioeléctricos o inalámbricos (también conocidos como estaciones móviles, equipos de usuario (UE) o, más generalmente, dispositivos terminales) se comunican mediante una red de acceso radioeléctrico (RAN) con una o más redes centrales. La red de acceso radioeléctrico (RAN) cubre una zona geográfica que se divide en zonas de célula, sirviendo a cada zona de célula una estación de base, por ejemplo, una estación de base radioeléctrica (RBS), que en algunas redes también puede denominarse, por ejemplo, un “nodo B” (en una red de sistema de telecomunicaciones móviles universales (UMTS)), “eNodo B” (en una red de evolución a largo plazo (LTE)), o, más generalmente, un nodo de acceso radioeléctrico. Una célula es una zona geográfica en la que se proporciona cobertura radioeléctrica mediante el equipo de estación de base radioeléctrica en un sitio de estación de base. Cada célula se identifica mediante un identificador dentro de la zona radioeléctrica local, que se difunde en la célula. Las estaciones de base se comunican a través de la interfaz aérea que funciona en radiofrecuencias con las unidades de equipo de usuario (UE) dentro del alcance de las estaciones de base.

En algunas redes de acceso radioeléctrico, varias estaciones de base pueden conectarse (por ejemplo, mediante líneas terrestres o microondas) a un controlador de red radioeléctrica (RNC), un controlador de estación de base (BSC) o una entidad de gestión de movilidad (MME). El controlador de red radioeléctrica supervisa y coordina diversas actividades de la pluralidad de estaciones de base conectadas al mismo. Los controladores de red radioeléctrica normalmente se conectan a una o más redes centrales.

El sistema de telecomunicaciones móviles universales (UMTS) es un sistema de comunicación móvil de tercera generación, que evolucionó a partir del sistema mundial para comunicaciones móviles (GSM). La red de acceso universal radioeléctrico terrestre (UTRAN) es esencialmente una red de acceso radioeléctrico que usa acceso múltiple por división de código de banda ancha (WCDMA) para unidades de equipo de usuario (UE).

La evolución a largo plazo (LTE) es una variante de una tecnología de acceso radioeléctrico de proyecto de asociación de tercera generación (3GPP) en la que los nodos de estación de base radioeléctrica se conectan a MME y pasarelas servidoras (S-GW) en una red central en vez de a nodos de controlador de red radioeléctrica (RNC). En general, en la LTE las funciones de un nodo de controlador de red radioeléctrica (RNC) se distribuyen entre los nodos de estaciones de base radioeléctricas (eNodo B en LTE), MME y S-GW.

Una visión actualmente popular del futuro de las redes celulares incluye máquinas u otros dispositivos autónomos que se comunican entre sí (o con un servidor de aplicación) sin interacción humana. Un escenario típico es hacer que unos sensores envíen mediciones de manera poco frecuente, en el que cada una de las transmisiones consistiría sólo en pequeñas cantidades de datos. Este tipo de comunicación habitualmente se denomina comunicación máquina a máquina (M2M) o comunicación de tipo de máquina (MTC).

Una de las principales características de la comunicación de tipo de máquina (MTC) es la transmisión poco frecuente de pequeñas cantidades de datos. Se espera que el número de dispositivos de MTC aumente de manera exponencial, pero el tamaño de datos por dispositivo seguirá siendo pequeño. En LTE, los procedimientos actuales de transferencia de datos no están optimizados para transferencias de datos pequeñas y sesiones de corta duración, lo que da como resultado una gran sobrecarga de señalización.

Para gestionar transferencias de datos pequeñas de manera más eficiente, el 3GPP está estudiando actualmente métodos para reducir la sobrecarga de señalización cuando se realiza una transición de RRC (control de recursos radioeléctricos) inactivo a RRC conectado. Una de las soluciones propuestas se denomina “reanudación de RRC”, que se basa en reutilizar el contexto de UE de la anterior conexión de RRC para el posterior establecimiento de conexión de RRC. Esto requiere el almacenamiento del contexto de UE en el eNB, y almacenando el contexto de UE el eNB puede evitar la señalización requerida para una activación de seguridad y un establecimiento de portador en la siguiente transición de RRC inactivo a RRC conectado. El término “RRC suspendido” también se usa en ocasiones para referirse a este nuevo estado en el que el UE no tiene una conexión de RRC establecida pero el contexto de UE está almacenado en caché en el u otro eNB.

La reanudación de RRC se efectúa introduciendo dos nuevos procedimientos, que se denominan “suspensión de RRC” y “reanudación de RRC” en el presente documento, y que se ilustran mediante los diagramas de señalización en las figuras 1 y 2 respectivamente. Las figuras 1 y 2 muestran la señalización entre un UE 2 y un eNB 4. En la figura 1, el UE 2 está en el estado o modo de RRC conectado, y está enviando datos 6 al eNB 4 en el enlace

ascendente (UL) y recibiendo datos 8 desde el eNB 4 en el enlace descendente (DL). Hay varias maneras o motivos por los que es necesario que se realice una transición de un UE 2 del estado de RRC conectado al estado de RRC inactivo, pero un motivo puede ser la expiración de un temporizador de inactividad (es decir, que monitoriza el tiempo transcurrido desde que se transmitieron los últimos datos entre el UE 2 y el eNB 4). Por tanto, tras la expiración de un temporizador de inactividad (mostrado por la caja 10), el eNB 4 suspende una conexión enviando una señal 12 al UE 2, que se muestra como “Suspensión de conexión de RRC” en la figura 1. Aunque no se muestra en la figura 1, tanto el UE 2 como el eNB 4 almacenan el contexto de UE para la conexión y un identificador asociado para el UE 2 (que se denomina en el presente documento un “ID de reanudación”). El contexto de UE contiene, por ejemplo, parámetros de configuración de portador y relacionados con la seguridad.

Haciendo referencia ahora a la figura 2, en la siguiente transición de RRC inactivo/suspendido a RRC conectado (por ejemplo, que puede producirse cuando el UE 2 tiene datos para enviar al eNB 4/red de comunicación), el UE 2 “reanuda” la conexión enviando un preámbulo 14 de acceso aleatorio al eNB 4, recibe una respuesta 16 de acceso aleatorio desde el eNB 4 y envía una señal 18 al eNB 4 solicitando que se reanude la conexión de RRC. Esta señal 18 se denomina en el presente documento “Solicitud de reanudación de conexión de RRC”. El UE 2 incluye el ID de reanudación recibido anteriormente en la “Solicitud de reanudación de conexión de RRC” 18, junto con un testigo de autorización.

Aunque no se muestra en la figura 2, el eNB 4 usa el ID de reanudación para recuperar el contexto de UE almacenado (posiblemente desde otro eNB). El eNB 4 usa el testigo de autorización para identificar de manera segura el UE. Suponiendo que se encuentra el contexto de UE y el testigo de autorización es válido, el eNB 4 responde con una señal 20 que indica que la conexión de RRC se ha reanudado satisfactoriamente. Esta señal 20 se denomina “Reanudación de conexión de RRC completada” en el presente documento. El eNB 4 activa entonces la seguridad de estrato de acceso (AS) usando la clave de base de AS antigua, K_{eNB} 22, que, por ejemplo, se usó para derivar la clave de cifrado que se usó para la conexión de RRC antes de suspenderse. El UE 2 está ahora en el estado o modo de RRC conectado, y puede enviar datos 24 al eNB 4 en el UL y recibir datos 26 desde el eNB 4 en el DL.

El procedimiento de reanudación de RRC no está limitado necesariamente a una única (es decir, la misma) célula o un único (es decir, el mismo) eNB, sino que también puede soportarse entre eNB. La reanudación de conexión inter-eNB se gestiona usando captura de contexto, mediante la cual el “eNB de reanudación” (es decir, el eNB que va a reanudar la conexión de RRC) recupera el contexto de UE desde el “eNB de suspensión” (es decir, el eNB que suspendió la conexión de RRC) a través de la interfaz X2 (una interfaz internodo que pueden usar los eNB para intercambiar información entre sí). El eNB de reanudación proporciona al eNB de suspensión el ID de reanudación que el eNB de suspensión usa para identificar el contexto de UE.

Debe observarse que la suspensión de conexión de RRC, la solicitud de reanudación de conexión de RRC y la reanudación de conexión de RRC completada sólo deben considerarse nombres a modo de ejemplo para estas señales/mensajes, pudiendo ser diferentes los nombres adoptados finalmente por el 3GPP en las especificaciones.

Otra optimización que está considerándose en el 3GPP es permitir que se transmitan datos de enlace ascendente en el primer mensaje de enlace ascendente, es decir, junto con la señal 18 (la solicitud de reanudación de conexión de RRC). De esta manera el número de señales/mensajes puede reducirse aún más.

En LTE, se cifran datos de plano de usuario entre el UE y el eNB basándose en una clave compartida, la clave de base de estrato de acceso (AS) K_{eNB}. Aunque la reanudación de RRC no es un traspaso, puede estar relacionada con la movilidad entre dos eNB, y por tanto debe proporcionar una compartimentación de K_{eNB}:s. En caso de un traspaso de X2 de LTE habitual la compartimentación se logra de la siguiente manera. El eNB que controla la célula de origen (es decir, la célula en la que se encuentra el UE antes del traspaso) calcula una nueva clave de base de AS que va a usarse en la célula objetivo (es decir, la célula a la que se va a entregar el UE). Esto es importante por motivos de seguridad ya que impide que la misma clave se use dos veces y también permite la confidencialidad de reenvío. La nueva clave de base de AS, denominada K_{eNB}*, la derivan el UE y el eNB de origen basándose en la identidad de célula física (PCI) de la célula objetivo, la frecuencia objetivo y el K_{eNB} anterior. En vez de usar una K_{eNB}, la derivación de KeNB* también puede realizarse basándose en un parámetro de siguiente salto (NH), que es un valor especial que proporciona la MME al eNB de origen. Se prefiere este tipo de derivación (denominada derivación vertical) pero requiere que esté disponible un valor de NH nuevo (sin usar) en el eNB de origen. Si no hay ningún NH nuevo disponible entonces la derivación de K_{eNB}* se denomina derivación horizontal y se basa en una K_{eNB}.

Sumario

Si se deriva una nueva K_{eNB} de manera similar cuando el eNB suspende un UE para una posterior reanudación de RRC, se presenta una situación ambigua si se transmiten datos en el primer mensaje de enlace ascendente en la reanudación de RRC. En particular, si el tipo de derivación de clave no se ha acordado de antemano, el UE y el eNB que reanudan la conexión pueden terminar con una K_{eNB}* diferente, lo que da como resultado un descifrado fallido de los datos de enlace ascendente. También se presenta el mismo problema si el UE usa un algoritmo de cifrado

diferente del del eNB de reanudación, o un algoritmo no soportado por el eNB de reanudación.

De manera similar, si el UE se suspende en una célula, y más tarde se reanuda en otra, puede producirse la misma ambigüedad. El motivo de ello es que el eNB que suspende el UE no puede proporcionar la misma clave de base al eNB con el que el UE reanuda la conexión, lo que quebrantaría el principio de compartimentación de claves en LTE.

Por tanto, existe la necesidad de mejoras en el procedimiento de reanudación de RRC propuesto para evitar algunas o la totalidad de las desventajas expuestas anteriormente.

El alcance de la invención se define mediante las reivindicaciones independientes adjuntas. Según un primer aspecto, se proporciona un método para hacer funcionar un dispositivo terminal. El método comprende hacer funcionar el dispositivo terminal en un estado conectado con respecto a la red de comunicación; y recibir una primera señal desde un primer nodo de acceso radioeléctrico en la red de comunicación que indica que ha de suspenderse el estado conectado, comprendiendo la primera señal información para su uso en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal y el primer nodo de acceso radioeléctrico u otro nodo de acceso radioeléctrico en la red de comunicación si se reanuda el estado conectado.

Según un segundo aspecto, se proporciona un producto de programa informático que comprende un medio legible por ordenador que tiene código legible por ordenador incorporado en el mismo, estando el código legible por ordenador configurado de tal manera que, tras la ejecución mediante un ordenador o procesador adecuado, se hace que el ordenador o procesador realice el método descrito anteriormente.

Según un tercer aspecto, se proporciona un dispositivo terminal. El dispositivo terminal está adaptado para funcionar en un estado conectado con respecto a la red de comunicación; y recibir una primera señal desde un primer nodo de acceso radioeléctrico en la red de comunicación que indica que ha de suspenderse el estado conectado, comprendiendo la primera señal información para su uso en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal y el primer nodo de acceso radioeléctrico u otro nodo de acceso radioeléctrico en la red de comunicación si se reanuda el estado conectado.

Según un cuarto aspecto, se proporciona otro dispositivo terminal. El dispositivo terminal comprende un procesador y una memoria, conteniendo dicha memoria instrucciones ejecutables por dicho procesador mediante las cuales dicho dispositivo terminal está operativo para funcionar en un estado conectado con respecto a la red de comunicación; y recibir una primera señal desde un primer nodo de acceso radioeléctrico en la red de comunicación que indica que ha de suspenderse el estado conectado, comprendiendo la primera señal información para su uso en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal y el primer nodo de acceso radioeléctrico u otro nodo de acceso radioeléctrico en la red de comunicación si se reanuda el estado conectado.

Según un quinto aspecto, se proporciona otro dispositivo terminal. El dispositivo terminal comprende un primer módulo configurado para hacer funcionar el dispositivo terminal en un estado conectado con respecto a la red de comunicación; y un segundo módulo configurado para recibir una primera señal desde un primer nodo de acceso radioeléctrico en la red de comunicación que indica que ha de suspenderse el estado conectado, comprendiendo la primera señal información para su uso en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal y el primer nodo de acceso radioeléctrico u otro nodo de acceso radioeléctrico en la red de comunicación si se reanuda el estado conectado.

Según un sexto aspecto, se proporciona un método para hacer funcionar un primer nodo de acceso radioeléctrico en una red de comunicación. El método comprende enviar una primera señal a un dispositivo terminal que está en un estado conectado con respecto a la red de comunicación, indicando la primera señal que ha de suspenderse el estado conectado, comprendiendo la primera señal información para su uso por parte del dispositivo terminal en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal y el primer nodo de acceso radioeléctrico u otro nodo de acceso radioeléctrico en la red de comunicación si se reanuda el estado conectado.

Según un séptimo aspecto, se proporciona un producto de programa informático que comprende un medio legible por ordenador que tiene código legible por ordenador incorporado en el mismo, estando el código legible por ordenador configurado de tal manera que, tras la ejecución mediante un ordenador o procesador adecuado, se hace que el ordenador o procesador realice el método descrito anteriormente.

Según un octavo aspecto, se proporciona un primer nodo de acceso radioeléctrico para su uso en una red de comunicación. El primer nodo de acceso radioeléctrico está adaptado para enviar una primera señal a un dispositivo terminal que está en un estado conectado con respecto a la red de comunicación, indicando la primera señal que ha de suspenderse el estado conectado, comprendiendo la primera señal información para su uso por parte del dispositivo terminal en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal y el primer nodo de acceso radioeléctrico u otro nodo de acceso radioeléctrico en la red de comunicación si se reanuda el estado conectado.

Según un noveno aspecto, se proporciona un primer nodo de acceso radioeléctrico para su uso en una red de comunicación. El primer nodo de acceso radioeléctrico comprende un procesador y una memoria, conteniendo dicha memoria instrucciones ejecutables por dicho procesador mediante las cuales dicho primer nodo de acceso radioeléctrico está operativo para enviar una primera señal a un dispositivo terminal que está en un estado conectado con respecto a la red de comunicación, indicando la primera señal que ha de suspenderse el estado conectado, comprendiendo la primera señal información para su uso por parte del dispositivo terminal en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal y el primer nodo de acceso radioeléctrico u otro nodo de acceso radioeléctrico en la red de comunicación si se reanuda el estado conectado.

Según un décimo aspecto, se proporciona un primer nodo de acceso radioeléctrico para su uso en una red de comunicación. El primer nodo de acceso radioeléctrico comprende un primer módulo configurado para enviar una primera señal a un dispositivo terminal que está en un estado conectado con respecto a la red de comunicación, indicando la primera señal que ha de suspenderse el estado conectado, comprendiendo la primera señal información para su uso por parte del dispositivo terminal en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal y el primer nodo de acceso radioeléctrico u otro nodo de acceso radioeléctrico en la red de comunicación si se reanuda el estado conectado.

Según un undécimo aspecto, se proporciona un método para hacer funcionar un segundo nodo de acceso radioeléctrico en una red de comunicación. El método comprende recibir una primera señal desde un dispositivo terminal cuyo estado conectado con respecto a la red de comunicación se ha suspendido, solicitando la primera señal la reanudación del estado conectado; enviar una segunda señal a un primer nodo de acceso radioeléctrico para solicitar información de contexto relacionada con el estado conectado del dispositivo terminal con la red de comunicación; y recibir una tercera señal desde el primer nodo de acceso radioeléctrico, comprendiendo la tercera señal la información de contexto y una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal y el segundo nodo de acceso radioeléctrico tras la reanudación del estado conectado.

Según un duodécimo aspecto, se proporciona un producto de programa informático que comprende un medio legible por ordenador que tiene código legible por ordenador incorporado en el mismo, estando el código legible por ordenador configurado de tal manera que, tras la ejecución mediante un ordenador o procesador adecuado, se hace que el ordenador o procesador realice el método descrito anteriormente.

Según un decimotercer aspecto, se proporciona un segundo nodo de acceso radioeléctrico para su uso en una red de comunicación. El segundo nodo de acceso radioeléctrico está adaptado para recibir una primera señal desde un dispositivo terminal cuyo estado conectado con respecto a la red de comunicación se ha suspendido, solicitando la primera señal la reanudación del estado conectado; enviar una segunda señal a un primer nodo de acceso radioeléctrico para solicitar información de contexto relacionada con el estado conectado del dispositivo terminal con la red de comunicación; y recibir una tercera señal desde el primer nodo de acceso radioeléctrico, comprendiendo la tercera señal la información de contexto y una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal y el segundo nodo de acceso radioeléctrico tras la reanudación del estado conectado.

Según un decimocuarto aspecto, se proporciona un segundo nodo de acceso radioeléctrico para su uso en una red de comunicación. El segundo nodo de acceso radioeléctrico comprende un procesador y una memoria, conteniendo dicha memoria instrucciones ejecutables por dicho procesador mediante las cuales dicho segundo nodo de acceso radioeléctrico está operativo para recibir una primera señal desde un dispositivo terminal cuyo estado conectado con respecto a la red de comunicación se ha suspendido, solicitando la primera señal la reanudación del estado conectado; enviar una segunda señal a un primer nodo de acceso radioeléctrico para solicitar información de contexto relacionada con el estado conectado del dispositivo terminal con la red de comunicación; y recibir una tercera señal desde el primer nodo de acceso radioeléctrico, comprendiendo la tercera señal la información de contexto y una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal y el segundo nodo de acceso radioeléctrico tras la reanudación del estado conectado.

Según un decimoquinto aspecto, se proporciona un segundo nodo de acceso radioeléctrico para su uso en una red de comunicación. El segundo nodo de acceso radioeléctrico comprende un primer módulo para recibir una primera señal desde un dispositivo terminal cuyo estado conectado con respecto a la red de comunicación se ha suspendido, solicitando la primera señal la reanudación del estado conectado; un segundo módulo para enviar una segunda señal a un primer nodo de acceso radioeléctrico para solicitar información de contexto relacionada con el estado conectado del dispositivo terminal con la red de comunicación; y un tercer módulo para recibir una tercera señal desde el primer nodo de acceso radioeléctrico, comprendiendo la tercera señal la información de contexto y una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal y el segundo nodo de acceso radioeléctrico tras la reanudación del estado conectado.

Por tanto, las técnicas descritas en el presente documento permiten una transferencia de datos instantánea (por ejemplo, en el mensaje de L3 inicial del procedimiento de acceso aleatorio en LTE). Una transferencia de datos instantánea reduce el retardo y el número de mensajes que es necesario intercambiar a través de la interfaz aérea,

particularmente en el caso de dispositivos de MTC en los que puede que sólo sea necesario transmitir una pequeña cantidad de datos en cualquier momento dado. Las técnicas descritas en el presente documento también evitan la necesidad de enviar datos en texto claro (es decir, no cifrado), lo que infringiría el modelo de seguridad de LTE, o de retardar el envío de datos hasta que se hayan proporcionado parámetros de seguridad como parte del procedimiento de reanudación.

Breve descripción de los dibujos

Características, objetos y ventajas de las técnicas actualmente divulgadas resultarán evidentes para los expertos en la técnica al leer la siguiente descripción detallada, en la que se harán referencias a las figuras adjuntas, en las que:

la figura 1 ilustra la señalización en un procedimiento de suspensión de conexión;

la figura 2 ilustra la señalización en un procedimiento de reanudación de conexión;

la figura 3 ilustra una red de LTE a modo de ejemplo;

la figura 4 es un diagrama de bloques de un dispositivo terminal según una realización;

la figura 5 es un diagrama de bloques de un nodo de acceso radioeléctrico según una realización;

la figura 6 es un diagrama de señalización que ilustra la señalización en una primera realización a modo de ejemplo;

la figura 7 es un diagrama de flujo que ilustra un método para hacer funcionar un dispositivo terminal según una realización general;

la figura 8 es un diagrama de flujo que ilustra un método para hacer funcionar un primer nodo de acceso radioeléctrico según otra realización general;

la figura 9 es un diagrama de flujo que ilustra un método para hacer funcionar un segundo nodo de acceso radioeléctrico según otra realización general;

la figura 10 es un diagrama de bloques de un dispositivo terminal según otra realización;

la figura 11 es un diagrama de bloques de un primer nodo de acceso radioeléctrico según otra realización;

la figura 12 es un diagrama de bloques de un segundo nodo de acceso radioeléctrico según otra realización;

la figura 13 es un diagrama de bloques de un dispositivo terminal según aún otra realización;

la figura 14 es un diagrama de bloques de un primer nodo de acceso radioeléctrico según aún otra realización;

la figura 15 es un diagrama de bloques de un segundo nodo de acceso radioeléctrico según aún otra realización.

Descripción detallada

A continuación se exponen detalles específicos, tales como realizaciones particulares con propósitos de explicación y no de limitación. No obstante, un experto en la técnica apreciará que pueden emplearse otras realizaciones aparte de estos detalles específicos. En algunos casos, se omiten descripciones detalladas de métodos, nodos, interfaces, circuitos y dispositivos que se conocen bien para no complicar la descripción con detalles innecesarios. Los expertos en la técnica apreciarán que las funciones descritas pueden implementarse en uno o más nodos usando un conjunto de circuitos de hardware (por ejemplo, puertas lógicas analógicas y/o discretas interconectadas para realizar una función especializada, ASIC, PLA, etc.) y/o usando datos y programas de software junto con uno o más microprocesadores digitales u ordenadores de uso general. Los nodos que se comunican usando la interfaz aérea también tienen un conjunto de circuitos de radiocomunicaciones adecuado. Además, cuando sea apropiado, puede considerarse que la tecnología se incorpore totalmente dentro de cualquier forma de memoria legible por ordenador, tal como una memoria de estado sólido, un disco magnético, o un disco óptico que contenga un conjunto apropiado de instrucciones informáticas que hagan que un procesador lleve a cabo las técnicas descritas en el presente documento.

La implementación de hardware puede incluir o abarcar, sin limitación, hardware de procesador de señal digital (DSP), un procesador de conjunto de instrucciones reducido, un conjunto de circuitos de hardware (por ejemplo, digitales o analógicos) que incluyen, pero sin limitarse a, circuito(s) integrado(s) de aplicación específica (ASIC) y/o matriz/matrices de puertas programable(s) in-situ (FPGA), y (cuando sea apropiado) máquinas de estados capaces de realizar tales funciones.

En cuanto a la implementación de ordenador, generalmente se entiende que un ordenador comprende uno o más procesadores, una o más unidades de procesamiento, uno o más módulos de procesamiento o uno o más controladores, y los términos ordenador, procesador, unidad de procesamiento, módulo de procesamiento y controlador pueden emplearse indistintamente. Cuando las proporciona un ordenador, procesador, unidad de procesamiento, módulo de procesamiento o controlador, las funciones puede proporcionarlas un único ordenador, procesador, unidad de procesamiento, módulo de procesamiento o controlador dedicado, un único ordenador, procesador, unidad de procesamiento, módulo de procesamiento o controlador compartido, o una pluralidad de ordenadores, procesadores, unidades de procesamiento, módulos de procesamiento o controladores individuales, algunos de los cuales pueden estar compartidos o distribuidos. Además, estos términos también se refieren a otro hardware capaz de realizar tales funciones y/o ejecutar software, tal como el hardware de ejemplo mencionado anteriormente.

Aunque en la descripción siguiente se usa el término equipo de usuario (UE), el experto en la técnica debe entender que “UE” es un término no limitativo que comprende cualquier nodo o dispositivo inalámbrico o móvil equipado con una interfaz radioeléctrica que permite al menos uno de: transmitir señales en un enlace ascendente (UL) y recibir y/o medir señales en un enlace descendente (DL). Un UE en el presente documento puede comprender un UE (en su sentido general) capaz de funcionar o al menos realizar mediciones en una o más frecuencias, frecuencias portadoras, portadoras de componente o bandas de frecuencia. Puede ser un “UE” que funciona en un modo de tecnología de acceso radioeléctrico (RAT) única o múltiple o multinorma. Al igual que en el caso de “UE”, los términos “dispositivo móvil” y “dispositivo terminal” pueden usarse indistintamente en la siguiente descripción, y se apreciará que un dispositivo de este tipo, particularmente un dispositivo de MTC, no tiene que ser necesariamente “móvil” en el sentido de que lo porta un usuario. En cambio, los términos “dispositivo móvil” y “dispositivo terminal” abarcan cualquier dispositivo que es capaz de comunicarse con redes de comunicación que funcionan según una o más normas de comunicación móvil, tales como el sistema mundial para comunicaciones móviles, GSM, UMTS, evolución a largo plazo, LTE, etc.

Una célula está asociada con una estación de base, en la que una estación de base comprende en sentido general cualquier nodo de red que transmite señales radioeléctricas en el enlace descendente y/o recibe señales radioeléctricas en el enlace ascendente. Algunas estaciones de base de ejemplo, o términos usados para describir estaciones de base, son eNodo B, eNB, nodo B, macro/micro/pico/femtoestación de base radioeléctrica, eNodo B doméstico (también conocido como femtoestación de base), retransmisor, repetidor, sensor, nodos radioeléctricos sólo de transmisión o nodos radioeléctricos sólo de recepción. Una estación de base puede funcionar o al menos realizar mediciones en una o más frecuencias, frecuencias portadoras o bandas de frecuencia y puede tener capacidad de agregación de portadora. También puede ser un nodo de tecnología de acceso radioeléctrico (RAT) única, RAT múltiple, o multinorma, por ejemplo, que usa los mismos o diferentes módulos de banda de base para diferentes RAT.

Debe observarse que el uso del término “nodo de acceso radioeléctrico” tal como se usa en el presente documento puede referirse a una estación de base, tal como un eNodo B, o un nodo de red en la red de acceso radioeléctrico (RAN) responsable de la gestión de recursos, tal como un controlador de red radioeléctrica (RNC).

A menos que se indique otra cosa en el presente documento, la señalización descrita se realiza mediante o bien enlaces directos o bien enlaces lógicos (por ejemplo, mediante protocolos de capa superior y/o mediante uno o más nodos de red).

La figura 3 muestra un diagrama de ejemplo de una arquitectura de red de acceso radioeléctrico terrestre universal UMTS evolucionado (E-UTRAN) como parte de un sistema 32 de comunicaciones basado en LTE al que pueden aplicarse las técnicas descritas en el presente documento. Los nodos en una red 34 central parte del sistema 32 incluyen una o más entidades 36 de gestión de movilidad (MME), un nodo de control de clave para la red de acceso de LTE, y una o más pasarelas 38 servidoras (SGW) que encaminan y reenvían paquetes de datos de usuario mientras actúan como anclaje de movilidad. Se comunican con estaciones de base o nodos 40 de acceso radioeléctrico denominados eNB en LTE, a través de una interfaz, por ejemplo, una interfaz S1. Los eNB 40 pueden incluir las mismas o diferentes categorías de eNB, por ejemplo, macro-eNB, y/o micro/pico/femto-eNB. Los eNB 40 se comunican entre sí a través de una interfaz internodo, por ejemplo, una interfaz X2. La interfaz S1 y la interfaz X2 se definen en la norma LTE. Se muestra un UE 42, y un UE 42 puede recibir datos de enlace descendente desde y enviar datos de enlace ascendente hasta una de las estaciones 40 de base, denominándose esa estación 40 de base la estación de base servidora del UE 42.

La figura 4 muestra un dispositivo 42 terminal (UE) que puede adaptarse o configurarse para funcionar según una o más de las realizaciones de ejemplo no limitativas descritas. El UE 42 comprende un procesador o unidad 50 de procesamiento que controla el funcionamiento del UE 42. La unidad 50 de procesamiento se conecta a una unidad 52 de transceptor (que comprende un receptor y un transmisor) con antena(s) 54 asociada(s) que se usan para transmitir señales hasta y recibir señales desde un nodo 40 de acceso radioeléctrico en la red 32. El UE 42 también comprende una memoria o unidad 56 de memoria que se conecta a la unidad 50 de procesamiento y que contiene instrucciones o código informático ejecutables por la unidad 50 de procesamiento y otra información o datos requeridos para el funcionamiento del UE 42.

La figura 5 muestra un nodo de acceso radioeléctrico (por ejemplo, una estación de base de red celular tal como un nodo B o un eNodo B) que puede adaptarse o configurarse para funcionar según las realizaciones de ejemplo descritas. El nodo 40 de acceso radioeléctrico comprende un procesador o unidad 60 de procesamiento que controla el funcionamiento del nodo 40 de acceso radioeléctrico. La unidad 60 de procesamiento se conecta a una unidad 62 de transceptor (que comprende un receptor y un transmisor) con antena(s) 64 asociada(s) que se usan para transmitir señales hasta, y recibir señales desde, el UE 42 en la red 32. El nodo 40 de acceso radioeléctrico también comprende una memoria o unidad 66 de memoria que se conecta a la unidad 60 de procesamiento y que contiene instrucciones o código informático ejecutables por la unidad 60 de procesamiento y otra información o datos requeridos para el funcionamiento del nodo 40 de acceso radioeléctrico. El nodo 40 de acceso radioeléctrico también incluye componentes y/o un conjunto 68 de circuitos para permitir que el nodo 40 de acceso radioeléctrico intercambie información con otro nodo 40 de acceso radioeléctrico (por ejemplo, mediante una interfaz X2), y/o con un nodo 36, 38 de red central (por ejemplo, mediante una interfaz S1). Se apreciará que las estaciones de base para su uso en otros tipos de red (por ejemplo, UTRAN o RAN de WCDMA) incluirán componentes similares a los mostrados en la figura 5 y un conjunto 68 de circuitos de interfaz apropiado para permitir las comunicaciones con los demás nodos de acceso radioeléctrico en esos tipos de redes (por ejemplo, otras estaciones de base, nodos de gestión de movilidad y/o nodos en la red central).

Se apreciará que sólo los componentes del UE 42 y del nodo 40 de acceso radioeléctrico requeridos para explicar las realizaciones presentadas en el presente documento se ilustran en las figuras 4 y 5.

Aunque las realizaciones de la presente divulgación se describirán principalmente en el contexto de LTE, los expertos en la técnica apreciarán que los problemas y soluciones descritos en el presente documento pueden aplicarse igualmente a otros tipos de redes de acceso inalámbrico y equipos de usuario (UE) que implementan otras normas y tecnologías de acceso, y por tanto la LTE (y el resto de la terminología específica de LTE usada en el presente documento) sólo deben considerarse ejemplos de las tecnologías a las que pueden aplicarse las técnicas.

Tal como se observó anteriormente, cuando se reanuda una conexión de RRC es deseable poder enviar datos de enlace ascendente al eNB en el primer mensaje de enlace ascendente, es decir, junto con la solicitud de reanudar la conexión de RRC (por ejemplo, con la señal 18 en la figura 2). Sin embargo, en LTE los datos han de cifrarse usando una clave de cifrado compartida, derivada a partir de la clave de base de AS K_{eNB}, y si se deriva una nueva clave de base de AS K_{eNB} (para su uso cuando se reanuda la conexión) cuando el eNB suspende un UE para una posterior reanudación de RRC, se presenta una situación ambigua si se transmiten datos en el primer mensaje de enlace ascendente en la reanudación de RRC si el tipo de derivación de clave no se ha acordado de antemano y/o si el UE usa un algoritmo de cifrado diferente del del eNB de reanudación, o un algoritmo de cifrado que el eNB de reanudación no soporta. Igualmente, en el caso de que un UE se suspenda en una célula y más tarde se reanude en otra, la misma ambigüedad puede producirse ya que el eNB que suspende el UE no puede proporcionar la misma clave de base al eNB con que el UE reanuda la conexión dado que esto quebrantaría el principio de compartimentación de claves en LTE.

Por tanto, según una técnica a modo de ejemplo específica, para permitir que un eNB que hospeda la célula en la que el UE reanudará una conexión descifre datos de enlace ascendente contenidos en una solicitud de reanudar la conexión (por ejemplo, en la primera trama de control de acceso al medio (MAC) de enlace ascendente junto con la solicitud de reanudación de conexión de RRC), el eNB que suspende el UE indica al UE información (por ejemplo, parámetros de derivación de clave) para su uso en la determinación de una clave de base de AS a partir de la que pueden derivarse claves de cifrado para cifrar datos que van a enviarse entre el UE y el eNB de reanudación, lo que permite que el UE calcule la clave de base de AS correcta para su uso con la célula en la que ha de reanudarse la conexión (y para que el eNB de reanudación calcule la clave de base de AS correcta). En algunas realizaciones a modo de ejemplo el eNB que suspende el UE puede indicar además el algoritmo de seguridad de estrato de acceso (AS) que ha de usarse cuando se suspende la conexión. Cuando el UE reanuda más tarde la conexión en una nueva célula, el eNB que suspendió el UE proporciona al eNB con el que el UE reanuda la conexión la clave de base de AS correcta e indica el algoritmo de seguridad de AS correcto. El algoritmo de seguridad de AS puede ser un algoritmo de cifrado, un algoritmo de integridad; la indicación también puede referirse a una indicación de un algoritmo de cada tipo.

Tal como se usa en el presente documento, el término “eNB de suspensión” se refiere al eNB que suspende, o inicia la suspensión de, la conexión de RRC con el UE, y el término “eNB de reanudación” se refiere al eNB que reanuda la conexión de RRC con el UE.

El diagrama de señalización en la figura 6 ilustra la suspensión y reanudación a modo de ejemplo de una conexión de RRC según las técnicas descritas en el presente documento. La señalización en la figura 6 proporciona una transferencia de datos de enlace ascendente “instantánea” en el sentido de que pueden enviarse datos de UL con la solicitud de reanudar la conexión de RRC.

La figura 6 ilustra la señalización entre un UE 42, un eNB 40 de suspensión y un eNB 40 de reanudación, y por tanto se supone que el eNB de reanudación y el eNB de suspensión son eNB diferentes. Sin embargo, es posible que el

UE pueda reanudar la conexión con el mismo eNB, y la variación de la señalización mostrada en la figura 6 requerida para abordar este escenario se describe con más detalle a continuación.

Inicialmente, el UE 42 tiene una conexión de RRC establecida con un eNB 40 (el eNB indicado en la figura 6 como el eNB de suspensión). Debido a algún desencadenador, por ejemplo, la expiración de un temporizador de inactividad de UE, el eNB 40 de suspensión decide suspender la conexión de RRC enviando una señal 601 al UE (indicado como el mensaje “Suspensión de conexión de RRC”).

Además del ID de reanudación, el mensaje 601 también contiene el contador de concatenación de siguiente salto, NCC (un parámetro que se usa en la derivación de K_{eNB}*) y la configuración de algoritmo de seguridad que va a usarse en la célula de reanudación.

Tras la recepción de la señal/mensaje 601, el UE 42 almacena el contexto de UE relacionado (es decir, el contexto de UE relacionado con la conexión de RRC que va a suspenderse) así como el NCC y la configuración de algoritmo de seguridad indicados en el mensaje 601, y el UE entra en un estado inactivo o suspendido de RRC (indicado mediante la caja 603).

El NCC es un parámetro existente en LTE que indica el número de derivaciones de clave verticales que se han realizado desde la K_{eNB} inicial. Dado que se usa un valor de siguiente salto, NH (un parámetro de “clave intermedia” que se usa en la derivación de la clave de base de AS, K_{eNB}*) nuevo (sin usar) para cada derivación de clave vertical, hay una correspondencia uno a uno entre NH y NCC (la única excepción es NCC=0 cuya correspondencia se establece con respecto a la K_{eNB} inicial). Además, dado que todas las K_{eNB}:s se derivan originalmente a partir de o bien la K_{eNB} inicial o un NH, cada K_{eNB} se asocia también de manera única con un NCC (sin embargo, lo contrario no es cierto).

El valor del NCC incluido en el mensaje 601 de suspensión de conexión de RRC depende de cómo el UE debe derivar la K_{eNB}*. Si un par {NH, NCC} sin usar está disponible en el eNB 40 de suspensión, el eNB (y más tarde el UE) derivarán la K_{eNB}* a partir del NH (esta es la derivación de clave vertical), de otro modo si ningún par {NH, NCC} sin usar está disponible en el eNB, el UE y el eNB de reanudación derivan la K_{eNB}* a partir de la K_{eNB} actual (esto es, la derivación de clave horizontal). En el primer caso el NCC asociado con el NH se envía al UE en el mensaje 601, y en el último caso el NCC asociado con la K_{eNB} actual se envía al UE en el mensaje 601.

Debe observarse que la derivación real de K_{eNB}* no se realiza en esta fase del procedimiento, sino más tarde cuando se conocen los parámetros de la célula en la que ha de reanudarse la conexión (concretamente se conoce el ID de célula física (PCI) y el número de canal de radiofrecuencia absoluto de EUTRA de enlace descendente (EARFCN-DL)).

Por tanto, después de una suspensión de la conexión de RRC, en un momento posterior en el tiempo llegan nuevos datos a la memoria intermedia de UL en el UE 42. Esto desencadena que el UE reanude la conexión de RRC enviando un preámbulo 605 de acceso aleatorio a un eNB de reanudación (es decir, el eNB con el que el UE desearía reanudar la conexión de RRC), recibiendo una respuesta 607 de acceso aleatorio y luego enviando una solicitud 609 de reanudación de conexión (“Solicitud de reanudación de conexión de RRC”) junto con los datos de enlace ascendente cifrados al eNB de reanudación. El UE 42 incluye su ID de reanudación y un testigo de autorización en la solicitud de reanudación de conexión de RRC. En algunas realizaciones, particularmente en las que el eNB de reanudación (o célula de reanudación) es diferente del eNB de suspensión (o célula de suspensión), el UE 42 también puede incluir un identificador del eNB de suspensión (o célula de suspensión) en la solicitud de reanudación de conexión de RRC. Los datos de enlace ascendente se cifran usando la nueva clave de base de AS K_{eNB}* derivada usando el NCC y la configuración de algoritmo de seguridad indicados en la señal 601.

En particular, la nueva clave de base de AS K_{eNB}* se deriva de la siguiente manera. Si el valor de NCC que recibió el UE en el mensaje 601 “Suspensión de conexión de RRC” desde el eNB de suspensión es igual al valor de NCC asociado con la K_{eNB} activa actualmente, entonces el UE deriva la K_{eNB}* a partir de la K_{eNB} activa actualmente y la PCI de la célula de reanudación y su frecuencia EARFCN-DL. Sin embargo, si el UE recibió un valor de NCC que era diferente del NCC asociado con la K_{eNB} activa actualmente, entonces el UE calcula en primer lugar el parámetro de siguiente salto (NH) correspondiente al NCC, y luego deriva la K_{eNB}* a partir del NH y la PCI de la célula de reanudación y su frecuencia EARFCN-DL.

Tras la recepción del mensaje 609, el eNB 40 de reanudación extrae el ID de reanudación y envía una solicitud 611 al eNB 40 de suspensión para recuperar el contexto de UE asociado. En algunas realizaciones el eNB de reanudación puede deducir a partir del ID de reanudación qué eNB es el eNB de suspensión, pero en otras realizaciones el eNB de reanudación puede identificar el eNB de suspensión o la célula de suspensión a partir de un identificador para el eNB de suspensión o la célula de suspensión que el UE 42 incluyó en la solicitud de reanudación de conexión de RRC.

El eNB 40 de suspensión recibe la solicitud 611, recupera el contexto de UE asociado con el ID de reanudación y envía el contexto de UE al eNB de reanudación en el mensaje 613 de respuesta. El mensaje 613 de respuesta

también incluye la K_{eNB}*, la configuración de algoritmo de seguridad y el testigo de autorización para el UE 42.

En el caso de que el eNB de suspensión no encuentre ningún contexto de UE, el eNB de suspensión responde al eNB de reanudación con un mensaje 613 de error que indica que no hay ningún UE asociado con el ID de reanudación.

Suponiendo que el mensaje 613 de respuesta contiene el contexto de UE, el eNB de reanudación verifica el testigo de autorización contenido en la solicitud 609 de reanudación sometiéndolo a una concordancia con el testigo de autorización recibido desde el eNB de suspensión (etapa 615). En algunas realizaciones la operación de concordancia puede ser una simple comparación, pero en otras realizaciones la operación de concordancia no es una simple comparación. El eNB de suspensión puede, por ejemplo, proporcionar un primer valor al eNB de reanudación, que calcula entonces una función de ese valor para producir un segundo valor que se compara con el testigo de autorización.

Suponiendo que el testigo de autorización (y por tanto el UE 42) se verifica, el eNB 40 de reanudación se asegura de que la configuración de algoritmo de seguridad se soporta y, en caso afirmativo, establece la seguridad de AS usando una K_{eNB}* (etapa 617).

Siempre que las etapas 615 y 617 anteriores sean satisfactorias, el eNB de reanudación puede derivar entonces la clave de cifrado a partir de la clave de base de AS y descifrar los datos de enlace ascendente recibidos en el mensaje 609 de solicitud de reanudación, y reenviar los datos de UL a la red central (etapa 619).

El eNB de reanudación envía entonces un mensaje 621 de compleción (indicado “Reanudación de conexión de RRC completada” en la figura 6) al UE para indicar que la conexión se ha reanudado.

El UE 42 está ahora en el estado o modo de RRC conectado, y puede enviar datos 623 al eNB 40 de reanudación en el UL y recibir datos 625 desde el eNB 40 de reanudación en el DL.

Sin embargo, si el eNB de reanudación no pudo obtener el contexto de UE o la etapa 615 no fue satisfactoria, la reanudación de conexión se interrumpe y se devuelve un mensaje de error al UE en vez del mensaje 621 de compleción. Si la etapa 617 no fue satisfactoria (es decir, debido a una configuración de algoritmo de seguridad no válida), la conexión de RRC todavía puede reanudarse pero el mensaje 621 de respuesta indicará que no se han reenviado datos de UL. En este caso la respuesta 621 también puede contener una o más de las configuraciones de algoritmo de seguridad soportadas para permitir que el UE determine la K_{eNB}* correcta. Sólo se indica una configuración por tipo de algoritmo de seguridad (integridad/cifrado).

Como alternativa a la inclusión de la configuración de algoritmo de seguridad en el mensaje 601 de suspensión de conexión de RRC, puede suponerse que la configuración de algoritmo de seguridad sigue siendo la misma cuando se reanuda la conexión de RRC tal como era antes de suspenderse. Por tanto, el eNB de suspensión proporciona la configuración de algoritmo de seguridad al eNB de reanudación, por ejemplo, en o junto al mensaje 613 de respuesta de contexto de UE. Si el eNB de reanudación soporta la configuración de algoritmo de seguridad entonces la conexión de RRC puede reanudarse tal como se muestra en la figura 6. De otro modo si el eNB de reanudación no soporta la configuración de algoritmo de seguridad, puede proporcionarse una configuración de seguridad alternativa en el mensaje 621 de respuesta desde el eNB de reanudación al UE. El eNB de reanudación también puede rechazar simplemente la solicitud 609 de reanudación de conexión de RRC o liberar la conexión de RRC. Si la solicitud 609 de reanudación de conexión de RRC se rechaza el UE puede, por ejemplo, intentar un restablecimiento de conexión de RRC. Si la conexión de RRC se libera el UE puede, por ejemplo, intentar un nuevo establecimiento de conexión de RRC a partir del estado inactivo.

En algunas realizaciones, en vez de (o además de) incluir un testigo de autorización en la solicitud 609 de reanudación de conexión de RRC, el UE puede aplicar una protección de integridad a toda la solicitud 609 de reanudación de conexión de RRC usando una clave de protección de integridad derivada a partir de la nueva clave de base de AS K_{eNB}* y el algoritmo de integridad en la configuración de algoritmo de seguridad. En la etapa 615 ó 617 el eNB de reanudación verificará entonces la identidad de UE verificando la protección de integridad del mensaje 609. Se apreciará que este enfoque requiere que el eNB de reanudación soporte la configuración de algoritmo de seguridad, y si ese no es el caso, la solicitud 609 de reanudación tendrá que rechazarse dado que no puede verificarse.

En la descripción anterior se supone que el eNB de suspensión es diferente del eNB de reanudación (es decir, se trata de una reanudación de RRC inter-eNB). En el escenario en el que el eNB de suspensión y el de reanudación son los mismos (es decir, se trata de una reanudación de RRC intra-eNB), el procedimiento es el mismo que el que se muestra en la figura 6 excepto porque las señales 611 y 613 se producen internamente en el eNB (es decir, el eNB busca en una memoria o base de datos usando el ID de reanudación y recupera el contexto de UE requerido).

Además, si una conexión se reanuda en la misma célula (según se identifica mediante su PCI y EARFCN-DL), el UE y el eNB pueden o bien derivar una nueva clave de base de AS, o bien seguir usando la existente. En este último

caso es importante que no se restablezca un RECUENTO de protocolo de convergencia de datos de paquetes (PDCP) para impedir que el mismo flujo de clave se use dos veces. Una opción en este caso es que el eNB de suspensión indique su preferencia por derivar una nueva clave de base de AS o siga usando la existente cuando se suspende la conexión de RRC.

Los diagramas de flujo en las figuras 7, 8 y 9 ilustran métodos generales para hacer funcionar un dispositivo 42 terminal, un primer nodo 40 de acceso radioeléctrico y un segundo nodo 40 de acceso radioeléctrico según las técnicas a modo de ejemplo descritas en el presente documento. El primer nodo 40 de acceso radioeléctrico corresponde al eNB 40 de suspensión en la figura 6 y el segundo nodo 40 de acceso radioeléctrico corresponde al eNB de reanudación en la figura 6.

La figura 7 ilustra el funcionamiento de un dispositivo terminal según una realización general. En la etapa 701, el dispositivo 42 terminal está funcionando en un estado conectado con respecto a una red 32 de comunicación. El estado conectado puede ser un estado de RRC conectado.

El dispositivo 42 terminal recibe entonces una primera señal desde un primer nodo 40 de acceso radioeléctrico en la red de comunicación (etapa 703). La primera señal indica que ha de suspenderse el estado conectado, y comprende información para su uso en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo 42 terminal y el primer nodo 40 de acceso radioeléctrico u otro nodo 40 de acceso radioeléctrico en la red 32 de comunicación si se reanuda el estado conectado.

En la realización específica de la figura 6, la primera señal corresponde a la suspensión de conexión de RRC 601.

En algunas realizaciones, tras la recepción de la primera señal, el dispositivo terminal almacena información de contexto relacionada con el estado conectado con la red de comunicación y almacena la información recibida para su uso en la determinación de una primera clave para cifrar datos. La información de contexto y/o la información recibida para su uso en la determinación de la primera clave pueden almacenarse en la unidad 56 de memoria. El dispositivo terminal pasa entonces a un estado inactivo (por ejemplo, RRC inactivo) o suspendido con respecto a la red de comunicación.

En algunas realizaciones la primera señal también puede comprender un identificador para el dispositivo terminal que el dispositivo terminal va a usar cuando se solicite la reanudación del estado conectado. Este identificador es el ID de reanudación en la realización de la figura 6. En algunas realizaciones la primera señal también puede comprender un testigo de autorización para el dispositivo terminal, y/o información que identifica una configuración de algoritmo de seguridad que va a usarse para cifrar datos. El identificador para el dispositivo terminal, el testigo de autorización y/o la información que identifica una configuración de algoritmo de seguridad que va a usarse para cifrar datos también puede almacenarlos el dispositivo terminal.

En algunas realizaciones, por ejemplo, cuando la red de comunicación está funcionando según las especificaciones de LTE, la información para su uso en la determinación de una primera clave para cifrar datos puede comprender un valor de contador de concatenación de siguiente salto, NCC.

Si ha de reanudarse el estado conectado, el dispositivo 42 terminal determina una primera clave para cifrar datos que van a enviarse tras la reanudación del estado conectado. La primera clave se determina usando la información recibida en la primera señal.

En algunas realizaciones, la información en la primera señal puede usarse para determinar si la primera clave ha de determinarse a partir de una segunda clave que usó anteriormente el dispositivo terminal para cifrar datos enviados entre el dispositivo terminal y el primer nodo de acceso radioeléctrico.

En algunas realizaciones, la información en la primera señal comprende un valor de contador (por ejemplo, un valor de NCC), y si el valor de contador concuerda con un valor de contador asociado con la segunda clave, la primera clave se determina a partir de la segunda clave e información relacionada con el nodo de acceso radioeléctrico con el que ha de reanudarse el estado conectado; y de otro modo (es decir, si el valor de contador no concuerda con un valor de contador asociado con la segunda clave) un valor de clave intermedia (por ejemplo, un valor de NH) se calcula a partir del valor de contador recibido en la primera señal y la primera clave se determina a partir del valor de clave intermedia e información relacionada con el nodo de acceso radioeléctrico con el que ha de reanudarse el estado conectado.

En algunas realizaciones, si ha de reanudarse el estado conectado con el primer nodo de acceso radioeléctrico, el dispositivo terminal puede usar una clave que usó anteriormente el dispositivo terminal para cifrar datos enviados entre el dispositivo terminal y el primer nodo de acceso radioeléctrico como la primera clave.

En algunas realizaciones, el dispositivo 42 terminal envía una segunda señal al primer nodo de acceso radioeléctrico u otro nodo de acceso radioeléctrico en la red de comunicación para solicitar la reanudación del estado conectado. La segunda señal corresponde a la solicitud 609 de reanudación de conexión de RRC en la realización específica de

la figura 6. La segunda señal puede enviarse, por ejemplo, cuando llegan nuevos datos a la memoria intermedia de UL del dispositivo 42 terminal.

En algunas realizaciones, la segunda señal también puede comprender un identificador para el dispositivo terminal proporcionado por el primer nodo de acceso radioeléctrico y/o un identificador para el primer nodo de acceso radioeléctrico. El identificador para el dispositivo terminal puede ser el ID de reanudación que se envió al dispositivo terminal en la primera señal. La segunda señal puede comprender también o alternativamente un testigo de autorización para el dispositivo terminal (por ejemplo, que el dispositivo terminal recibió en la primera señal).

En algunas realizaciones, la segunda señal comprende además datos que van a enviarse desde el dispositivo terminal a la red 32 de comunicación. Los datos los habrá cifrado el dispositivo 42 terminal usando la primera clave. En algunas realizaciones, el dispositivo terminal habrá cifrado los datos usando la primera clave según una configuración de algoritmo de seguridad indicada en la primera señal. En realizaciones alternativas, el dispositivo terminal habrá cifrado los datos usando la primera clave según una configuración de algoritmo de seguridad usada anteriormente con el primer nodo de acceso radioeléctrico (independientemente de si el dispositivo terminal está intentando reanudar el estado conectado con el primer nodo 40 de acceso radioeléctrico u otro nodo 40 de acceso radioeléctrico).

En algunas realizaciones, después de enviar la segunda señal a un nodo de acceso radioeléctrico, el dispositivo terminal puede recibir una tercera señal desde ese nodo de acceso radioeléctrico que indica que se ha reanudado el estado conectado o que se produjo un error al reanudarse el estado conectado. La tercera señal corresponde a la reanudación de conexión de RRC completada 621 (o la señal 621 de error equivalente) en la realización de la figura 6.

En algunos casos, por ejemplo, si el nodo de acceso radioeléctrico no puede descifrar los datos cifrados, la tercera señal puede indicar que se produjo un error al reanudarse el estado conectado e indicar además una configuración de algoritmo de seguridad que va a usar el dispositivo terminal para cifrar datos.

La figura 8 ilustra el funcionamiento de un primer nodo 40 de acceso radioeléctrico según una realización general. El nodo 40 de acceso radioeléctrico está funcionando en una red 32 de comunicación y hay un dispositivo 42 terminal que está en un estado conectado con respecto a la red 32 de comunicación. El primer nodo 40 de acceso radioeléctrico corresponde al primer nodo 40 de acceso radioeléctrico descrito anteriormente con respecto al método en la figura 7. En una primera etapa, el primer nodo 40 de acceso radioeléctrico envía una primera señal al dispositivo terminal (etapa 801). La primera señal (que en la realización específica de la figura 6 corresponde al mensaje 601 de suspensión de conexión de RRC) indica que ha de suspenderse el estado conectado, y comprende información para su uso por parte del dispositivo terminal en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal y el primer nodo de acceso radioeléctrico u otro nodo de acceso radioeléctrico en la red de comunicación si se reanuda el estado conectado.

En algunas realizaciones la primera señal comprende además un identificador para el dispositivo terminal que el dispositivo terminal va a usar cuando se solicite la reanudación del estado conectado. Este identificador corresponde al ID de reanudación en la realización específica de la figura 6.

En algunas realizaciones, la primera señal comprende además un testigo de autorización para el dispositivo terminal, y/o información que identifica una configuración de algoritmo de seguridad que va a usarse para cifrar datos.

En algunas realizaciones, la información para su uso en la determinación de la primera clave para cifrar datos comprende un valor de NCC.

En algunas realizaciones, después de enviar la primera señal en la etapa 801, el primer nodo de acceso radioeléctrico almacena información de contexto relacionada con el estado conectado del dispositivo terminal, por ejemplo, en la unidad 66 de memoria.

En algunas realizaciones, el primer nodo 40 de acceso radioeléctrico recibe una segunda señal desde el dispositivo terminal para solicitar la reanudación del estado conectado. La segunda señal corresponde a la solicitud 609 de reanudación de conexión de RRC en la realización específica de la figura 6.

En algunas realizaciones, la segunda señal comprende además datos cifrados, y, por tanto, en algunas realizaciones, el primer nodo de acceso radioeléctrico intenta descifrar los datos cifrados usando la primera clave.

En algunas realizaciones, la segunda señal comprende un identificador para el dispositivo terminal que se envió al dispositivo terminal en la primera señal (por ejemplo, el ID de reanudación), y el primer nodo de acceso radioeléctrico usa el identificador recibido para recuperar información de contexto relacionada con el estado conectado del dispositivo terminal (por ejemplo, desde la unidad 66 de memoria).

En algunas realizaciones, el primer nodo de acceso radioeléctrico envía una tercera señal al dispositivo terminal que indica que se ha reanudado el estado conectado o que se produjo un error al reanudarse el estado conectado. La tercera señal corresponde al mensaje 621 de reanudación de conexión de RRC completada en la realización específica de la figura 6.

En algunas realizaciones, si se produjo un error al reanudarse el estado conectado, la tercera señal puede indicar que se produjo un error e indicar una configuración de algoritmo de seguridad que va a usar el dispositivo terminal para cifrar datos.

En algunas realizaciones, el primer nodo de acceso radioeléctrico puede determinar una primera clave para cifrar datos tras la reanudación del estado conectado con el dispositivo terminal.

En algunas realizaciones, el primer nodo de acceso radioeléctrico puede determinar si la primera clave ha de determinarse a partir de una segunda clave que se usó anteriormente para cifrar datos enviados entre el primer nodo de acceso radioeléctrico y el dispositivo terminal. En algunas realizaciones, el primer nodo de acceso radioeléctrico mantiene un valor de contador (por ejemplo, un valor de NCC), y el primer nodo de acceso radioeléctrico puede determinar si la primera clave ha de determinarse a partir de la segunda clave basándose en el valor de contador. En particular, si el valor de contador concuerda con un valor de contador asociado con la segunda clave, el primer nodo de acceso radioeléctrico determina la primera clave a partir de la segunda clave e información relacionada con el primer nodo de acceso radioeléctrico, y si el valor de contador no concuerda con un valor de contador asociado con la segunda clave, la primera clave se determina a partir de un valor de clave intermedia (por ejemplo, un valor de NH) e información relacionada con el primer nodo de acceso radioeléctrico.

En algunas realizaciones, la primera clave es una clave que se usó anteriormente para cifrar datos enviados entre el dispositivo terminal y el primer nodo de acceso radioeléctrico.

En realizaciones en las que el dispositivo 42 terminal intenta reanudar el estado conectado con otro nodo de acceso radioeléctrico (por ejemplo, un segundo nodo 40 de acceso radioeléctrico), el primer nodo 40 de acceso radioeléctrico puede recibir una solicitud, desde el segundo nodo de acceso radioeléctrico, de información de contexto relacionada con el estado conectado del dispositivo terminal con la red de comunicación. Esta solicitud corresponde al mensaje 611 de solicitud de contexto de UE en la realización de la figura 6. En respuesta a la recepción de la solicitud, el primer nodo de acceso radioeléctrico recupera información de contexto relacionada con el estado conectado del dispositivo terminal desde una memoria, y envía la información de contexto recuperada al segundo nodo de acceso radioeléctrico. El primer nodo de acceso radioeléctrico también puede enviar la primera clave, un testigo de autorización para el dispositivo terminal, una configuración de algoritmo de seguridad que va a usar el dispositivo terminal para cifrar datos, y/o la información para su uso por parte del dispositivo terminal en la determinación de la primera clave al segundo nodo 40 de acceso radioeléctrico.

La figura 9 ilustra el funcionamiento de un segundo nodo 40 de acceso radioeléctrico según una realización general. El nodo 40 de acceso radioeléctrico está funcionando en una red 32 de comunicación y hay un dispositivo 42 terminal cuyo estado conectado con respecto a la red 32 de comunicación se ha suspendido. El segundo nodo 40 de acceso radioeléctrico corresponde al segundo nodo 40 de acceso radioeléctrico descrito anteriormente con respecto al método en la figura 7.

En una primera etapa, la etapa 901, el segundo nodo 40 de acceso radioeléctrico recibe una primera señal desde el dispositivo terminal para solicitar la reanudación del estado conectado. Esta primera señal corresponde a la solicitud 609 de reanudación de conexión de RRC en la realización específica de la figura 6.

El segundo nodo de acceso radioeléctrico envía entonces una segunda señal a un primer nodo de acceso radioeléctrico para solicitar información de contexto relacionada con el estado conectado del dispositivo terminal con la red de comunicación (etapa 903). La segunda señal corresponde al mensaje 611 de solicitud de contexto de UE en la realización específica de la figura 6.

Después de enviar la segunda señal, el segundo nodo de acceso radioeléctrico recibe una tercera señal desde el primer nodo de acceso radioeléctrico, comprendiendo la tercera señal la información de contexto y una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal y el segundo nodo de acceso radioeléctrico tras la reanudación del estado conectado (etapa 905). La tercera señal corresponde al mensaje 613 de respuesta de contexto de UE en la realización específica de la figura 6.

En algunas realizaciones, la primera señal comprende además un identificador para el dispositivo terminal (por ejemplo, el ID de reanudación) y/o un identificador para el primer nodo de acceso radioeléctrico. En realizaciones en las que sólo se incluye en la primera señal el identificador para el dispositivo terminal, el segundo nodo 40 de acceso radioeléctrico puede usar el identificador para que el dispositivo terminal identifique el nodo de acceso radioeléctrico al que ha de enviarse la solicitud de información de contexto.

En algunas realizaciones, la primera señal comprende además un testigo de autorización para el dispositivo

terminal. En realizaciones adicionales o alternativas, la primera señal también comprende una configuración de algoritmo de seguridad que va a usar el dispositivo terminal para cifrar datos.

En algunas realizaciones, la primera señal comprende además datos cifrados desde el dispositivo terminal. En algunas realizaciones, el segundo nodo de acceso radioeléctrico puede intentar descifrar los datos cifrados usando la primera clave. En algunas realizaciones, si los datos cifrados pueden descifrarse, el segundo nodo de acceso radioeléctrico envía una cuarta señal al dispositivo terminal que indica que se ha reanudado el estado conectado. La cuarta señal corresponde al mensaje 621 de reanudación de conexión de RRC completada en la realización específica de la figura 6. Alternativamente, si los datos cifrados no pueden descifrarse, el segundo nodo de acceso radioeléctrico puede enviar una cuarta señal al dispositivo terminal que indica que se produjo un error al reanudarse el estado conectado. En algunas realizaciones, cuando la cuarta señal indica que se produjo un error, la cuarta señal puede comprender además una indicación de una configuración de algoritmo de seguridad que va a usar el dispositivo terminal para cifrar datos.

En algunas realizaciones, después de recibirse la tercera señal, el segundo nodo de acceso radioeléctrico puede verificar la identidad del dispositivo terminal. En algunas realizaciones, verificar la identidad del dispositivo terminal puede comprender verificar un testigo de autorización para el dispositivo terminal y/o verificar una protección de integridad de la primera señal. En algunas realizaciones, una cuarta señal que indica que se produjo un error al reanudarse el estado conectado puede enviarse al dispositivo terminal si no puede verificarse la identidad del dispositivo terminal. En algunas realizaciones, puede enviarse al dispositivo terminal una cuarta señal que indica que se produjo un error al reanudarse el estado conectado si la tercera señal procedente del primer nodo de acceso radioeléctrico no se recibe o si la tercera señal recibida no comprende información de contexto y/o una primera clave.

Por tanto, según las técnicas a modo de ejemplo descritas en el presente documento, se permite que un UE transmita rápidamente datos de plano de usuario cuando se reanuda una conexión de RRC. Esto es útil, por ejemplo, en casos de uso en los que millones de sensores envían pequeñas cantidades de datos de manera relativamente poco frecuente, pero también en teléfonos inteligentes habituales.

Se observa que el 3GPP está estudiando la gestión de UE para IdC (internet de las cosas) celular, que hace uso de un estado que es similar al estado de RRC suspendido, es decir, un estado en el que la información de AS se almacena en caché en el UE y en la red para una posterior transición sin problemas a un estado en el que pueden intercambiarse datos entre el UE y la red, y este estado también se beneficiará de esta nueva funcionalidad en el contexto de los aspectos de seguridad. Una gestión de UE similar también se considera una opción viable para la próxima evolución de la norma de 3GPP, que en ocasiones se denomina 5G.

La figura 10 es un diagrama de bloques de un dispositivo 42 terminal según otra realización. El dispositivo 42 terminal comprende un procesador 1010 y una memoria 1020. La memoria 1020 contiene instrucciones ejecutables por el procesador 1010 mediante las cuales el dispositivo 42 terminal está operativo para funcionar en un estado conectado con respecto a la red 32 de comunicación, y recibir una primera señal desde un primer nodo 40 de acceso radioeléctrico en la red 32 de comunicación que indica que ha de suspenderse el estado conectado. La primera señal comprende información para su uso en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo 42 terminal y el primer nodo 40 de acceso radioeléctrico u otro nodo 40 de acceso radioeléctrico en la red 32 de comunicación si se reanuda el estado conectado.

La figura 11 es un diagrama de bloques de un primer nodo 40 de acceso radioeléctrico según otra realización. El primer nodo 40 de acceso radioeléctrico está destinado para su uso en una red 32 de comunicación, y el primer nodo de acceso radioeléctrico comprende un procesador 1110 y una memoria 1120, y la memoria 1120 contiene instrucciones ejecutables por el procesador 1110 mediante las cuales el primer nodo 40 de acceso radioeléctrico está operativo para enviar una primera señal a un dispositivo 42 terminal que está en un estado conectado con respecto a la red 32 de comunicación. La primera señal indica que ha de suspenderse el estado conectado, y la primera señal comprende información para su uso por parte del dispositivo 42 terminal en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal 32 y el primer nodo 40 de acceso radioeléctrico u otro nodo 40 de acceso radioeléctrico en la red 32 de comunicación si se reanuda el estado conectado.

La figura 12 es un diagrama de bloques de un segundo nodo 40 de acceso radioeléctrico según otra realización. El segundo nodo 40 de acceso radioeléctrico está destinado para su uso en una red 32 de comunicación, y el segundo nodo 40 de acceso radioeléctrico comprende un procesador 1210 y una memoria 1220. La memoria 1220 contiene instrucciones ejecutables por el procesador 1210 mediante las cuales el segundo nodo 40 de acceso radioeléctrico está operativo para recibir una primera señal desde un dispositivo 42 terminal cuyo estado conectado con respecto a la red 32 de comunicación se ha suspendido, solicitando la primera señal la reanudación del estado conectado; enviar una segunda señal a un primer nodo 40 de acceso radioeléctrico para solicitar información de contexto relacionada con el estado conectado del dispositivo 42 terminal con la red 32 de comunicación; y recibir una tercera señal desde el primer nodo 40 de acceso radioeléctrico, comprendiendo la tercera señal la información de contexto y una primera clave para cifrar datos que van a enviarse entre el dispositivo 42 terminal y el segundo nodo 40 de

acceso radioeléctrico tras la reanudación del estado conectado.

La figura 13 es un diagrama de bloques de un dispositivo 42 terminal según aún otra realización. El dispositivo 42 terminal comprende un primer módulo 1310 configurado para hacer funcionar el dispositivo 42 terminal en un estado conectado con respecto a la red de comunicación; y un segundo módulo 1320 configurado para recibir una primera señal desde un primer nodo 40 de acceso radioeléctrico en la red 32 de comunicación que indica que ha de suspenderse el estado conectado. La primera señal comprende información para su uso en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo 42 terminal y el primer nodo 40 de acceso radioeléctrico u otro nodo 40 de acceso radioeléctrico en la red 32 de comunicación si se reanuda el estado conectado.

La figura 14 es un diagrama de bloques de un primer nodo 40 de acceso radioeléctrico según aún otra realización. El primer nodo 40 de acceso radioeléctrico está destinado para su uso en una red 32 de comunicación, y comprende un primer módulo 1410 configurado para enviar una primera señal a un dispositivo 42 terminal que está en un estado conectado con respecto a la red 32 de comunicación. La primera señal indica que ha de suspenderse el estado conectado, y la primera señal comprende información para su uso por parte del dispositivo 42 terminal en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo 42 terminal y el primer nodo 40 de acceso radioeléctrico u otro nodo 40 de acceso radioeléctrico en la red 32 de comunicación si se reanuda el estado conectado.

La figura 15 es un diagrama de bloques de un segundo nodo 40 de acceso radioeléctrico según aún otra realización. El segundo nodo 40 de acceso radioeléctrico está destinado para su uso en una red 32 de comunicación, y comprende un primer módulo 1510 para recibir una primera señal desde un dispositivo 42 terminal cuyo estado conectado con respecto a la red 32 de comunicación se ha suspendido, solicitando la primera señal la reanudación del estado conectado; un segundo módulo 1520 para enviar una segunda señal a un primer nodo 40 de acceso radioeléctrico para solicitar información de contexto relacionada con el estado conectado del dispositivo 42 terminal con la red 32 de comunicación; y un tercer módulo 1530 para recibir una tercera señal desde el primer nodo 40 de acceso radioeléctrico, comprendiendo la tercera señal la información de contexto y una primera clave para cifrar datos que van a enviarse entre el dispositivo 42 terminal y el segundo nodo 40 de acceso radioeléctrico tras la reanudación del estado conectado.

Los módulos ilustrados en las figuras 13-15 y comentados anteriormente pueden implementarse en algunas realizaciones como programas informáticos/instrucciones para su ejecución mediante uno o más procesadores (por ejemplo, el procesador 1010 en un dispositivo terminal, el procesador 1110 en un primer nodo de acceso radioeléctrico o el procesador 1210 en un segundo nodo de acceso radioeléctrico tal como se ilustra en las figuras 10-12).

A un experto en la técnica se le ocurrirán modificaciones y otras variantes de la(s) realización/realizaciones descrita(s) que tienen el beneficio de las enseñanzas presentadas en las descripciones anteriores y los dibujos asociados. Por tanto, ha de entenderse que la(s) realización/realizaciones no ha(n) de limitarse a los ejemplos específicos divulgados y que se pretende incluir modificaciones y otras variantes dentro del alcance de esta divulgación. Aunque pueden emplearse términos específicos en el presente documento, se usan sólo en sentido genérico y descriptivo y no con propósitos de limitación.

REIVINDICACIONES

1. Método para hacer funcionar un dispositivo terminal, comprendiendo el método:

hacer funcionar (701) el dispositivo terminal en un estado conectado con respecto a la red de comunicación; y

recibir (703) una primera señal desde un primer nodo de acceso radioeléctrico en la red de comunicación que indica que ha de suspenderse el estado conectado, comprendiendo la primera señal información para su uso en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal y el primer nodo de acceso radioeléctrico u otro nodo de acceso radioeléctrico en la red de comunicación si se reanuda el estado conectado, comprendiendo además la primera señal un identificador para el dispositivo terminal que el dispositivo terminal va a usar cuando se solicite la reanudación del estado conectado.

2. Método según la reivindicación 1, en el que, tras la recepción de la primera señal, el método comprende además las etapas de:

almacenar información de contexto relacionada con el estado conectado con la red de comunicación;

almacenar la información recibida para su uso en la determinación de una primera clave para cifrar datos; y

hacer que el dispositivo terminal pase a un estado inactivo o suspendido con respecto a la red de comunicación.

3. Método según la reivindicación 1 ó 2, en el que la información para su uso en la determinación de una primera clave para cifrar datos comprende un valor de contador de concatenación de siguiente salto, NCC.

4. Método según cualquiera de las reivindicaciones 1-3, en el que el método comprende además la etapa de:

determinar una primera clave para cifrar datos que van a enviarse tras la reanudación del estado conectado usando la información en la primera señal.

5. Método según la reivindicación 4, en el que la etapa de determinar (703) una primera clave para cifrar datos comprende:

usar la información en la primera señal para determinar si la primera clave ha de determinarse a partir de una segunda clave que usó anteriormente el dispositivo terminal para cifrar datos enviados entre el dispositivo terminal y el primer nodo de acceso radioeléctrico.

6. Método según la reivindicación 5, en el que la información en la primera señal comprende un valor de contador, y en el que la etapa de usar la información en la primera señal para determinar si la primera clave ha de determinarse a partir de una segunda clave que usó anteriormente el dispositivo terminal comprende:

determinar la primera clave a partir de la segunda clave e información relacionada con el nodo de acceso radioeléctrico con el que ha de reanudarse el estado conectado en el caso de que el valor de contador concuerde con un valor de contador asociado con la segunda clave; y

en el caso de que el valor de contador no concuerde con un valor de contador asociado con la segunda clave, calcular un valor de clave intermedia a partir del valor de contador recibido en la primera señal, y determinar la primera clave a partir del valor de clave intermedia e información relacionada con el nodo de acceso radioeléctrico con el que ha de reanudarse el estado conectado.

7. Método según la reivindicación 6, en el que el valor de contador es un valor de contador de concatenación de siguiente salto, NCC, y/o el valor de clave intermedia es un valor de siguiente salto, NH.

8. Método según cualquiera de las reivindicaciones 1-3, en el que en el caso de que el estado conectado haya de reanudarse con el primer nodo de acceso radioeléctrico, la primera clave comprende una clave que usó anteriormente el dispositivo terminal para cifrar datos enviados entre el dispositivo terminal y el primer nodo de acceso radioeléctrico.

9. Método según cualquiera de las reivindicaciones 1-8, en el que el método comprende además la etapa de:

enviar una segunda señal al primer nodo de acceso radioeléctrico u otro nodo de acceso radioeléctrico en la red de comunicación para solicitar la reanudación del estado conectado.

10. Método según la reivindicación 9, en el que la segunda señal comprende además datos que van a enviarse desde el dispositivo terminal a la red de comunicación, en el que los datos se cifran usando la primera clave.

11. Método según cualquiera de las reivindicaciones 1-10, en el que el estado conectado es un estado conectado de control de recursos radioeléctricos, RRC.

12. Método para hacer funcionar un primer nodo de acceso radioeléctrico en una red de comunicación, comprendiendo el método:

enviar (801) una primera señal a un dispositivo terminal que está en un estado conectado con respecto a la red de comunicación, indicando la primera señal que ha de suspenderse el estado conectado, comprendiendo la primera señal información para su uso por parte del dispositivo terminal en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo terminal y el primer nodo de acceso radioeléctrico u otro nodo de acceso radioeléctrico en la red de comunicación si se reanuda el estado conectado, comprendiendo además la primera señal un identificador para el dispositivo terminal que el dispositivo terminal va a usar cuando se solicite la reanudación del estado conectado.

13. Método según la reivindicación 12, en el que la información para su uso en la determinación de la primera clave para cifrar datos comprende un valor de contador de concatenación de siguiente salto, NCC.

14. Método según las reivindicaciones 12 ó 13, en el que el método comprende además la etapa de:

recibir una segunda señal desde el dispositivo terminal para solicitar la reanudación del estado conectado.

15. Método según la reivindicación 14, en el que la segunda señal comprende además datos cifrados.

16. Método según la reivindicación 15, en el que el método comprende además la etapa de:

intentar descifrar los datos cifrados usando la primera clave.

17. Método según cualquiera de las reivindicaciones 12-16, en el que el estado conectado es un estado conectado de control de recursos radioeléctricos, RRC.

18. Dispositivo (42) terminal, estando el dispositivo (42) terminal adaptado para:

funcionar en un estado conectado con respecto a la red (32) de comunicación; y

recibir una primera señal desde un primer nodo (40) de acceso radioeléctrico en la red (32) de comunicación que indica que ha de suspenderse el estado conectado, comprendiendo la primera señal información para su uso en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo (42) terminal y el primer nodo (40) de acceso radioeléctrico u otro nodo (40) de acceso radioeléctrico en la red (32) de comunicación si se reanuda el estado conectado, comprendiendo además la primera señal un identificador para el dispositivo terminal que el dispositivo terminal va a usar cuando se solicite la reanudación del estado conectado.

19. Dispositivo (42) terminal según la reivindicación 18, en el que el dispositivo (42) terminal está adaptado además para, tras la recepción de la primera señal:

almacenar información de contexto relacionada con el estado conectado con la red (32) de comunicación;

almacenar la información recibida para su uso en la determinación de una primera clave para cifrar datos; y

hacer que el dispositivo (42) terminal pase a un estado inactivo o suspendido con respecto a la red (32) de comunicación.

20. Dispositivo (42) terminal según la reivindicación 18 ó 19, en el que la información para su uso en la determinación de una primera clave para cifrar datos comprende un valor de contador de concatenación de siguiente salto, NCC.

21. Dispositivo (42) terminal según cualquiera de las reivindicaciones 18-20, en el que el dispositivo (42) terminal está adaptado además para:

determinar una primera clave para cifrar datos que van a enviarse tras la reanudación del estado conectado usando la información en la primera señal.

22. Dispositivo terminal según la reivindicación 21, en el que el dispositivo (42) terminal está adaptado para determinar una primera clave para cifrar datos mediante lo siguiente:

usar la información en la primera señal para determinar si la primera clave ha de determinarse a partir de una segunda clave que usó anteriormente el dispositivo (42) terminal para cifrar datos enviados entre el dispositivo (42) terminal y el primer nodo (40) de acceso radioeléctrico.

23. Dispositivo (42) terminal según la reivindicación 22, en el que la información en la primera señal comprende un valor de contador, y en el que el dispositivo (42) terminal está adaptado para usar la información en la primera señal para determinar si la primera clave ha de determinarse a partir de una segunda clave que usó anteriormente el dispositivo (42) terminal mediante lo siguiente:

determinar la primera clave a partir de la segunda clave e información relacionada con el nodo (40) de acceso radioeléctrico con el que ha de reanudarse el estado conectado en el caso de que el valor de contador concuerde con un valor de contador asociado con la segunda clave; y

en el caso de que el valor de contador no concuerde con un valor de contador asociado con la segunda clave, calcular un valor de clave intermedia a partir del valor de contador recibido en la primera señal, y determinar la primera clave a partir del valor de clave intermedia e información relacionada con el nodo (40) de acceso radioeléctrico con el que ha de reanudarse el estado conectado.

24. Dispositivo (42) terminal según la reivindicación 23, en el que el valor de contador es un valor de contador de concatenación de siguiente salto, NCC, y/o el valor de clave intermedia es un valor de siguiente salto, NH.

25. Dispositivo (42) terminal según cualquiera de las reivindicaciones 18-20, en el que en el caso de que el estado conectado haya de reanudarse con el primer nodo (40) de acceso radioeléctrico, la primera clave comprende una clave que usó anteriormente el dispositivo (42) terminal para cifrar datos enviados entre el dispositivo (42) terminal y el primer nodo (40) de acceso radioeléctrico.

26. Dispositivo (42) terminal según cualquiera de las reivindicaciones 18-25, en el que el dispositivo (42) terminal está adaptado además para:

enviar una segunda señal al primer nodo (40) de acceso radioeléctrico u otro nodo (40) de acceso radioeléctrico en la red (32) de comunicación para solicitar la reanudación del estado conectado.

27. Dispositivo (42) terminal según la reivindicación 26, en el que la segunda señal comprende además datos que van a enviarse desde el dispositivo (42) terminal a la red (32) de comunicación, en el que los datos se cifran usando la primera clave.

28. Dispositivo terminal según cualquiera de las reivindicaciones 18-27, en el que el estado conectado es un estado conectado de control de recursos radioeléctricos, RRC.

29. Primer nodo (40) de acceso radioeléctrico para su uso en una red (32) de comunicación, en el que el primer nodo (40) de acceso radioeléctrico está adaptado para:

enviar una primera señal a un dispositivo (42) terminal que está en un estado conectado con respecto a la red de comunicación, indicando la primera señal que ha de suspenderse el estado conectado, comprendiendo la primera señal información para su uso por parte del dispositivo (42) terminal en la determinación de una primera clave para cifrar datos que van a enviarse entre el dispositivo (42) terminal y el primer nodo (40) de acceso radioeléctrico u otro nodo (40) de acceso radioeléctrico en la red (32) de comunicación si se reanuda el estado conectado, comprendiendo además la primera señal un identificador para el dispositivo terminal que el dispositivo terminal va a usar cuando se solicite la reanudación del estado conectado.

30. Primer nodo (40) de acceso radioeléctrico según la reivindicación 29, en el que la información para su uso en la determinación de la primera clave para cifrar datos comprende un valor de contador de concatenación de siguiente salto, NCC.

31. Primer nodo (40) de acceso radioeléctrico según las reivindicaciones 29 ó 30, en el que el primer nodo (40) de acceso radioeléctrico está adaptado además para:

recibir una segunda señal desde el dispositivo (42) terminal para solicitar la reanudación del estado conectado.

32. Primer nodo (40) de acceso radioeléctrico según la reivindicación 31, en el que la segunda señal

comprende además datos cifrados.

33. Primer nodo (40) de acceso radioeléctrico según la reivindicación 32, en el que el primer nodo (40) de acceso radioeléctrico está adaptado además para:

intentar descifrar los datos cifrados usando la primera clave.

34. Primer nodo de acceso radioeléctrico según cualquiera de las reivindicaciones 29-33, en el que el estado conectado es un estado conectado de control de recursos radioeléctricos, RRC.

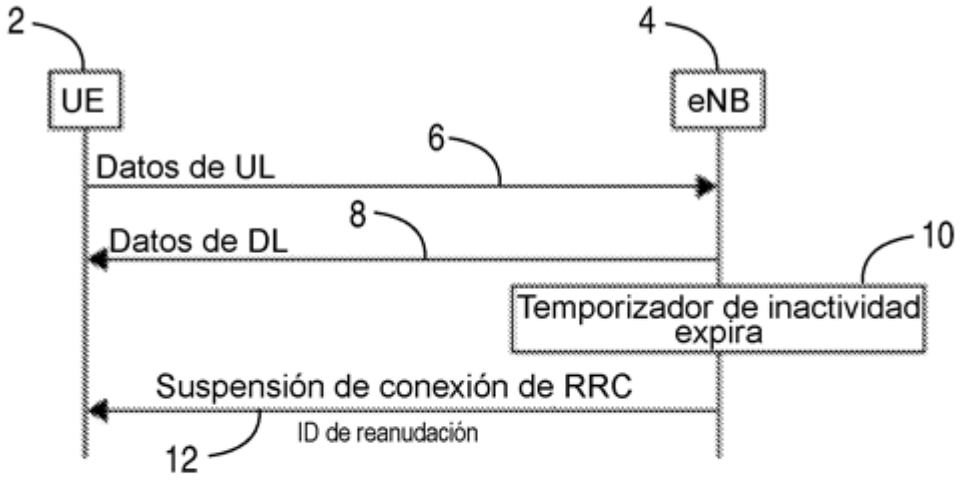

Figura 1

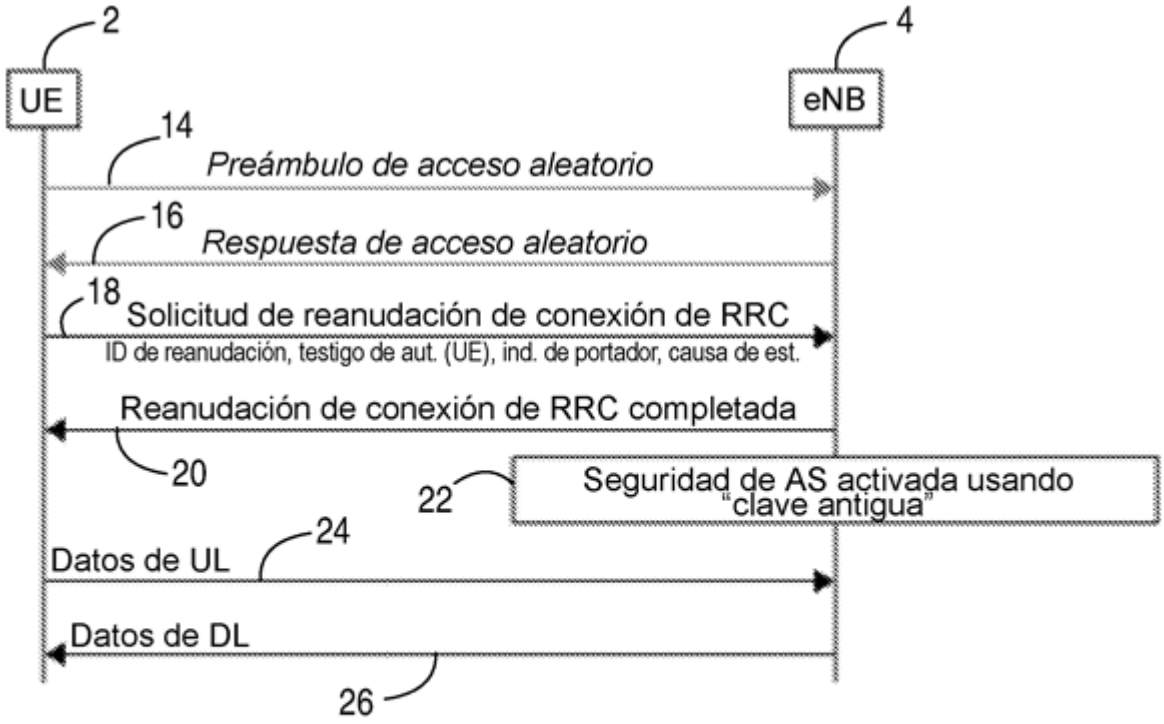

Figura 2

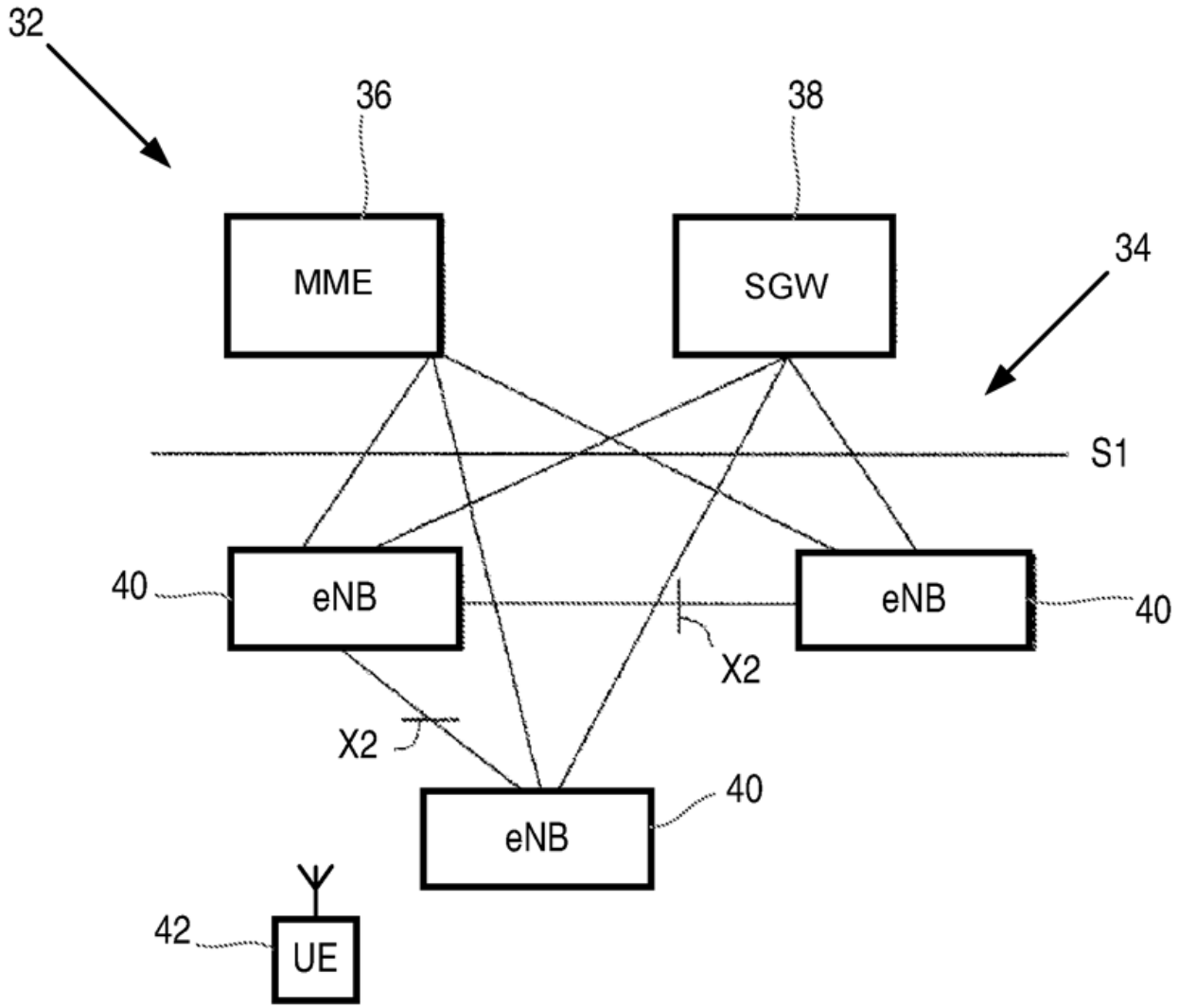

Figura 3

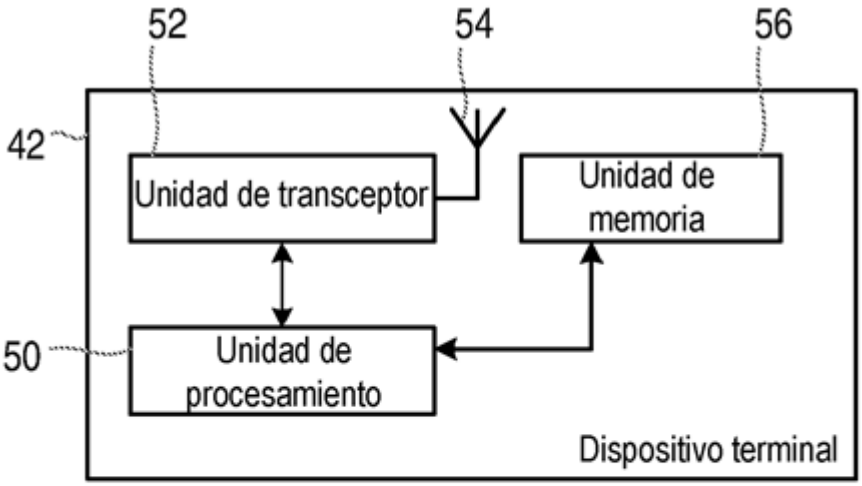

Figura 4

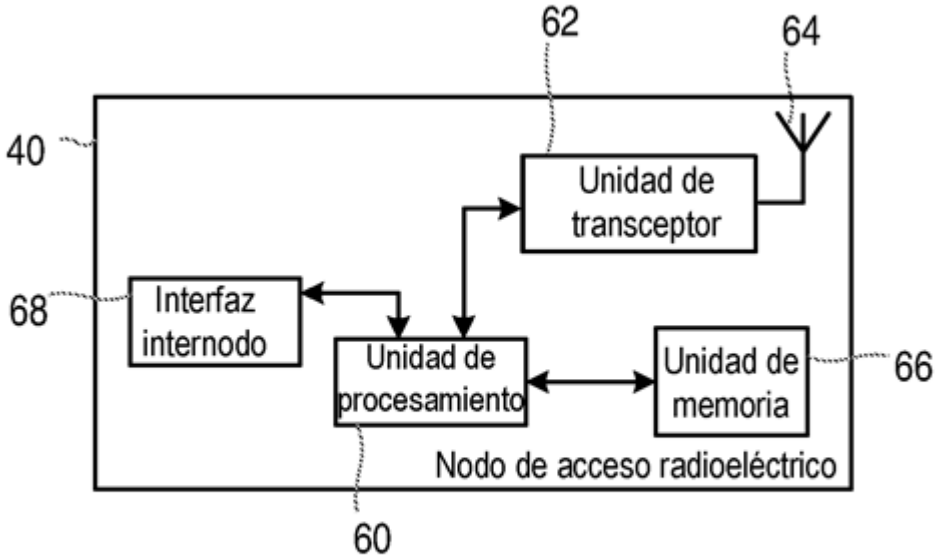

Figura 5

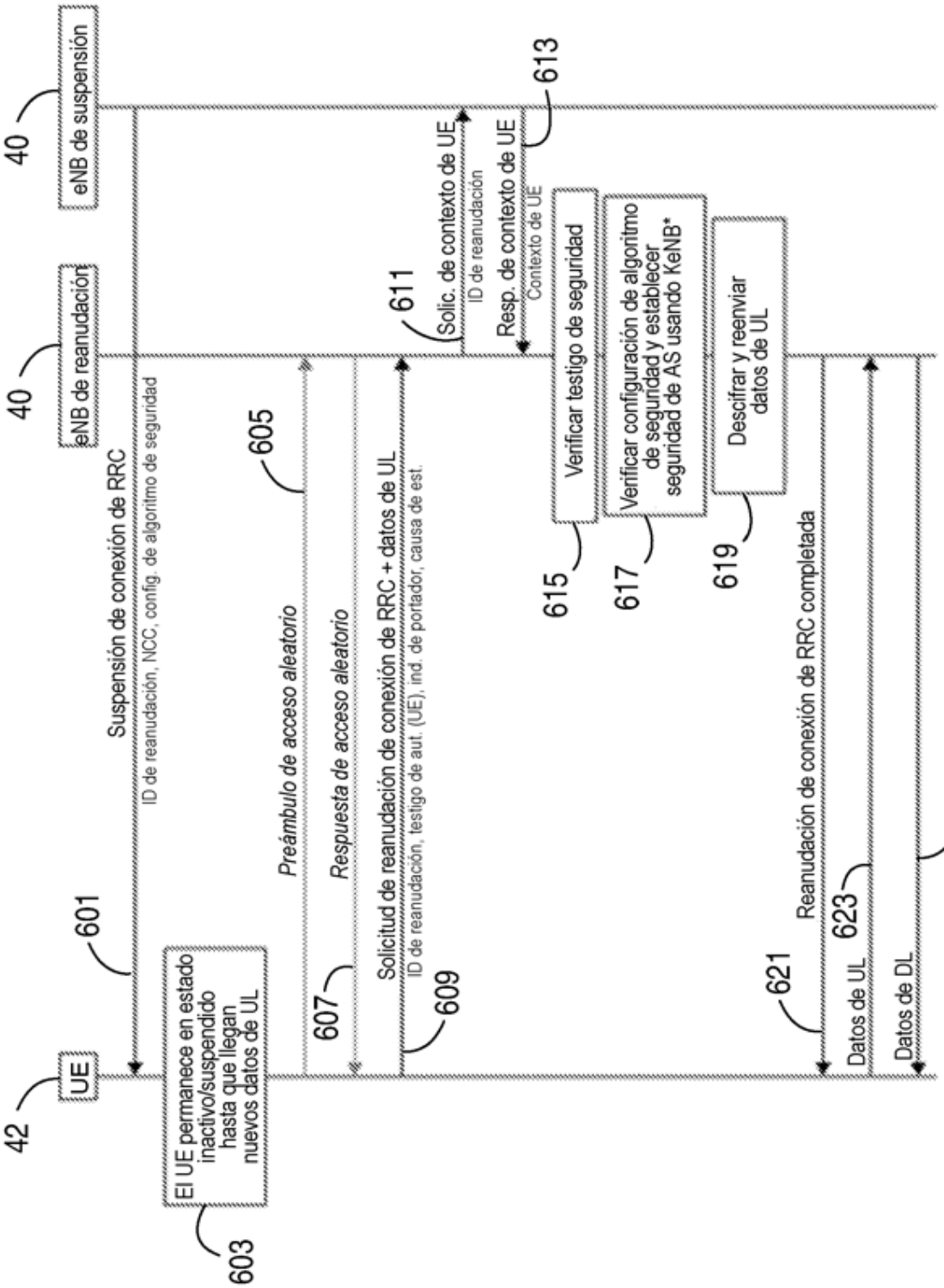
42
UE
40
eNB de reanudación
40
eNB de suspensión
El UE permanece en estado inactivo/suspendido hasta que llegan nuevos datos de UL
603
601
Suspensión de conexión de RRC
ID de reanudación, NCC, config. de algoritmo de seguridad
605
Preámbulo de acceso aleatorio
607
Respuesta de acceso aleatorio
609
Solicitud de reanudación de conexión de RRC + datos de UL
ID de reanudación, testigo de aut. (UE), ind. de portador, causa de est.
611
Solic. de contexto de UE
ID de reanudación
613
Resp. de contexto de UE
Contexto de UE
615
Verificar testigo de seguridad
617
Verificar configuración de algoritmo de seguridad y establecer seguridad de AS usando KeNB*
619
Descifrar y reenviar datos de UL
621
Reanudación de conexión de RRC completada
623
Datos de UL
625
Datos de DL

Figura 6

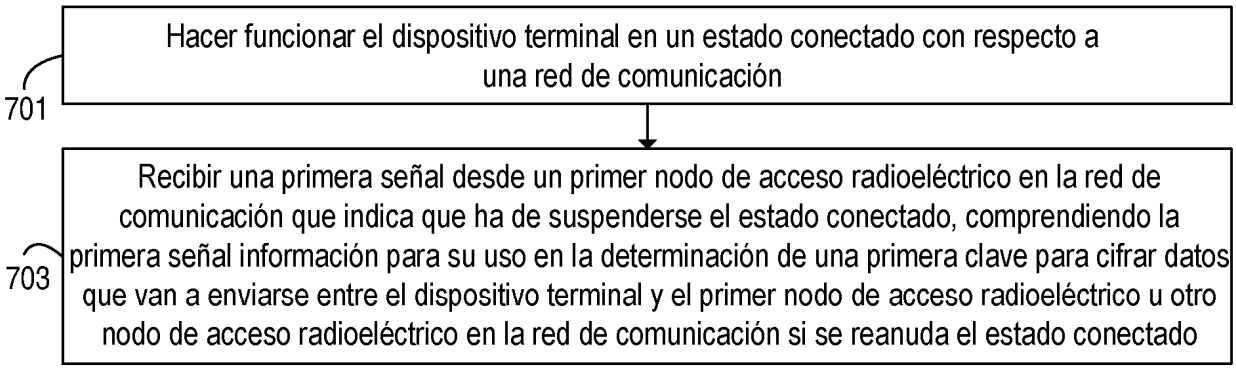

Figura 7

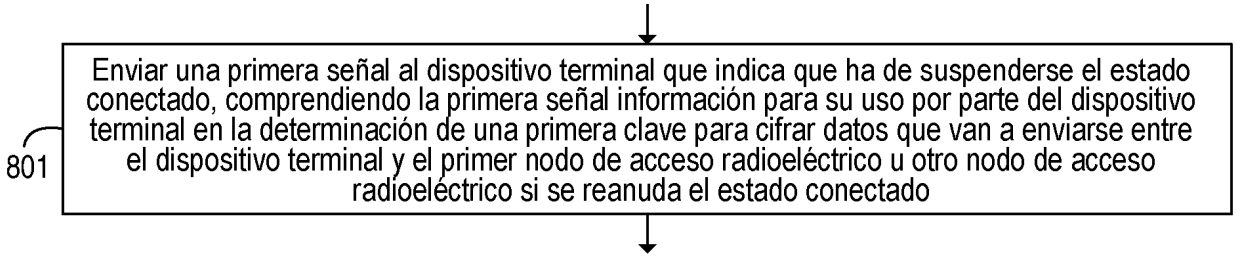

Figura 8

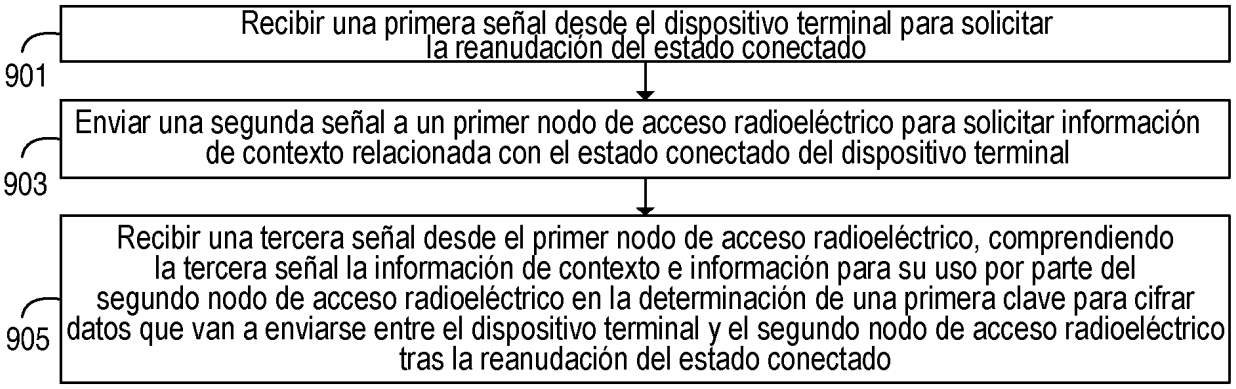

Figura 9

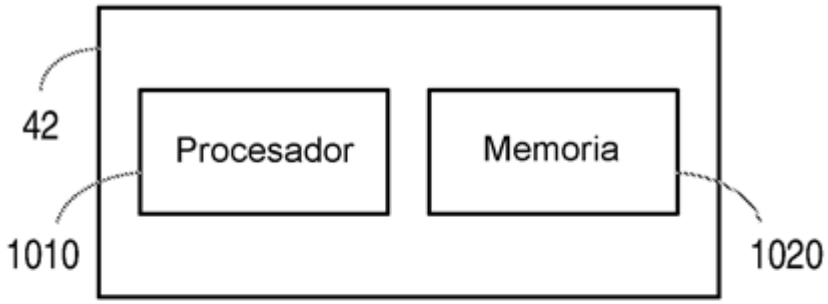

Figura 10

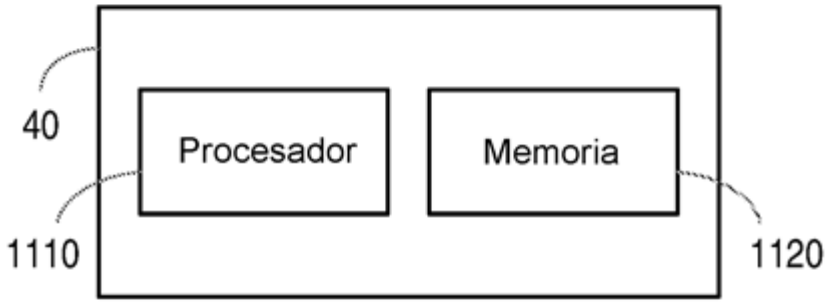

Figura 11

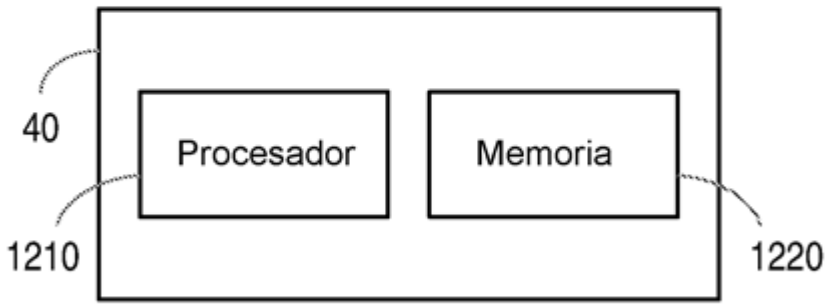

Figura 12

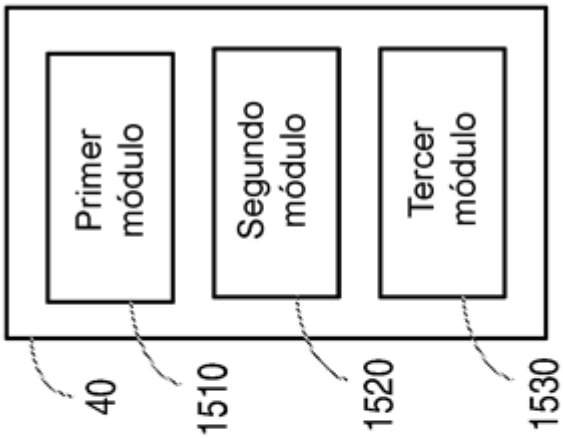

Figura 15

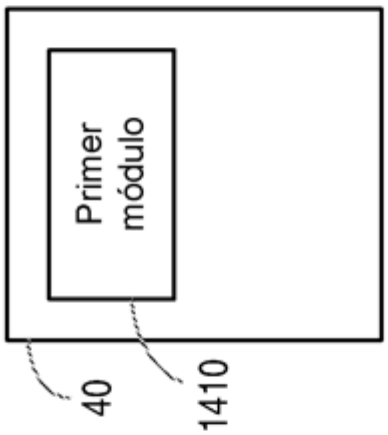

Figura 14

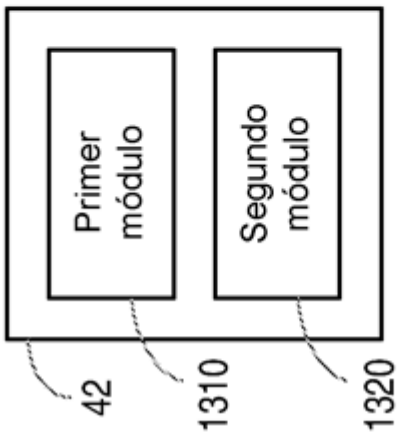

Figura 13