(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 761 890**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/02 (2009.01)
H04W 84/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.04.2007 PCT/US2007/067722**

(87) Fecha y número de publicación internacional: **08.11.2007 WO07127972**

(96) Fecha de presentación y número de la solicitud europea: **29.04.2007 E 07761538 (3)**

(97) Fecha y número de publicación de la concesión europea: **16.10.2019 EP 2014055**

(54) Título: **Transmisión ininterrumpida durante un cambio en la configuración de cifrado**

(30) Prioridad:

28.04.2006 US 795775 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.05.2020

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 Morehouse Drive
San Diego, CA 92121-1714, US

(72) Inventor/es:

MAHESHWARI, SHAILESH;
CHIKKAPPA, KIRAN y
RAMACHANDRAN, VIVEKC/O QUALCOMM INC.

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Transmisión ininterrumpida durante un cambio en la configuración de cifrado

[0001] La presente solicitud reivindica prioridad a la solicitud provisional de los Estados Unidos con n.º de serie 60/795.775, titulada "Performance Improvement to reduce call drops in bad radio conditions during security reconfiguration [Mejora del rendimiento para reducir las caídas de llamada en malas condiciones de radio durante la reconfiguración de seguridad]", presentada el 28 de abril de 2006, asignada al cesionario de la misma.

ANTECEDENTES

I. Campo

[0002] La presente divulgación se refiere en general a la comunicación y, más concretamente, a técnicas para enviar información durante un cambio en la configuración de cifrado.

II. Antecedentes

[0003] Las redes de comunicación inalámbrica están ampliamente implantadas para proporcionar diversos servicios de comunicación, tales como voz, vídeo, datos en paquetes, mensajería, radiodifusión etc. Estas redes inalámbricas pueden ser redes de acceso múltiple, que pueden prestar soporte a múltiples usuarios compartiendo los recursos de red disponibles. Ejemplos de dichas redes de acceso múltiple incluyen redes de acceso múltiple por división de código (CDMA), redes de acceso múltiple por división de tiempo (TDMA), redes de acceso múltiple por división de frecuencia (FDMA) y redes FDMA ortogonales (OFDMA), etc.

[0004] Una red inalámbrica puede usar cifrado para proteger la información enviada por el aire. Los términos "cifrado" y “encriptación” son sinónimos y se usan indistintamente. Al comienzo de una llamada, la información puede enviarse en lenguaje no cifrado hasta que se establece una configuración de cifrado. La configuración de cifrado puede indicar un algoritmo particular y/o parámetros relevantes (por ejemplo, claves de seguridad) para usar en el cifrado. Después de establecer la configuración de cifrado, se puede enviar un mensaje para indicar que el cifrado comenzará en el momento de activación designado. La información puede enviarse con cifrado después del momento de activación.

[0005] La configuración de cifrado se puede cambiar durante la llamada. Después de completar el cambio, se puede enviar un mensaje para indicar que el cifrado con la nueva configuración comenzará en el momento de activación designado. La información puede enviarse usando la configuración de cifrado antigua antes de este momento de activación y usando la configuración de cifrado nueva después del momento de activación.

[0006] Para asegurar que no se pierda información a causa de un cambio en la configuración de cifrado, la transmisión puede suspenderse desde el momento en que se envía un mensaje respecto a la configuración de cifrado nueva hasta el momento en que se recibe un acuse de recibo del mensaje. Esto asegura que una entidad receptora tenga conocimiento de la siguiente transmisión con la configuración de cifrado nueva. Sin embargo, un cierto retardo está asociado con el envío del acuse de recibo, y suspender la transmisión durante este tiempo puede afectar negativamente al rendimiento. Por ejemplo, si la información de tiempo crítico no puede enviarse durante el período de suspensión, puede caer la llamada o se pueden producir otros efectos perjudiciales.

[0007] Por lo tanto, existe una necesidad en la técnica de técnicas para enviar información durante un cambio en la configuración de cifrado.

[0008] Se llama la atención del documento US 2005/086466 A1, que describe los detalles de un aparato y procedimiento para determinar el momento de activación del cifrado de enlace ascendente en un equipo de usuario del sistema universal de telecomunicaciones móviles. El momento de activación de cifrado se determina para portadores de radio que no sean RB2 midiendo la velocidad de transferencia de datos en cada portador de radio objetivo durante el tiempo que tarda un sondeo o un mensaje RRC enviado desde el equipo de usuario UE que acusará recibo por parte de la red UTRAN. Para RB2, el momento de activación del cifrado de enlace ascendente se determina teniendo en cuenta el tamaño del mensaje de respuesta de RRC y los datos que ya se han puesto en cola en RB2 para su transmisión.

SUMARIO

[0009] De acuerdo con la presente invención, se proporcionan un procedimiento como se expone en la reivindicación 1, un aparato como se expone en la reivindicación 4, y un medio legible por procesador como se expone en la reivindicación 14. Los modos de realización preferentes se reivindican en las reivindicaciones dependientes.

[0010] Las técnicas para enviar información sin interrupción durante un cambio en la configuración de cifrado se describen en el presente documento. Un equipo de usuario (UE) se comunica con una red de comunicación

inalámbrica para una llamada. El UE puede ser un teléfono celular o algún otro dispositivo. La red inalámbrica puede ser una red del sistema universal de telecomunicaciones móviles (UMTS) o alguna otra red inalámbrica.

[0011] El UE envía la primera información a la red inalámbrica usando una primera configuración de cifrado. La red inalámbrica puede iniciar un procedimiento de control del modo de seguridad para cambiar la configuración de cifrado. Como parte de este procedimiento, el UE selecciona un momento de activación para una segunda configuración de cifrado y envía un mensaje de seguridad con el momento de activación. Este momento de activación es el momento en que el UE aplica la segunda configuración de cifrado a la transmisión enviada a la red inalámbrica. Después, el UE envía una segunda información (por ejemplo, un mensaje de notificación de la medición) usando la primera configuración de cifrado después de enviar el mensaje de seguridad y antes del momento de activación. El UE puede recibir un acuse de recibo de la red inalámbrica para el mensaje de seguridad antes del momento de activación. El UE envía una tercera información usando la segunda configuración de cifrado después del momento de activación. La primera, segunda y tercera información pueden comprender mensajes de señalización, datos, etc.

[0012] El UE puede seleccionar el momento de activación en base a (a) cualquier mensaje pendiente para enviar usando la primera configuración de cifrado antes de enviar el mensaje de seguridad, (b) la longitud del mensaje de seguridad y (c) uno o más mensajes para enviar usando la primera configuración de cifrado después de enviar el mensaje de seguridad. La primera, segunda y tercera información y el mensaje de seguridad pueden enviarse en unidades de datos de protocolo (PDU) a las que se les asignan números de secuencia secuenciales. El UE puede seleccionar un número de secuencia de activación en base a el número de secuencia de la siguiente PDU a enviar, el número de las PDU a enviar antes del mensaje de seguridad, el número de las PDU a enviar para el mensaje de seguridad y el número de las PDU a enviar usando la primera configuración de cifrado después de enviar el mensaje de seguridad. Para asegurar que la segunda configuración de cifrado se use solo después de que la red inalámbrica haya recibido satisfactoriamente el mensaje de seguridad, el UE puede suspender la transmisión de las PDU con números de secuencia mayores o iguales que el número de secuencia de activación hasta que se reciba un acuse de recibo de la red inalámbrica para el mensaje de seguridad.

[0013] La red inalámbrica también puede aplicar las técnicas de manera análoga para la transmisión en el enlace descendente. Esto permite que la red inalámbrica evite la suspensión de la transmisión de enlace descendente durante un cambio en la configuración de cifrado. A continuación, se describen en más detalle diversos aspectos y características de la divulgación.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0014]

La FIG. 1 muestra un UE que se comunica con una red de acceso por radio terrestre UMTS (UTRAN).

La FIG. 2 muestra la señalización intercambiada entre el UE y la UTRAN para cambiar la configuración de cifrado.

La FIG. 3 muestra la señalización intercambiada entre el UE y la UTRAN para cambiar la configuración de cifrado sin suspensión de las transmisiones de enlace descendente y enlace ascendente.

La FIG. 4 muestra un cronograma del UE para un cambio en la configuración de cifrado con un momento de activación de enlace ascendente retardado.

La FIG. 5 muestra un cronograma para determinar un número de secuencia de activación.

La FIG. 6 muestra un proceso realizado por una entidad transmisora.

La FIG. 7 muestra un proceso realizado por una entidad receptora.

La FIG. 8 muestra un diagrama de bloques del UE y la UTRAN.

DESCRIPCIÓN DETALLADA

[0015] Las técnicas descritas en el presente documento se pueden usar para diversas redes de comunicación inalámbrica. Los términos "red" y "sistema" pueden intercambiarse frecuentemente. Por ejemplo, las técnicas pueden usarse para redes CDMA, TDMA, FDMA y OFDMA. Una red de CDMA puede implementar una tecnología de radio tal como CDMA de banda ancha (W-CDMA), cdma2000, etc.; cdma2000 abarca las normas IS-2000, IS-95 e IS-856. Una red TDMA puede implementar una tecnología de radio como el sistema global para comunicaciones móviles (GSM), el sistema digital avanzado de telefonía móvil (D-AMPS), etc. Estas diversas normas y tecnologías de radio son conocidas en la técnica. W-CDMA y GSM se describen en documentos de una organización llamada "Proyecto de Colaboración de Tercera Generación" (3GPP). cdma2000 se describe en documentos de una organización llamada "Segundo Proyecto de Colaboración de Tercera Generación" (3GPP2). Los documentos del 3GPP y del 3GPP2 están

a disposición del público. Para una mayor claridad, se describen ciertos aspectos de las técnicas para una red UMTS que implementa W-CDMA.

[0016] La **FIG. 1** muestra un UE 110 que se comunica con una UTRAN 120 en 3GPP. UTRAN 120 incluye un número de nodos B que admiten comunicación por radio para un número de UE. Para simplificar, únicamente se muestran tres nodos B 130 y un UE 110 en la FIG. 1. Un nodo B en general es una estación fija que se comunica con los UE y también puede denominarse un nodo B mejorado, una estación base, un punto de acceso, una estación transceptora base (BTS), etc. Cada nodo B proporciona cobertura de comunicación para un área geográfica particular. Un nodo B y/o su área de cobertura se pueden denominar "célula", dependiendo del contexto en el que se usa el término. Un controlador de red de radio (RNC) 140 está acoplado a los nodos B 130 y proporciona coordinación y control para estos nodos B.

[0017] El UE 110 puede ser estacionario o móvil y también se puede denominar una estación móvil, un terminal de acceso, una estación, una estación de abonado, etc. El UE 110 puede ser un teléfono celular, un asistente personal digital (PDA), un dispositivo inalámbrico, una tarjeta módem, un dispositivo manual, un ordenador portátil, etc. El UE 110 se puede comunicar con uno o más nodos B en el enlace descendente y/o el enlace ascendente en cualquier momento dado. El enlace descendente (o enlace directo) se refiere al enlace de comunicación desde los nodos B al UE, y el enlace ascendente (o enlace inverso) se refiere al enlace de comunicación desde el UE a los nodos B.

[0018] El UE 110 se puede comunicar con la UTRAN 120 usando una pila de protocolos que incluye una capa de control de recursos de radio (RRC), una capa de control de enlace de radio (RLC), una capa de control de acceso al medio (MAC) y una capa física. La capa RRC forma parte de la capa 3. Las capas RLC y MAC forman parte de la capa 2, que comúnmente se denomina capa de enlace de datos. La capa RRC proporciona un servicio de transferencia de información a un estrato sin acceso (NAS), que es una capa funcional que admite mensajes de tráfico y señalización entre el UE 110 y una red central (CN) con la que interactúa la UTRAN 120. La capa RRC también es responsable de controlar la configuración de las capas 1 y 2. La capa RLC proporciona fiabilidad para la transmisión de información (por ejemplo, datos y/o señalización) y realiza la retransmisión automática (ARQ) de información descodificada por error. La capa MAC realiza funciones como la codificación de información. La capa física proporciona un mecanismo para transmitir información por el aire. En el lado de UTRAN, la capa física se implementa típicamente en los nodos B 130, y las capas RLC, MAC y RRC se implementan típicamente en el RNC 140.

[0019] El UE 110 puede comunicarse con la UTRAN 120 a través de uno o más portadores de radio en la capa 2. Un portador de radio es un servicio proporcionado por la capa 2 para la transferencia de datos de tráfico entre el UE y la UTRAN. Un portador de radio de señalización (SRB) es un portador de radio usado para enviar mensajes RRC. SRB2 es un portador de radio de señalización que se usa para la mayoría de los mensajes RRC. Cada portador de radio está asociado con una configuración específica de canales lógicos en la capa RLC, canales de transporte en la capa MAC y canales físicos en la capa física. Los portadores de radio y los portadores de radio de señalización se describen en el documento 3GPP TS 25.331, titulado "Radio Resource Control (RRC); Protocol Specification", de junio de 2006, que está disponible al público.

[0020] El UE 110 y la UTRAN 120 pueden comunicarse con cifrado para proteger la información enviada por el aire. El UE 110 y la UTRAN 120 pueden realizar un procedimiento de control del modo de seguridad para establecer una configuración de cifrado, que puede indicar un algoritmo de cifrado específico y/o parámetros específicos a usar en el cifrado. El cifrado se puede realizar sobre la información enviada en los portadores de radio y los portadores de radio de señalización de acuerdo con la configuración de cifrado. También se puede realizar un procedimiento de control del modo de seguridad para cambiar la configuración de cifrado. El cifrado se puede realizar de acuerdo con la configuración de cifrado nueva.

[0021] La **FIG. 2** muestra cronogramas en el UE 110 y la UTRAN 120 de la señalización intercambiada entre el UE y UTRAN para cambiar la configuración de cifrado. Al comienzo de una llamada, se establece una configuración de cifrado, y tanto el UE 110 como la UTRAN 120 envían información usando esta configuración de cifrado. En el tiempo T_0, el UE 110 y la UTRAN 120 participan en un procedimiento de control del modo de seguridad para cambiar la configuración de cifrado. Para comenzar a cifrar con la configuración de cifrado nueva, la UTRAN 120 envía un mensaje de COMANDO DEL MODO DE SEGURIDAD en el enlace descendente comenzando en el tiempo T_1 y finalizando en el tiempo T_2. Este mensaje se envía en un modo con acuse de recibo RLC (RLC-AM) usando la configuración de cifrado antigua. El UE 110 recibe y descodifica correctamente el mensaje de COMANDO DEL MODO DE SEGURIDAD y, en el tiempo T_3, envía un acuse de recibo de capa 2 (L2 ACK) para indicar la recepción satisfactoria del mensaje. El UE 110 también envía un mensaje de MODO DE SEGURIDAD COMPLETO en el enlace ascendente en RLC-AM usando la configuración de cifrado antigua que comienza en el tiempo T_4 y finaliza en el tiempo T_5. La UTRAN 120 recibe y descodifica correctamente el mensaje y envía un L2 ACK para este mensaje en el tiempo T_6.

[0022] La FIG. 2 también muestra cuándo se aplican las configuraciones de cifrado antiguas y nuevas para las transmisiones de enlace descendente y de enlace ascendente. Para el enlace descendente, el mensaje de COMANDO DEL MODO DE SEGURIDAD enviado por la UTRAN 120 transporta un elemento de información (IE) que contiene un momento de activación de cifrado del enlace descendente. Este momento de activación del enlace descendente es el momento en que la UTRAN 120 aplica la configuración de cifrado nueva a la transmisión de enlace descendente. El

momento de activación del enlace descendente puede establecerse al final del mensaje de COMANDO DEL MODO DE SEGURIDAD, como se muestra en la FIG. 2, de modo que la configuración de cifrado nueva se aplique al siguiente mensaje enviado en el enlace descendente. La UTRAN 120 usa la configuración de cifrado antigua para la transmisión de enlace descendente hasta el momento de activación del enlace descendente y usa la configuración de cifrado nueva después del momento de activación del enlace descendente. La UTRAN 120 puede suspender la transmisión de enlace descendente después de enviar el mensaje de COMANDO DEL MODO DE SEGURIDAD y puede reanudar la transmisión de enlace descendente después de recibir el L2 ACK para este mensaje desde el UE 110, como se muestra en la FIG. 2.

[0023] Para el enlace ascendente, el mensaje de MODO DE SEGURIDAD COMPLETO enviado por el UE 110 transporta un elemento de información que contiene un momento de activación de cifrado del enlace ascendente. Este momento de activación del enlace ascendente es el momento en que se aplica la configuración de cifrado nueva a la transmisión de enlace ascendente. El momento de activación del enlace ascendente puede establecerse al final del mensaje de MODO DE SEGURIDAD COMPLETO, como se muestra en la FIG. 2, de modo que la configuración de cifrado nueva se aplique al siguiente mensaje enviado en el enlace ascendente. El UE 110 usa la configuración de cifrado antigua para la transmisión de enlace ascendente hasta el momento de activación del enlace ascendente y usa la configuración de cifrado nueva después del momento de activación del enlace ascendente. El UE 110 puede suspender la transmisión de enlace ascendente después de enviar el mensaje de MODO DE SEGURIDAD COMPLETO y puede reanudar la transmisión de enlace ascendente después de recibir el L2 ACK para este mensaje desde la UTRAN 120, como se muestra en la FIG. 2.

[0024] Durante la llamada, el UE 110 puede buscar periódicamente células vecinas y realizar mediciones para las células detectadas por el UE 110. El UE 110 puede enviar notificaciones de medición a la UTRAN 120 cuando se desencadenan por ciertos eventos. Por ejemplo, los eventos desencadenantes pueden corresponder a mediciones débiles para la célula que actualmente sirve al UE 110, mediciones fuertes para células vecinas, etc. La UTRAN 120 puede usar las notificaciones de medición para mantener un conjunto activo para el UE 110, seleccionar una célula adecuada para servir al UE 110, iniciar el traspaso de UE 110 a una célula mejor a fin de mantener la llamada para el UE 110, etc. El conjunto activo puede incluir la célula designada para servir al UE 110 (la célula de servicio) y las células que podrían servir al UE 110 (células candidatas). El UTRAN 120 puede enviar un mensaje de actualización del conjunto activo al UE 110. Este mensaje puede añadir enlaces de radio para células nuevas fuertes y/o eliminar enlaces de radio para células viejas débiles.

[0025] Como se muestra en la FIG. 2, el UE 110 puede suspender la transmisión de enlace ascendente y la UTRAN puede suspender la transmisión de enlace descendente al cambiar la configuración de cifrado. La suspensión de la transmisión de enlace ascendente puede hacer que el UE 110 retarde el envío de notificaciones de medición a la UTRAN 120. Estas notificaciones de medición se pueden usar para el mantenimiento activo del equipo y pueden ser especialmente importantes para mantener la llamada en malas condiciones de radio. El retardo en el envío de las notificaciones de medición a causa de la suspensión de la transmisión de enlace ascendente puede dar como resultado que el conjunto activo contenga células débiles, lo que a su vez provoca que caiga la llamada. En consecuencia, la suspensión de la transmisión de enlace descendente puede hacer que la UTRAN 120 retarde el envío del mensaje de actualización del conjunto activo al UE 110, lo que también puede provocar la caída de la llamada.

[0026] Una razón para suspender la transmisión de enlace ascendente durante un cambio en la configuración de cifrado es asegurar que el UE 110 no envíe un mensaje usando la configuración de cifrado nueva hasta que la UTRAN 120 tenga conocimiento de que se está aplicando la configuración de cifrado nueva. Para la implementación mostrada en la FIG. 2, si la UTRAN 120 descodifica el mensaje de MODO DE SEGURIDAD COMPLETO por error y no envía un L2 ACK, entonces el UE 110 no enviará mensajes usando la configuración de cifrado nueva puesto que la UTRAN 120 no sabrá cuándo UE 110 ha comenzado a usar la configuración de cifrado nueva. La suspensión de la transmisión de enlace ascendente asegura así que la UTRAN 120 pueda descifrar todos los mensajes enviados por el UE 110 en el enlace ascendente.

[0027] En un aspecto, el UE 110 puede enviar mensajes (por ejemplo, mensajes de notificación de la medición) en el enlace ascendente durante un cambio en la configuración de cifrado de manera que la UTRAN 120 pueda descifrar los mensajes. Esto se puede lograr seleccionando un momento de activación de enlace ascendente apropiado para la configuración de cifrado nueva, como se describe a continuación. De manera similar, la UTRAN 120 puede enviar mensajes (por ejemplo, mensajes de actualización del conjunto activo) en el enlace descendente durante un cambio en la configuración de cifrado de manera que el UE 110 pueda descifrar los mensajes. Esto se puede lograr seleccionando un momento de activación de enlace descendente apropiado para la configuración de cifrado nueva.

[0028] La **FIG. 3** muestra cronogramas en el UE 110 y la UTRAN 120 de la señalización intercambiada entre el UE y UTRAN para cambiar la configuración de cifrado sin suspensión de las transmisiones de enlace descendente y enlace ascendente. Al comienzo de una llamada, se establece una configuración de cifrado, y tanto el UE 110 como la UTRAN 120 envían información usando esta configuración de cifrado. En el tiempo T_0, el UE 110 y la UTRAN 120 participan en un procedimiento de control del modo de seguridad para cambiar la configuración de cifrado. Para comenzar a cifrar con la configuración de cifrado nueva, la UTRAN 120 envía un mensaje de COMANDO DEL MODO

DE SEGURIDAD en el enlace descendente comenzando en el tiempo T_1 y finalizando en el tiempo T_2. El UE 110 recibe y descodifica correctamente el mensaje y envía un L2 ACK en el tiempo T_3. El UE 110 también envía un mensaje de MODO DE SEGURIDAD COMPLETO en el enlace ascendente usando la configuración de cifrado antigua que comienza en el tiempo T_4 y finaliza en el tiempo T_5. La UTRAN 120 recibe y descodifica correctamente el mensaje y envía un L2 ACK en el tiempo T_7.

[0029] La FIG. 3 también muestra cuándo se aplican las configuraciones de cifrado antiguas y nuevas para las transmisiones de enlace descendente y de enlace ascendente. Para el enlace descendente, la UTRAN 120 selecciona un momento de activación del enlace descendente de T_6, que es una cantidad de tiempo posterior al final del mensaje de COMANDO DEL MODO DE SEGURIDAD en el tiempo T_2. La diferencia entre T_6 y T_2 es el retardo en la aplicación de la configuración de cifrado nueva en el enlace descendente. La UTRAN 120 usa la configuración de cifrado antigua para la transmisión de enlace descendente hasta el momento de activación del enlace descendente en T_6 y usa la configuración de cifrado nueva después del momento de activación del enlace descendente. Si la UTRAN 120 recibe el L2 ACK antes del momento de activación del enlace descendente, como se muestra en la FIG. 2, entonces la UTRAN 120 no suspende la transmisión de enlace descendente. La UTRAN 120 continúa usando la configuración de cifrado antigua después de recibir el L2 ACK y comienza a usar la configuración de cifrado nueva después del momento de activación del enlace descendente.

[0030] Para el enlace ascendente, el UE 110 selecciona un momento de activación del enlace ascendente de Tg, que es una cantidad de tiempo posterior al final del mensaje de MODO DE SEGURIDAD COMPLETO en el tiempo T_5. La diferencia entre T_8 y T_5 es el retardo en la aplicación de la configuración de cifrado nueva en el enlace ascendente. El UE 110 usa la configuración de cifrado antigua para la transmisión de enlace ascendente hasta el momento de activación del enlace ascendente en T_8 y usa la configuración de cifrado nueva después del momento de activación del enlace ascendente. Si el UE 110 recibe el L2 ACK antes del momento de activación del enlace ascendente, como se muestra en la FIG. 2, entonces el UE 110 no suspende la transmisión de enlace ascendente. El UE 110 continúa usando la configuración de cifrado antigua después de recibir el L2 ACK y comienza a usar la configuración de cifrado nueva después del momento de activación del enlace ascendente.

[0031] Como se muestra en la FIG. 3, el UE 110 no suspende la transmisión de enlace ascendente ni retarda la suspensión de la transmisión de enlace ascendente cuando se cambia la configuración de cifrado si el momento de activación del enlace ascendente es posterior al L2 ACK desde la UTRAN 120. De manera similar, la UTRAN no suspende la transmisión de enlace descendente ni retarda la suspensión de la transmisión de enlace descendente cuando se cambia la configuración de cifrado si el momento de activación del enlace descendente es posterior al L2 ACK del UE 110. Los tiempos de activación del enlace ascendente y el enlace descendente pueden seleccionarse en base a diversos factores, tales como el retardo esperado a la hora de recibir el ACK L2, la cantidad de información que se debe enviar antes de conmutar a la configuración de cifrado nueva, las condiciones de radio actuales, etc. Al evitar o retardar la suspensión de transmisión de enlace ascendente, el UE 110 puede enviar mensajes de notificación de la medición de manera oportuna para asegurar el mantenimiento adecuado del conjunto activo por parte de la UTRAN 120, lo que puede reducir la probabilidad de una caída de llamada. Al evitar o retardar la suspensión de la transmisión de enlace descendente, la UTRAN 120 puede enviar mensajes de actualización del conjunto activo de manera oportuna, lo que también puede reducir la probabilidad de una caída de llamada.

[0032] En general, el momento de activación para un enlace dado puede darse de diversas maneras. En la capa RLC, la información se envía en las RLC PDU a las que se asignan números de secuencia (SN) secuencialmente crecientes de 0 a 4095, que vuelven a 0 y continúan. En RLC-AM, que se usa para enviar mensajes en SRB2, las RLC PDU que son recibidas por error por una entidad receptora son reenviadas por una entidad transmisora. La entidad receptora puede obtener las RLC PDU descodificadas correctamente fuera de secuencia y puede usar el número de secuencia de cada RLC PDU para reordenar las RLC PDU y proporcionar estas RLC PDU en el orden correcto a una capa superior. El momento de activación puede darse en términos de número de secuencia RLC.

[0033] La **FIG. 4** muestra un cronograma de ejemplo para el UE 110 durante un cambio en la configuración de cifrado con un momento de activación del enlace ascendente retardado para evitar la suspensión de la transmisión de enlace ascendente. El mensaje de MODO DE SEGURIDAD COMPLETO puede enviarse en un número particular de las RLC PDU. El momento de activación del enlace ascendente se puede dar en términos del número de secuencia de la primera RLC PDU para enviar usando la configuración de cifrado nueva. En el ejemplo que se muestra en la FIG. 3, el mensaje de MODO DE SEGURIDAD COMPLETO se envía en dos RLC PDU con números de secuencia de *n* y *n+1*. Si el momento de activación del enlace ascendente se establece en el siguiente número de secuencia RLC de *n+2*, entonces el UE 110 no podrá enviar la siguiente RLC PDU hasta que se reciba un L2 ACK para el mensaje de MODO DE SEGURIDAD COMPLETO.

[0034] Sin embargo, el momento de activación del enlace ascendente puede retardarse a fin de evitar la suspensión de la transmisión de enlace ascendente. Esto se puede lograr seleccionando un número de secuencia de RLC que esté disponible en el futuro (en lugar del número de secuencia de RLC justo después del mensaje de MODO DE SEGURIDAD COMPLETO) como el momento de activación del enlace ascendente. La cantidad de tiempo de espera en el futuro es la cantidad de retardo en la aplicación de la configuración de cifrado nueva, que puede seleccionarse en base a diversos factores como se analiza a continuación. En el ejemplo que se muestra en la FIG. 3, se puede

enviar un mensaje de notificación de la medición en tres RLC PDU, y el momento de activación del enlace ascendente se retarda por tres RLC PDU para permitir que el UE 110 envíe un mensaje de notificación de la medición. En este caso, el momento de activación del enlace ascendente se establece en el número de secuencia RLC *n+5.* El mensaje de notificación de la medición puede enviarse usando la configuración de cifrado antigua en las RLC PDU *n+2*, *n+3* y *n+4* sin ningún retardo. Los mensajes posteriores se pueden enviar usando la configuración de cifrado nueva en la RLC PDU *n+5* y más allá, después de recibir el L2 ACK desde la UTRAN 120. En la mayoría de los casos, el mensaje de MODO DE SEGURIDAD COMPLETO enviado en las RLC PDU *n* y *n+1* será descodificado correctamente por la UTRAN 120, que luego puede enviar un L2 ACK en algún momento antes del final de la RLC PDU *n+4*. En estos casos, el UE 110 recibiría el L2 ACK antes del momento de activación del enlace ascendente, como se muestra en la FIG. 4, y puede enviar mensajes usando la configuración de cifrado nueva sin ninguna suspensión de transmisión de enlace ascendente.

[0035] En un diseño, el momento de activación del enlace ascendente se puede definir de la siguiente manera:

$$SN_{activación} = SN_{siguiente} + N_{antes} + N_{SMC} + N_{después}, \quad \text{Ec. (1)}$$

donde $SN_{siguiente}$ es el número de secuencia de la siguiente RLC PDU para enviar en el enlace ascendente,

$N_{anterior}$ es el número de las RLC PDU a enviar antes de enviar el mensaje de MODO DE SEGURIDAD COMPLETO,

N_{SMC} es el número de las RLC PDU a enviar para el mensaje de MODO DE SEGURIDAD COMPLETO,

$N_{después}$ es el número de RLC PDU a enviar con la configuración de cifrado antigua después de enviar el mensaje de MODO DE SEGURIDAD COMPLETO, y

$SN_{activación}$ es un número de secuencia de activación para el momento de activación del enlace ascendente.

[0036] El momento de activación del enlace ascendente/número de secuencia se puede determinar siempre que se reciba un mensaje de COMANDO DEL MODO DE SEGURIDAD desde la UTRAN 120. $SN_{siguiente}$ puede ser el número de secuencia de la siguiente RLC PDU para enviar después de recibir el mensaje de COMANDO DEL MODO DE SEGURIDAD. N_{antes} puede determinarse, por ejemplo, en base a los mensajes pendientes que se encuentran en una memoria intermedia en el UE 110 y listos para ser enviados a la UTRAN 120 cuando se recibe el mensaje de COMANDO DEL MODO DE SEGURIDAD. N_{antes} puede ser cero si no hay mensajes pendientes en la memoria intermedia o si estos mensajes pueden retardarse y enviarse más tarde usando la configuración de cifrado nueva. N_{SMC} es típicamente un valor conocido, por ejemplo, NSMC = 2 si el mensaje de MODO DE SEGURIDAD COMPLETO se puede enviar en dos RLC PDU.

[0037] $N_{después}$ puede determinarse en base a todos los mensajes que se enviarán a la UTRAN 120 usando la configuración de cifrado antigua después de enviar el mensaje de MODO DE SEGURIDAD COMPLETO, de la siguiente manera:

$$N_{después} = \sum_{m=1}^{M} N_m, \quad \text{Ec. (2)}$$

donde

N_m es el número de las RLC PDU a enviar para el mensaje *m*, y

M es el número de mensajes a enviar usando la configuración de cifrado antigua después de enviar el mensaje de MODO DE SEGURIDAD COMPLETO

[0038] La ecuación (2) explica el hecho de que se pueden enviar diferentes mensajes en diferentes números de las RLC PDU. En el ejemplo que se muestra en la FIG. 4, la configuración $N_{después}$ = 3 permite que el UE 110 envíe un mensaje de notificación de la medición en tres RLC PDU. Los M mensajes de notificación de la medición también se pueden enviar estableciendo $N_{después}$ = 3M. Un delta o compensación se puede añadir a, o restar de, la suma en la ecuación (2) para tener en cuenta cualquier factor, por ejemplo, los retardos de procesamiento, etc. En general, $N_{después}$ puede seleccionarse para que sea más largo que el retardo esperado para recibir el L2 ACK desde la UTRAN 120 en el mensaje de MODO DE SEGURIDAD COMPLETO. Esto evitaría la suspensión de la transmisión de enlace ascendente en el escenario probable en el que la UTRAN 120 descodifica correctamente el mensaje de MODO DE SEGURIDAD COMPLETO y envía oportunamente el L2 ACK.

[0039] La **FIG. 5** muestra un cronograma de ejemplo para determinar el número de secuencia de activación para un cambio en la configuración de cifrado con un momento de activación de enlace ascendente retardado. En este ejemplo, el número de secuencia de la siguiente RLC PDU para enviar en el enlace ascendente es $SN_{siguiente} = n - N_{antes}$. Se pueden enviar $N_{anterior}$ RLC PDU con los números de secuencia de $n - N_{antes}$ a n -1 para los mensajes

pendientes antes del mensaje de MODO DE SEGURIDAD COMPLETO. Se pueden enviar dos RLC PDU con números de secuencia de *n* y *n* + 1 para el mensaje de MODO DE SEGURIDAD COMPLETO. Las $N_{después}$ RLC PDU con números de secuencia de *n* + 2 a *n* + $N_{después}$ + 1 pueden enviarse para uno o más mensajes usando la configuración de cifrado antigua después de enviar el mensaje de MODO DE SEGURIDAD COMPLETO. En este ejemplo, el número de secuencia de activación puede establecerse en $SN_{activación}$ = *n*+ $N_{después}$ + 2.

[0040] El envío de mensajes usando la configuración de cifrado antigua después de enviar el mensaje de MODO DE SEGURIDAD COMPLETO permite a la UTRAN 120 descifrar correctamente estos mensajes independientemente del estado del mensaje de MODO DE SEGURIDAD COMPLETO. En el ejemplo que se muestra en la FIG. 4, si el mensaje de MODO DE SEGURIDAD COMPLETO se descodifica por error, la UTRAN 120 no enviará un L2 ACK pero aún puede descifrar el mensaje de notificación de la medición enviado usando la configuración de cifrado antigua. El UE 110 volverá a enviar el mensaje de MODO DE SEGURIDAD COMPLETO, por ejemplo, después de recibir un L2 ACK para el mensaje de notificación de la medición, pero no uno para el mensaje de MODO DE SEGURIDAD COMPLETO. Tras descodificar satisfactoriamente la segunda transmisión del mensaje de MODO DE SEGURIDAD COMPLETO, la UTRAN 120 puede reordenar las RLC PDU y pasar el mensaje de notificación de la medición de inmediato. Si el mensaje de notificación de la medición no se ha enviado usando la configuración de cifrado antigua, el UE 110 puede enviar este mensaje después de recibir un L2 ACK de la UTRAN 120 para la segunda transmisión del mensaje de MODO DE SEGURIDAD COMPLETO, lo que retardará aún más la recepción del mensaje de notificación de la medición por parte de la UTRAN 120.

[0041] Una configuración de cifrado se considera pendiente después de que haya comenzado un procedimiento de control del modo de seguridad y hasta que se alcanza el momento de activación. La UTRAN 120 puede iniciar otro procedimiento de control del modo de seguridad mientras exista una configuración de cifrado pendiente. Para un procedimiento de control del modo de seguridad dado, la UTRAN 120 puede (i) seleccionar un momento de activación de enlace descendente adecuado si no existe una configuración de cifrado pendiente o (b) usar el momento de activación de enlace descendente para una configuración de cifrado pendiente si existe. La UTRAN 120 puede enviar uno o más mensajes de COMANDO DEL MODO DE SEGURIDAD mientras exista una configuración de cifrado pendiente, pero cada uno de estos mensajes conllevará el mismo momento de activación del enlace descendente. Esta restricción evita la necesidad de mantener múltiples tiempos de activación para los procedimientos de control del modo de seguridad superpuestos.

[0042] La misma operación también se puede aplicar para el enlace ascendente. El UE 110 puede (i) seleccionar un momento de activación del enlace ascendente adecuado si no existe una configuración de cifrado pendiente o (b) usar el momento de activación del enlace ascendente para una configuración de cifrado pendiente si existe. El UE 110 puede enviar uno o más mensajes de MODO DE SEGURIDAD COMPLETO mientras exista una configuración de cifrado pendiente, pero cada uno de estos mensajes conllevará el mismo momento de activación del enlace ascendente.

[0043] El UE 110 puede mantener un indicador pendiente que puede establecerse en verdadero (o “1”) si existe una configuración de cifrado pendiente o en falso (o “0”) si no existe una configuración de cifrado pendiente. El UE 110 puede usar este indicador pendiente para seleccionar el momento de activación del enlace ascendente, por ejemplo, cada vez que se recibe un mensaje de COMANDO DEL MODO DE SEGURIDAD desde la UTRAN 120. El UE 110 también puede almacenar el momento de activación del enlace ascendente pendiente, que se denota como $SN_{pendiente}$.

[0044] En un diseño, el UE 110 puede establecer el momento de activación del enlace ascendente de la siguiente manera:

10 Si (Indicador_Pendiente = falso)

20 Entonces $SN_{activación} = SN_{siguiente} + N_{antes} + N_{SMC} + N_{después}$

30 Si (Indicador_Pendiente = verdadero) y

40 Si $\{(SN_{pendiente} - SN_{siguiente}) \geq (N_{antes} + N_{SMC})\}$

50 Entonces $SN_{activación} = SN_{pendiente}$

60 Sino $SN_{activación} = SN_{siguiente} + N_{antes} + N_{SMC} + N_{después}$

[0045] En el pseudocódigo anterior, el momento de activación del enlace ascendente puede establecerse como se muestra en la ecuación (1) cuando no existe una configuración de cifrado pendiente (líneas 10 y 20). Si existe una configuración de cifrado pendiente, el momento de activación del enlace ascendente pendiente se usa si está lo suficientemente lejos como para permitir la transmisión de las N_{antes} RLC PDU antes del mensaje de MODO DE SEGURIDAD COMPLETO, así como de las NSMC RLC PDU para este mensaje (líneas 30, 40 y 50). De lo contrario, si las N_{antes} + NSMC RLC PDU no pueden enviarse antes del momento de activación del enlace ascendente pendiente, entonces el momento de activación del enlace ascendente puede establecerse como se muestra en la ecuación (1)

(línea 60). Sin embargo, las RLC PDU no se envían usando la configuración de cifrado nueva hasta que se recibe un L2 ACK para el mensaje de MODO DE SEGURIDAD COMPLETO.

[0046] El UE 110 puede enviar la transmisión en el enlace ascendente de la siguiente manera:

1. Enviar las RLC PDU con números de secuencia inferiores a $SN_{activación}$ usando la configuración de cifrado antigua,

2. Enviar las RLC PDU con números de secuencia mayores o iguales a $SN_{activación}$ usando la configuración de cifrado nueva, y

3. Suspender el envío de las RLC PDU con números de secuencia mayores o iguales a la $SN_{activación}$ hasta que se reciba un L2 ACK para el mensaje de COMANDO DEL MODO DE SEGURIDAD.

[0047] La **FIG. 6** muestra un proceso 600 realizado por una entidad transmisora, que puede ser el UE 110 para la transmisión de enlace ascendente o la UTRAN 120 para la transmisión de enlace descendente. La primera información se envía usando una primera configuración de cifrado (bloque 612). Se selecciona un momento de activación para una segunda configuración de cifrado, por ejemplo, durante un procedimiento de control del modo de seguridad (bloque 614). Se envía un mensaje de seguridad con el momento de activación a una entidad receptora (bloque 616). Este mensaje de seguridad puede ser un mensaje de MODO DE SEGURIDAD COMPLETO enviado por el UE 110 en el enlace ascendente, un mensaje de COMANDO DEL MODO DE SEGURIDAD enviado por la UTRAN 120 en el enlace descendente, o algún otro mensaje. La segunda información se envía usando la primera configuración de cifrado después de enviar el mensaje de seguridad y antes del momento de activación (bloque 618). La segunda información puede comprender un mensaje de notificación de la medición, un mensaje de actualización del conjunto activo, etc. Se puede recibir un acuse de recibo del mensaje de seguridad antes del momento de activación (bloque 620). La tercera información se envía usando la segunda configuración de cifrado después del momento de activación (bloque 622). La primera, segunda y tercera información pueden comprender señalización, mensajes, datos, etc., o cualquier combinación de los mismos.

[0048] Para el bloque 614, el momento de activación puede seleccionarse para que sea una cantidad de tiempo después del final del mensaje de seguridad. El momento de activación se puede seleccionar en base a (a) cualquier mensaje pendiente para enviar usando la primera configuración de cifrado antes de enviar el mensaje de seguridad, (b) la longitud del mensaje de seguridad y (c) al menos un mensaje para enviar usando la primera configuración de cifrado después de enviar el mensaje de seguridad. Si existe una configuración de cifrado pendiente, entonces el momento de activación puede establecerse en un momento de activación pendiente, por ejemplo, si este momento de activación pendiente permite enviar mensajes pendientes y el mensaje de seguridad usando la primera configuración de cifrado. El momento de activación también se puede establecer de forma normal, incluso cuando existe una configuración de cifrado pendiente.

[0049] La primera, segunda y tercera información y el mensaje de seguridad pueden enviarse en las PDU con números de secuencia secuenciales, y puede usarse un número de secuencia de activación como el momento de activación. El número de secuencia de activación puede ser el número de secuencia de una PDU que es un número particular de las PDU después de la última PDU para el mensaje de seguridad. Por ejemplo, el número de secuencia de activación puede determinarse en base al número de secuencia de la siguiente PDU a enviar, el número de las PDU a enviar antes del mensaje de seguridad, el número de las PDU a enviar para el mensaje de seguridad y el número de las PDU a enviar usando la primera configuración de cifrado después de enviar el mensaje de seguridad, como se muestra en la ecuación (1). La transmisión de las PDU con números de secuencia mayores o iguales que el número de secuencia de activación puede suspenderse hasta que se reciba un acuse de recibo del mensaje de seguridad.

[0050] La **FIG. 7** muestra un proceso 700 realizado por una entidad receptora, que puede ser el UE 110 para la transmisión de enlace descendente o la UTRAN 120 para la transmisión de enlace ascendente. La primera información se recibe y descifra en base a una primera configuración de cifrado (bloque 712). Se recibe un mensaje de seguridad con un momento de activación para una segunda configuración de cifrado, por ejemplo, durante un procedimiento de control del modo de seguridad (bloque 714). El mensaje de seguridad puede ser un mensaje de COMANDO DEL MODO DE SEGURIDAD recibido por el UE 110 en el enlace descendente, un mensaje de MODO DE SEGURIDAD COMPLETO recibido por la UTRAN 120 en el enlace ascendente, o algún otro mensaje. Se puede enviar un acuse de recibo del mensaje de seguridad antes del momento de activación (bloque 716). La segunda información se recibe después del mensaje de seguridad y antes del momento de activación (bloque 718). La segunda información, que puede comprender un mensaje de notificación de la medición, un mensaje de actualización del conjunto activo, etc., se descifra en base a la primera configuración de cifrado (bloque 720). La tercera información se recibe después del momento de activación (bloque 722) y se descifra en base a la segunda configuración de cifrado (bloque 724).

[0051] Las técnicas descritas en el presente documento pueden evitar la suspensión de la transmisión al mismo tiempo que aseguran que una entidad receptora pueda descifrar la información enviada usando las configuraciones de cifrado nuevas y antiguas. Las técnicas pueden mejorar el rendimiento, por ejemplo, reducir la probabilidad de una

caída de llamada durante un cambio en la configuración de cifrado en alta movilidad y/o malas condiciones de radio. Las técnicas pueden incluir una o más de las siguientes ventajas:

- permitir que el UE envíe mensajes de notificación de la medición y otros mensajes sensibles en cuanto al tiempo cuando la configuración de cifrado esté pendiente,

- permitir que la UTRAN envíe mensajes de actualización del conjunto activo y otros mensajes cuando la configuración de cifrado esté pendiente,

- evitar un escenario en el que el UE y la UTRAN necesiten mantener múltiples configuraciones de seguridad pendientes, y

- cumplir los procedimientos de seguridad W-CDMA descritos en el documento 3GPP TS 25.331.

[0052] La **FIG. 8** muestra un diagrama de bloques del UE 110 y la UTRAN 120. En el enlace ascendente, en el UE 110, un procesador de datos/señalización 810 procesa (por ejemplo, formatea, codifica y modula) información para enviar a la UTRAN 120 de acuerdo con una tecnología de radio (por ejemplo, W-CDMA) y genera segmentos de salida. Un transmisor (TMTR) 812 puede acondicionar (por ejemplo, convertir en analógico, filtrar, amplificar y aumentar en frecuencia) los segmentos de salida y generar una señal de enlace ascendente, que puede transmitirse a través de una antena 814. En la UTRAN 120, las señales de enlace inverso del UE 110 y otros UE se reciben a través de una antena 830 y se acondicionan (por ejemplo, se filtran, se amplifican, se disminuyen en frecuencia y se digitalizan) mediante un receptor (RCVR) 832 para obtener muestras. Un procesador de datos/señalización 834 procesa (por ejemplo, desmodula y descodifica) las muestras para obtener la información enviada por el UE 110 y otros UE.

[0053] En el enlace descendente, en la UTRAN 120, la información a enviar a los UE es procesada por el procesador de datos/señalización 834 y acondicionada adicionalmente por un transmisor 832 para generar una señal de enlace descendente, que se transmite a través de la antena 832. En el UE 110, la señal de enlace descendente desde la UTRAN 120 se recibe a través de la antena 814, acondicionada por un receptor 812, y procesada por el procesador de datos/señalización 810 para obtener la información enviada por la UTRAN 120 al UE 110.

[0054] Los controladores/procesadores 820 y 840 controlan el funcionamiento en el UE 110 y la UTRAN 120, respectivamente. Los procesadores 810, 820, 834 y/o 840 pueden implementar el proceso 600 en la FIG. 6 para la transmisión, el proceso 700 en la FIG. 7 para la recepción y/u otros procesos para prestar soporte a la comunicación con cifrado. Las memorias 822 y 842 almacenan datos y códigos de programa para el UE 110 y la UTRAN 120, respectivamente. La memoria 822 puede almacenar configuraciones de cifrado para el UE 110. La memoria 842 puede almacenar configuraciones de cifrado para el UE 110 y otros UE atendidos por la UTRAN 120. La UTRAN 120 se puede comunicar con otras entidades de red por medio de una unidad de comunicación (Com.) 844.

[0055] La FIG. 8 muestra un diagrama de bloques simplificado del UE 110 y la UTRAN 120. En general, el UE 110 y la UTRAN 120 pueden incluir un número cualquiera de procesadores, memorias, unidades de comunicación, etc.

[0056] Las técnicas descritas en el presente documento se pueden implementar mediante diversos medios. Por ejemplo, estas técnicas se pueden implementar en hardware, firmware, software o una combinación de los mismos. Para una implementación en hardware, las unidades de procesamiento usadas para llevar a cabo las técnicas en una entidad dada (por ejemplo, un UE o una UTRAN) pueden implementarse en uno o más circuitos integrados de aplicación específica (ASIC), procesadores de señales digitales (DSP), dispositivos de procesamiento digital de señales (DSPD), dispositivos lógicos programables (PLD), matrices de puertas programables *in situ* (FPGA), procesadores, controladores, microcontroladores, microprocesadores, dispositivos electrónicos, otras unidades electrónicas diseñadas para realizar las funciones descritas en el presente documento, un ordenador, o una combinación de los mismos.

[0057] Para una implementación de firmware y/o software, las técnicas pueden implementarse con módulos (por ejemplo, procedimientos, funciones, etc.) que realizan las funciones descritas en el presente documento. Los códigos de firmware y/o software pueden almacenarse en una memoria (por ejemplo, memoria 822 o 842 en la FIG. 8) y ejecutarse mediante un procesador (por ejemplo, procesador 820 o 840). La memoria puede implementarse dentro del procesador o externa al procesador.

[0058] Un aparato que implementa las técnicas descritas en el presente documento puede ser una unidad autónoma o puede formar parte de un dispositivo. El dispositivo puede ser (i) un circuito integrado (CI) autónomo, (ii) un conjunto de uno o más CI que pueden incluir CI de memoria para almacenar datos y/o instrucciones, (iii) un ASIC, tal como un módem de estación móvil (MSM), (iv) un módulo que puede estar integrado dentro de otros dispositivos, (v) un teléfono celular, un dispositivo inalámbrico, un microteléfono o una unidad móvil, (vi) etc.

[0059] La descripción previa de la divulgación se proporciona para permitir que cualquier experto en la técnica realice o use la divulgación. Diversas modificaciones de la divulgación resultarán fácilmente evidentes a los expertos en la técnica, y los principios genéricos definidos en el presente documento se pueden aplicar a otras variantes sin apartarse del alcance de la divulgación. Por tanto, la divulgación no está prevista para limitarse a los ejemplos descritos en el presente documento, sino que se le debe conceder el alcance más amplio consecuente con las reivindicaciones.

REIVINDICACIONES

1. Un procedimiento (600) que comprende:

enviar (612), desde una entidad transmisora (110, 120) a una entidad receptora (120, 110), una primera información usando una primera configuración de cifrado;

seleccionar (614), mediante la entidad transmisora durante un procedimiento de control del modo de seguridad, un momento de activación para una segunda configuración de cifrado;

enviar (616), desde la entidad transmisora a la entidad receptora, un primer mensaje de seguridad con el momento de activación;

enviar (618), desde la entidad transmisora a la entidad receptora, una segunda información usando la primera configuración de cifrado después de enviar el primer mensaje de seguridad y antes del momento de activación;

enviar (622), desde la entidad transmisora a la entidad receptora, una tercera información usando la segunda configuración de cifrado después del momento de activación; y

caracterizado por que la selección del momento de activación se basa en un retardo esperado a la hora de recibir un acuse de recibo para el primer mensaje de seguridad y las condiciones de radio actuales.

2. El procedimiento de la reivindicación 1, en el que la primera, segunda y tercera información y el primer mensaje de seguridad se envían en unidades de datos de protocolo, PDU, con números de secuencia secuenciales, y en el que la selección del momento de activación mediante la entidad transmisora comprende:

determinar, mediante la entidad transmisora, un número de secuencia de activación en base a un número de secuencia de una siguiente PDU a enviar, un número de PDU a enviar antes del primer mensaje de seguridad, un número de PDU a enviar para el primer mensaje de seguridad y un número de PDU a enviar usando la primera configuración de cifrado después de enviar el primer mensaje de seguridad, y

utilizar, mediante la entidad transmisora, el número de secuencia de activación como el momento de activación.

3. El procedimiento de la reivindicación 2, que comprende además:

suspender, mediante la entidad transmisora, el envío de las PDU con números de secuencia mayores o iguales que el número de secuencia de activación hasta que se reciba un acuse de recibo (620) del primer mensaje de seguridad.

4. Un aparato que comprende:

medios para enviar una primera información usando una primera configuración de cifrado a una entidad receptora;

medios para seleccionar, durante un procedimiento de control del modo de seguridad, un momento de activación para una segunda configuración de cifrado;

medios para enviar un primer mensaje de seguridad con el momento de activación a la entidad receptora;

medios para enviar, a la entidad receptora, una segunda información usando la primera configuración de cifrado después de enviar el primer mensaje de seguridad y antes del momento de activación;

medios para enviar, a la entidad receptora, una tercera información usando la segunda configuración de cifrado después del momento de activación; y

caracterizado por que la selección del momento de activación se basa en un retardo esperado a la hora de recibir un acuse de recibo para el primer mensaje de seguridad y las condiciones de radio actuales.

5. El aparato de la reivindicación 4, en el que la primera, segunda y tercera información y el primer mensaje de seguridad se envían en unidades de datos de protocolo, PDU, con números de secuencia secuenciales, y en el que los medios para seleccionar el momento de activación comprenden:

medios para determinar un número de secuencia de activación en base a un número de secuencia de una siguiente PDU a enviar, un número de PDU a enviar antes del primer mensaje de seguridad, un número de PDU a enviar para el primer mensaje de seguridad y un número de PDU a enviar usando la primera configuración de cifrado después de enviar el primer mensaje de seguridad, y

medios para usar el número de secuencia de activación como el momento de activación.

6. El aparato de la reivindicación 4, en el que los medios comprenden:

al menos un procesador (810, 820, 834, 840) configurado para enviar la primera información usando la primera configuración de cifrado, seleccionar el momento de activación para la segunda configuración de cifrado, enviar el primer mensaje de seguridad con el momento de activación, retardar una suspensión de las transmisiones que se producen después de recibir el acuse de recibo del primer mensaje de seguridad y antes del momento de activación, enviar la segunda información usando la primera configuración de cifrado después de enviar el primer mensaje de seguridad y antes del momento de activación, y enviar la tercera información usando el segundo configuración de cifrado después del momento de activación; y el aparato además comprende:

una memoria (822, 842) acoplada al al menos un procesador y configurada para almacenar las configuraciones de cifrado primera y segunda.

7. El aparato de la reivindicación 6, en el que el al menos un procesador está configurado para seleccionar el momento de activación de modo que sea una cantidad de tiempo particular después del final del envío del primer mensaje de seguridad.

8. El aparato de la reivindicación 4, en el que los medios para seleccionar el momento de activación están configurados para seleccionar el momento de activación en base a los mensajes pendientes a enviar usando la primera configuración de cifrado antes de enviar el primer mensaje de seguridad.

9. El aparato de la reivindicación 4, en el que la primera, segunda y tercera información y el primer mensaje de seguridad se envían en unidades de datos de protocolo, PDU, con números de secuencia secuenciales, y en el que los medios para seleccionar el momento de activación comprenden:

medios para seleccionar un número de secuencia de una PDU que es un número particular de las PDU después de una última PDU para el primer mensaje de seguridad como un número de secuencia de activación; y

medios para usar el número de secuencia de activación como el momento de activación.

10. El aparato de la reivindicación 9, que comprende además medios para suspender la transmisión de las PDU con números de secuencia mayores o iguales que el número de secuencia de activación hasta que se reciba el acuse de recibo del primer mensaje de seguridad.

11. El aparato de la reivindicación 4, que comprende además medios para recibir el acuse de recibo del primer mensaje de seguridad antes del momento de activación.

12. El aparato de la reivindicación 4, que comprende además medios para establecer el momento de activación a un momento de activación pendiente si existe la configuración de cifrado pendiente y un momento de activación pendiente asociado con la configuración de cifrado pendiente permite enviar los mensajes pendientes y el segundo mensaje de seguridad usando la primera configuración de cifrado.

13. El aparato de la reivindicación 4, en el que el al menos un mensaje comprende uno o más de un mensaje de notificación de la medición o un mensaje de actualización del conjunto activo, y en el que el primer mensaje de seguridad comprende uno o más de un mensaje de MODO DE SEGURIDAD COMPLETO enviado en el enlace ascendente o un mensaje de COMANDO DEL MODO DE SEGURIDAD enviado en el enlace descendente.

14. Un medio legible por ordenador que comprende instrucciones que, cuando se ejecutan en un procesador, hacen que el procesador realice el procedimiento de cualquiera de las reivindicaciones 1 a 3.

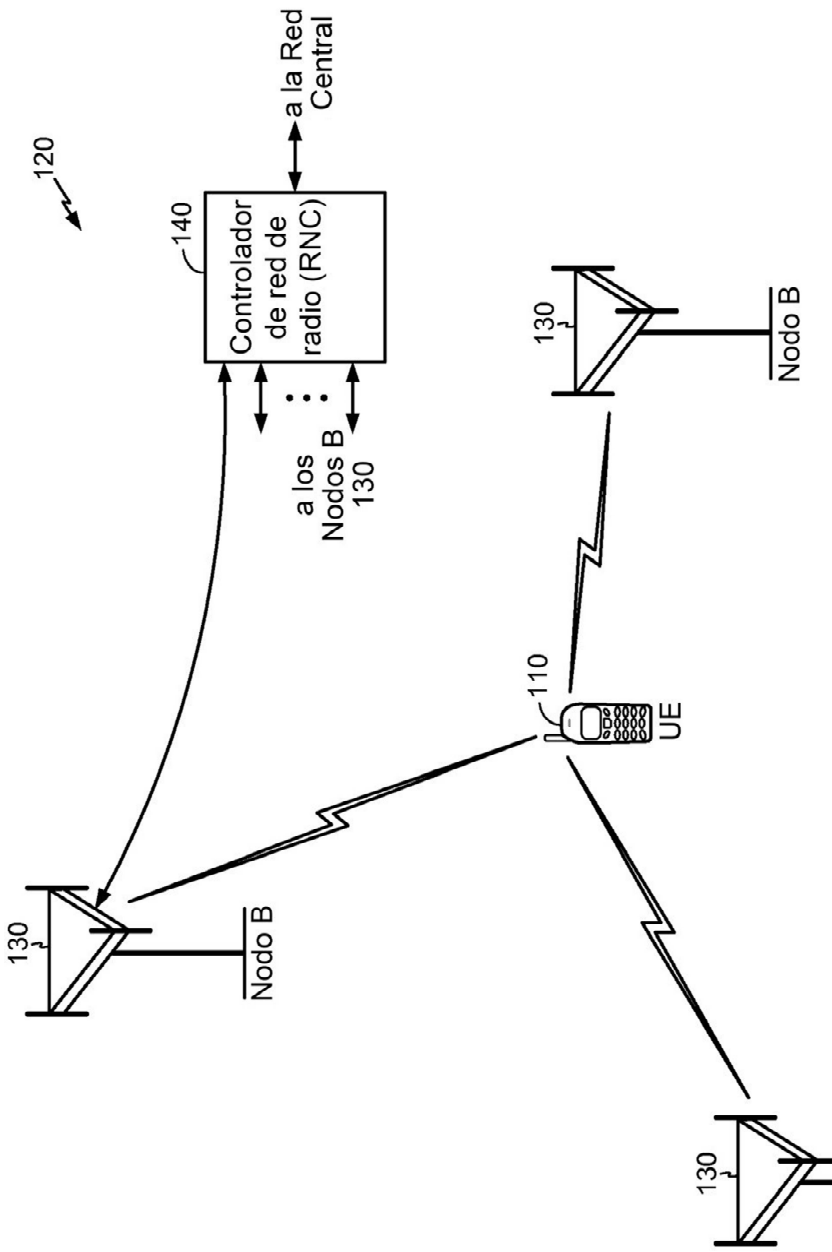
120
140
Controlador de red de radio (RNC)
a la Red Central
a los Nodos B 130
130
Nodo B
110
UE

FIG. 1

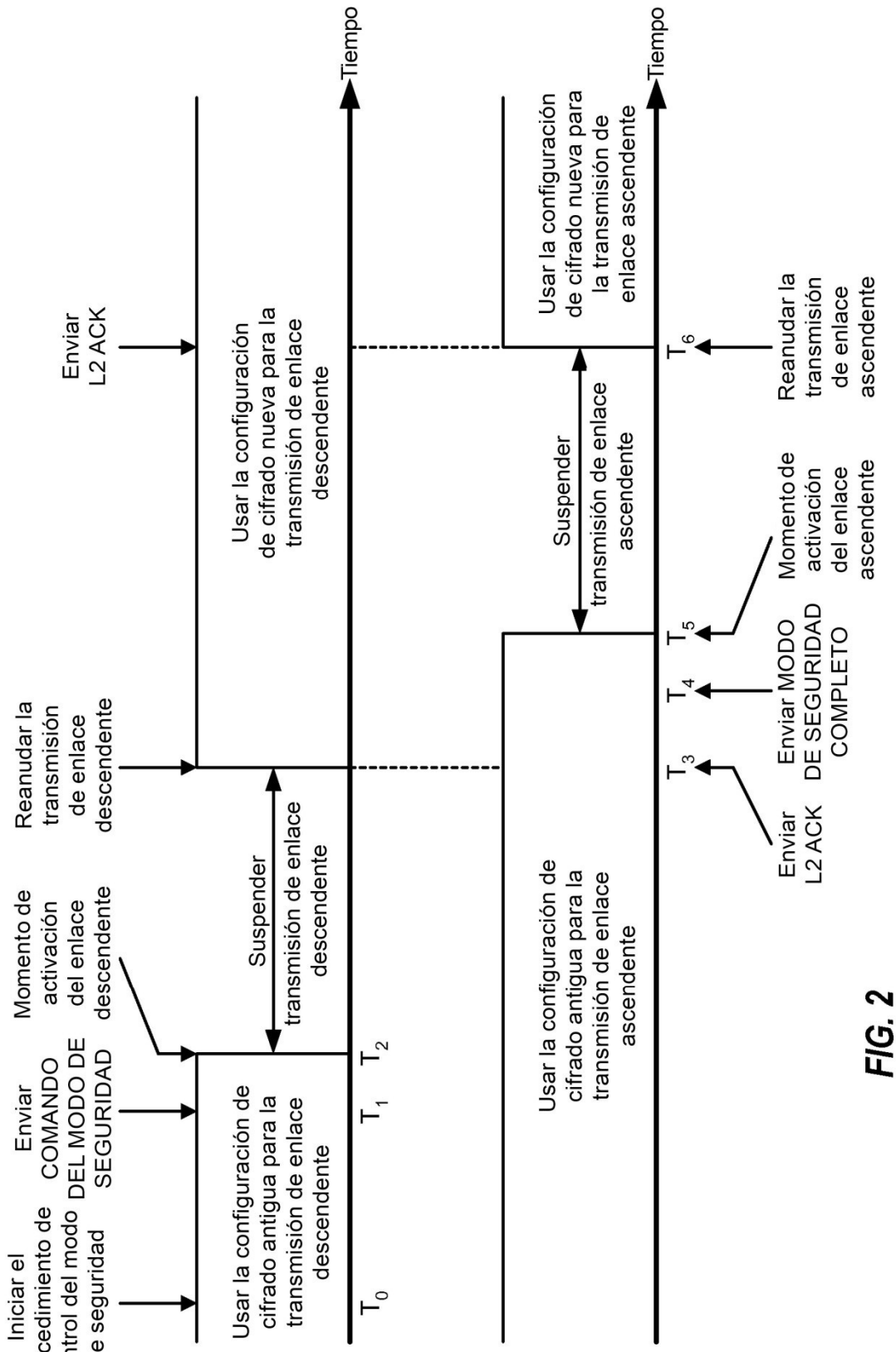
UTRAN
UE
Tiempo
Tiempo
Iniciar el procedimiento de control del modo de seguridad
Enviar COMANDO DEL MODO DE SEGURIDAD
Momento de activación del enlace descendente
Reanudar la transmisión de enlace descendente
Enviar L2 ACK
Usar la configuración de cifrado antigua para la transmisión de enlace descendente
Suspender transmisión de enlace descendente
Usar la configuración de cifrado nueva para la transmisión de enlace descendente
T0
T1
T2
Usar la configuración de cifrado antigua para la transmisión de enlace ascendente
Suspender transmisión de enlace ascendente
Usar la configuración de cifrado nueva para la transmisión de enlace ascendente
T3
T4
T5
T6
Enviar L2 ACK
Enviar MODO DE SEGURIDAD COMPLETO
Momento de activación del enlace ascendente
Reanudar la transmisión de enlace ascendente

FIG. 2

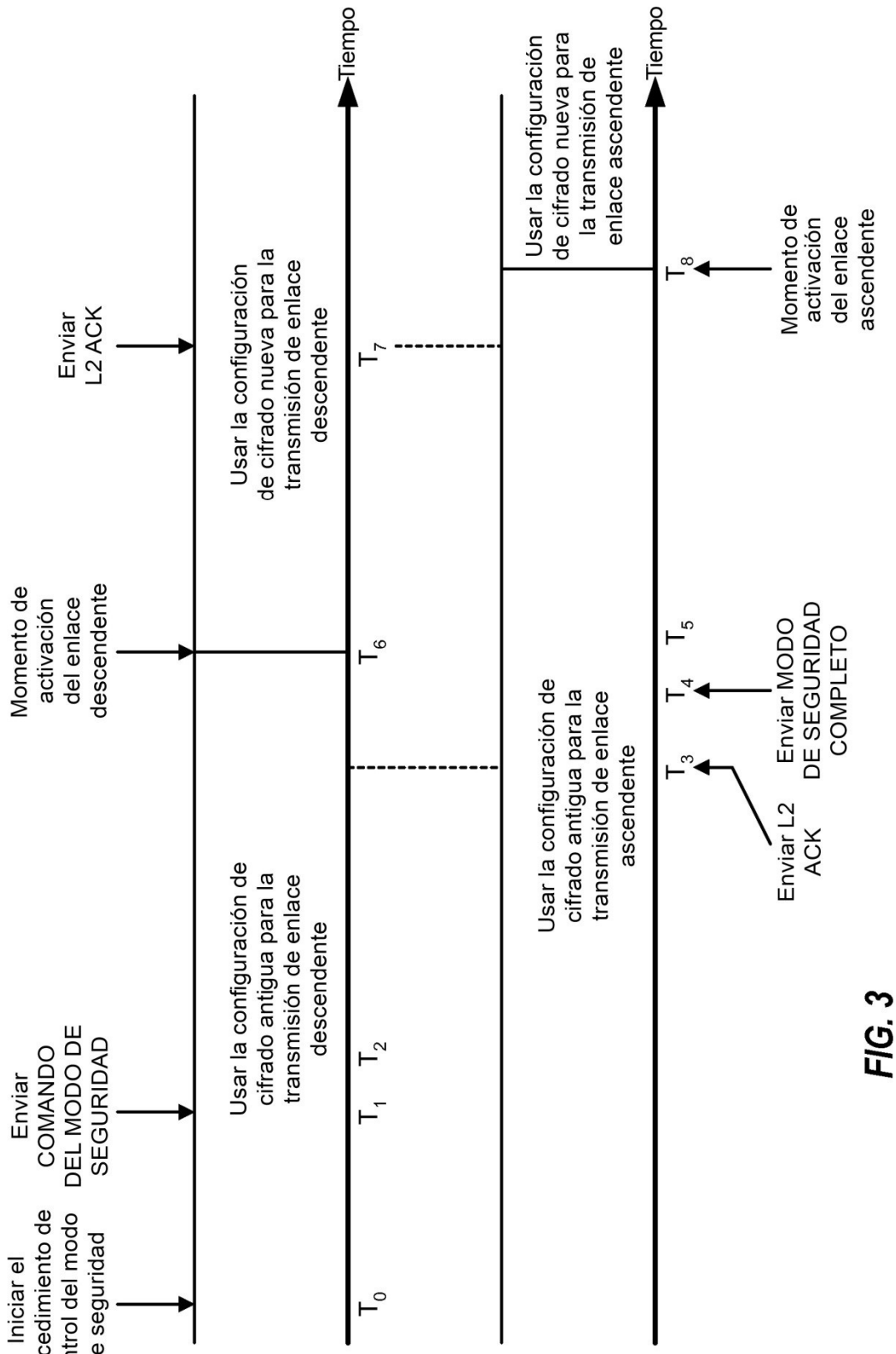
UTRAN
UE
Tiempo
Tiempo
Iniciar el procedimiento de control del modo de seguridad
Enviar COMANDO DEL MODO DE SEGURIDAD
Usar la configuración de cifrado antigua para la transmisión de enlace descendente
Momento de activación del enlace descendente
Enviar L2 ACK
Usar la configuración de cifrado nueva para la transmisión de enlace descendente
Usar la configuración de cifrado antigua para la transmisión de enlace ascendente
Enviar L2 ACK
Enviar MODO DE SEGURIDAD COMPLETO
Usar la configuración de cifrado nueva para la transmisión de enlace ascendente
Momento de activación del enlace ascendente
T0
T1
T2
T3
T4
T5
T6
T7
T8

FIG. 3

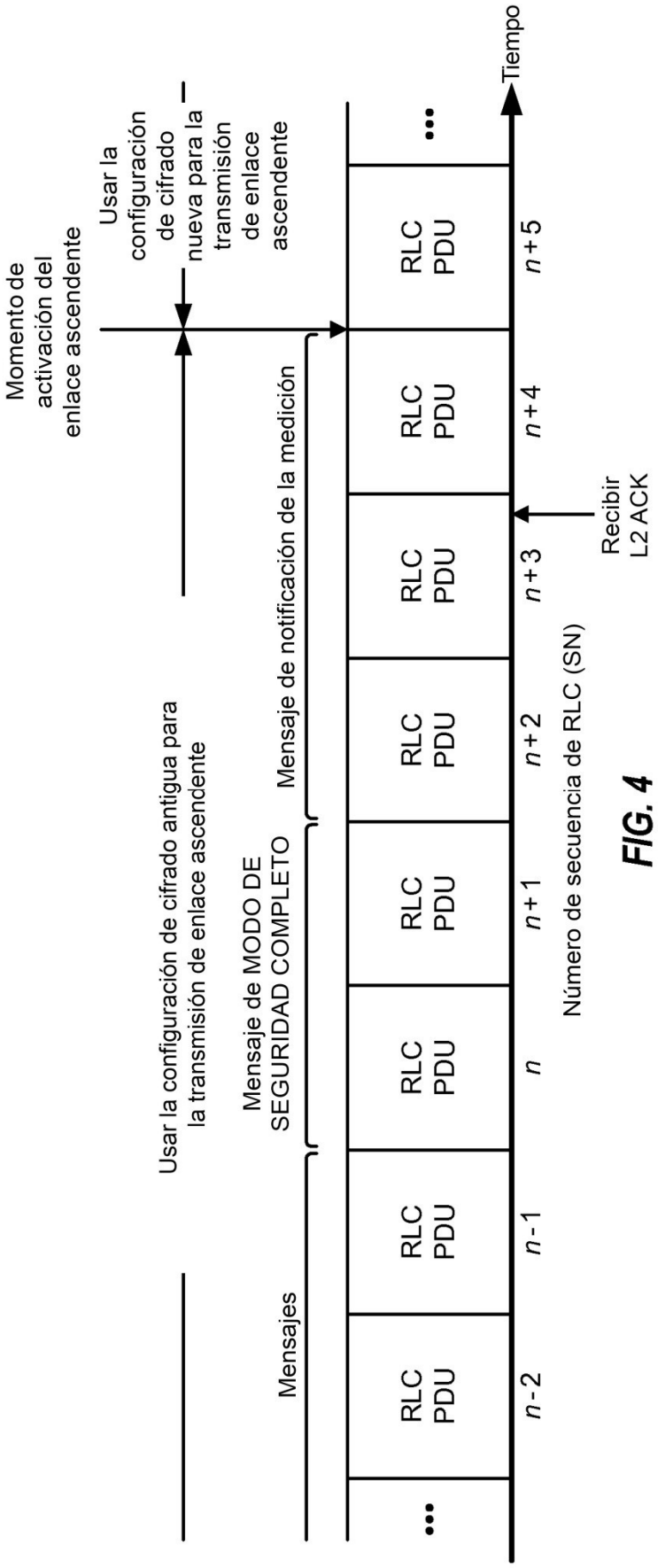
Momento de activación del enlace ascendente
Usar la configuración de cifrado nueva para la transmisión de enlace ascendente
Usar la configuración de cifrado antigua para la transmisión de enlace ascendente
Mensaje de MODO DE SEGURIDAD COMPLETO
Mensaje de notificación de la medición
Mensajes
RLC PDU
n-2
n-1
n
n+1
n+2
n+3
n+4
n+5
Recibir L2 ACK
Número de secuencia de RLC (SN)
Tiempo

FIG. 4

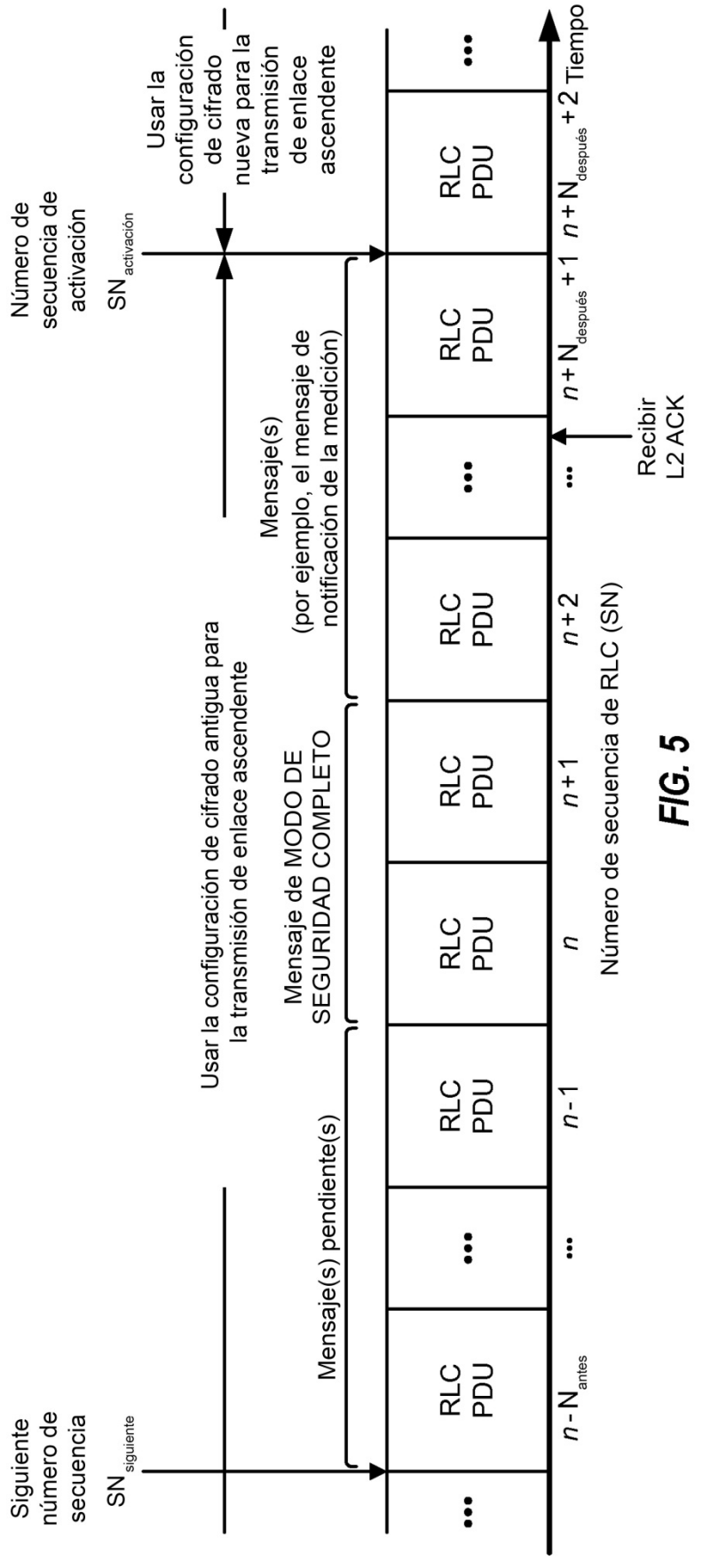
Siguiente número de secuencia
$SN_{siguiente}$
Número de secuencia de activación
$SN_{activación}$
Usar la configuración de cifrado nueva para la transmisión de enlace ascendente
Usar la configuración de cifrado antigua para la transmisión de enlace ascendente
Mensaje(s) pendiente(s)
Mensaje de MODO DE SEGURIDAD COMPLETO
Mensaje(s) (por ejemplo, el mensaje de notificación de la medición)
RLC PDU
$n - N_{antes}$
$n-1$
n
$n+1$
$n+2$
$n + N_{después} + 1$
$n + N_{después} + 2$
Número de secuencia de RLC (SN)
Recibir L2 ACK
Tiempo

FIG. 5

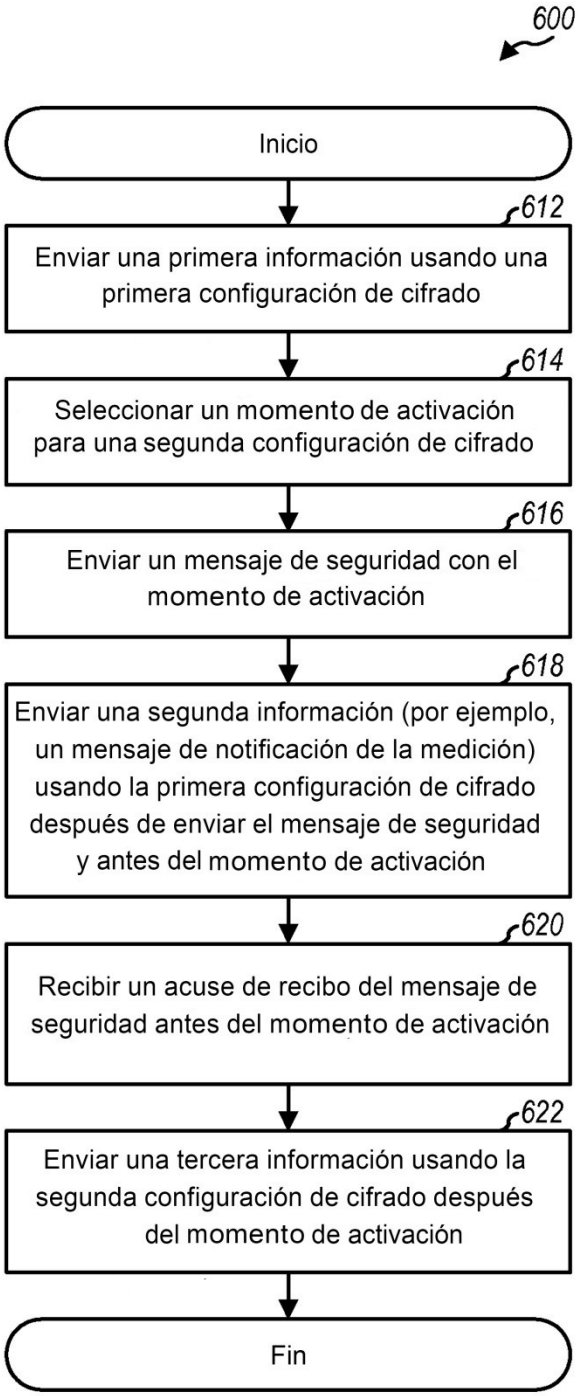
600
Inicio
612
Enviar una primera información usando una primera configuración de cifrado
614
Seleccionar un momento de activación para una segunda configuración de cifrado
616
Enviar un mensaje de seguridad con el momento de activación
618
Enviar una segunda información (por ejemplo, un mensaje de notificación de la medición) usando la primera configuración de cifrado después de enviar el mensaje de seguridad y antes del momento de activación
620
Recibir un acuse de recibo del mensaje de seguridad antes del momento de activación
622
Enviar una tercera información usando la segunda configuración de cifrado después del momento de activación
Fin

FIG. 6

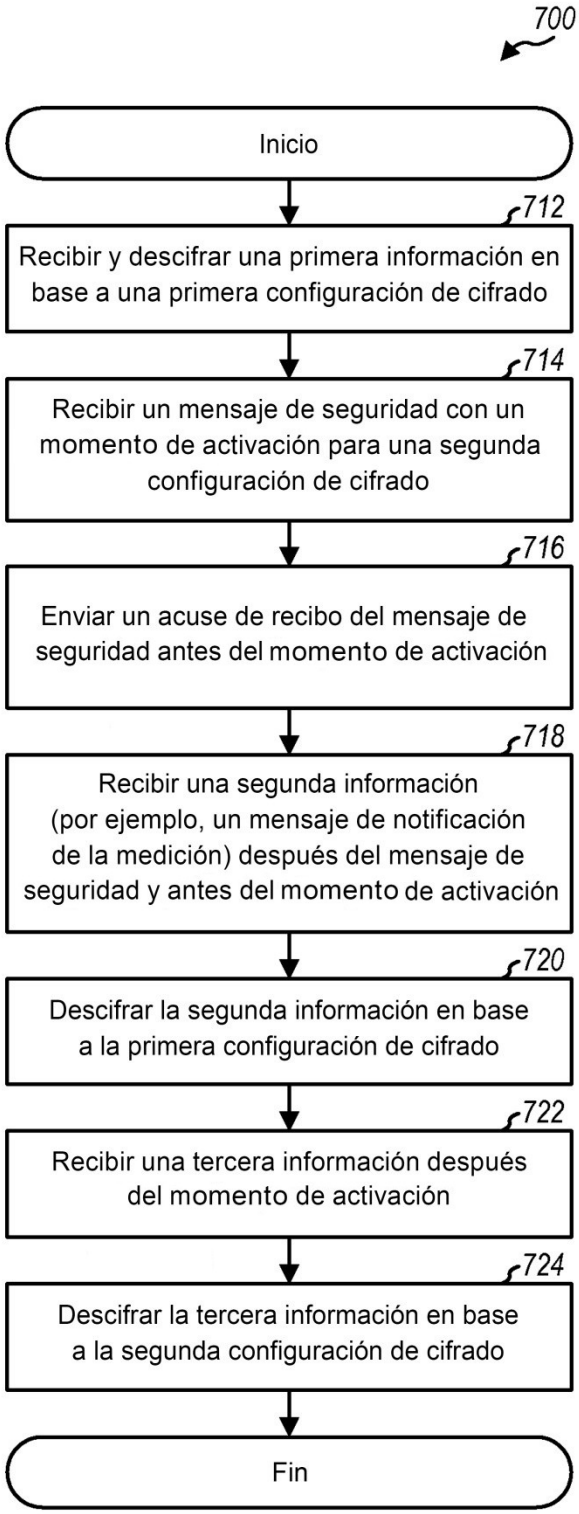
700
Inicio
712
Recibir y descifrar una primera información en base a una primera configuración de cifrado
714
Recibir un mensaje de seguridad con un momento de activación para una segunda configuración de cifrado
716
Enviar un acuse de recibo del mensaje de seguridad antes del momento de activación
718
Recibir una segunda información (por ejemplo, un mensaje de notificación de la medición) después del mensaje de seguridad y antes del momento de activación
720
Descifrar la segunda información en base a la primera configuración de cifrado
722
Recibir una tercera información después del momento de activación
724
Descifrar la tercera información en base a la segunda configuración de cifrado
Fin

FIG. 7

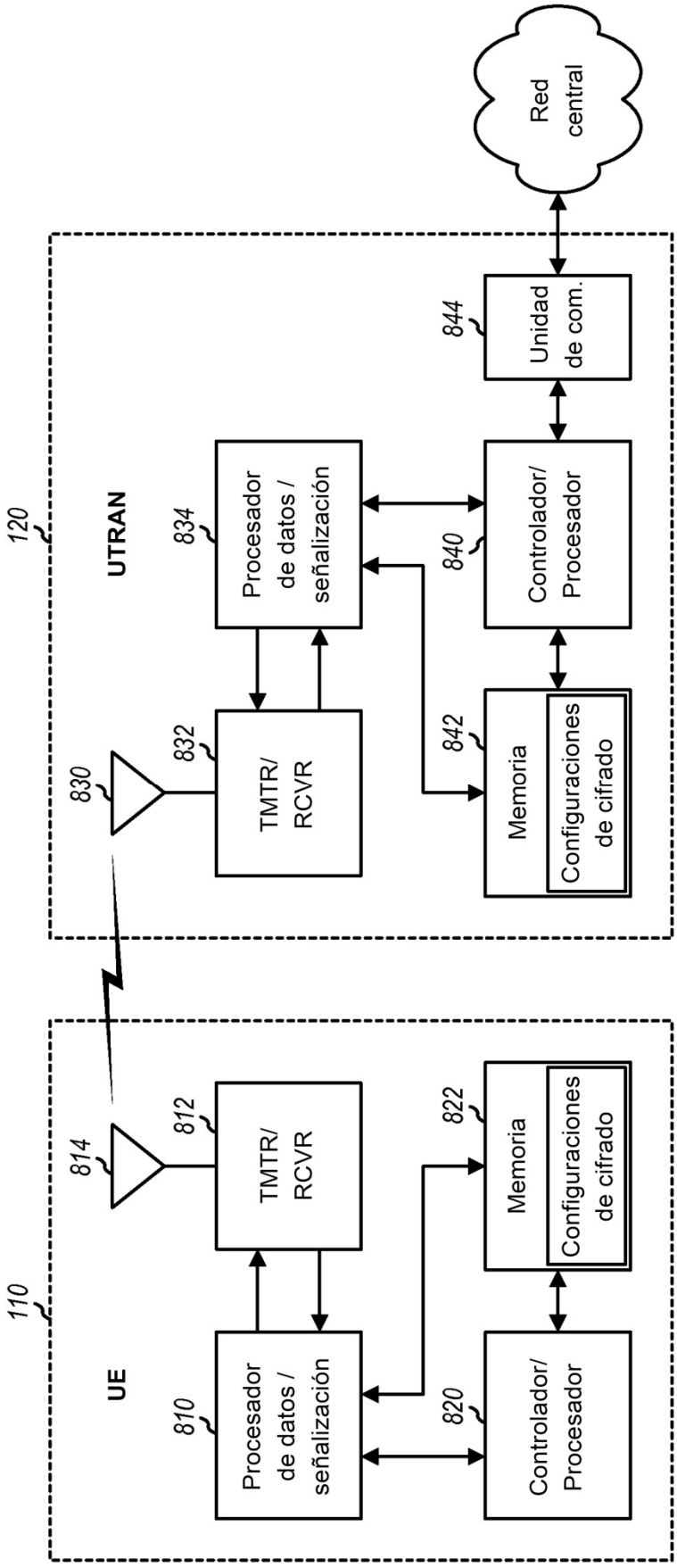
Red central
120
UTRAN
844
Unidad de com.
834
Procesador de datos / señalización
840
Controlador/ Procesador
830
832
TMTR/ RCVR
842
Memoria
Configuraciones de cifrado
110
UE
814
812
TMTR/ RCVR
822
Memoria
Configuraciones de cifrado
810
Procesador de datos / señalización
820
Controlador/ Procesador

FIG. 8