(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 268 121**

(51) Int. Cl.:
H04L 1/00 (2006.01)
H04L 12/56 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **02786310 .9**
(86) Fecha de presentación : **08.11.2002**
(87) Número de publicación de la solicitud: **1451963**
(87) Fecha de publicación de la solicitud: **01.09.2004**

(54) Título: **Reconfiguración de seguridad en un sistema universal de telecomunicaciones móviles.**

(30) Prioridad: **28.11.2001 US 333485 P**
30.09.2002 US 259435

(45) Fecha de publicación de la mención BOPI:
16.03.2007

(45) Fecha de la publicación del folleto de la patente:
16.03.2007

(73) Titular/es:
TELEFONAKTIEBOLAGET LM ERICSSON (publ)
164 83 Stockholm, SE

(72) Inventor/es: **Palm, Hakan;**
Johannesson, Regina;
Krishnarajah, Ainkaran y
Berggren, Anders

(74) Agente: **Ungría López, Javier**

DESCRIPCIÓN

Reconfiguración de seguridad en un sistema universal de telecomunicaciones móviles.

Solicitud de prioridad

Esta solicitud reivindica prioridad por la Solicitud de Patente Provisional de Estados Unidos número 60/333.485, presentada el 28 de noviembre de 2001.

Campo de la invención

La presente invención se refiere a comunicaciones del Sistema Universal de Telecomunicaciones Móviles (UMTS), y más en concreto, a las funciones de seguridad en un UMTS.

Antecedentes y resumen de la invención

Un sistema de comunicaciones ejemplar es el Sistema Universal de Telecomunicaciones Móviles (UMTS) descrito en la especificación 3GPP así como otros sistemas de comunicaciones. Una arquitectura ejemplar simplificada para un sistema UMTS se ilustra en la figura 1 e incluye un equipo de usuario (UE) 12 que comunica por una interface de aire/radio U_u con una red de acceso por radio (RAN) 14 denominada a veces una Red Terrestre de Acceso por Radio UMTS (UTRAN). La RAN 14 comunica con una o más redes centrales 16. En la figura 1, una red central de conmutación de circuitos 18 y una red central de conmutación de paquetes 20 comunican con la RAN 14 por respectivas interfaces I_u-PS.

Una ilustración más detallada de una UTRAN 22 se representa en la figura 2. La UTRAN 22 incluye uno o varios sistemas de red de radio (RNS) 24. Cada RN 24 incluye uno o más controladores de red de radio (RNC) 26. Los RNCs comunican por una interface I_{ur}. Cada RNC está acoplado a una o varias estaciones de base, cada una de las cuales se denomina en la UTRAN un nodo B 28. El RNC y cada nodo B comunican por una interface I_{ub}. Cada nodo B realiza comunicaciones de radio mediante una o más celdas con varios UEs. En la figura 2, cada de nodo B 28 se representa con tres celdas C1-C3.

La figura 3 muestra la arquitectura de protocolo de radio UTRAN con información más detallada respecto a la misma disponible en 3GPP TS25.301. La arquitectura de protocolo está dividida en cinco capas incluyendo una capa de aplicación, una capa de transporte, una capa de control de recurso de radio (RRC), una capa de enlace, y una capa física. El lado izquierdo de la pila de protocolo desde la capa RRC y debajo representa el plano de control donde se conducen las señales de control. El lado derecho de la pila de protocolo representa el plano de usuario donde se comunica el tráfico de usuario. La información se comunica a través de la UTRAN usando canales lógicos denominados portadoras de radio. En el plano de control, las portadoras de radio se denominan portadoras de radio de señal y podrían incluir, por ejemplo, portadoras de radio de señales 0-4. En el plano de usuario, las otras portadoras de radio, como las portadoras de radio 5-31, se utilizan para transportar el tráfico de usuario. Estas portadoras son transportadas después por canales de transporte físicos por la interface de capa física/radio. Más detalles relativos al servicio de portadora de acceso de radio proporcionado por la UTRAN se pueden hallar en 3GPP TS 23.107.

Aunque se ofrecen detalles con respecto a la UTRAN, existen otras redes de acceso de radio. Un ejemplo es la red de acceso de radio GSM/EDGE (GERAN) que se desarrolló a partir de GSM a la evolución a tasas de datos mejoradas para GSM (EDGE). Aunque la presente invención es aplicable en particular a la UTRAN, puede ser aplicada en cualquier RAN.

Las funciones de seguridad en un sistema de comunicaciones suministran algún tipo de confidencialidad y/o autenticación para una comunicación. En UMTS, una función de seguridad de confidencialidad ejemplar es el cifrado o la encriptación de los datos de usuario, y una función de seguridad de autenticación ejemplar es la protección de integridad de las señales de control. Las señales de control enviadas entre un equipo de usuario/estación de radio móvil y la red de radio son consideradas la información sensible cuya integridad debe ser protegida. Con respecto a la protección de integridad de las señales de control, se hace referencia a la especificación 3GPP TS 33.102, y en particular, a la sección 6.5 que se refiere a la integridad de enlace de acceso.

El cifrado/encriptación se pueden llevar a cabo para tráfico de usuario. El cifrado se lleva a cabo en el plano de usuario en la subcapa de control de enlace de radio (RLC) de la capa de enlace, es decir, si el modo RLC es reconocido o no reconocido, o en la subcapa de control de acceso de medios (Mac), es decir, si el modo es el modo transparente RLC. La protección/autenticación profesional de las señales de control se lleva a cabo en el plano de control en la capa RRC. Cuando se ha de establecer una conexión (que puede ser considerada como un tipo de canal lógico) con un equipo de usuario a través de la UTRAN, se lleva a cabo un procedimiento de establecimiento de modo de seguridad para proteger la integridad de los mensajes de control enviados entre el UE y la UTRAN. Los ejemplos de mensajes de señales de control incluyen los mensajes de búsqueda, mensajes de transferencia, la petición de conexión RRC, establecimiento y mensajes de liberación, los mensajes de información de difusión del sistema, etc.

Se puede utilizar algoritmos diferentes para cifrar/encriptar datos de usuario y para proteger la integridad de las señales de control. Un algoritmo de cifrado puede generar una clave de cifrado (CK). Un ejemplo de tal algoritmo

de cifrado es un algoritmo "f8" descrito en 3GPP TS 33.102. De forma semejante, un algoritmo de protección de integridad/autentificación puede generar una clave de protección de integridad (IK). Un ejemplo de tal algoritmo de protección de integridad es un algoritmo "f9" descrito en 3GPP TS 33.102. La pareja de "claves" generadas por los algoritmos de cifrado y protección de integridad se denomina a veces un "conjunto de claves". Recuérdese por la figura 1 que la UTRAN puede estar acoplada a diferentes redes centrales tal como una red de conmutación de circuitos y una red de conmutación de paquetes. Un par de claves para un dominio de conmutación de circuitos se puede denotar (CK_{cs}, IK_{cs}), y para el dominio de conmutación de paquetes (CK_{ps}, IK_{ps}).

Cuando un UE inicia una sesión (por ejemplo, una sesión multimedia), se establece una conexión de 3 de Control de Recurso de Radio (RRC) dentro de la UTRAN. Parte de ese establecimiento de conexión incluye un procedimiento de autentificación donde se establece una configuración de seguridad para un dominio de red central específico. La configuración de seguridad para un dominio de la red central puede ser desglosada en dos partes. Una primera parte de la configuración de seguridad es desde la red central a la UTRAN usando un mensaje de Orden de Modo de Seguridad de RANAP (véase 3GPP TS 25.413). Una segunda parte es desde la UTRAN al UE usando una Orden de Modo de Seguridad de RRC (véase 3GPP TS 25.331).

Un procedimiento ejemplar para establecer una configuración de seguridad entre la UTRAN y UE se ilustra en la figura 4. Inicialmente, la estación móvil/equipo de usuario establece una conexión RRC con un RNC sirviente (SRNC) en la UTRAN. Esta conexión es iniciada para un dominio de red central especial. Por ejemplo, la conexión podría soportar una aplicación de navegador de web que funcionaría en el UE, y por lo tanto, la conexión sería una red central de conmutación de paquetes. Durante el establecimiento de conexión de RRC, los valores de parámetro necesarios para establecer una configuración de seguridad inicial para la conexión son transferidos entre el UE y el SRNC al mismo tiempo que las capacidades de seguridad del UE. El SRNC guarda los valores de configuración de seguridad y las capacidades de seguridad de UE.

El UE envía un mensaje de capa de protocolo inicial 3 (L3) incluyendo su identidad de usuario, (por ejemplo, IMSI), para iniciar un establecimiento de conexión usando un registro de posición visitante (VLR) para una conexión de conmutación de circuitos o un nodo de soporte de GPRS sirviente (SGSN) para una conexión del tipo de dominio de conmutación de paquetes. Se llevan a cabo procedimientos de autenticación y generación de clave entre el VLR/SGSN y el UE donde se genera un par de claves de integridad y cifrado para la conexión y se guarda por el UE. El VLR/SGSN también determina qué algoritmos de integridad y cifrado se puede emplear: UIA significa algoritmo de integridad UMTS y UEA significa algoritmo de encriptación de UMTS. El VLR/SGSN envía a una Orden de Modo de Seguridad al SRNC para suministrar los algoritmos de integridad y encriptado permitidos (UIAs y UEAs) así como la clave de integridad (IK) y la clave de cifrado (CK).

El SRNC escoge un algoritmo de integridad y un algoritmo de encriptación apropiados y genera parámetros necesarios para los algoritmos seleccionados. Un ejemplo de tal parámetro es un valor aleatorio generado en la red (consúltese FRESH en la especificación 3GPP). El SRNC envía una Orden de Modo de Seguridad al UE que incluye el dominio de red central, el algoritmo de integridad seleccionado, y parámetros como el valor aleatorio. También se envía la salida/resultado del algoritmo de integridad seleccionado. Esa salida/resultado se designa MAC-I, de Código-Integridad de Autorización de Mensaje, y se genera como una función de la clave de integridad (IK), el mensaje cuya integridad ha de ser protegida, el número aleatorio, una dirección de señales (es decir, enlace ascendente o enlace descendente), y un valor de recuento correspondiente a un número de secuencia de mensaje (MSN) del mensaje RRC corriente. El UE verifica esta información que incluye generar el MAC-I usando los mismos parámetros, y reconoce que el modo de seguridad está completo en los mensajes 9, 10, y 11. De allí en adelante, el cifrado y el descifrado así como la autentificación de mensajes para esta conexión se llevan a cabo usando los parámetros de seguridad configurados.

El número de secuencia de mensaje corriente (MSN) para la protección de integridad se denomina en la especificación 3GPP el recuento-I. Para cada portadora de radio de seña 0-4 hay un valor de recuento-I por portadora de radio de señal de enlace ascendente y un recuento-I por portadora de radio de señal de enlace descendente. Recuento-I se compone de dos partes. Un número de secuencia corto que constituye los bits menos significativos del recuento es un número de secuencia RRC de cuatro bits (RRC SN) y está disponible en cada unidad de datos de paquetes RRC (PDU). El número de secuencia largo es un número de hipertrama RRC (RRC HFN) que se incrementa cada ciclo de número de secuencia RRC. El RRC HFN se inicializa en el mensaje 1 (valores START) como uno de los valores de parámetro de configuración de seguridad.

En consecuencia, las portadoras de radio de señal usadas para transferir mensajes de señales de los dominios de servicio de red central son protegidos en integridad por la clave de integridad del dominio de servicio de red central para el que tuvo lugar la negociación de modo de seguridad más reciente. Si se piden servicios adicionales, si los servicios se piden desde otra red central, desde la misma red de núcleo, o si se pide una conexión adicional, podría ser necesario cambiar la configuración de integridad de una conexión de señal en curso, de integridad ya protegida.

Un ejemplo de tal reconfiguración de seguridad sobre la interface de aire es un procedimiento de control de modo de seguridad de RRC descrito en 3GPPTS 25.331, sección 8.1.12, e ilustrado en la figura 5. El propósito de este procedimiento es iniciar/reiniciar el cifrado con una nueva configuración de cifrado para portadoras de radio de tráfico de datos, e iniciar o modificar la configuración de protección de integridad para todas las portadoras de radio de señales de control. Para iniciar o modificar la configuración de protección de integridad, la UTRAN envía una Orden de Modo

de Seguridad al UE. A la recepción de la Orden de Modo de Seguridad, el UE establece un valor de activación en la dirección de enlace ascendente, y se establece un valor de activación por la UTRAN en la dirección de enlace descendente para todas las portadoras de radio de señal. Se especifica un valor de activación para cada portadora de radio afectada. Este valor de activación indica efectivamente cuándo se deberá usar la nueva configuración de seguridad/integridad con las nuevas claves de integridad y cifrado.

En un acercamiento, el UE puede establecer el valor de activación de enlace ascendente para una portadora de acceso de radio correspondiente como el número de secuencia de mensaje RRC corriente (RRC $SN_{current}$) más una constante k. Recuérdese que el número de secuencia de mensaje RRC es el valor de cuatro bits usado para sellar cada mensaje RRC con un número. La constante, por ejemplo, puede ser determinada sobre la base de un número máximo de retransmisiones de una Actualización de Celda o un mensaje de Actualización de área de enrutamiento transmitido por el UE a la UTRAN. Tal mensaje de actualización es enviado en la dirección de enlace ascendente por el UE a la UTRAN en una portadora de radio de señal, por ejemplo, RB0. Este ajuste del valor de activación hasta que algún mensaje sea transmitido en el futuro significa que el UE enviará mensajes de actualización usando la configuración de seguridad antigua, incluyendo las claves de cifrado e integridad antiguas comenzando en el mensaje de número de secuencia corriente (RRC $SN_{current}$). La configuración antigua es usada hasta que se transmite un mensaje futuro que tenga el número de secuencia de mensaje de activación (RRC $SN_{current}$ + k). Solamente cuando el número de secuencia de mensaje llegue a (RRC $SN_{current}$ + k), se aplicará la nueva configuración de seguridad. Poniendo el número de activación a algún número de secuencia de mensaje futuro, el UE puede enviar las actualizaciones de celda y los otros mensajes a la UTRAN usando la configuración de seguridad antigua aunque esté teniendo lugar la reconfiguración de seguridad. Los mensajes de actualización de celda son particularmente importantes, especialmente para un equipo de usuario que se desplaza rápidamente, para asegurar que la ubicación corriente del móvil sea conocida por la UTRAN.

Por lo tanto, el beneficio de este procedimiento de configuración de seguridad es que la actualización de celda y los otros mensajes importantes pueden ser enviados con la configuración de seguridad antigua con el propósito de que la UTRAN pueda recibir tales mensajes mientras tiene lugar el proceso de reconfiguración de seguridad. Por desgracia, una desventaja de este acercamiento es que el mecanismo para indicar el uso de la nueva configuración de seguridad es imperfecto.

El problema es que el UE tiene que enviar un cierto número de mensajes de ACTUALIZACIÓN DE CELDA antes de usar la nueva configuración de seguridad y de que se libere la antigua configuración de seguridad. En el ejemplo anterior, ese tiempo es cuando el mensaje corriente recibido en la UTRAN del UE tiene un número de secuencia de mensaje igual a RRC $SN_{current}$ + k. Este acercamiento supone que el UE se está moviendo entre bastantes celdas de manera que las k ACTUALIZACIONES DE CELDA tendrán lugar en un período de tiempo relativamente breve. Para un UE no móvil o que se desplaza lentamente, es probable que tal número de activación de mensajes de actualización de celda no sea enviado en un período de tiempo razonable (si lo es). Como resultado, la nueva configuración de seguridad, por ejemplo, para un UE nuevo a la conexión de red central, no se implementará y el nuevo servicio o conexión pedido no se suministrará.

La presente invención proporciona una solución para el problema antes identificado en un método mejorado para proteger la seguridad de una comunicación entre una radio móvil y una red de acceso de radio (RAN). Se establece una conexión a través de la RAN para soportar una comunicación con la radio móvil. La conexión está configurada con una primera configuración de seguridad. Uno o más mensajes son enviados por la conexión que usa la primera conexión de seguridad, teniendo cada mensaje un número de secuencia de mensaje. Cuando se determina que hay que configurar la conexión a una segunda configuración de seguridad, se establece un número de secuencia de mensaje de activación asociado con la reconfiguración. Cuando el proceso de reconfiguración está completo y segunda configuración de seguridad ha de ser activada, se envía el mensaje siguiente por la conexión con el número de secuencia de mensaje de activación. Hasta ese tiempo y durante la reconfiguración, cuando la radio móvil transmite un mensaje con un número de secuencia de mensaje más bajo que el número de secuencia de mensaje de activación a la RAN, usa la primera configuración de seguridad. Un ejemplo de tal mensaje es un mensaje de actualización de celda o un mensaje de actualización de área.

La primera configuración de seguridad corresponde, por ejemplo, a una primera conexión relacionada con la sesión que implica la radio móvil, y la segunda configuración de seguridad podría corresponder, por ejemplo, a una segunda conexión asociada con la sesión. En una sesión multimedia, la primera conexión podía estar relacionada con un tipo de medios y la segunda conexión con otro tipo.

La configuración de seguridad podría referirse a la protección de integridad de un mensaje, donde el mensaje incluye las señales de control relacionadas con la conexión. La primera configuración de seguridad podría incluir una primera clave de protección de integridad usada para autentificar las señales de control. La segunda configuración de seguridad incluye una segunda clave de protección de integridad. La configuración de seguridad también podría referirse a la protección de confidencialidad de la conexión. Por ejemplo, la primera configuración de seguridad incluye una primera clave de encriptado usada para encriptar tráfico de datos asociado con la conexión, y la segunda configuración de seguridad incluye una segunda clave de encriptación usada para encriptar el tráfico de datos.

El número de secuencia de mensaje de activación corresponde a un número de secuencia de mensaje futuro que es más grande que el número de mensaje próximo en la secuencia de mensajes. En una realización no limitativa ejemplar, el número de secuencia de mensaje de activación se establece usando el número máximo de retransmisiones de un mensaje. El número de secuencia de mensaje de activación es enviado con el mensaje próximo a la terminación de la operación de reconfiguración, incluso cuando el número de mensajes de activación no ha sido transmitido al tiempo en que la reconfiguración de seguridad todavía no está completa. De este modo, se evitan los retardos innecesarios o indefinidos asociados con la reconfiguración de seguridad.

Breve descripción de los dibujos

Los anteriores y otros objetos, características, y ventajas de la presente invención se pueden entender más fácilmente con referencia a la siguiente descripción tomada en unión con los dibujos acompañantes.

La figura 1 ilustra un diagrama de bloque simplificado de un sistema de comunicaciones UMTS ejemplar en el que se podría emplear la presente invención.

La figura 2 ilustra los detalles adicionales de un tipo UTRAN de red de acceso de radio.

La figura 3 ilustra protocolos varios usados en la UTRAN para establecer una conexión con una radio móvil.

La figura 4 ilustra un diagrama de señales de establecimiento de autentificación y conexión.

La figura 5 ilustra un diagrama de señales de reconfiguración de seguridad.

La figura 6 ilustra procedimientos ejemplares en forma de diagrama de flujo para implementar una realización ejemplar de la presente invención.

Las figuras 7A y 7B ilustran diagramas de bloques funcionales simplificados de un equipo de usuario en un controlador de la red de radio.

Y la figura 8 ilustra un diagrama de señales para implementar una reconfiguración de seguridad de conformidad con una realización detallada, ejemplar y no limitativa de la presente invención.

Descripción detallada

En la descripción siguiente, a los efectos de explicación y no de limitación, se exponen detalles específicos, como las realizaciones especiales, los procedimientos, técnicas, etcétera, con el fin de ofrecer una comprensión minuciosa de la presente invención. Sin embargo, será evidente a los expertos en la materia que la presente invención se puede llevar a la práctica en otras realizaciones que se apartan de estos detalles específicos. Por ejemplo, aunque la presente invención se describe en una aplicación ejemplar para sistemas UMTS, la presente invención se podría emplear en cualquier sistema de radio celular.

En algunos casos, las descripciones detalladas de métodos conocidos, interfaces, dispositivos, y técnicas de señalización se omiten para no oscurecer la descripción de la presente invención con detalles superfluos. Además, los bloques funcionales individuales se representan en algunas figuras. Los expertos en la materia apreciarán que las funciones puedan ser implementadas usando circuitos de equipo físico individuales, usando software que funcione en unión con un microprocesador digital adecuadamente programado o ordenador de propósito general, usando un circuito integrado específico de aplicación (ASIC), y/o usando uno o más procesadores de señales digitales (PSD).

La presente invención se puede implementar en cualquier sistema de comunicaciones de radio que incluya una red de acceso de radio. Con respecto a esto, se hace referencia ahora al diagrama de flujo ilustrado en la figura 6 que muestra un conjunto de procedimientos ejemplares no restrictivos para implementar la presente invención. Inicialmente, se establece una conexión a través de la red de acceso de radio para soportar una comunicación con un equipo de usuario (paso S1). La conexión se configura usando una primera configuración de seguridad (paso S2). Se envía uno o más mensajes por la conexión usando la primera configuración de seguridad. Cada mensaje tiene su propio número de secuencia de mensaje (MSN), es decir MSN = 1, 2, 3, ... (paso S3). Se determina que hay que reconfigurar la conexión (o una conexión adicional para una sesión de multimedia que implica el equipo de usuario) a una segunda configuración de seguridad (paso S4). Se establece un número de secuencia de mensaje de activación a los efectos de la reconfiguración de seguridad (paso S5). Cuando la segunda configuración de seguridad está lista para ser aplicada, se envía un mensaje siguiente usando el número de secuencia de mensaje de activación (paso S6).

En otras palabras, siempre que la segunda configuración de seguridad está lista para la activación, no se usa el número de mensaje en secuencia normal para el mensaje siguiente. En cambio, el número de secuencia de mensaje de activación se usa para indicar que el UE y la RAN deben enviar los mensajes usando ahora la segunda configuración de seguridad. Hasta el envío de ese mensaje que incluye el número de secuencia de mensaje de activación, los mensajes son enviados entre el UE y la RAN usando la primera configuración de seguridad. De este modo, los mensajes importantes, como mensajes de actualización de celda o mensajes de actualización de área, pueden ser enviados, por ejemplo, del UE a la RAN para actualizar la posición del UE durante el tiempo en que está teniendo lugar el proceso

de configuración de seguridad. Por otro lado, la presente invención evita retardos excesivos al activar la segunda configuración de seguridad enviando el número de secuencia de mensaje de activación con el mensaje próximo enviado después de terminar el proceso de reconfiguración.

Otro ejemplo más detallado de la presente invención se describirá ahora en el contexto de un sistema UMTS en el que la red de acceso de radio corresponde a un UTRAN como se ilustra en las figuras 2 y 3. En el diagrama de bloques simplificado de la figura 7A, el equipo de usuario 12 incluye circuitería de procesado de datos 30 acoplado a la circuitería radio transceptora 32, que a su vez está acoplada a una antena 34. La circuitería de procesado de datos 30 efectúa las funciones para implementar las varias operaciones de configuración de seguridad y reconfiguración asociadas con la presente invención. La figura 7B ilustra un controlador de red de radio simplificado 26 de la UTRAN. El RNC 26 incluye la circuitería de procesado de datos 40 acoplada a varias interfaces incluyendo una interface 42 a las redes centrales, una interface 44 para Bs de nodo, y una interface 46 a otros RNCs en la UTRAN. La circuitería de procesado de datos 40 lleva a cabo funciones para implementar varias operaciones de configuración y reconfiguración de seguridad con la presente invención.

Se dirige la atención al diagrama de señales ejemplar mostrado en la figura 8 para reconfigurar una configuración de seguridad para una conexión establecida entre el UE y la UTRAN. Se supone en el diagrama que se establece una conexión que implica el UE y que tiene lugar una configuración de seguridad inicial para la conexión. En el primer bloque funcional indicado para el UE, el UE pone a cero el número de secuencia de mensaje de control de recurso de radio de enlace ascendente para varias portadoras de radio incluyendo RB0, 1, 2, 3, y 4. El UE y la UTRAN cuentan el número de mensajes enviados a partir de este valor inicializado para cada portadora de radio usando un valor de recuento-I MSN para cada portadora. El valor MSN inicial es cero. El UE también pone una constante, etiquetada aquí N302, igual a algún valor mostrado como 3. En este ejemplo, esa constante es igual a varias retransmisiones permitidas del mensaje de actualización de celda/actualización de área de enrutamiento UTRAN (URA).

Cuando es necesaria una operación de reconfiguración de seguridad, la UTRAN envía al UE una Orden de Modo de Seguridad, que es reconocida por el UE en un reconocimiento de Orden de Modo de Seguridad de capa 2. Después de dicho reconocimiento, el UE pone un número de secuencia de mensaje de activación para cada portadora de enlace ascendente con el ejemplo indicado en la figura para RB0 = 0 + N302 + 1 = 4. El UE envía un mensaje de Modo de Seguridad completo a la UTRAN. Mientras espera que la UTRAN reconozca el mensaje de Modo de Seguridad completo que indica que el proceso de reconfiguración ha terminado, el UE envía un mensaje de actualización de celda a la UTRAN usando la configuración de seguridad inicial. Después de enviar el mensaje de actualización de celda, el recuento MSN de enlace ascendente para RB0 se incrementa a 1. Otro mensaje de actualización de celda es enviado por el UE antes de que la UTRAN reconozca el mensaje de Modo de Seguridad completo usando la configuración de seguridad inicial.

Cuando el UE recibe el reconocimiento del mensaje de Modo de Seguridad completo de la UTRAN, el UE sabe que la UTRAN recibió el mensaje de Modo de Seguridad completo que indica que la reconfiguración de seguridad está completa. En este momento el UE y UTRAN son libres para usar la nueva configuración de seguridad. Por lo tanto, el UE pone el recuento MSN, que está actualmente en 2, al número de secuencia de mensaje activado, que es 4. Envía el mensaje siguiente, un mensaje de actualización de celda, usando la nueva configuración de seguridad. Dado que el mensaje incluye el recuento RRC MSN establecido en el MSN de activación, la UTRAN también sabe usar la nueva configuración de seguridad.

Aunque la presente invención se ha descrito con respecto a las realizaciones especiales, los expertos en la materia reconocerán que la presente invención no se limita a estas realizaciones ejemplares específicas. Diferentes formatos, realizaciones, y adaptaciones además de los mostrados y descritos, así como muchas variaciones, modificaciones, y disposiciones equivalentes, también se pueden usar para implementar la invención. Por lo tanto, aunque que la presente invención se ha descrito en relación con sus realizaciones preferidas, se ha de entender que esta descripción es solamente ilustrativa y ejemplar de la presente invención.

REIVINDICACIONES

1. Un método para proteger la seguridad de una comunicación entre una radio móvil y una red de acceso de radio (RAN) incluyendo establecer una conexión a través de la RAN para soportar una comunicación con la radio móvil, **caracterizado** por:

configurar la conexión con una primera configuración de seguridad;

enviar uno o más mensajes por la conexión usando la primera conexión de seguridad, teniendo cada mensaje un número de secuencia de mensaje;

determinar la necesidad de reconfigurar la conexión a una segunda configuración de seguridad;

poner un número de secuencia de mensaje de activación relacionado con la reconfiguración; y

cuando la segunda configuración de seguridad ha de ser activada, enviar un mensaje siguiente con el número de secuencia de mensaje de activación.

2. El método de la reivindicación 1, donde cuando la segunda configuración de seguridad es activada, los mensajes siguientes son enviados usando la segunda configuración de seguridad.

3. El método de la reivindicación 2, donde el mensaje siguiente es enviado usando la segunda configuración de seguridad.

4. El método de la reivindicación 1, donde durante la reconfiguración, la radio móvil transmite un mensaje con un número de secuencia de mensaje más bajo que el número de secuencia de mensaje de activación a la RAN usando la primera configuración de seguridad.

5. El método de la reivindicación 4, donde el mensaje transmitido por la radio móvil es un mensaje de actualización de celda o un mensaje de actualización de área.

6. El método de la reivindicación 1, donde la primera configuración de seguridad corresponde a una primera conexión asociada con una sesión que implica la radio móvil y la segunda configuración de seguridad corresponde a una segunda conexión asociada con la sesión.

7. El método de la reivindicación 6, donde la sesión es una sesión multimedia, y la primera conexión se refiere a un tipo de medios y la segunda conexión se refiere a otro tipo de medios.

8. El método de la reivindicación 1, donde la configuración de seguridad se refiere a la protección de integridad del mensaje.

9. El método de la reivindicación 8, donde el mensaje incluye un mensaje de control relacionado con la conexión.

10. El método de la reivindicación 9, donde la primera configuración de seguridad incluye una primera clave de protección de integridad usada para autentificar la señal de control, y la segunda configuración de seguridad incluye una segunda clave de protección de integridad usada para autentificar la señal de control.

11. El método de la reivindicación 1, donde la configuración de seguridad se refiere a la protección de confidencialidad de la comunicación, y la comunicación incluye tráfico de datos relacionado con la conexión.

12. El método de la reivindicación 11, donde la primera configuración de seguridad incluye una primera clave de encriptado usada para encriptar el tráfico de datos, y la segunda configuración de seguridad incluye una segunda clave de encriptado usada para encriptar el tráfico de datos.

13. El método de la reivindicación 1, incluyendo además:

poner el número de secuencia de mensaje de activación usando un número máximo de retransmisiones de un mensaje.

14. El método de la reivindicación 13, donde el mensaje es un mensaje de actualización de celda o un mensaje de actualización de área transmitido por la radio móvil a la RAN.

15. El método de la reivindicación 1, donde el número de secuencia de mensaje de activación corresponde a un número de secuencia de mensaje futuro más grande que un número de secuencia de mensaje próximo.

16. El método de la reivindicación 1, donde el paso de enviar se lleva a cabo para aplicar la segunda configuración de seguridad incluso cuando el número de secuencia de mensaje de activación de los mensajes no ha sido transmitido al tiempo que la reconfiguración de seguridad ha terminado.

17. Una radio móvil (12) configurada para comunicar con una entidad mediante una conexión establecida a través de una red de acceso de radio (RAN) (14), comprendiendo circuitería transceptora de radio (32) y circuitería de procesado de datos (30), **caracterizada** porque la circuitería de procesado de datos (30) está configurada para llevar a cabo las tareas siguientes:

establecer una primera configuración de seguridad para la conexión;

enviar uno o más mensajes por la conexión usando la primera conexión de seguridad, teniendo cada mensaje un número de secuencia de mensaje;

determinar si la conexión ha de ser reconfigurada a una segunda configuración de seguridad;

determinar un número de secuencia de mensaje de activación asociado con la reconfiguración; y

cuando la segunda configuración de seguridad ha de ser activada, enviar un mensaje siguiente con el número de secuencia de mensaje de activación.

18. La radio móvil de la reivindicación 17, donde cuando la segunda configuración de seguridad es activada, los mensajes siguientes enviados y recibidos por la radio móvil usan la segunda configuración de seguridad.

19. La radio móvil de la reivindicación 18, donde la circuitería de procesado de datos (30) está configurada para transmitir el mensaje siguiente usando la segunda configuración de seguridad.

20. La radio móvil de la reivindicación 19, donde durante la reconfiguración, la circuitería de procesado de datos (30) está configurada para transmitir un mensaje con un número de secuencia de mensaje más bajo que el número de secuencia de mensaje de activación a la RAN usando la primera configuración de seguridad.

21. La radio móvil de la reivindicación 20, donde el mensaje transmitido por la radio móvil es un mensaje de actualización de celda o un mensaje de actualización de área.

22. La radio móvil de la reivindicación 17, donde la primera configuración de seguridad corresponde a una primera conexión asociada con una sesión que implica la radio móvil y la segunda configuración de seguridad corresponde a una segunda conexión asociada con la sesión.

23. La radio móvil de la reivindicación 22, donde la sesión es una sesión multimedia, y la primera conexión se refiere a un tipo de medios y la segunda conexión se refiere a otro tipo de medios.

24. La radio móvil de la reivindicación 17, donde la configuración de seguridad se refiere a la protección de integridad del mensaje, y el mensaje incluye un mensaje de control relacionado con la conexión.

25. La radio móvil de la reivindicación 24, donde la primera configuración de seguridad incluye una primera clave de protección de integridad usada para autentificar la señal de control, y la segunda configuración de seguridad incluye una segunda clave de protección de integridad usada para autentificar la señal de control.

26. La radio móvil de la reivindicación 17, donde la configuración de seguridad se refiere a la protección de confidencialidad de la comunicación, y la comunicación incluye tráfico de datos relacionado con la conexión.

27. La radio móvil de la reivindicación 26, donde la primera configuración de seguridad incluye una primera clave de encriptado usada para encriptar el tráfico de datos, y la segunda configuración de seguridad incluye una segunda clave de encriptado usada para encriptar el tráfico de datos.

28. La radio móvil de la reivindicación 17, donde la circuitería de procesado de datos (30) está configurada para poner el número de secuencia de mensaje de activación usando un número máximo de retransmisiones de un mensaje.

29. La radio móvil de la reivindicación 28, donde el mensaje es un mensaje de actualización de celda o un mensaje de actualización de área transmitido por la radio móvil a la RAN.

30. La radio móvil de la reivindicación 17, donde el número de secuencia de mensaje de activación corresponde a un número de secuencia de mensaje futuro más grande que un número de secuencia de mensaje próximo.

31. La radio móvil de la reivindicación 17, donde la circuitería de procesado de datos (30) está configurada para aplicar la segunda configuración de seguridad incluso cuando el número de activación de los mensajes no ha sido transmitido cuando la reconfiguración de seguridad ha terminado.

32. Un nodo (26) de red de acceso de radio (RAN) para establecer una conexión de radio móvil (12) por la RAN (14) para soportar comunicaciones que implican la radio móvil, **caracterizado** por circuitería de procesado de datos (40) configurada para efectuar las funciones siguientes:

establecer un primer parámetro de configuración de seguridad para la conexión;

enviar o recibir uno o más mensajes por la conexión usando la primera conexión de seguridad, teniendo cada mensaje un número de secuencia de mensaje;

determinar si la conexión ha de ser reconfigurada a una segunda configuración de seguridad;

enviar un mensaje de cambio de configuración de seguridad a la radio móvil;

detectar un mensaje siguiente de la radio móvil con un número de secuencia de mensaje de activación; y

al detectar el mensaje próximo, activar la segunda configuración de seguridad para la conexión.

33. El nodo de RAN de la reivindicación 32, donde cuando la segunda configuración de seguridad es activada, los mensajes siguientes son enviados usando la segunda configuración de seguridad.

34. El nodo de RAN de la reivindicación 33, donde el mensaje siguiente es enviado usando la segunda configuración de seguridad.

35. El nodo de RAN de la reivindicación 32, donde la circuitería de procesado de datos (40) está configurada para transmitir una orden de modo de seguridad a la radio móvil (12) cuando la conexión ha de ser reconfigurada a la segunda configuración de seguridad.

36. El nodo de RAN de la reivindicación 35, donde la circuitería de procesado de datos (40) está configurada para detectar un mensaje completo de modo de seguridad de la radio móvil (12), en respuesta a la orden de modo de seguridad, que incluye el número de secuencia de mensaje de activación.

37. El nodo de RAN de la reivindicación 36, donde la circuitería de procesado de datos (40) está configurada para transmitir un mensaje de reconocimiento completo de modo de seguridad a la radio móvil (12) para indicar a la radio móvil (12) que la reconfiguración de seguridad está completa.

38. El nodo de RAN de la reivindicación 32, donde la circuitería de procesado de datos (40) está configurada para detectar durante la reconfiguración un mensaje de la radio móvil (40) que tiene un número de secuencia de mensaje más bajo que el número de secuencia de mensaje de activación para la RAN usando la primera configuración de seguridad.

39. El nodo de RAN de la reivindicación 38, donde el mensaje transmitido por la radio móvil (12) es un mensaje de actualización de celda o un mensaje de actualización de área.

40. El nodo de RAN de la reivindicación 32, donde la configuración de seguridad se refiere a la protección de integridad del mensaje, y el mensaje incluye un mensaje de control relacionado con la conexión.

41. El nodo de RAN de la reivindicación 40, donde la primera configuración de seguridad incluye una primera clave de protección de integridad usada para autentificar la señal de control, y la segunda configuración de seguridad incluye una segunda clave de protección de integridad usada para autentificar la señal de control.

42. El nodo de RAN de la reivindicación 32, donde la configuración de seguridad se refiere a la protección de confidencialidad de la comunicación, y la comunicación incluye tráfico de datos relacionado con la conexión.

43. El nodo de RAN de la reivindicación 42, donde la primera configuración de seguridad incluye una primera clave de encriptado usada para encriptar el tráfico de datos, y la segunda configuración de seguridad incluye una segunda clave de encriptado usada para encriptar el tráfico de datos.

44. El nodo de RAN de la reivindicación 32, donde el número de secuencia de mensaje de activación corresponde a un número de secuencia de mensaje futuro más grande que un número de secuencia de mensaje próximo.

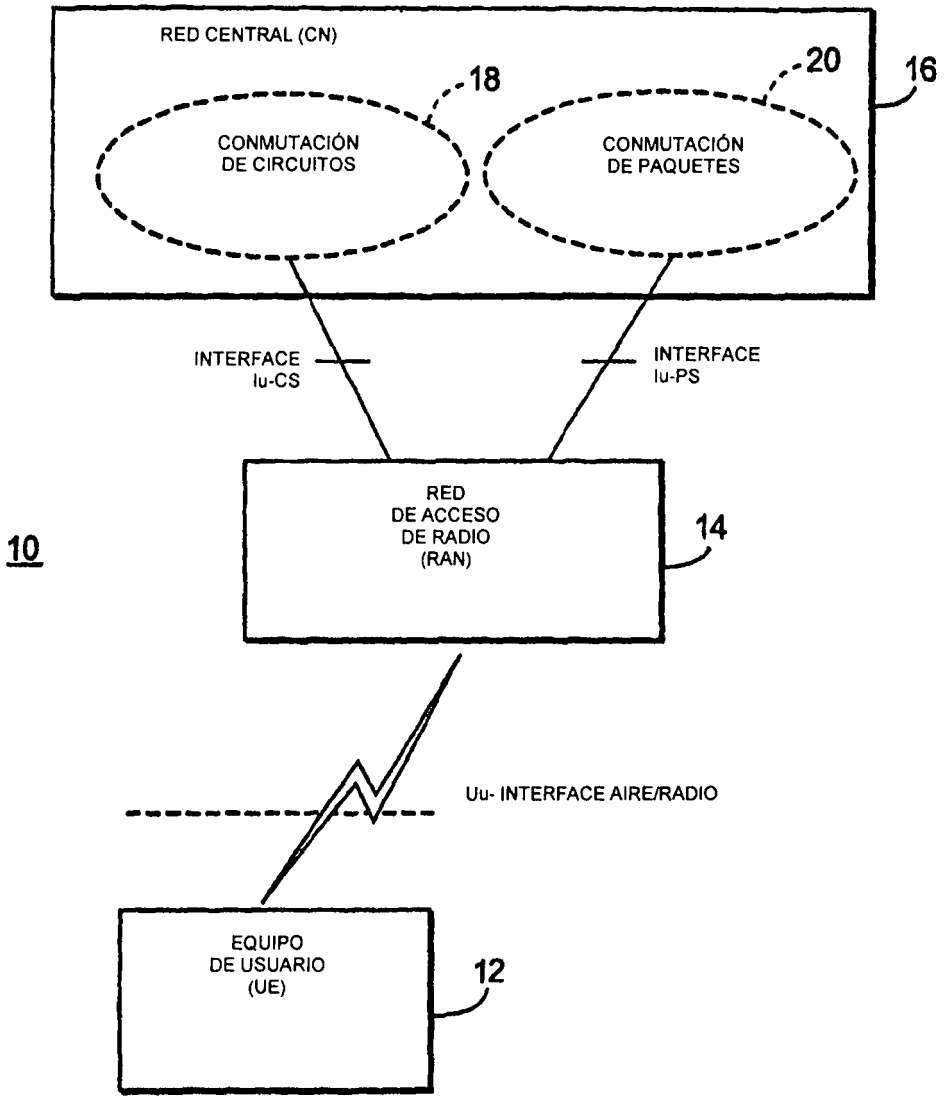
RED CENTRAL (CN)
18
20
16
CONMUTACIÓN
DE CIRCUITOS
CONMUTACIÓN
DE PAQUETES
INTERFACE
Iu-CS
INTERFACE
Iu-PS
RED
DE ACCESO
DE RADIO
(RAN)
14
10
Uu- INTERFACE AIRE/RADIO
EQUIPO
DE USUARIO
(UE)
12

Fig. 1

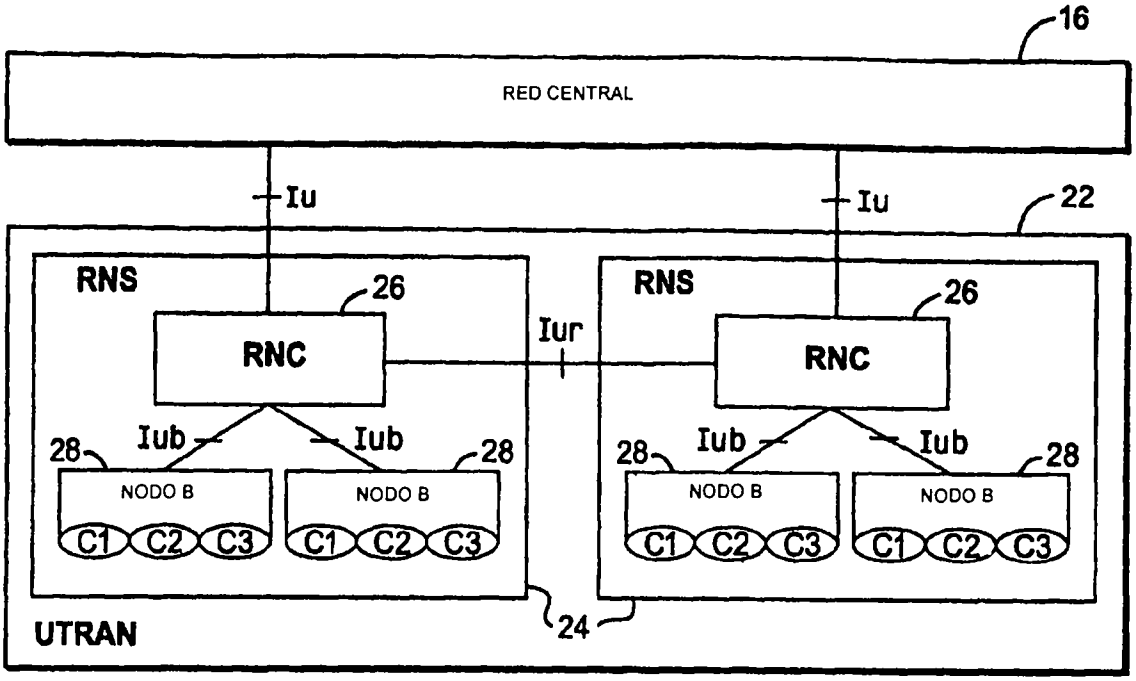
16
RED CENTRAL
Iu
Iu
22
RNS
26
RNC
Iur
RNS
26
RNC
Iub
Iub
28
28
NODO B
NODO B
C1
C2
C3
C1
C2
C3
Iub
Iub
28
28
NODO B
NODO B
C1
C2
C3
C1
C2
C3
24
UTRAN

Fig. 2

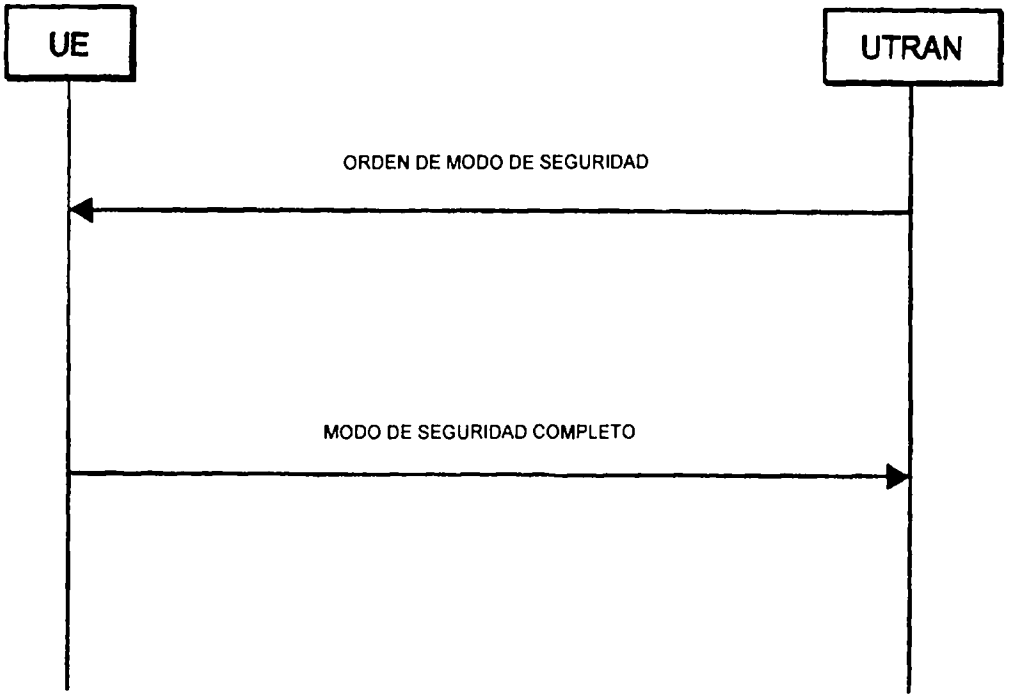
UE
UTRAN
ORDEN DE MODO DE SEGURIDAD
MODO DE SEGURIDAD COMPLETO

Fig. 5

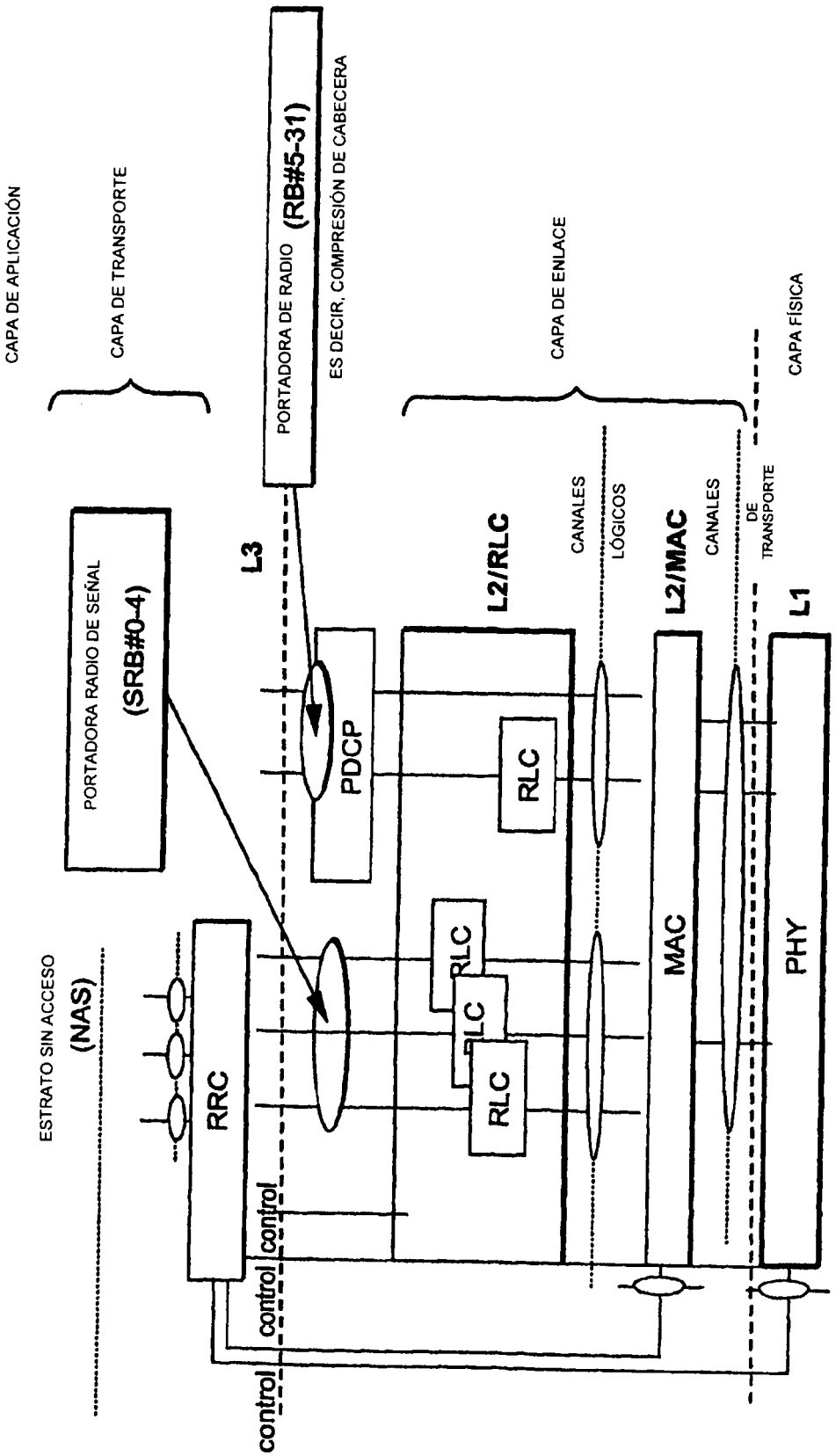
CAPA DE APLICACIÓN
CAPA DE TRANSPORTE
PORTADORA DE RADIO (RB#5-31)
ES DECIR, COMPRESIÓN DE CABECERA
CAPA DE ENLACE
CAPA FÍSICA
PORTADORA RADIO DE SEÑAL (SRB#0-4)
L3
L2/RLC
CANALES LÓGICOS
L2/MAC
CANALES DE TRANSPORTE
L1
ESTRATO SIN ACCESO (NAS)
RRC
PDCP
RLC
RLC
RLC
RLC
MAC
PHY
control
control
control

Fig. 3

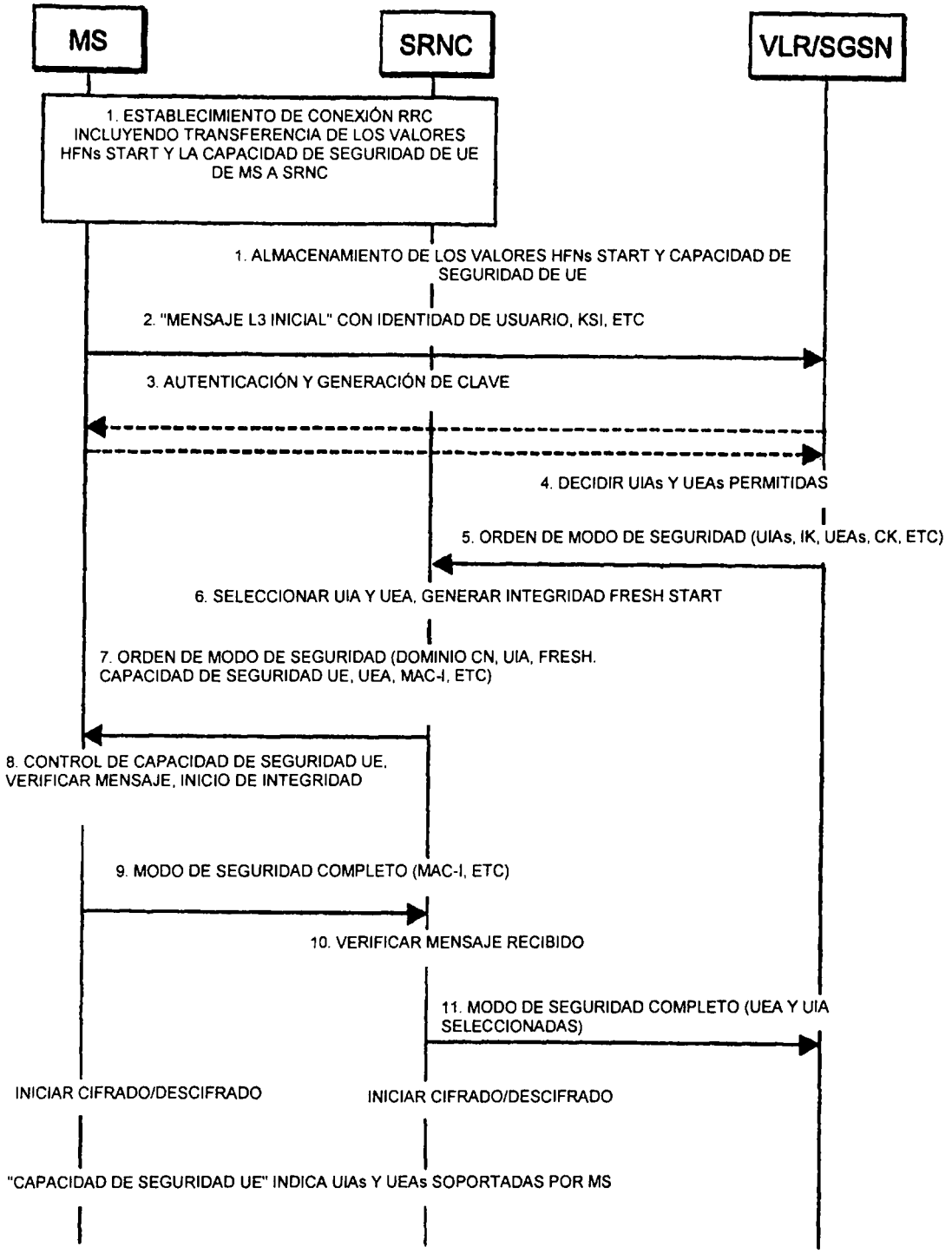
MS
SRNC
VLR/SGSN
1. ESTABLECIMIENTO DE CONEXIÓN RRC INCLUYENDO TRANSFERENCIA DE LOS VALORES HFNs START Y LA CAPACIDAD DE SEGURIDAD DE UE DE MS A SRNC
1. ALMACENAMIENTO DE LOS VALORES HFNs START Y CAPACIDAD DE SEGURIDAD DE UE
2. "MENSAJE L3 INICIAL" CON IDENTIDAD DE USUARIO, KSI, ETC
3. AUTENTICACIÓN Y GENERACIÓN DE CLAVE
4. DECIDIR UIAs Y UEAs PERMITIDAS
5. ORDEN DE MODO DE SEGURIDAD (UIAs, IK, UEAs, CK, ETC)
6. SELECCIONAR UIA Y UEA, GENERAR INTEGRIDAD FRESH START
7. ORDEN DE MODO DE SEGURIDAD (DOMINIO CN, UIA, FRESH. CAPACIDAD DE SEGURIDAD UE, UEA, MAC-I, ETC)
8. CONTROL DE CAPACIDAD DE SEGURIDAD UE, VERIFICAR MENSAJE, INICIO DE INTEGRIDAD
9. MODO DE SEGURIDAD COMPLETO (MAC-I, ETC)
10. VERIFICAR MENSAJE RECIBIDO
11. MODO DE SEGURIDAD COMPLETO (UEA Y UIA SELECCIONADAS)
INICIAR CIFRADO/DESCIFRADO
INICIAR CIFRADO/DESCIFRADO
"CAPACIDAD DE SEGURIDAD UE" INDICA UIAs Y UEAs SOPORTADAS POR MS

Fig. 4

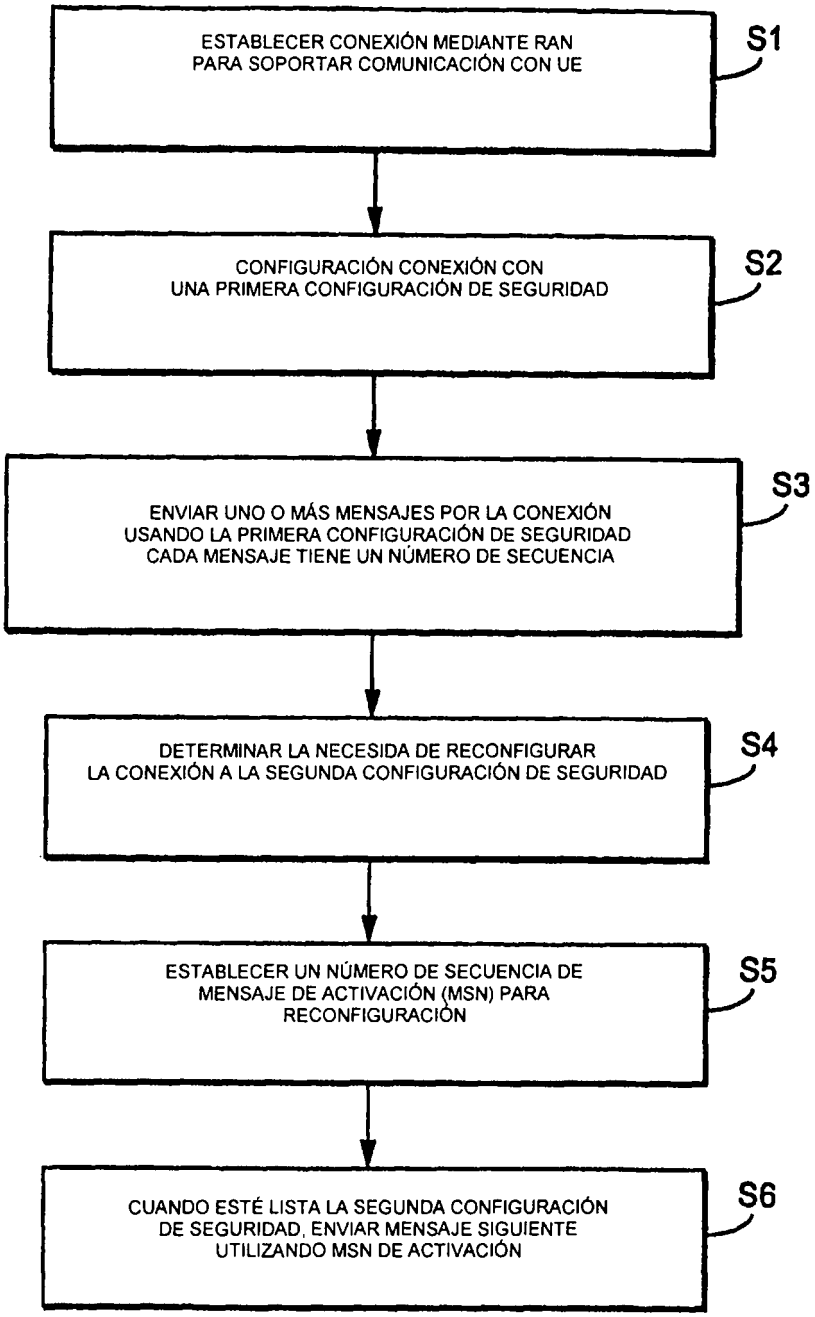
ESTABLECER CONEXIÓN MEDIANTE RAN PARA SOPORTAR COMUNICACIÓN CON UE
S1
CONFIGURACIÓN CONEXIÓN CON UNA PRIMERA CONFIGURACIÓN DE SEGURIDAD
S2
ENVIAR UNO O MÁS MENSAJES POR LA CONEXIÓN USANDO LA PRIMERA CONFIGURACIÓN DE SEGURIDAD CADA MENSAJE TIENE UN NÚMERO DE SECUENCIA
S3
DETERMINAR LA NECESIDA DE RECONFIGURAR LA CONEXIÓN A LA SEGUNDA CONFIGURACIÓN DE SEGURIDAD
S4
ESTABLECER UN NÚMERO DE SECUENCIA DE MENSAJE DE ACTIVACIÓN (MSN) PARA RECONFIGURACIÓN
S5
CUANDO ESTÉ LISTA LA SEGUNDA CONFIGURACIÓN DE SEGURIDAD, ENVIAR MENSAJE SIGUIENTE UTILIZANDO MSN DE ACTIVACIÓN
S6

Fig. 6

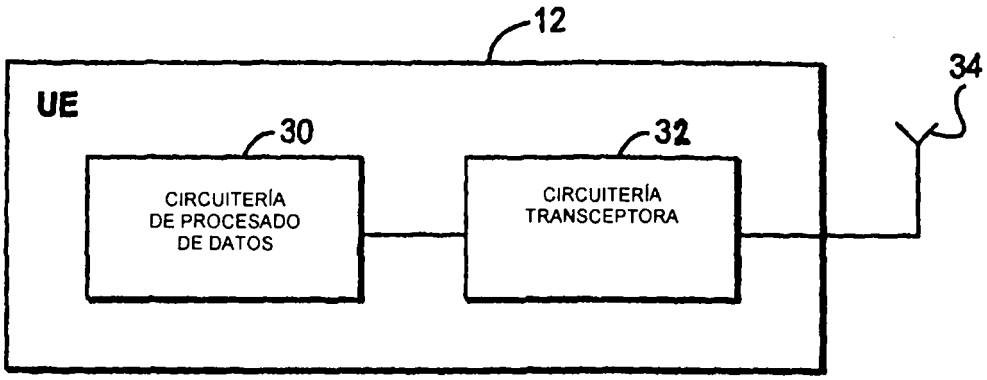
12
UE
30
32
34
CIRCUITERÍA DE PROCESADO DE DATOS
CIRCUITERÍA TRANSCEPTORA

Fig. 7A

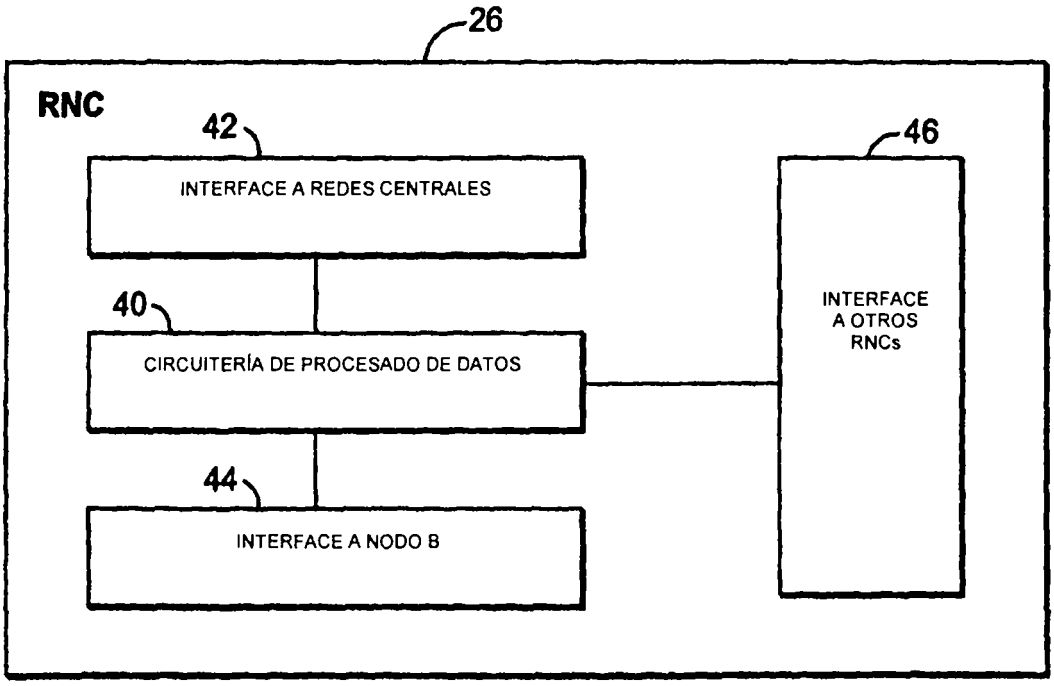
26
RNC
42
46
INTERFACE A REDES CENTRALES
40
CIRCUITERÍA DE PROCESADO DE DATOS
INTERFACE A OTROS RNCs
44
INTERFACE A NODO B

Fig. 7B

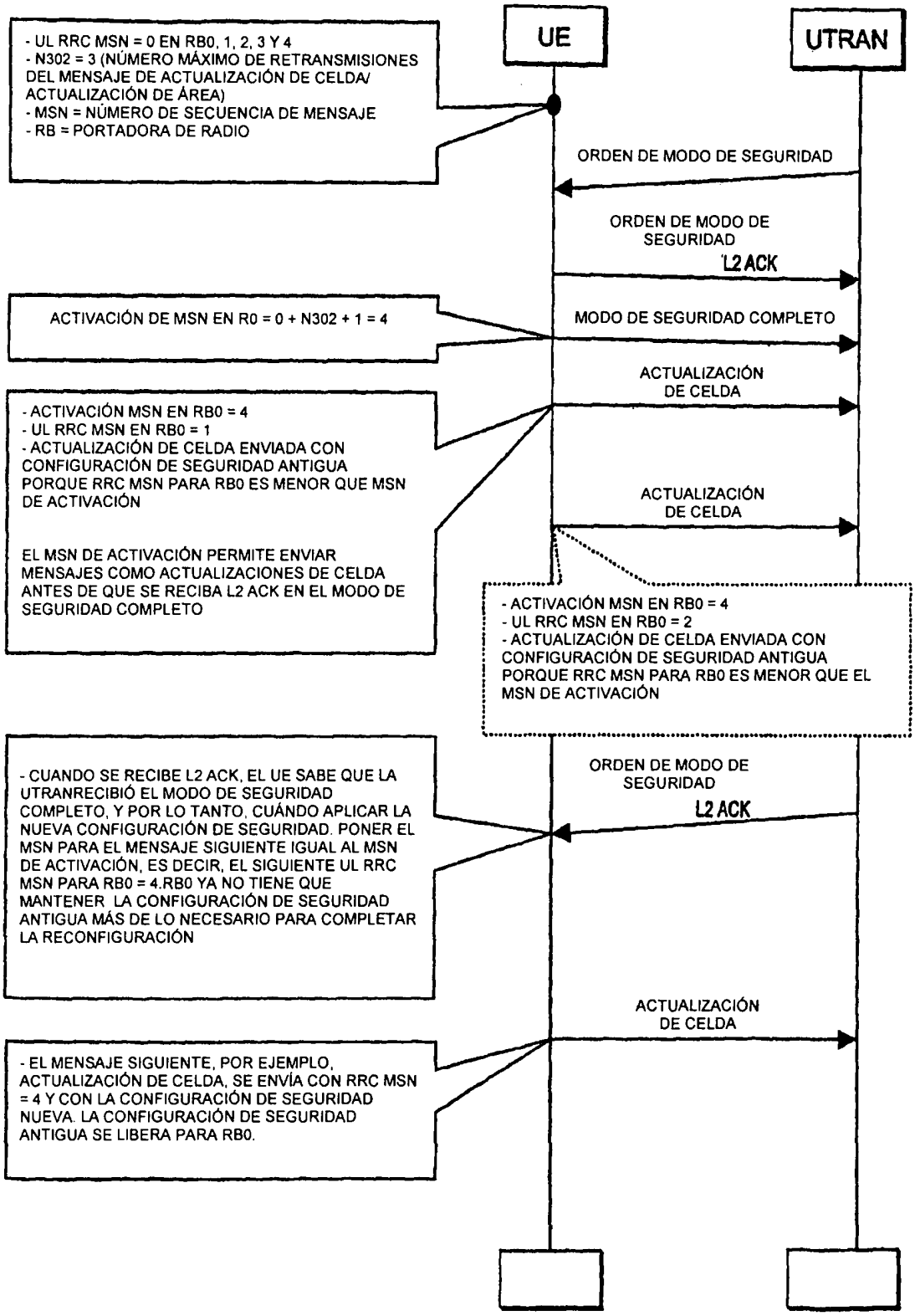
- UL RRC MSN = 0 EN RB0, 1, 2, 3 Y 4
- N302 = 3 (NÚMERO MÁXIMO DE RETRANSMISIONES DEL MENSAJE DE ACTUALIZACIÓN DE CELDA/ ACTUALIZACIÓN DE ÁREA)
- MSN = NÚMERO DE SECUENCIA DE MENSAJE
- RB = PORTADORA DE RADIO
UE
UTRAN
ORDEN DE MODO DE SEGURIDAD
ORDEN DE MODO DE SEGURIDAD
L2 ACK
ACTIVACIÓN DE MSN EN R0 = 0 + N302 + 1 = 4
MODO DE SEGURIDAD COMPLETO
ACTUALIZACIÓN DE CELDA
- ACTIVACIÓN MSN EN RB0 = 4
- UL RRC MSN EN RB0 = 1
- ACTUALIZACIÓN DE CELDA ENVIADA CON CONFIGURACIÓN DE SEGURIDAD ANTIGUA PORQUE RRC MSN PARA RB0 ES MENOR QUE MSN DE ACTIVACIÓN
EL MSN DE ACTIVACIÓN PERMITE ENVIAR MENSAJES COMO ACTUALIZACIONES DE CELDA ANTES DE QUE SE RECIBA L2 ACK EN EL MODO DE SEGURIDAD COMPLETO
ACTUALIZACIÓN DE CELDA
- ACTIVACIÓN MSN EN RB0 = 4
- UL RRC MSN EN RB0 = 2
- ACTUALIZACIÓN DE CELDA ENVIADA CON CONFIGURACIÓN DE SEGURIDAD ANTIGUA PORQUE RRC MSN PARA RB0 ES MENOR QUE EL MSN DE ACTIVACIÓN
- CUANDO SE RECIBE L2 ACK, EL UE SABE QUE LA UTRANRECIBIÓ EL MODO DE SEGURIDAD COMPLETO, Y POR LO TANTO, CUÁNDO APLICAR LA NUEVA CONFIGURACIÓN DE SEGURIDAD. PONER EL MSN PARA EL MENSAJE SIGUIENTE IGUAL AL MSN DE ACTIVACIÓN, ES DECIR, EL SIGUIENTE UL RRC MSN PARA RB0 = 4.RB0 YA NO TIENE QUE MANTENER LA CONFIGURACIÓN DE SEGURIDAD ANTIGUA MÁS DE LO NECESARIO PARA COMPLETAR LA RECONFIGURACIÓN
ORDEN DE MODO DE SEGURIDAD
L2 ACK
ACTUALIZACIÓN DE CELDA
- EL MENSAJE SIGUIENTE, POR EJEMPLO, ACTUALIZACIÓN DE CELDA, SE ENVÍA CON RRC MSN = 4 Y CON LA CONFIGURACIÓN DE SEGURIDAD NUEVA. LA CONFIGURACIÓN DE SEGURIDAD ANTIGUA SE LIBERA PARA RB0.

Fig. 8