(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 573 257**

(51) Int. CI.:

H04W 12/02 (2009.01)
H04W 12/10 (2009.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.07.2008 E 08796196 (7)**

(97) Fecha y número de publicación de la concesión europea: **30.03.2016 EP 2172069**

(54) Título: **Métodos y aparato para implementar seguridad de estrato de no acceso (NAS) en un dispositivo inalámbrico de la Evolución a largo plazo**

(30) Prioridad:

18.07.2007 US 950486 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.06.2016

(73) Titular/es:

INTERDIGITAL TECHNOLOGY CORPORATION (100.0%)
200 Bellevue Parkway, Suite 300
Wilmington, DE 19809, US

(72) Inventor/es:

MUKHERJEE, RAJAT, P.;
WANG, PETER, S.;
SAMMOUR, MOHAMMED y
SOMASUNDARAM, SHANKAR

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Métodos y aparato para implementar seguridad de estrato de no acceso (NAS) en un dispositivo inalámbrico de la Evolución a largo plazo

Campo tecnológico

El método y aparato se refieren a las comunicaciones inalámbricas. Más particularmente, el método y aparato se refieren a las comunicaciones seguras en un dispositivo inalámbrico según la Evolución a largo plazo.

Antecedentes

Los actuales objetivos para el programa Evolución a largo plazo (LTE – Long Term Evolution, en inglés) del Proyecto de asociación de tercera generación (3GPP – Third Generation Partnership Project, en inglés) van a proporcionar nueva tecnología, nueva arquitectura y nuevos métodos a los ajustes y configuraciones de la LTE, con el fin de proporcionar una mayor eficiencia espectral y una menor latencia, para una mejor utilización de los recursos de radio para experiencias de usuario más rápidas y mejores aplicaciones y servicios con un menor coste.

Como parte de este proceso de evolución, el grupo del 3GPP utilizará arquitecturas de seguridad en LTE diferentes de las utilizadas en el Sistema de telefonía móvil universal (UMTS – Universal Mobile Telephone System, en inglés) y el Sistema Global para comunicaciones mediante telefonía móvil (GSM – Global System for Mobile Communications, en inglés). Para comparar, los procedimientos de Autenticación y Codificación (AKA – Authentication and Key, en inglés) de UMTS en el dominio de paquetes conmutados (PS – Packet Switched, en inglés) serán la base para los nuevos procedimientos de LTE propuestos.

La figura 1 muestra una pila de protocolo de estrato de acceso 100 de UMTS. Los procedimientos de AKA y cifrado de UMTS se extienden sobre múltiples capas de protocolo y utilizan señalización tanto de estrato de no acceso (NAS – Non-Access Stratum, en inglés) como de control de recursos de radio (RRC – Radio Resource Control, en inglés) para alcanzar sus objetivos. Generalmente, la identificación y la autenticación de la unidad de transmisión recepción inalámbrica (WTRU - Wireless Transmit Receive Unit, en inglés) se consigue mediante señalización de NAS. Una vez que la autenticación a nivel de NAS se ha efectuado, se activa el cifrado y/o la protección en integridad por parte de la red utilizando la Orden de modo de seguridad, que es un mensaje del RRC. Una vez que la seguridad se ha activado utilizando la Orden de modo de seguridad en la capa de RRC, la WTRU pasa las claves de cifrado e integridad (CK – Ciphering Key e IK – Integrity Key, en inglés) al estrato de acceso (AS – Access Stratum, en inglés) utilizando la primitiva GMMAS-SECURITY-RES sobre el GMMAS-SAP (definido entre Gestión de movilidad de GPRS (GMM – GPRS Mobility Management, en inglés) y el AS). Tras recibir estas claves, el RRC 110 las pasa al controlador del enlace de radio (RLC – Radio Link Controller, en inglés) 120 y al control del acceso al medio (MAC – Medium Access Control, en inglés) 130 utilizando la primitiva CRLC-CONFIG (sobre el C-SAP entre el RRC y el RLC) y la primitiva CMAC-CONFIG (sobre el C-SAP entre el RRC y el MAC). El C-SAP (no mostrado) es un Punto de acceso a servicios para la señalización de plano-C entre el RRC y las capas inferiores. La protección de cifrado e integridad actual se realiza normalmente en el RLC 120, pero se realiza en el MAC 130 en caso de tráfico en modo de RLC transparente. Las capas inferiores (es decir, MAC / RLC) son responsables de asegurar que los mensajes previstos para las capas superiores (por ejemplo, los mensajes de NAS de Capa 3) han sido protegidos en integridad y/o cifrados correctamente. De lo contrario, las capas inferiores ignoran / borran el mensaje. Una vez que la seguridad ha sido activada, la seguridad de todos los plano-C y plano-U se realiza en el RLC o el MAC.

Para LTE, se ha propuesto una arquitectura radicalmente diferente para mejorar la seguridad. La principal diferencia es que en lugar de una única capa de seguridad (es decir, en el MAC / RLC) existen tres capas de seguridad: seguridad de NAS, seguridad de RRC y seguridad de plano-U. Cada capa tiene sus propias claves. La seguridad de NAS termina en la entidad de gestión de movilidad (MME – Mobility Management Entity, en inglés) y se realiza en la capa de NAS. La seguridad de RRC termina en el Nodo B evolucionado (e-NB – evolved Node B, en inglés) y se realiza en el Protocolo de convergencia de datos en paquetes (PDCP – Packet Data Convergence Protocol, en inglés). La seguridad de plano-U consiste en solo cifrado (ninguna protección en integridad) y se realiza también en el PDCP. Dicho de manera corta, los procedimientos de AKA se completan en el NAS y se obtienen las claves de seguridad de NAS. Los parámetros de seguridad de RRC / Plano-U se obtienen de una manera separada criptográficamente a partir de las claves de NAS. El conocimiento de las claves de RRC / Plano-U no permiten a un atancante determinar las claves de NAS. El fundamento principal para esta decisión era que en LTE sería posible tener diferentes e-NB en ubicaciones vulnerables, tal como en un hogar. RRC, y por lo tanto la seguridad, termina en el e-NB, de manera que esto se consideraba un riesgo en seguridad. Por ello, se adoptaron dos niveles de seguridad para el estándar.

La figura 2 es un diagrama de bloques de jerarquía de claves en LTE 200. Como se muestra en la figura 2, el USIM (en la unidad de transmisión / recepción inalámbrica (WTRU)) y el centro de autenticación (AuC – Authentication Centre, en inglés) 205 comparten una K secreta 210. Como parte de una señalización de autenticación y codificación (AKA) (similar a los procedimientos de AKA de UMTS actuales) el USIM y el AuC / HSS obtienen una clave de cifrado (CK) 215 y una clave de integridad (IK) 220. El procedimiento para obtener la CK 215 y la IK 220 es similar al de UMTS, en el que AuC / HSS obtiene un Vector de autenticación y envía una pregunta de seguridad a la

WTRU en un mensaje de NAS al que la WTRU responde y que el HSS / AuC verifica. A diferencia del UMTS, no obstante, en el que CK 215 e IK 220 son proporcionadas a las capas de MAC / RLC para efectuar el cifrado y/o la protección en integridad, en LTE la CK 215 y la IK 220 se utilizan para obtener las claves restantes en la jerarquía de claves que empieza con una clave maestra – la llamada clave K_{ASME} 225. Las claves restantes se obtienen a partir de la clave K_{ASME} utilizando diferentes funciones de obtención de clave (KDF – Key Derivation Functions, en inglés) y realizando un truncado.

La K_{eNB} 230 es una clave obtenida por medio de la WTRU y la MME a partir de la K_{ASME} 225 o por medio de la WTRU y el eNB de objetivo a partir de la K_{eNB}* durante una transferencia de eNB. La K_{eNB} 230 se utiliza para la obtención de claves para tráfico de RRC y la obtención de claves para tráfico ascendente o para obtener una clave de transición K_{eNB}* durante una transferencia de eNB.

La $K_{NAS\ int}$ 235 es una clave que se utiliza para la protección en integridad de la señalización de NAS con un algoritmo de integridad particular. Esta clave es obtenida por la WTRU y la MME 237 a partir de la K_{ASME} 225, así como un identificador para el algoritmo de integridad que utiliza una KDF.

La $K_{NAS\ enc}$ 240 es una clave que se utiliza para el cifrado de la señalización de NAS con un algoritmo de encriptación particular. Esta clave es obtenida por la WTRU y la MME 237 a partir de la K_{ASME} 225, así como un identificador para el algoritmo de encriptación que utiliza una KDF.

La $K_{UP\ enc}$ 245 es una clave que se utiliza para el cifrado del tráfico ascendente con un algoritmo de encriptación particular. Esta clave es obtenida por la WTRU y el eNB 247 a partir de la K_{eNB} 230, así como de un identificador para el algoritmo de encriptación que utiliza una KDF.

La $K_{RRC\ int}$ 250 es una clave que se utiliza para la protección en integridad del tráfico de RRC con un algoritmo de integridad particular. La $K_{RRC\ int}$ 250 es obtenida por la WTRU y el eNB 247 a partir de la K_{eNB} 230, así como un identificador para el algoritmo de encriptación que utiliza una KDF.

La $K_{RRC\ enc}$ 255 es una clave que se utiliza para el cifrado de la señalización de RRC con un algoritmo de encriptación particular. La $K_{RRC\ enc}$ 255 es obtenida por la WTRU y el eNB 247 a partir de la K_{eNB} 230, así como un identificador para el algoritmo de encriptación que utiliza una KDF.

Las claves de RRC y del plano-U pueden ser obtenidas con el C-RNTI como dato de entrada.

En la arquitectura de seguridad de UTRAN existente, una comprobación para un correcto cifrado y/o protección en integridad se realiza en el RLC o el MAC. El único escenario de manejo de fallo en seguridad actualmente en el NAS es si falla la autenticación. No obstante, con un procedimiento de cifrado y protección en integridad separado en el NAS, sería deseable definir procedimientos de NAS en respuesta a escenarios en los cuales se recibe un mensaje de NAS sin estar correctamente protegido en cifrado y/o en integridad.

El NAS se basa en el AS, es decir, el RLC o el MAC, para verificar que cualquier mensaje de Capa-3 (L3 – Layer 3, en inglés) recibido tiene las credenciales de seguridad correctas, es decir, estaban cifrados y adecuadamente protegidos en integridad. Dado que la nueva arquitectura de LTE que tiene seguridad de capa de NAS independiente de la seguridad de AS, y que el NAS verifica la seguridad de los mensajes de L3, este planteamiento resulta inadecuado, dado que la comprobación de la seguridad de NAS se efectúa como parte de los procedimientos definidos en el comportamiento de NAS. Así, resultaría deseable la definición de acciones para el NAS en caso de fallo.

Dado que las claves de NAS son independientes de las claves de RRC / plano-U (a continuación, en esta memoria, claves de AS) es posible iniciar / reconfigurar el cifrado de NAS independientemente del cifrado y de la protección en integridad del AS. Resultaría deseable tener nuevos mensajes y procedimientos para este proceso. Asimismo, la expiración de la clave puede estar ligada al estado del NAS / RRC de la WTRU. Resultaría deseable disponer de procedimientos para el manejo de las claves de la WTRU.

El RRC típicamente recibe las nuevas CK e IK del NAS y las pasa al MAC y al RLC, donde se realiza el cifrado / protección en integridad. No obstante, en LTE, el cifrado de AS y la protección en integridad serán efectuados por el PDCP. De este modo, resultaría deseable disponer de nuevos procedimientos de capas cruzadas y primitivas para un adecuado funcionamiento de la seguridad.

El alcance del “3rd Generation Partnership Project; Technical Specification Group \ Services and System Aspects; Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution (SAE) (Release 8)”, 3GPP TR 33.821 V0.4.0, es la base y seguimiento de las decisiones en una RAN evolucionada a largo plazo (de LTE) y de Evolución de arquitectura del sistema (SAE – System Architecture Evolution, en inglés) del 3GPP para la versión 8.

Compendio

Un método y aparato tal como se define en las reivindicaciones 1 y 9 se refieren a un sistema de comunicación inalámbrica que incluye una unidad de transmisión / recepción (WTRU) configurada para recibir mensajes no cifrados y cifrados. Los mensajes no cifrados pueden incluir solicitudes de identidad, solicitudes de autenticación, órdenes de modo de seguridad de estrato de no acceso (NAS) y respuestas de actualización del área de seguimiento. Los mensajes cifrados pueden proceder del NAS y del controlador de recursos de radio (RRC). Los mensajes preferiblemente están cifrados utilizando claves de seguridad.

Breve descripción de los dibujos

Es preciso tener una compresión más detallada a partir de la descripción siguiente, dada a modo de ejemplo, y que se comprenderá junto con los dibujos que se acompañan, en los cuales:

la figura 1 es una pila de protocolo de estrato de acceso de acuerdo con la técnica anterior;

la figura 2 es un diagrama de bloques de la jerarquía de claves en LTE de acuerdo con la técnica anterior;

la figura 3 es un diagrama de bloques de una realización en la que el agente puede ser la capa equivalente de Gestión de Movilidad en NAS de LTE o una nueva sub-capa para la seguridad o algún otro agente, y los parámetros de seguridad definidos para un mensaje dado son incorrectos;

la figura 4 es un diagrama de bloques de una cabecera de protocolo de capa 3 mejorada que incluye un número de secuencia de NAS;

la figura 5 es un diagrama de bloques que ilustra procedimientos de manejo de claves en una WTRU tras la transición del modo EMM_Conectado al modo de EMM_Reposo;

la figura 6 es un diagrama de bloques de una pila de protocolo de estrato de acceso para LTE; y

la figura 7 es un diagrama de bloques de un sistema de comunicación inalámbrica configurado para el intercambio de mensajes cifrados y no cifrados en LTE.

Descripción detallada

Cuando se nombra a continuación en esta memoria, la terminología “unidad de transmisión / recepción inalámbrica (WTRU)” incluye, pero no está limitada a un equipo de usuario (UE – User Equipment, en inglés), una estación de telefonía móvil, una unidad de abonado fijo o móvil, un localizador, un teléfono celular, un asistente digital personal (PDA – Personal Digital Assistant, en inglés), un ordenador, o cualquier otro tipo de dispositivo de usuario capaz de operar en un entorno inalámbrico. Cuando se nombra a continuación en esta memoria, la terminología “estación de base” incluye, pero no está limitada a un Nodo B, Nodo B mejorado (eNB), un controlador de sitio, un punto de acceso (AP – Access Point, en inglés), o cualquier otro tipo de dispositivo de interfaz con capacidad de operación en un entorno inalámbrico.

Manejo del fallo de seguridad en el NAS

Los procedimientos que se explican a continuación pueden ser utilizados si existen problemas con la seguridad en alguna otra capa, por ejemplo, en la capa de PDCP que efectúa cifrado / protección en integridad de RRC. Un procedimiento para el manejo del fallo en seguridad en el NAS es proporcionar un grupo de mensajes de NAS que pueden ser recibidos por una WTRU sin cifrado y/o protección en integridad en el NAS que está activado. Tal lista solo existe para los mensajes de NAS de UTRAN, que son diferentes de los mensajes de NAS de LTE, y pueden ser recibidos sin que esté activado el cifrado de RLC / MAC. El grupo de mensajes de NAS que pueden ser recibidos por una WTRU sin cifrado y/o protección en integridad en el NAS activado puede incluir, pero no estar limitado a.

solicitud de identidad;

solicitud de autenticación;

orden de modo de seguridad de NAS (esta solo puede ser recibida si al menos la protección en integridad en NAS está activada); y

respuesta de actualización de área de seguimiento.

En la MME es posible recibir los siguientes mensajes sin cifrado y/o protección en integridad:

respuesta de identidad;

respuesta de autenticación; y

solicitud de actualización de área de seguimiento.

Además, se puede obligar a que mientras los mensajes anteriores puedan ser recibidos sin cifrado y/o protección en integridad activados, si el cifrado y/o la protección en integridad han sido ya activados, entonces estos mensajes deban estar cifrados y/o con protección en integridad.

Algunos otros mensajes de NAS solo pueden ser enviados si la seguridad tanto de NAS como de RRC ha sido activada. Algunos mensajes de NAS pueden ser enviados si la seguridad de NAS ha sido activada (independiente de la seguridad de RRC).

La figura 3 es un diagrama de bloques 300 de una realización en la que el agente puede ser la capa equivalente de gestión de movilidad en NAS de LTE, o una nueva sub-capa para seguridad, o algún otro agente. Una vez que un mensaje de NAS se ha recibido 305, el agente responsable de la comprobación del estado de la seguridad del mensaje de NAS comprobará si los parámetros de seguridad para el mensaje son apropiados 310. Si los parámetros de seguridad definidos para un mensaje dado son incorrectos 315, es decir, las comprobaciones de seguridad fallan o el mensaje no está cifrado, o si un mensaje (dependiendo de los campos de discriminador de protocolo y de tipo de mensaje en la cabecera) debería haber sido recibido cifrado y/o con protección en integridad, pero no lo fue, la capa de NAS, sub-capa o el agente, pueden tomar alguna o todas las acciones siguientes en cualquier secuencia. Las acciones tomadas pueden depender del tipo de mensaje cuyos parámetros de seguridad han fallado. Los procedimientos que se definen a continuación, pueden ser utilizados también si existen problemas con la seguridad en alguna otra capa (por ejemplo, la seguridad de RRC falla):

las acciones del agente pueden ser definidas mediante implementación 320;

el agente puede ignorar y/o borrar el mensaje 325;

el agente puede informar del fallo a alguna otra capa de protocolo (por ejemplo, RRC), entidad en la red WTRU (por ejemplo, USIM / UICC) 330. Si el agente comprueba la seguridad y encuentra un error puede activar, por ejemplo, un mensaje a la red informando a la red del error. El informe puede incluir la razón para el fallo. Si alguna otra capa de protocolo / entidad ha sido informada de tal fallo, su respuesta puede ser similar a las descritas aquí;

el agente puede iniciar una reautenticación con la red 335;

el agente puede moverse al modo de gestión de movilidad (EMM_Reposo) del sistema de paquetes evolucionado (EPS) o al estado EMM_Eliminado del registro 340;

el agente puede guardar un recuento del número de fallos y realizar algunas acciones tras fallos 345 repetidos. Estas acciones pueden ser las mismas que las definidas en esta memoria.

El agente puede intentar la reconexión a la red 350; o

el agente puede borrar algunos o todos los protocolos de seguridad (claves / números de secuencia / identificadores de conjunto de claves) que están almacenados, o puede señalar la entidad en la WTRU, bien directamente o a través de un intermediario, que almacena / gestiona los parámetros de seguridad para hacerlo 355.

Si los parámetros de seguridad son correctos, el mensaje de NAS puede ser procesado como se define para el protocolo específico y el tipo de mensaje 360. Como ejemplo, este agente puede ser la capa equivalente de gestión de movilidad en NAS de LTE o una nueva sub-capa para seguridad o algún otro agente.

Impactos del protocolo de capa 3

La cabecera del protocolo de L3 existente no contiene un número de secuencia. La cabecera de un mensaje de L3 estándar está compuesta por dos octetos. La cabecera está estructurada en tres partes principales, el discriminador de protocolo (1/2 octeto), un octeto de tipo mensaje y medio octeto. El medio octeto se utiliza en algunos casos como identificador de transacción, en algunos otros casos como sub-discriminador de protocolo y se denomina en caso contrario indicador de salto. Por ejemplo, si el discriminador de protocolo está ajustado a GMM, entonces puede ser utilizado como indicador de salto. Si el discriminador de protocolo está ajustado a SM, entonces puede ser utilizado como un TI o como un sub-discriminador de protocolo. Si se utiliza como indicador de salto, significa que para los mensajes de GMM los primeros 4 bits no tienen significado y son 'saltados'.

El discriminador de protocolo distingue entre mensajes de gestión de movilidad (MM), de gestión de movilidad de GPRS (GMM), de gestión de sesión (SM – Session Management, en inglés) y otros. Aunque el tipo de mensaje indica la clase de mensaje, por ejemplo, solicitud de conexión o activación de contexto de PDP, el identificador de la transacción permite a las entidades de transferencia en la WTRU y en la red distinguir hasta 16 flujos de mensajes bidireccionales diferentes para un discriminador de protocolo dado y un punto de acceso a servicio (SAP – Service Access Point, en inglés) dado. Tal flujo de mensajes se denomina transacción. Se define asimismo un mecanismo de extensión para un Identificador de transacción (TI – Transaction Identifier, en inglés). Este mecanismo permite distinguir hasta 256 flujos de mensajes bidireccionales diferentes para un discriminador de protocolo y un SAP dados. Por ejemplo, cuando la WTRU intenta obtener una dirección de IP, existe una entidad de SM en la WTRU y

en la red. Si la WTRU intenta entonces obtener otra dirección de IP, se crea otro par de entidades de SM en la WTRU y en la red. El TI identifica a qué transacción, es decir, par, está dirigido un mensaje de SM particular.

La figura 4 es un diagrama de bloques de una cabecera de protocolo de L3 400 mejorada que incluye un número de secuencia de NAS 410. Como la cabecera de protocolo de L3 existente, la cabecera mejorada está compuesta por dos octetos, y estructurada en tres partes principales. Las tres partes principales son el discriminador de protocolo 420 (1/2 octeto), un octeto de tipo mensaje y medio octeto utilizado en algunos casos como identificador de transacción 430, en algunos otros casos como sub-discriminador de protocolo, y se denomina de lo contrario indicador de salto. Por ejemplo, si el discriminador de protocolo está ajustado a GMM, entonces puede ser utilizado como un indicador de salto. Si el discriminador de protocolo está ajustado a SM, entonces puede ser utilizado como TI o como sub-discriminador de protocolo. Si se utiliza como indicador de salto, significa que para los mensajes de GMM los primeros 4 bits no tienen significado y son 'saltados'. La cabecera mejorada incluye un número de secuencia para un mensaje de NAS 410, denominado a continuación en esta memoria SN de NAS. Puede estar incluido en la cabecera de protocolo de un mensaje de NAS o como elemento de información (IE – Information Element, en inglés) en su contenido. El identificador de transacción puede funcionar asimismo como número de secuencia. El SN de NAS puede tener un periodo de incremento predefinido o negociado. Como ejemplo, podría ser por cada PDU de NAS (es decir, mensaje). La capa de NAS puede ser capaz de realizar una detección duplicada sobre la base del número de secuencia o utilizando cualquier otro número que se incrementa utilizando el SN de NAS, donde las PDU de NAS duplicadas recibidas son ignoradas.

El SN de NAS puede ser guardado para cada portador de radio de señalización de AS o por SAP, independientemente del discriminador de protocolo o del tipo de mensaje. Es posible guardarlo también por cada TI.

Es posible utilizar un valor de RECUENTO en la capa de NAS. Incrementar el valor de RECUENTO de manera predefinida / negociada, por ejemplo, en cada mensaje de L3, puede proteger frente a ataques de reproducción o suplantación. Esto es factible con cifrado a nivel de NAS. Es posible definir un único RECUENTO-C para cifrado y un único RECUENTO-I para protección en integridad, para todos los SAP. Es posible definir una combinación de RECUENTO-C y/o RECUENTO-I y/o valores de RECUENTO únicos para los SAP. El RECUENTO puede consistir en dos parámetros; un número de secuencia de NAS (SN) que se incrementa de una manera regular predefinida / negociada, por ejemplo, por cada unidad de datos de protocolo (PDU) de NAS o por cada PDU de NAS en un SAP dado, y un número de hiper-trama de NAS (NAS HFN – NAS Hyper-Frame Number, en inglés). El HFN de NAS puede ser un contador que se incrementa en uno por cada x números de incrementos de SN de NAS. El parámetro RECUENTO, en todo o en parte, puede ser inicializado sobre la base de un valor de INICIO durante el acceso inicial / obtención de clave / autenticación / transición de reposo a activo. El parámetro RECUENTO puede ser utilizado como dato de entrada a los algoritmos de comprobación de cifrado / descifrado, protección en integridad / integridad para asegurar la seguridad.

El valor de RECUENTO puede precisar ser establecido antes de la activación de la seguridad de NAS. La longitud del parámetro RECUENTO-C podría ser 32 bits, o podría ser reducido a un valor menor, puesto que para mensajes de NAS podría no ser necesario un valor de SN elevado. Asimismo, la longitud del campo de SN y del propio campo del HFN podría ser modificada dentro del parámetro RECUENTO-C para optimizarla para procedimientos a nivel de NAS. Es posible utilizar motores de cifrado de la técnica anterior para NAS. Se debe realizar un cambio adecuado al motor de cifrado para que contenga un valor de RECUENTO-C menor o un cambio en el valor del campo del SN y del HFN.

De manera alternativa, el valor de RECUENTO de NAS puede ser el SN de NAS, dado que el SN de NAS puede ser protegido mediante el encriptado del RRC, de manera que no está abierto y por lo tanto un HFN oculto no es absolutamente necesario. La seguridad de NAS puede ser activada no antes de que la seguridad de NAS y el SN de NAS puedan ser reiniciados tras la activación de la seguridad de NAS. Además, es posible duplicar la detección en el NAS utilizando el valor RECUENTO de NAS.

Sería preciso definir parámetros adicionales en lugar de la longitud del mensaje o del ID de portador, que son datos de entrada al motor de cifrado, o sería preciso definir procedimientos adicionales en el NAS para extraer estos parámetros cuando la seguridad de NAS encripta el mensaje.

De manera alternativa en el lado de la WTRU en lugar de tener 2 motores de cifrado separados para RRC y NAS, es posible utilizar un motor de cifrado que puede funcionar con parámetros tanto de RRC como de NAS.

Otro cifrado de mensajes a nivel de NAS puede ser opcional, y la WTRU puede indicar en su información de capacidad si soporta o no cifrado a nivel de NAS.

Manejo de claves en la WTRU tras la transición desde el modo EMM conectado al modo EMM en reposo

Típicamente, cuando una WTRU pasa del modo EMM_Conectado al modo EMM_Reposo la conexión del RRC se libera. En las transiciones de activo a reposo, un eNB típicamente no almacena información de estado acerca de la WTRU correspondiente. El eNB típicamente borra las claves actuales de su memoria.

Para esta realización en particular, en las transiciones de activo a reposo, el eNB puede borrar al menos una de K_{eNB}, $K_{RRC\ enc}$ y $K_{RRC\ int}$ y $K_{UP\ enc}$. No obstante, la MME puede almacenar K_{ASME}.

La figura 5 es un diagrama de bloques que ilustra procedimientos de manejo de claves 500 en una WTRU tras la transición del modo EMM_Conectado al modo EMM_Reposo. Hasta ahora, los procedimientos de WTRU no han sido definidos en respuesta a esta transición. Un procedimiento posible sería que tras la transición al modo EMM_Reposo 510, la WTRU pudiese proporcionar una indicación de la transición a la entidad que almacena las claves de seguridad 520 en la WTRU, tal como UICC, USIM o Equipo de telefonía móvil. Otro posible procedimiento sería que es posible que la WTRU proporcione 520 una indicación a la entidad de almacenamiento cuando el e-NB de servicio cambia mientras está en modo EMM_Reposo 530, tal como durante la reselección de una célula para diferente e-NB. La indicación de la WTRU a la entidad de almacenamiento puede incluir la identidad del e-NB de manera que se puedan obtener nuevas claves de e-NB, RRC y plano-U. A modo de ejemplo, las indicaciones pueden ser proporcionadas por el NAS y/o el AS. Con este propósito, es posible definir primitivas predeterminadas, que incluyen mensajes, IE, interfaces y SAP entre capas de protocolo de la entidad indicadora y/o entre la entidad indicadora y la entidad de almacenamiento. Se comprenderá que las primitivas predeterminadas incluyen primitivas tanto nuevas como existentes que es posible utilizar. Tras la recepción de tal indicación de transición, la entidad de almacenamiento dentro de la WTRU preferiblemente borrará las claves apropiadas 540, por ejemplo, al menos una de K_{eNB}, $K_{RRC\ enc}$, $K_{RRC\ int}$ y $D_{UP\ enc}$. Puede elegir guardar o borrar las claves de seguridad de NAS y las claves de ASME 550.

La entidad de almacenamiento puede borrar la $K_{RRC\ enc}$, la $K_{RRC\ int}$ y la $K_{UP\ enc}$ tras la recepción de una indicación de transición de activo a reposo, y borrar la K_{eNB} cuando se recibe una indicación de un cambio en el e-NB de servicio, tal como durante la reselección para un e-NB diferente. Puede elegir guardar o borrar las claves de seguridad de NAS u las claves de ASME. Tras la reselección a una célula que pertenece a un e-NB diferente, lo que se determina leyendo la identificación del e-NB en el canal de emisión, la WTRU puede generar una nueva K^*_{eNB} utilizando la K_{eNB} y un “identificador de siguiente salto”.

La entidad de almacenamiento no puede borrar ninguna clave tras la transición de activo a reposo o tras la transición a un nuevo e-NB en modo de reposo mientras que puede borrar claves tras la transición de reposo a activo.

La entidad de almacenamiento no puede borrar ninguna clave tras la transición de activo a reposo o tras la transición a un nuevo e-NB en modo reposo. Por el contrario, puede borrarlas cuando se van a generar nuevas claves, por ejemplo, cuando un eNB recibe una solicitud de conexión de RRC o se asigna un nuevo C-RNTI.

Un cambio en el ID de la célula de servicio / C-RNTI puede ser indicado 560 a la entidad de almacenamiento. Esta indicación puede ser proporcionada por el NAS y/o el AS. De manera alternativa, las claves pueden ser almacenadas con un valor de temporizador 570 asociado. Cuando una WTRU pasa de reposo a activo o de activo a reposo, el tiempo puede controlar cuánto tiempo puede seguir siendo válida una clave antes de ser eventualmente borrada.

Impactos a la capa de PDCP debido a la arquitectura de cifrado propuesta

Típicamente, el cifrado para el tráfico de RRC y del plano-U puede ser realizado en la capa de PDCP. Esto impone muchos cambios de arquitectura en el PDCP.

En esta realización, la capa de PDCP tiene la capacidad de recibir las claves de seguridad del RRC y las claves de seguridad del plano-U de capas superiores. Las primitivas se pueden definir según las necesidades. Específicamente el RRC o el NAS o el USIM pueden proporcionar al PDCP las claves de cifrado requeridas y los valores de INICIO o RECUENTO o HFN o SN requeridos. La capa de PDCP puede asimismo tener la capacidad de calcular estos valores por sí misma, basándose en la información de la cabecera del RRC.

Con referencia a la figura 1, el tráfico del plano-C no pasa a través del PDCP. Dado que es posible fijar diferentes portadores de radio utilizando diferentes parámetros RECUENTO, es preferible que la capa de PDCP pueda distinguir entre diferentes clases de tráfico. Para ello, las SDU entrantes o las primitivas que transportan las SDU pueden tener información explícita relativa a las portadoras de radio destinadas. La capa de PDCP puede determinarlo por sí misma y cifrar / proteger la integridad de acuerdo con ello.

La figura 6 es un diagrama de bloques de una pila de protocolo de estrato de acceso para LTE 600. Con referencia a la figura 6, el tráfico del plano-C pasa a través de la capa de PDCP 610. La capa de PDCP 610 comprueba la seguridad de las PDU de PDCP entrantes. Si la capa de PDCP 610 observa que los parámetros de seguridad de una PDU entrante (que va a ser mapeada bien a un portador de radio de datos o a un portador de radio de señalización) son incorrectos (es decir, si, por ejemplo, la comprobación de la integridad de la PDU del PDCP falla) puede efectuar al menos una de las acciones que siguen en cualquier secuencia. Las acciones realizadas pueden depender del tipo de mensaje cuyos parámetros de seguridad han fallado. Los procedimientos definidos a continuación pueden ser asimismo utilizados si existen problemas con la seguridad en alguna otra capa, por ejemplo, si la seguridad de NAS falla:

las acciones del PDCP pueden ser definidas mediante implementación;

el PDCP puede ignorar y/o borrar el mensaje;

puede informar del fallo a alguna otra capa de protocolo, tal como la entidad de RRC en la WTRU; otra capa de protocolo puede ser informada de tal fallo;

puede guardar un recuento del número de fallos y tomar realizar acciones tras fallos repetidos (por ejemplo, X número de fallos en Y mensajes o unidades de tiempo) tal como las definidas en esta memoria o algunas otras acciones;

puede borrar algunos o todos los parámetros de seguridad, tal como claves y números de secuencia, que están almacenados o puede señalar la entidad en la WTRU, directa o indirectamente, que almacena o gestiona los parámetros de seguridad para hacerlo; y

un informe del fallo a otras capas de protocolo puede incluir la razón del fallo.

El HFN de PDCP puede ser utilizado para constituir un valor de RECUENTO. Este valor de RECUENTO puede ser utilizado en los algoritmos de cifrado y/o de protección en integridad del PDCP 510 y puede ser inicializado mediante un valor de INICIO. Pueden existir múltiples valores de RECUENTO para cada portador de radio que el PDCP puede proteger. El RRC 620 y las capas de PDCP 610 pueden ser capaces de intercambiar información relativa al valor de RECUENTO o a sus constituyentes.

La capa de PDCP 610 puede comprobar la protección en integridad de un mensaje. Esto está en línea con la asunción de que la protección en integridad está en el PDCP 610. No obstante, actualmente la palabra de código de autenticación de mensaje (MAC) adjunta al mensaje para certificar su integridad se calcula en el RRC 620 adjunto al mensaje de RRC y se baja al RLC 630 / control de acceso al medio (MAC) 640. El mensaje completo, incluida la palabra de MAC, está cifrado. Asimismo, la capa de PDCP 610 puede no ser capaz de determinar si un mensaje de RRC necesita protección.

En el lado de transmisión, la capa de RRC 620 puede indicar a la capa de PDCP 610 si un mensaje de RRC dado requiere o no requiere protección en integridad y/o cifrado. La capa de PDCP 610 puede utilizar esta indicación para determinar si efectuar un cifrado y/o protección en integridad en los mensajes de RRC para ser enviados a las PDU de PDCP.

Esta indicación puede ser una indicación explícita proporcionada por el RRC a la capa de PDCP en cada mensaje de RRC enviado por el RRC al PDCP utilizando nuevos bits. Alternativa o adicionalmente, la indicación puede ser implícita, por ejemplo, cifrado y/o protección en integridad en el PDCP siempre estará activado a menos que se indique, o siempre estará desactivado a menos que se indique otra cosa por parte del RRC. Como ejemplo, sería posible utilizar un indicador de 2 bits por parte de la capa de RRC 620 para indicar cualquier combinación de cifrado y protección en integridad que esté activa. Tal indicación puede ser enviada con cada mensaje del RRC pasado al PDCP o puede aplicar a todos los mensajes de RRC y es preferible, puesto que algunos mensajes de RRC pueden no estar cifrados y/o protegidos en integridad.

De manera alternativa o, además, la capa de RRC 620 puede indicar a la capa de PDCP 610 que todos los mensajes de RRC que empiezan con un mensaje de RRC dado estarán protegidos en integridad.

De manera alternativa o, además, la capa de RRC 620 puede indicar a la capa de PDCP 610 que todos los mensajes de RRC que empiezan con un mensaje de RRC dado estarán cifrados.

De manera alternativa o, además, la capa de RRC 620 puede indicar a la capa de PDCP 610 que todos los mensajes de RRC que empiezan con un mensaje de RRC dado estarán cifrados y protegidos en integridad.

De manera alternativa o, además, la capa de RRC 620 puede proporcionar una lista de mensajes de RRC genéricos a la capa de PDCP 610 y sus parámetros de seguridad asociados. La lista puede incluir mensajes que pueden ser recibidos sin cifrar y/o sin protección en integridad, tal como, por ejemplo, un Restablecimiento de conexión de RRC. La lista puede incluir mensajes que pueden ser recibidos con cifrado y/o con protección de integridad.

De manera alternativa o, además, es posible definir una marca de comprobación de cifrado y/o de integridad, opcionalmente por parte de la capa de RRC 620, que, si está establecida, la capa de PDCP 610 cifrará y/o comprobará la integridad de todos los mensajes de RRC. La capa de PDCP 610 comprobará de este modo esta marca antes de la comprobación del cifrado y la integridad. Pueden existir marcas separadas ajustadas para cifrado y protección de integridad.

Para todos los mecanismos de indicación diferentes anteriores la indicación puede ser facilitada por cada portador de radio de señalización (SRB – Signaling Radio Bearer, en inglés), es decir, la capa de RRC 620 puede indicar a la capa de PDCP 610 que la indicación para el cifrado y/o la protección en integridad aplica a los mensajes de RRC mapeados por la capa de PDCP 610 al SRB específico.

Para que un mensaje sea transmitido, la capa de PDCP 610 puede en primer lugar proteger en integridad y después cifrar o puede cifrar primero y después proteger en integridad. Antes de cualquier operación, puede rellenar el

mensaje con el fin de conseguir una longitud óptima para el cifrado y/o la protección en integridad. Antes de la operación de seguridad la capa de PDCP 610 puede asignar un SN. El SN puede ser un SN de PDCP, o puede reutilizar un SN de RRC, o puede utilizar otro número de secuencia, tal como, por ejemplo, un número de secuencia común. Antes de la operación de seguridad, la capa de PDCP 610 puede efectuar una compresión de cabecera para el tráfico del plano-U.

La palabra de MAC para protección en integridad puede ser calculada sobre los datos de texto no cifrado, los datos cifrados y/o toda o parte de la cabecera de PDCP.

El cifrado puede ser realizado sobre todo el mensaje, incluyendo una palabra de MAC y/o el mensaje del texto no cifrado y/o sus partes.

El cifrado puede ser realizado asimismo sobre toda o parte de la cabecera de PDCP, por ejemplo, excluyendo el SN.

Se puede incluir una indicación de si la carga útil ha sido cifrada y/o protegida en integridad. Por ejemplo, la capa de PDCP 610 en el lado de transmisión puede incluir un IE indicando la presencia de información de comprobación de integridad y/o que el cifrado está activado. Esta indicación puede estar cifrada. Esta indicación puede indicar la posición de la palabra de MAC dentro del mensaje para que la capa de PDCP la compruebe. La capa de PDCP 610 en el lado de recepción puede utilizar esta indicación para decidir si descifrar y/o comprobar la integridad.

La capa de PDCP 610 y el protocolo pueden incluir una palabra de MAC para la comprobación de la integridad en una posición predefinida dentro de la cabecera de PDCP / mensaje para el receptor. De manera alternativa, la posición de una palabra de MAC puede ser indicada a la capa de PDCP 610 de recepción. Tal indicación puede ser, como ejemplo, un campo de desfase en la cabecera.

Dependiendo del orden de la operación de seguridad en el lado de transmisión, el PDCP de recepción descifrará un mensaje entrante en primer lugar y, a continuación, comprobará su integridad, o primero comprobará la integridad y a continuación descifrará el mensaje. Las operaciones de seguridad en la unidad de recepción son en el orden inverso al de la unidad de transmisión. La posición de la palabra de MAC dentro de la cabecera de PDCP / mensaje puede ser asistida mediante un campo de indicación.

La capa de PDCP 610 puede decidir si el cifrado y/o la protección en integridad no es satisfactoria para un mensaje particular. Esto significa que el PDCP determinará si el mensaje ha sido o no cifrado y/o protegido en integridad correctamente.

La capa de PDCP 610 puede indicar a la capa de RRC el estado de seguridad del mensaje que está pasando a la capa de RRC 620, por ejemplo, si el mensaje es recibido con cifrado y/o protección en integridad. O, como ejemplo adicional, si la comprobación de protección en integridad tuvo o no éxito. La indicación puede ser implícita, es decir, solo proporcionada cuando existe un error, por ejemplo, si la comprobación de la protección en integridad falla. La capa de RRC 620 puede entonces decidir si la protección para un mensaje particular es aceptable. El comportamiento del RRC cuando se le notifica un error puede ser tal como se define para el PDCP en el párrafo [0064]. De manera alternativa o, además, la capa de RRC puede notificar a la red el fallo de la comprobación de integridad añadiendo un elemento de información (al mensaje de RRC que envía a la red) que informa a la red del fallo.

En caso de error, la capa de PDCP 610 puede llevar a cabo las etapas descritas en los escenarios de manejo del fallo presentados anteriormente. Si el mensaje del RRC es ASN.1 codificado y la palabra de MAC está incluida en la capa de RRC 620, la capa de PDCP 610 puede mirar en la capa de RRC y comprobar la palabra de MAC. Puede hacer eso si la marca que indica protección en integridad está establecida.

Procedimientos de seguridad transversal

La capa de RRC / PDCP puede recibir las claves de eNB / RRC / plano-U de la capa de NAS o de la USIM. De manera alternativa, el RRC / PDCP puede generar sus propias claves. Como ejemplo, la capa de RRC puede generar las claves e-NB / RRC / plano-U utilizando parámetros recibidos desde la red en la señalización de RRC y el ASME recibido desde el NAS y otros parámetros recibidos desde otras capas de protocolo (por ejemplo, la identidad de célula física de la célula en la cual la WTRU se encuentra actualmente o cuyo acceso es posible obtener a partir de la capa física). Estas claves de seguridad se pueden pasar entre el NAS y el RRC / PDCP, o entre el RRC y el PDCP utilizando primitivas predeterminadas, incluyendo primitivas nuevas o existentes, sobre SAP nuevos o existentes. Cada capa puede tener la capacidad de indicar un error, es decir, un fallo de seguridad, a las capas superiores / inferiores.

La figura 7 es un diagrama de bloques de un sistema de comunicación inalámbrico 700 configurado para intercambio de mensajes cifrados y no cifrados en LTE. El sistema incluye una estación de base 705 y una unidad de transmisión / recepción inalámbrica (WTRU) 710. La estación de base 705 y la WTRU 710 se comunican a través de un enlace de comunicaciones inalámbrico.

Como se muestra en la figura 7, la WTRU 710 incluye un transmisor 720, un receptor 730 y un procesador 740. El procesador 740 está unido a una memoria temporal 750 y a una memoria 760. El procesador 740 está configurado para procesar mensajes de NAS que contienen parámetros de seguridad utilizando al menos una técnica descrita anteriormente.

También mostrada en la figura 7 se encuentra la estación de base 705 que incluye un transmisor 765, un receptor 770 y un procesador 780. El procesador 780 está unido a una memoria temporal 790 y a una memoria 795. El procesador 780 está configurado para procesar mensajes de NAS que contienen parámetros de seguridad que utilizan al menos una técnica descrita anteriormente.

Aunque las características y elementos se describen en combinaciones particulares, cada característica o elemento puede ser utilizado solo sin ninguna otra característica ni elemento, o en varias combinaciones con o sin otras características y elementos. Los métodos o diagramas de flujo proporcionados pueden ser implementados en un programa informático, software o firmware realizado de manera tangible en un medio de almacenamiento legible por ordenador, para su ejecución mediante un ordenador de propósito general o un procesador. Ejemplos de medios de almacenamiento legibles por ordenador incluyen una memoria de solo lectura (ROM – Read Only Memory, en inglés), una memoria de acceso aleatorio (RAM – Random Access Memory, en inglés), un registro, una memoria oculta, dispositivos de memoria de semiconductores, medios magnéticos tales como discos duros internos y discos desmontables, medios opto-magnéticos y medios ópticos tales como discos de CD-ROM, y discos versátiles digitales (DVD – Digital Versatile Disk, en inglés).

Procesadores adecuados incluyen, a modo de ejemplo, un procesador de propósito general, un procesador de propósito especial, un procesador convencional, un procesador de señal digital (DSP – Digital Signal Processor, en inglés), una pluralidad de microprocesadores, uno o más procesadores en asociación con un núcleo de DSP, un controlador, un microcontrolador, circuitos integrados específicos para una aplicación (ASIC – Application Specific Integrated Circuits, en inglés), circuitos de matrices de puertas programables en campo (FPGA – Field Programmable Gate Array, en inglés) y otro tipo de circuito integrado (IC - Integrated Circuit, en inglés) y/o una máquina de estados.

Un procesador en asociación con software puede ser utilizado para implementar un transceptor de radiofrecuencia para su utilización en una unidad de transmisión / recepción (WTRU), un equipo de usuario (UE), un terminal, una estación de base, un controlador de red de radio (RNC) o cualquier ordenador anfitrión. La WTRU puede ser utilizada junto con módulos, implementados en hardware y/o software, tal como una cámara, un módulo de cámara de video, un videoteléfono, un altavoz, un dispositivo de vibración, un altavoz, un micrófono, un transceptor de televisión, unos cascos inalámbricos, un teclado, un módulo de Bluetooth®, una unidad de radio de frecuencia modulada (FM), una unidad de visualización de pantalla de cristal líquido (LCD – Liquid Crystal Display, en inglés), una unidad de visualización de diodos emisores de luz orgánicos (OLED – Organic Light-Emitting Diode, en inglés), un reproductor de música digital, un reproductor de medios, un módulo reproductor de videojuegos, un navegador por Internet y/o un módulo de red de área local inalámbrica (WLAN – Wireless Local Area Network, en inglés).

Realizaciones

1. Una unidad de transmisión / recepción (WTRU) configurada para implementar seguridad en las comunicaciones inalámbricas de evolución a largo plazo (LTE), comprendiendo la WTRU:

un receptor configurado para recibir un mensaje de estrato de no acceso (NAS), conteniendo el mensaje de NAS parámetros de seguridad; y

un procesador configurado para:

determinar si los parámetros de seguridad son correctos; y

llevar a cabo un procedimiento de seguridad basado en la determinación.

2. La WTRU de la realización 1, en la que el procesador comprende:

un motor controlador de recursos de radio (RRC) de cifrado; y

un motor de NAS de cifrado.

3. La WTRU de cualquiera de las realizaciones 1 – 2, en el que el procesador comprende:

un motor de cifrado configurado para operar con parámetros tanto del RRC como de NAS.

4. La WTRU de la realización 1, en la que el procedimiento de seguridad incluye al menos uno de lo siguiente: ignorar el mensaje, borrar el mensaje, informar de un fallo a otra capa de protocolo, iniciar una reautenticación, pasar al modo de gestión de movilidad (EMM_Reposo) del sistema de paquetes evolucionado (EPS), pasar al estado EMM_Eliminado del registro, guardar el recuento del número de fallos, proceder a una reconexión a una red y borrar los parámetros de seguridad.

5. Un método para implementar seguridad en un dispositivo inalámbrico de la evolución a largo plazo (LTE), comprendiendo el método:

recibir un mensaje de estrato de no acceso (NAS), conteniendo el mensaje de NAS parámetros de seguridad;

determinar si los parámetros de seguridad son correctos; y

llevar a cabo un procedimiento de seguridad basado en la determinación.

6. El método de la realización 5, en el que el procedimiento de seguridad incluye al menos uno de lo siguiente: ignorar el mensaje, borrar el mensaje, informar de un fallo a otra capa de protocolo, iniciar una reautenticación, pasar al modo de gestión de movilidad (EMM_Reposo) del sistema de paquetes evolucionado (EPS), pasar al estado EMM_Eliminado del registro, guardar el recuento del número de fallos, proceder a una reconexión a una red y borrar los parámetros de seguridad.

7. El método de cualquiera de las realizaciones 5 – 6, en el que el mensaje de NAS contiene una cabecera de protocolo que incluye un número de secuencia de NAS.

8. El método de cualquiera de las realizaciones 5 – 7, que comprende, además:

efectuar una detección duplicada basada en el número de secuencia de NAS.

9. El método de cualquiera de las realizaciones 5 – 8, en el que el número de secuencia de NAS funciona como un identificador de transacción.

10. El método de cualquiera de las realizaciones 5 – 8, en el que el número de secuencia de NAS contiene un periodo de incremento predefinido.

11. El método de cualquiera de las realizaciones 5 – 8, en el que el número de secuencia de NAS contiene un período de incremento negociado.

12. El método de cualquiera de las realizaciones 5 – 11, en el que el mensaje de NAS está correlacionado con un valor de RECUENTO.

13. El método de la realización 12, en el que el valor de RECUENTO está cifrado (RECUENTO-C).

14. El método de cualquiera de las realizaciones 11 – 12, en el que el valor de RECUENTO es para protección en integridad (RECUENTO-I).

15. El método de cualquiera de las realizaciones 11 – 14, en el que el valor de RECUENTO es una combinación de un RECUENTO-C y un RECUENTO-I.

16. El método de cualquiera de las realizaciones 11 – 15, en el que el valor de RECUENTO comprende:

un número de secuencia de NAS (SN); y

un número de hipertrama de NAS (HFN).

17. El método de cualquiera de las realizaciones 11 – 16, en el que el HFN de NAS es un contador.

18. El método de cualquiera de las realizaciones 12 – 17, en el que el valor de RECUENTO se utiliza como dato de entrada a un algoritmo de protección en integridad de cifrado.

19. El método de la realización 12 – 18, en el que el valor de RECUENTO se utiliza como dato de entrada a un algoritmo de protección en integridad de descifrado.

20. El método de cualquiera de las realizaciones 12 – 19, en el que el valor de RECUENTO se configura antes de la activación de la seguridad de NAS.

21. El método de cualquiera de las realizaciones 12 – 20, en el que el valor de RECUENTO es 32 bits o menos.

22. El método de cualquiera de las realizaciones 16 – 21, en el que el SN y el HFN son configurables.

23. El método de cualquiera de las realizaciones 12 – 22, en el que el valor de RECUENTO es el número de secuencia de NAS (SN) y la detección duplicada se efectúa utilizando el valor de RECUENTO.

24. El método de cualquiera de las realizaciones 5 – 23, en el que el mensaje de NAS indica información de capacidad de unidad de transmisión / recepción inalámbrica (WTRU).

25. El método de la realización 24, en el que la información de capacidad de WTRU indica soporte para el cifrado a nivel de NAS.

26. Un método para implementar seguridad en un dispositivo inalámbrico de evolución a largo plazo (LTE), comprendiendo el método:

recibir una unidad de datos de protocolo (PDU) del protocolo de convergencia de datos en paquetes (PDCP), incluyendo la PDU de PDCP parámetros de seguridad;

determinar si los parámetros de seguridad son correctos; y

llevar a cabo un procedimiento de seguridad basado en la determinación.

27. El método de la realización 26, que comprende, además:

enviar una indicación desde la capa del controlador de recursos de radio (RRC) a una capa de PDCP indicando si un mensaje de RRC requiere al menos uno de protección en integridad y cifrado.

28. El método de cualquiera de las realizaciones 26 -27, que comprende, además:

enviar una indicación desde la capa de RRC a la capa de PDCP indicando que el mensaje de RRC que se va a transmitir no requiere al menos uno de protección en integridad y cifrado.

29. El método de cualquiera de las realizaciones 27 – 28, que comprende, además:

indicar a una capa de PDCP que todos los mensajes de RRC serán cifrados o protegidos en integridad.

30. El método de cualquiera de las realizaciones 27 – 29, que comprende, además:

indicar a una capa de PDCP que todos los mensajes de RRC que empiezan con un mensaje de RRC predeterminado estarán cifrados y con protección en integridad.

31. El método de cualquiera de las realizaciones 27 – 30, que comprende, además:

establecer una marca de comprobación de cifrado o de integridad en el RRC para cifrar o comprobar en integridad los mensajes de RRC.

32. El método de la realización 31, que comprende, además:

cifrar los mensajes de RRC en la capa de PDCP antes de transmitirlos como PDU de PDCP y descifrar todas las PDU de PDCP recibidas correspondientes a mensajes de RRC si la marca de cifrado está configurada, y no realizar cifrado y descifrado si la marca de cifrado no está configurada.

33. El método de cualquiera de las realizaciones 31 – 32, que comprende, además:

adjuntar un código de autenticación de mensaje en las PDU de PDCP correspondientes a los mensajees de RRC transmitidos y realizar una comprobación de integridad en todas las PDU de PDCP recibidas que mapean a los mensajes de RRC si la marca de comprobación de integridad está establecida, y no adjuntar ni comprobar la integridad si la marca no está establecida.

34. El método de cualquiera de las realizaciones 27 – 33, que comprende, además:

establecer una marca de cifrado y de comprobación de integridad en el RRC para cifrar y comprobar en integridad los mensajes de RRC.

35. El método de la realización 34, que comprende, además:

cifrar los mensajes de RRC antes de transmitirlos como PDU de PDCP, descifrar las PDU de PDCP recibidas correspondientes a los mensajes de RRC, adjuntar un código de autenticación de mensaje en las PDU de PDCP correspondientes a los mensajes de RRC transmitidos y efectuar una comprobación de integridad en todas las PDU de PDCP recibidas que mapean a los mensajes de RRC si la marca de cifrado y comprobación de integridad está establecida, y no realizar cifrado, descifrado, adición y comprobación de integridad si la marca no está establecida.

36. El método de cualquiera de las realizaciones 27 – 35, que comprende, además:

proporcionar una lista de mensajes de RRC genéricos y sus parámetros asociados al PDCP.

37. El método de cualquiera de las realizaciones 27 – 36, en el que la capa de PDCP no realiza al menos un cifrado o protección en integridad de mensajes de RRC a menos que el RRC le indique que lo haga.

38. El método de cualquiera de las realizaciones 27 – 37, que comprende, además:

cifrar el mensaje de RRC; y

proteger en integridad el mensaje de RRC.

39. El método de cualquiera de las realizaciones 27 – 38, en el que el mensaje de RRC es rellenado para conseguir una longitud óptima para el cifrado o la protección en integridad.

40. El método de cualquiera de las realizaciones 26 – 39, que comprende, además:

calcular una palabra de código de autenticación de mensaje (MAC) para la protección en integridad sobre datos de texto no cifrado, datos cifrados, una cabecera de PDCP parcial o una cabecera de PDCP completa.

41. El método de cualquiera de las realizaciones 26 – 40, en el que el cifrado se efectúa sobre datos de texto no cifrado parciales.

42. El método de cualquiera de las realizaciones 26 – 41, que comprende, además:

indicar si una carga útil ha sido cifrada o protegida en integridad.

43. El método de cualquiera de las realizaciones 26 – 42, que comprende, además:

predefinir una palabra de código de autenticación de mensaje (MAC) en una posición dentro de la PDU de PDCP, incluyendo la PDU de PDCP una cabecera.

44. El método de la realización 43, en el que la posición de la palabra de MAC predefinida es en la cabecera de la PDU de PDCP.

45. El método de cualquiera de las realizaciones 26 – 44, en el que el procedimiento de seguridad incluye al menos uno de lo siguiente: ignorar un mensaje de RRC, borrar el mensaje, informar de un fallo en un informe de fallo, guardar el recuento del número de fallos y borrar los parámetros de seguridad.

46. El método de la realización 45, en el que el informe de fallos incluye la razón del fallo.

47. El método de cualquiera de las realizaciones 26 – 46, que comprende, además:

utilizar un número de hipertrama de PDCP (HFN) para constituir un valor de RECUENTO.

48. Un método para implementar seguridad en un dispositivo inalámbrico de la evolución a largo plazo (LTE), comprendiendo el método:

recibir un mensaje en una capa de protocolo de convergencia de datos de protocolo (PDCP);

descifrar el mensaje; y

efectuar una comprobación de integridad del mensaje recibido.

49. El método de la realización 48, en el que la comprobación de integridad del mensaje recibido se efectúa antes del descifrado del mensaje.

50. El método de cualquiera de las realizaciones 48 – 49, que comprende, además:

determinar la posición de una palabra de código de autenticación del mensaje (MAC) dentro del mensaje recibido.

51. El método de cualquiera de las realizaciones 48 – 50, que comprende, además:

determinar si el cifrado y la protección en integridad son satisfactorios.

52. El método de cualquiera de las realizaciones 48 – 51, que comprende, además:

indicar el estado de seguridad del mensaje recibido a una capa de controlador de recursos de radio (RRC).

53. El método de cualquiera de las realizaciones 48 – 52, que comprende, además:

enviar una indicación desde la capa de PDCP a una capa de controlador de recursos de radio (RRC) indicando si la comprobación de la integridad ha fallado en un mensaje de RRC recibido.

54. El método de cualquiera de las realizaciones 48 – 53, que comprende, además:

enviar una indicación desde la capa de PDCP a una capa de controlador de recursos de radio (RRC) indicando si la comprobación de la integridad ha tenido éxito en un mensaje de RRC recibido.

55. El método de cualquiera de las realizaciones 48 – 54, que comprende, además:

enviar una indicación desde la capa de PDCP a la capa de RRC de que la comprobación de la integridad ha fallado solo si se produce un número de fallos predeterminado en un intervalo de tiempo predeterminado o número de mensajes de RRC recibidos.

56. El método de cualquiera de las realizaciones 48 – 55, que comprende, además:

comprobar una palabra de código de autenticación de mensaje (MAC) en una capa de controlador de recursos de radio (RRC) del PDCP cuando el mensaje recibido es un mensaje codificado ASN.1.

57. El método de cualquiera de las realizaciones 48 – 56, en el que implementar seguridad incluye al menos uno de lo siguiente: ignorar el mensaje, borrar el mensaje, informar de un fallo en un informe de fallos, guardar el recuento del número de fallos y borrar los parámetros de seguridad.

58. El método de la realización 57, en el que el informe de fallos incluye una razón para el fallo.

59. Un método para el manejo de claves en una unidad de transmisión / recepción (WTRU) tras la transición del modo EMM_Conectado al modo EMM_Reposo, comprendiendo el método:

indicar la transición a una entidad de almacenamiento en la WTRU; y borrar un primer conjunto de claves.

60. El método de la realización 59, que comprende, además:

guardar las claves de seguridad de NAS y las claves de ASME.

61. El método de cualquiera de las realizaciones 59 – 60, que comprende, además:

borrar las claves de seguridad de NAS y las claves de ASME.

62. El método de cualquiera de las realizaciones 59 – 61, en el que la indicación se proporciona mediante un estrato de no acceso (NAS).

63. El método de cualquiera de las realizaciones 59 – 62, en el que la indicación se proporciona mediante un estrato de acceso (AS).

64. El método de cualquiera de las realizaciones 59 – 63, en el que la indicación se proporciona utilizando primitivas predeterminadas.

65. El método de cualquiera de las realizaciones 59 – 65, en el que la indicación se proporciona cuando un e-NB de servicio cambia mientras se encuentra en modo EMM_Reposo.

66. El método de cualquiera de las realizaciones 59 – 66, en el que el primer conjunto de claves incluye al menos una de las siguiente: K_{eNB}, $K_{RRC\ enc}$, $K_{RRC\ int}$ y $K_{UP\ enc}$.

67. El método de cualquiera de las realizaciones 59 – 67, en el que la entidad de almacenamiento borra $K_{RRC\ enc}$, $K_{RRC\ int}$ y $K_{UP\ enc}$ tras la recepción de la indicación.

68. El método de cualquiera de las realizaciones 59 – 68, en el que la entidad de almacenamiento borra K_{eNB} tras la recepción de la indicación.

69. El método de cualquiera de las realizaciones 59 – 69, que comprende, además:

generar un segundo conjunto de claves tras la recepción de la indicación.

70. El método de cualquiera de las realizaciones 59 – 70, en el que la indicación indica un cambio en la célula de servicio.

71. El método de cualquiera de las realizaciones 59 – 71, en el que el primer conjunto de claves incluye un valor de temporizador.

72. El método de cualquiera de las realizaciones 5 – 72, que comprende, además:

recibir claves desde una capa de NAS o desde un USIM.

73. El método de la realización 72, en el que las claves recibidas son pasadas entre la capa de estrato de no acceso (NAS) a un RRC / PDCP utilizando primitivas predeterminadas.

74. El método de cualquiera de las realizaciones 73 – 75, en el que las claves recibidas son pasadas entre el RRC y el PDCP utilizando primitivas predeterminadas.

REIVINDICACIONES

1. Método para llevar a cabo un procedimiento de seguridad de estrato de no acceso, NAS en comunicaciones inalámbricas, comprendiendo el método:

recibir (305), en una unidad de transmisión / recepción, WTRU, un mensaje de NAS que comprende un número de secuencia de NAS, SN de NAS, (410) y una cabecera de protocolo (400);

efectuar una comprobación de integridad (310) en el mensaje de NAS utilizando un valor de RECUENTO como dato de entrada a un algoritmo de integridad, en el que el valor de RECUENTO comprende un SN de NAS (410) y un HFN de NAS que puede ser un contador que se incrementa en uno por cada número predeterminado de incrementos de SN de NAS;

en repuesta al mensaje de NAS recibido (315), fallar la comprobación de integridad (310), ignorando el mensaje de NAS; y

en respuesta al mensaje de NAS recibido, borrar la comprobación de integridad (310), procesando (360) el mensaje de NAS.

2. El método de la reivindicación 1, en el que el mensaje de NAS incluye además una cabecera (400) que incluye además un discriminador de protocolo (420), un octeto de tipo de mensaje, un identificador de transacción, TI (430) y un sub-discriminador de protocolo.

3. El método de la reivindicación 1, en el que el SN de NAS (410) se encuentra en la cabecera de protocolo recibida (400) del mensaje de NAS.

4. El método de la reivindicación 1, en el que el SN de NAS (410) se recibe como contenido de un elemento de información, IE.

5. El método de la reivindicación 2, en el que el TI (430) funciona como el SN de NAS (410).

6. El método de la reivindicación 1, en el que el SN de NAS (410) tiene un periodo de incremento predefinido o un periodo de incremento negociado.

7. El método de la reivindicación 1, en el que el valor de RECUENTO se incrementa de manera predefinida o de manera negociada.

8. El método de la reivindicación 1, en el que ignorar el mensaje de NAS incluye al menos uno de: ignorar (325) el mensaje de NAS, borrar (325) el mensaje de NAS, informar (330) de un fallo a otra capa de protocolo, iniciar (335) una reautenticación, pasar (340) al modo de EMM_Reposo de gestión de movilidad del sistema de paquetes evolucionado, EPS, pasar (340) al estado EMM_Eliminado del registro, guardar (345) un recuento del número de fallos, proceder a la reconexión (350) a una red, y borrar (355) el SN de NAS.

9. Una unidad de transmisión / recepción inalámbrica, WTRU (710) configurada para llevar a cabo un procedimiento de seguridad de estrato de no acceso, NAS en comunicaciones inalámbricas, comprendiendo la WTRU (710):

un receptor (730) configurado para recibir (305) un mensaje de NAS que comprende un número de secuencia de NAS, SN de NAS, (410) y una cabecera de protocolo (400);

un procesador (740) configurado para efectuar una comprobación de integridad (310) en el mensaje de NAS utilizando un valor de RECUENTO como dato de entrada a un algoritmo de integridad, en el que el valor de RECUENTO incluye un SN de NAS (410), y un HFN de NAS que puede ser un contador que se incrementa en uno por cada número predeterminado de incrementos del SN de NAS;

en respuesta al mensaje de NAS (315) de fallo en la comprobación de integridad (310), el procesador (740) está configurado además para ignorar el mensaje de NAS; y

en respuesta al mensaje de NAS de borrar la comprobación de integridad (310), el procesador (740) está configurado además para procesar (360) el mensaje de NAS.

10. La WTRU de la reivindicación 9, en la que el mensaje de NAS incluye además una cabecera de mensaje (400) que comprende un discriminador de protocolo (420), un octeto de tipo de mensaje, un identificador de transacción, TI (430) y un discriminador de protocolo.

11. La WTRU de la reivindicación 9, en la que el SN de NAS (410) está en la cabecera del protocolo recibida (400) del mensaje de NAS.

12. La WTRU de la reivindicación 9, en la que el SN de NAS (410) se recibe como contenido de un elemento de información, IE.

13. La WTRU de la reivindicación 10, en la que el TI (430) funciona como el SN de NAS (410).

14. La WTRU de la reivindicación 11, en la que el SN de NAS (410) tiene un periodo de incremento predefinido o un periodo de incremento negociado.

15. La WTRU de la reivindicación 9, en la que el valor de RECUENTO se incrementa de manera predefinida o de manera negociada.

16. La WTRU de la reivindicación 9, en la que ignorar el mensaje de NAS incluye al menos uno de: ignorar (325) el mensaje de NAS, borrar (325) el mensaje de NAS, informar (330) de un fallo a otra capa de protocolo, iniciar (335) una reautenticación, pasar (340) al modo EMM_Reposo de Gestión de movilidad del sistema de paquetes evolucionado, EPS, pasar (340) al estado EMM_Eliminado del registro, guardar (345) un registro del número de fallos, proceder a la reconexión (350) a una red, y borrar (355) el SN de NAS.

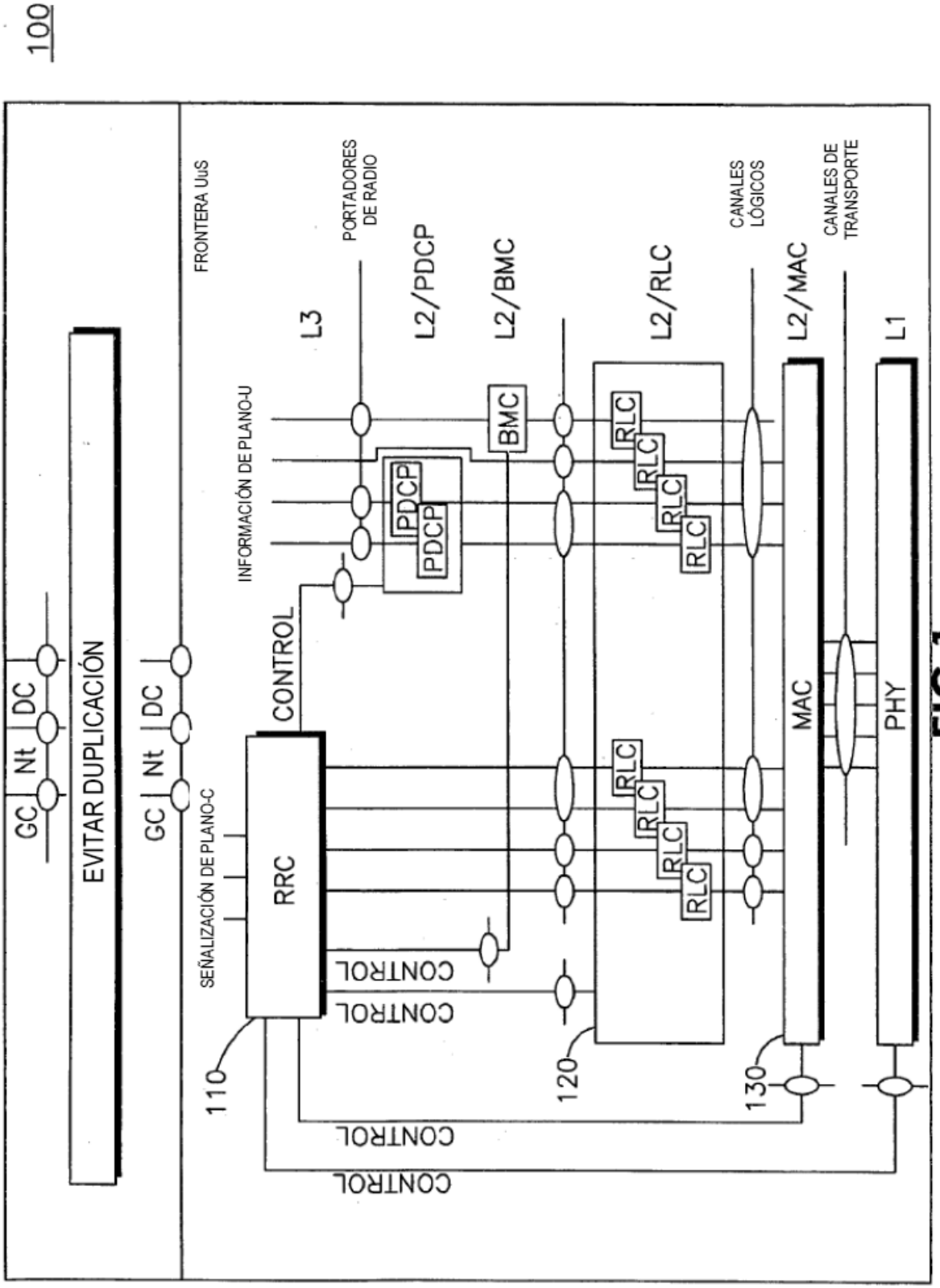
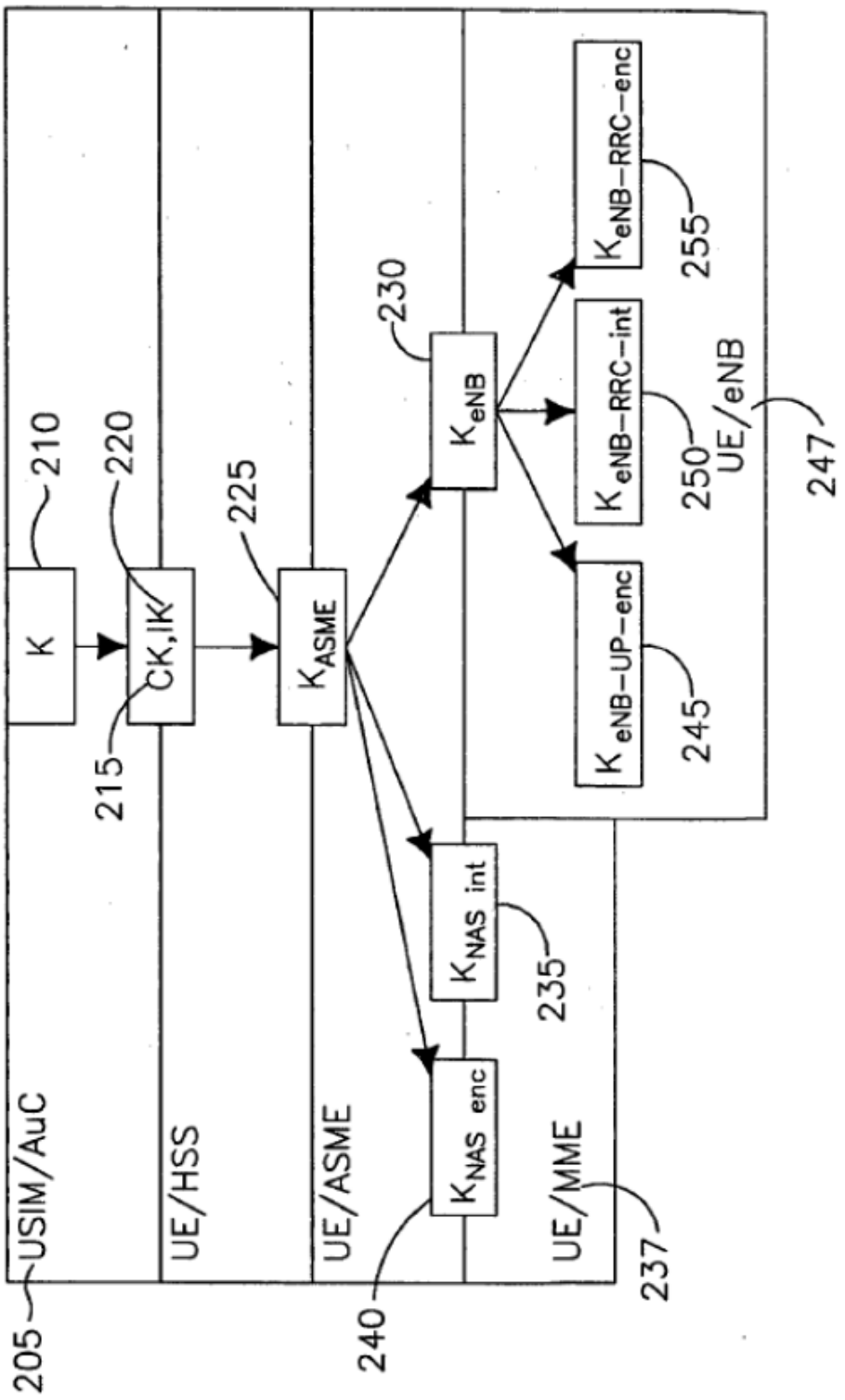

100
GC
Nt
DC
EVITAR DUPLICACIÓN
FRONTERA UuS
INFORMACIÓN DE PLANO-U
SEÑALIZACIÓN DE PLANO-C
L3
L2/PDCP
L2/BMC
L2/RLC
L2/MAC
L1
PORTADORES DE RADIO
CANALES LÓGICOS
CANALES DE TRANSPORTE
RRC
CONTROL
PDCP
BMC
RLC
MAC
PHY
110
120
130
TÉCNICA ANTERIOR

FIG.1



TÉCNICA ANTERIOR

FIG.2

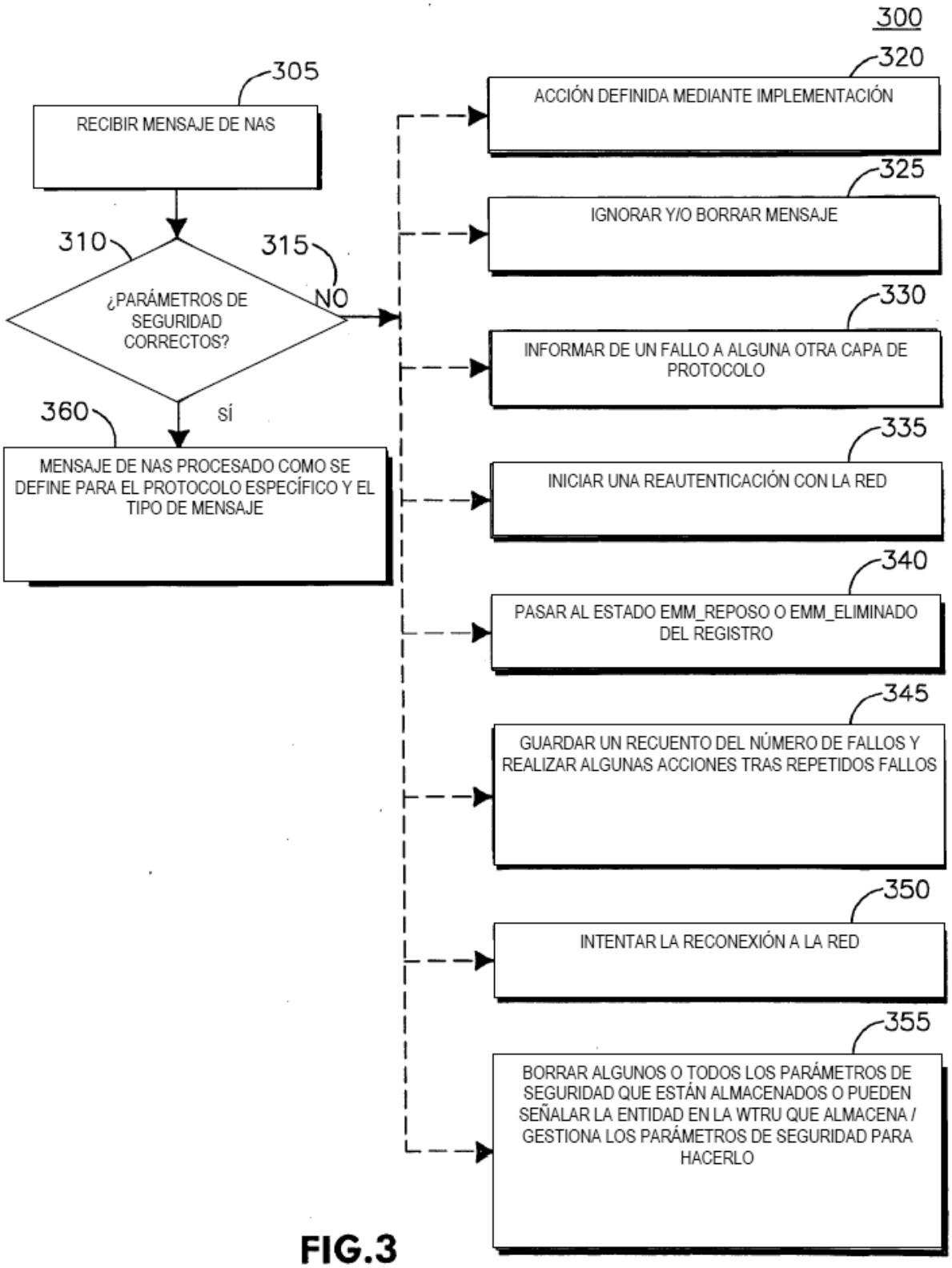

300
305
RECIBIR MENSAJE DE NAS
310
315
¿PARÁMETROS DE SEGURIDAD CORRECTOS?
NO
SÍ
360
MENSAJE DE NAS PROCESADO COMO SE DEFINE PARA EL PROTOCOLO ESPECÍFICO Y EL TIPO DE MENSAJE
320
ACCIÓN DEFINIDA MEDIANTE IMPLEMENTACIÓN
325
IGNORAR Y/O BORRAR MENSAJE
330
INFORMAR DE UN FALLO A ALGUNA OTRA CAPA DE PROTOCOLO
335
INICIAR UNA REAUTENTICACIÓN CON LA RED
340
PASAR AL ESTADO EMM_REPOSO O EMM_ELIMINADO DEL REGISTRO
345
GUARDAR UN RECUENTO DEL NÚMERO DE FALLOS Y REALIZAR ALGUNAS ACCIONES TRAS REPETIDOS FALLOS
350
INTENTAR LA RECONEXIÓN A LA RED
355
BORRAR ALGUNOS O TODOS LOS PARÁMETROS DE SEGURIDAD QUE ESTÁN ALMACENADOS O PUEDEN SEÑALAR LA ENTIDAD EN LA WTRU QUE ALMACENA / GESTIONA LOS PARÁMETROS DE SEGURIDAD PARA HACERLO

FIG.3

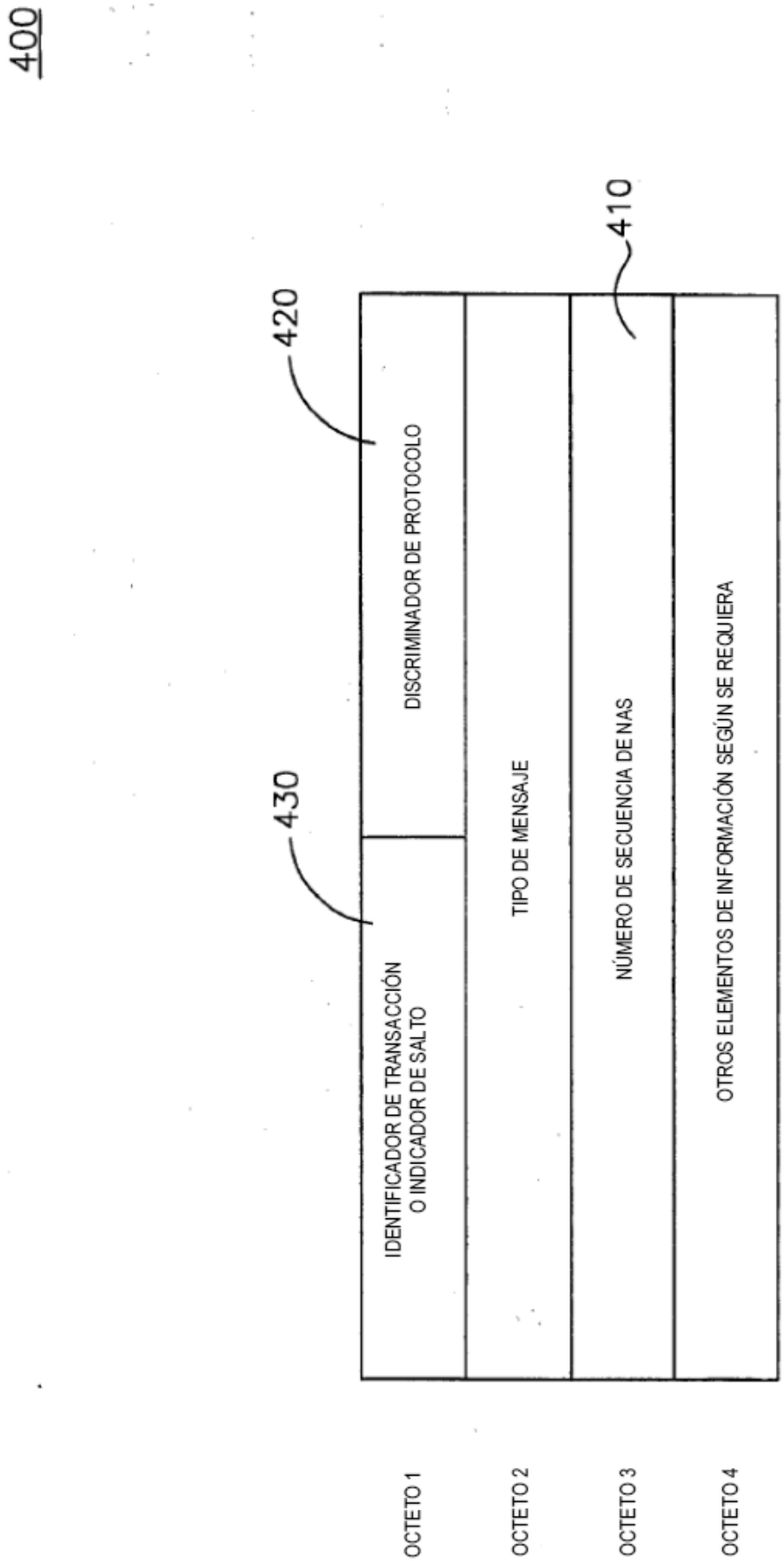

400
410
420
430
DISCRIMINADOR DE PROTOCOLO
TIPO DE MENSAJE
NÚMERO DE SECUENCIA DE NAS
OTROS ELEMENTOS DE INFORMACIÓN SEGÚN SE REQUIERA
IDENTIFICADOR DE TRANSACCIÓN O INDICADOR DE SALTO
OCTETO 1
OCTETO 2
OCTETO 3
OCTETO 4

FIG.4

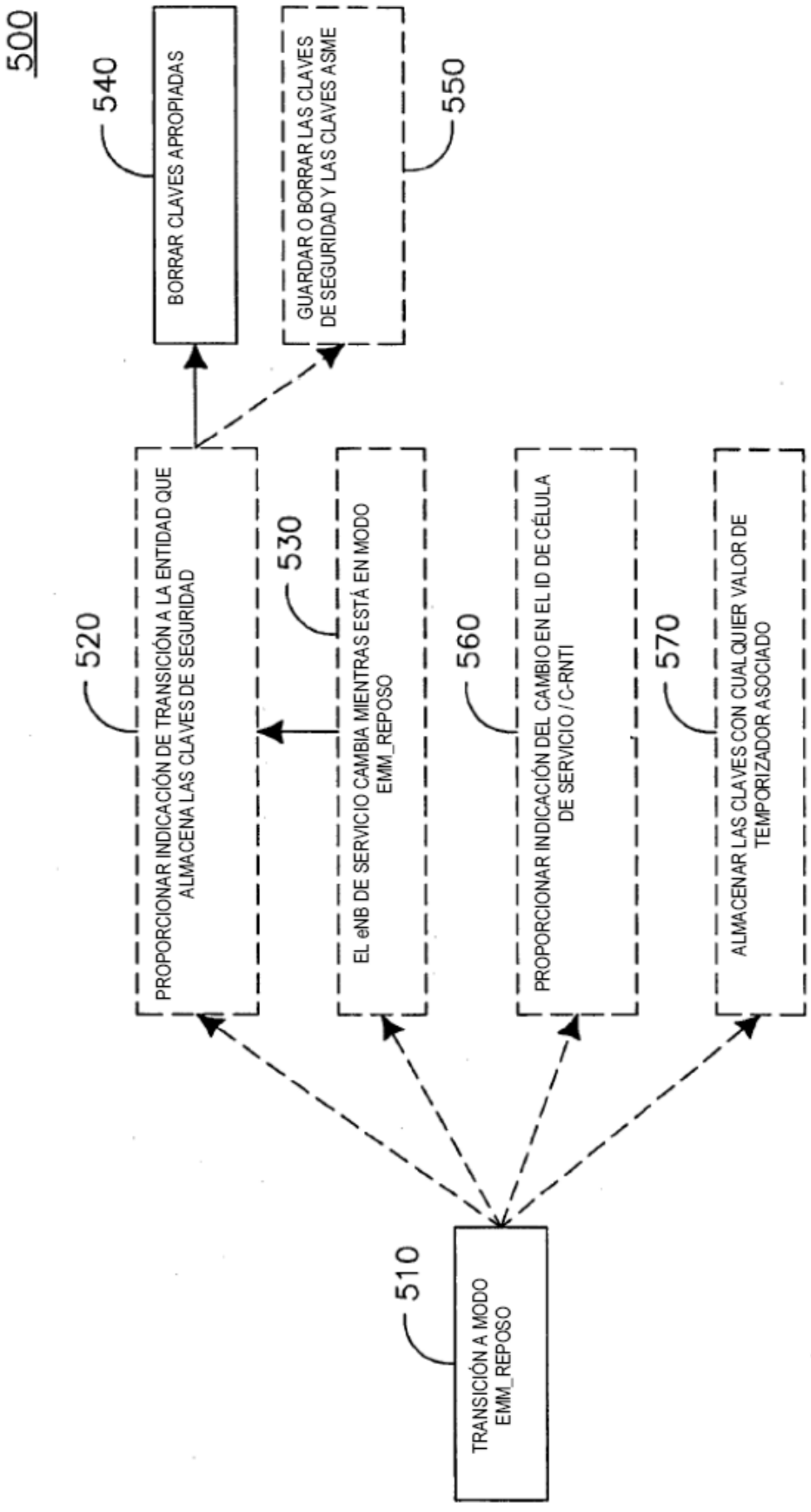

500
510
TRANSICIÓN A MODO EMM_REPOSO
520
PROPORCIONAR INDICACIÓN DE TRANSICIÓN A LA ENTIDAD QUE ALMACENA LAS CLAVES DE SEGURIDAD
530
EL eNB DE SERVICIO CAMBIA MIENTRAS ESTÁ EN MODO EMM_REPOSO
560
PROPORCIONAR INDICACIÓN DEL CAMBIO EN EL ID DE CÉLULA DE SERVICIO / C-RNTI
570
ALMACENAR LAS CLAVES CON CUALQUIER VALOR DE TEMPORIZADOR ASOCIADO
540
BORRAR CLAVES APROPIADAS
550
GUARDAR O BORRAR LAS CLAVES DE SEGURIDAD Y LAS CLAVES ASME

FIG.5

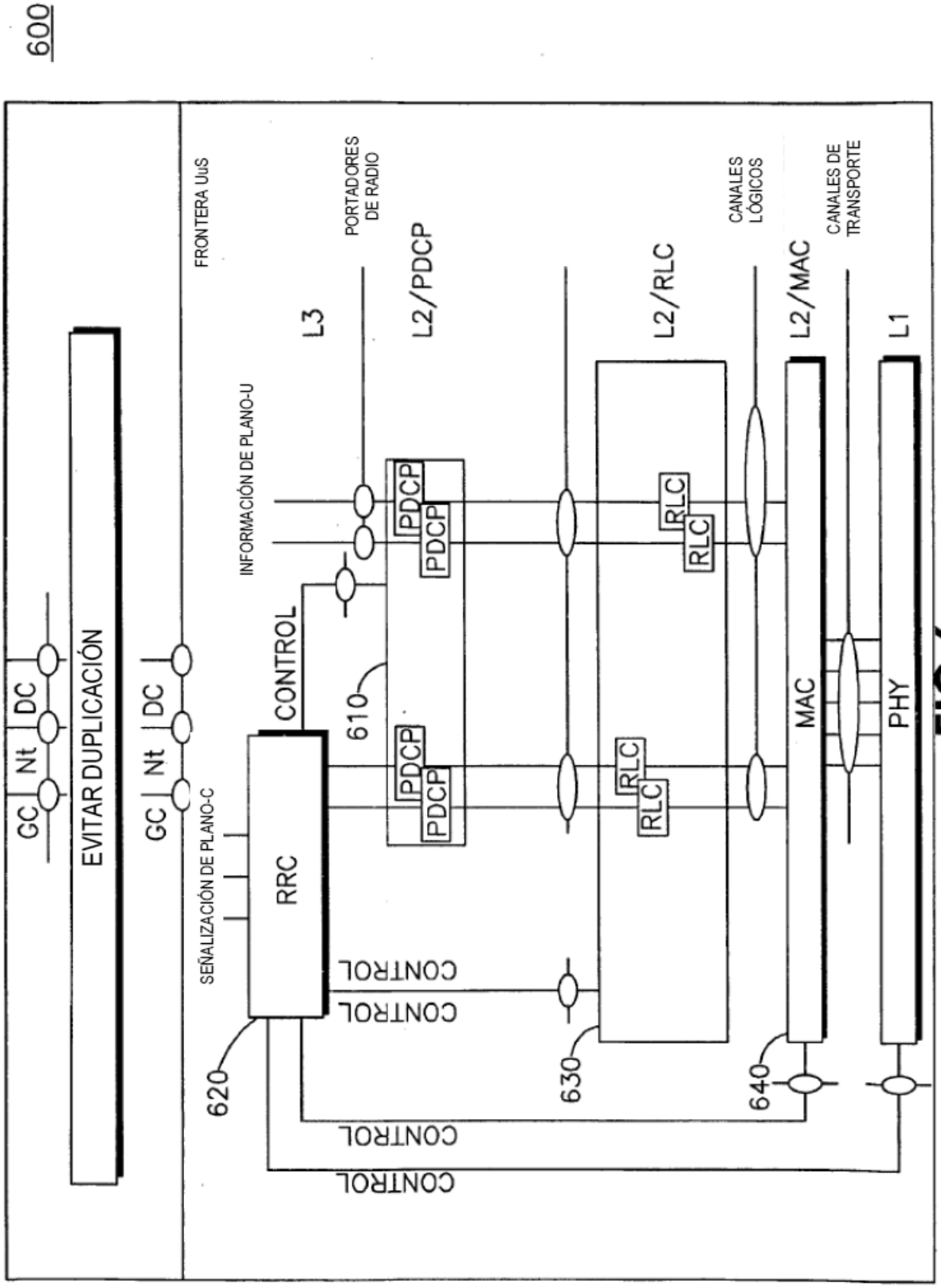

600
GC
Nt
DC
EVITAR DUPLICACIÓN
GC
Nt
DC
FRONTERA UuS
SEÑALIZACIÓN DE PLANO-C
INFORMACIÓN DE PLANO-U
L3
RRC
CONTROL
610
620
PORTADORES DE RADIO
L2/PDCP
PDCP
PDCP
PDCP
PDCP
CONTROL
CONTROL
630
L2/RLC
RLC
RLC
RLC
RLC
CANALES LÓGICOS
L2/MAC
MAC
640
CANALES DE TRANSPORTE
L1
PHY
CONTROL
CONTROL

FIG.6

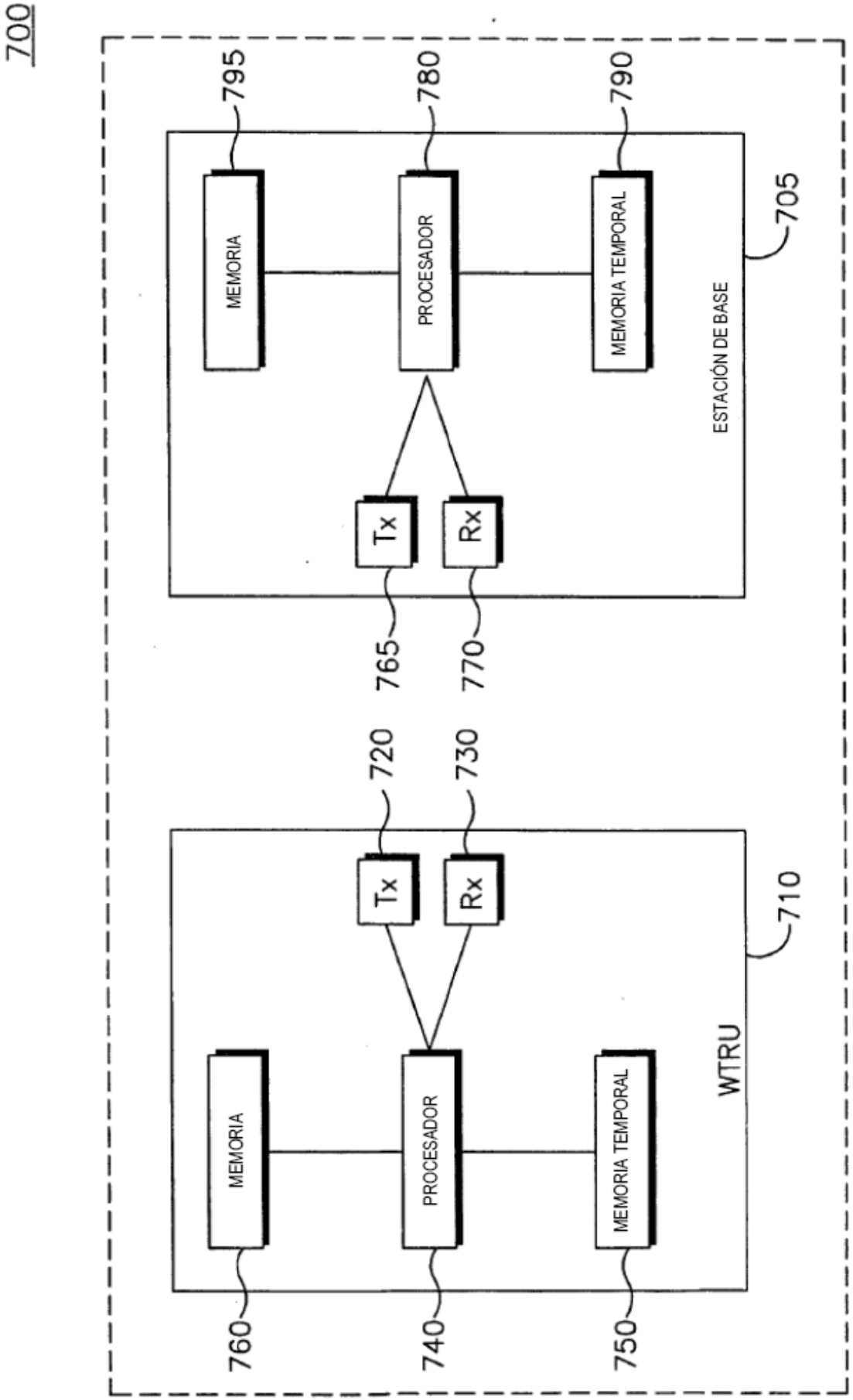

700
795
780
790
MEMORIA
PROCESADOR
MEMORIA TEMPORAL
705
ESTACIÓN DE BASE
Tx
Rx
765
770
720
730
Tx
Rx
710
WTRU
MEMORIA
PROCESADOR
MEMORIA TEMPORAL
760
740
750

FIG.7