(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 598 378**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/04 (2009.01)
H04W 36/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.01.2014 PCT/SE2014/050122**

(87) Fecha y número de publicación internacional: **07.08.2014 WO14120077**

(96) Fecha de presentación y número de la solicitud europea: **30.01.2014 E 14706972 (8)**

(97) Fecha y número de publicación de la concesión europea: **20.07.2016 EP 2951975**

(54) Título: **Generación de claves de seguridad para conectividad dual**

(30) Prioridad:

30.01.2013 US 201361758373 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.01.2017

(73) Titular/es:

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

(72) Inventor/es:

WAGER, STEFAN;
VIRKKI, VESA;
TEYEB, OUMER;
JOHANSSON, NIKLAS y
NORRMAN, KARL

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Generación de claves de seguridad para conectividad dual

Campo técnico

La tecnología divulgada en este documento se refiere en general a las redes de telecomunicaciones inalámbricas, y más particularmente se refiere a técnicas para la manipulación de claves de seguridad en situaciones de conectividad dual, es decir, situaciones en las que un terminal móvil está conectado a múltiples estaciones base simultáneamente.

Antecedentes

En un sistema de radio celular típico, los terminales móviles (también conocido como equipo de usuario, los UE, terminales inalámbricos, y/o estaciones móviles) se comunican a través de una red de acceso radio (RAN) con una o más redes de núcleo, que proporcionan acceso a redes de datos, tales como la Internet, y/o a la red de telecomunicaciones pública conmutada (PSTN). Una RAN cubre un área geográfica que se divide en áreas de célula, con cada área de célula que es servida por una estación base de radio (también referida como una estación base, un nodo de RAN, un "Nodo B", y/o un NodoB mejorado o "eNodoB"). Un área de célula es un área geográfica sobre la que la cobertura de radio es provista por el equipo de estación base en un emplazamiento de estación base. Las estaciones base se comunican a través de canales de comunicación de radio con terminales inalámbricos dentro del rango de las estaciones base.

Los operadores de sistemas de comunicaciones celulares han comenzado a ofrecer servicios de datos de banda ancha móviles basados, por ejemplo, en tecnologías inalámbricas WCDMA (acceso múltiple por división de código de banda ancha), HSPA (acceso de paquetes de alta velocidad), y evolución a largo plazo (LTE). Impulsado por la introducción de nuevos dispositivos diseñados para aplicaciones de datos, los requisitos de rendimiento del usuario final continúan aumentando. La adopción incrementada de la banda ancha móvil ha resultado en un crecimiento significativo en el tráfico manejado por las redes de datos inalámbricas de alta velocidad. En consecuencia, se desean técnicas que permitan a los operadores de telefonía celular gestionar redes de manera más eficiente.

Las técnicas para mejorar el rendimiento de enlace descendente pueden incluir técnicas de transmisión de múltiples antenas de múltiple entrada múltiple salida (MIMO), comunicación multi-flujo, despliegue de múltiples portadoras, etc. Puesto que las eficiencias espectrales por enlace pueden estar acercándose a los límites teóricos, los siguientes pasos pueden incluir la mejora de las eficiencias espectrales por unidad de superficie. Otras eficiencias para redes inalámbricas se pueden conseguir, por ejemplo, cambiando una topología de las redes tradicionales para proporcionar una uniformidad incrementada de las experiencias del usuario a través de una célula. Un enfoque es mediante el despliegue de las denominadas redes heterogéneas.

Una red homogénea es una red de estaciones base (también conocidas como Nodos B, Nodos B mejorados, o eNB) en una disposición prevista, que proporciona servicios de comunicaciones para una colección de terminales de usuario (también referidos como nodos de equipo de usuario, los UE y/o terminales inalámbricos), en la que todas las estaciones base típicamente tienen niveles similares de transmisión de potencia, patrones de antena, suelos de ruido del receptor, y/o conectividad de red de retorno a la red de datos. Por otra parte, todas las estaciones base en una red homogénea pueden generalmente ofrecer acceso sin restricciones a los terminales de usuario en la red, y cada estación base puede servir a más o menos un mismo número de terminales de usuario. Los sistemas de comunicaciones inalámbricas celulares actuales en esta categoría pueden incluir, por ejemplo, GSM (sistema global para las comunicaciones móviles), WCDMA, HSDPA (acceso de paquetes descendente de alta velocidad), LTE (evolución a largo plazo), WiMAX (interoperabilidad mundial para acceso por microondas), etc.

En una red heterogénea, las estaciones base de baja potencia (también conocidas como nodos de baja potencia (LPN), micro nodos, pico nodos, femto nodos, nodos de relé, nodos de unidad de radio remota, nodos RRU, células pequeñas, los RRU, etc.) pueden desplegarse junto con o como una capa superpuesta en las macro estaciones base planificadas y/o colocadas regularmente. Una macro estación base (MBS) puede por lo tanto proporcionar servicio sobre un área de macrocélulas relativamente grande, y cada LPN puede dar servicio a un área de célula LPN relativamente pequeña respectiva dentro del área de macrocélulas relativamente grande.

La potencia transmitida por un LPN puede ser relativamente pequeña, por ejemplo, 2 vatios, en comparación con la potencia transmitida por una macro estación base, que puede ser de 40 vatios para una típica macro estación base. Un LPN puede ser desplegado, por ejemplo, para reducir/eliminar un orificio(s) de cobertura en la cobertura provista por las macro estaciones base, y/o para descargar el tráfico de las macro estaciones base, para incrementar la capacidad en una localización de tráfico alto o el llamado punto caliente. Debido a su baja potencia de transmisión y su tamaño físico más pequeño, un LPN puede ofrecer una mayor flexibilidad para la adquisición del emplazamiento.

Por lo tanto, una red heterogénea cuenta con un despliegue de múltiples capas de nodos de alta potencia (los HPN), tales como macro estaciones base, y nodos de baja potencia (los LPN), tales como las denominadas pico estaciones

base o pico nodos. Los LPN y los HPN en una región dada de una red heterogénea pueden operar en la misma frecuencia, en cuyo caso el despliegue puede ser referido como un despliegue heterogéneo de co-canal, o en diferentes frecuencias, en cuyo caso el despliegue puede ser referido como un despliegue heterogéneo de interfrecuencia o de multiportadora o de multifrecuencias.

El proyecto asociación de tercera generación (3GPP) continúa desarrollando especificaciones para las características avanzadas y mejoradas en el contexto del sistema de telecomunicaciones inalámbricas de cuarta generación conocida como LTE (evolución a largo plazo). En la versión 12 de las especificaciones de LTE y más allá, se tendrán en cuenta mejoras adicionales relacionadas con los nodos de baja potencia y despliegues heterogéneos en el marco de las actividades "de mejoras de células pequeñas". Algunas de estas actividades se centrarán en lograr un grado aún mayor de interfuncionamiento entre las macro capas y de baja potencia, en particular mediante el uso de un conjunto de técnicas y tecnologías que se refiere como "la conectividad de doble capa" o simplemente "la conectividad dual."

Como se muestra en la figura 1, la conectividad dual implica que el dispositivo tiene conexiones simultáneas a ambas macro capas y de baja potencia. La figura 1 ilustra un ejemplo de una red heterogénea en la que un terminal móvil 101 usa múltiples flujos, por ejemplo, un flujo de anclaje desde la macro estación base (o "eNB de anclaje") 401A y un flujo auxiliar desde una estación base pico (o un "eNB auxiliar") 401B. Hay que señalar que la terminología puede variar - la estación base de anclaje y la estación base auxiliar en una configuración como la mostrada en la figura 1 pueden a veces ser referidas como estaciones base "maestro" y "esclavo" o de acuerdo con otros nombres. Debería señalarse, además, que mientras que los términos "anclaje/auxiliar" y "maestro/esclavo" sugieren una relación jerárquica entre las estaciones base que participan en un escenario de conectividad dual, muchos de los principios y técnicas asociados con la conectividad dual pueden aplicarse a los escenarios de despliegue donde no existe tal relación jerárquica, por ejemplo, entre las estaciones base peer. En consecuencia, mientras que los términos "estación base de anclaje" y "estación base auxiliar" se usan en este documento, se debe entender que las técnicas y aparatos descritos en este documento no se limitan a realizaciones que usan esa terminología, ni están necesariamente limitados a realizaciones que tienen la relación jerárquica sugerida por la figura 1.

La conectividad dual puede implicar, en diversas realizaciones y/o escenarios:

- Control y separación de datos donde, por ejemplo, es provista la señalización de control para la movilidad a través de la macro capa al mismo tiempo que es provista la conectividad de datos de alta velocidad a través de la capa de baja potencia.

- Una separación entre enlace descendente y enlace ascendente, donde es provista la conectividad de enlace descendente y de enlace ascendente a través de diferentes capas.

- Diversidad para la señalización de control, donde la señalización de control de recursos de radio (RRC) puede ser provista a través de múltiples enlaces, mejorando aún más el rendimiento de movilidad.

La macro asistencia que incluye la conectividad dual puede proporcionar varios beneficios:

- Soporte mejorado para la movilidad - manteniendo el punto de anclaje de movilidad en la macro capa, como se ha descrito anteriormente, es posible mantener la movilidad sin fisuras entre las capas macro y de baja potencia, así como entre los nodos de baja potencia.

- Transmisiones de baja sobrecarga desde la capa de baja potencia - transmitiendo solamente la información requerida para la experiencia del usuario individual, es posible evitar la sobrecarga que viene de soportar la movilidad en modo reposo dentro de la capa de área local, por ejemplo.

- Equilibrio de la carga energía-eficiencia - apagando los nodos de baja potencia cuando no hay transmisión de datos en curso, es posible reducir el consumo de energía de la capa de baja potencia.

- Optimización por enlace - seleccionando el punto de terminación para el enlace ascendente y el enlace descendente por separado, la selección de nodo puede ser optimizada para cada enlace.

Uno de los problemas en el uso de la conectividad dual es cómo mapear los portadores de radio de datos (los DRB) en el flujo de anclaje y el flujo auxiliar, respectivamente. Una opción para separar los DRB entre dos estaciones base, como se muestra en la figura 1, es mantener el plano de control (RRC) en el eNB de anclaje y distribuir las entidades PDCP de modo que algunas de ellas estén en el eNB de anclaje y algunas de ellas en el eNB auxiliar. Como se discute en más detalle a continuación, este enfoque puede producir beneficios de eficiencia del sistema importantes. Sin embargo, este enfoque crea problemas relacionados con la manipulación de claves de seguridad que se usan para la protección de confidencialidad e integridad de los datos transmitidos hacia y desde el terminal móvil.

Otra técnica anterior es el documento EP 2320592.

Sumario

La invención se define por las reivindicaciones independientes.

En los sistemas de LTE, la capa de control de recursos de radio (RRC) configura entidades de protocolo de convergencia de paquete de datos (PDCP) con las claves de cifrado y los datos de configuración, como datos que indican qué algoritmos de seguridad deberían ser aplicados en conexión con el correspondiente portador de radio. En un escenario de conectividad dual, la capa RRC puede ser manejada exclusivamente por el nodo de anclaje, mientras que las entidades PDCP pueden ser manejadas en cada uno de los nodos de estación base de anclaje y auxiliar. Puesto que la estación base de anclaje y la estación base auxiliar pueden ser implementadas en nodos separados físicamente, la suposición de que el RRC puede configurar las entidades PDCP a través de interfaces de programa de aplicación internos (las API) ya no se mantiene.

Las realizaciones de ejemplo divulgadas en este documento están dirigidas a la generación segura de un conjunto de claves de cifrado para ser usadas para la comunicación entre un terminal inalámbrico en la conectividad dual y un eNB auxiliar. En algunas realizaciones, una clave de base para el eNB auxiliar se genera a partir de la clave de seguridad del eNB de anclaje. La clave de base se puede usar entonces para generar las claves para la comunicación segura entre el terminal inalámbrico y el eNB auxiliar.

Las realizaciones de las técnicas divulgadas incluyen, por ejemplo, un método, adecuado para la implementación en un nodo de red, para la generación de claves de seguridad para las comunicaciones seguras entre un terminal inalámbrico y una estación base de anclaje y entre el terminal inalámbrico y una estación base auxiliar, donde el terminal inalámbrico es o está a punto de ser conectado dualmente a la estación base de anclaje y a la estación base auxiliar. El método de ejemplo incluye la generación de una clave de seguridad auxiliar para la estación base auxiliar, basada, al menos en parte, en una clave de estación base de anclaje. La clave de seguridad auxiliar generada se envía entonces a la estación base auxiliar, para su uso por la estación base auxiliar en el cifrado de tráfico de datos enviado al terminal inalámbrico o en la generación de una o más claves de seguridad auxiliares adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base auxiliar mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base auxiliar. La clave de estación base de anclaje, o una clave derivada de la clave de la estación base de anclaje, se usa para cifrar los datos enviados al terminal inalámbrico por la estación base de anclaje mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base auxiliar.

También se divulga aquí otro método para generar una clave de seguridad auxiliar a una estación base auxiliar. Al igual que el método resumido anteriormente, este método también es adecuado para la implementación en un nodo de red, para la generación de claves de seguridad para las comunicaciones seguras entre un terminal inalámbrico y una estación base de anclaje y entre el terminal inalámbrico y una estación base auxiliar, donde el terminal inalámbrico es o está a punto de ser conectado dualmente a la estación base de anclaje y a la estación base auxiliar. En este método, sin embargo, el método puede llevarse a cabo en un nodo de red que no sea la estación base de anclaje, usando una clave principal que puede ser desconocida para la estación base de anclaje.

De acuerdo con este segundo método de ejemplo, una clave de seguridad principal es compartida entre el nodo de red y el terminal inalámbrico. Esta clave puede ser desconocida para la estación base de anclaje, en algunas realizaciones. El método continúa con la generación de una clave de seguridad auxiliar para la estación base auxiliar, basada, al menos en parte, en la clave de seguridad principal. La clave de seguridad auxiliar generada se envía entonces a la estación base auxiliar, para su uso por la estación base auxiliar en el cifrado del tráfico de datos enviado al terminal inalámbrico o en la generación de una o más claves de seguridad auxiliares adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base auxiliar mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base auxiliar. En algunas realizaciones, la clave de seguridad auxiliar generada se envía directamente a la estación base auxiliar de manera que la estación base de anclaje no tiene conocimiento de la clave, mientras que en otras realizaciones la clave de seguridad auxiliar generada se envía a la estación base auxiliar indirectamente, a través de la estación base de anclaje.

Otras realizaciones de la tecnología divulgada en el presente documento incluyen el aparato de nodo de red y el aparato terminal móvil, cada uno configurado para llevar a cabo uno de los métodos de ejemplo resumidos anteriormente o variantes de los mismos.

Breve descripción de los dibujos

La figura 1 es un diagrama esquemático que ilustra un ejemplo de un despliegue de la conectividad dual heterogéneo con flujos de anclaje y auxiliar a un terminal móvil.

La figura 2 ilustra los componentes de la arquitectura del sistema E-UTRAN.

La figura 3 ilustra detalles de la arquitectura de protocolo de la estación base en un escenario de conectividad dual.

La figura 4 ilustra una jerarquía de derivación de claves basada en una clave de estación base de anclaje.

La figura 5 ilustra una jerarquía de derivación de claves basada en una clave MME.

La figura 6 es un diagrama de flujo del proceso que ilustra un método de ejemplo como el implementado por un nodo de red de ejemplo.

La figura 7 es un diagrama de flujo del proceso que ilustra un método de ejemplo como el implementado por un terminal inalámbrico.

La figura 8 y la figura 9 ilustran cada un diagrama de flujo del proceso que corresponde a realizaciones de ejemplo de las técnicas divulgadas en breve.

La figura 10 es un diagrama de bloques que ilustra un aparato de estación base de anclaje de ejemplo, de acuerdo con las técnicas divulgadas en breve.

La figura 11 es un diagrama de bloques que ilustra otro aparato de nodo de red de ejemplo, de acuerdo con las técnicas divulgadas en breve.

La figura 12 ilustra los componentes de un terminal inalámbrico de ejemplo configurado de acuerdo con algunas de las realizaciones divulgadas en breve.

Descripción detallada

Ahora se describirán con más detalle conceptos de la invención a continuación con referencia a los dibujos que se acompañan, en los que se muestran ejemplos de realizaciones de los conceptos de la invención. Estos conceptos de la invención pueden, sin embargo, ser encarnados de muchas formas diferentes y no debe interpretarse como limitados a las realizaciones expuestas en el presente documento. Más bien, estas realizaciones son provistas para que esta divulgación sea minuciosa y completa, y transmita completamente el alcance de los actuales conceptos de la invención para los expertos en la técnica. También hay que señalar que estas realizaciones no son mutuamente excluyentes. Se puede asumir tácitamente que los componentes de una realización están presentes o se usan en otra realización.

Para fines de ilustración y explicación solamente, estas y otras realizaciones de los actuales conceptos de la invención se describen en el presente documento en el contexto de operar en una red de acceso radio (RAN) que se comunica a través de canales de comunicación de radio con terminales móviles (también referidos como terminales inalámbricos o los UE). Como se usa en el presente documento, un terminal móvil, terminal inalámbrico, o UE pueden incluir cualquier dispositivo que recibe datos de una red de comunicación, y puede incluir, pero está limitado, un teléfono móvil (teléfono "celular"), laptop/ordenador portátil, ordenador de bolsillo, ordenador de mano, ordenador de sobremesa, una máquina a máquina (M2M) o un dispositivo de tipo MTC, un sensor con una interfaz de comunicación inalámbrica, etc.

El sistema universal de telecomunicaciones móviles (UMTS) es un sistema de comunicación móvil de tercera generación, que evolucionó desde el sistema global para las comunicaciones móviles (GSM), y está destinado a proporcionar servicios de comunicaciones móviles mejorados basados en tecnología de acceso múltiple por división de código de banda ancha (WCDMA). UTRAN, abreviatura de red de acceso radio terrestre UMTS, es un término colectivo para los Nodo B y controladores de red de radio que conforman la red de acceso de radio UMTS. Por lo tanto, UTRAN es esencialmente una red de acceso radio que usa acceso múltiple por división de código de banda ancha (WCDMA) para los UE.

El proyecto asociación de tercera generación (3GPP) se ha comprometido a seguir evolucionando las tecnologías de red de acceso radio basados en GSM y UTRAN. En este sentido, las especificaciones para la red de acceso de radio terrestre universal evolucionada (E-UTRAN) están en curso dentro de 3GPP. La red de acceso de radio terrestre universal evolucionada (E-UTRAN) comprende la evolución a largo plazo (LTE) y la evolución del sistema de arquitectura (SAE).

Hay que señalar que aunque la terminología de LTE se usa generalmente en esta divulgación para ejemplificar realizaciones de los conceptos de la invención, esto no debería ser visto como una limitación del alcance de los conceptos de la invención solo en estos sistemas. Otros sistemas inalámbricos, incluidas las variaciones y sucesores de LTE de 3GPP y sistemas WCDMA, WiMAX (interoperabilidad mundial para acceso por microondas), UMB (banda ancha ultramóvil), HSDPA (acceso de paquetes descendente de alta velocidad), GSM (sistema global para las comunicaciones móviles, etc.), también pueden beneficiarse de la explotación de las realizaciones de los

actuales conceptos de la invención divulgados en este documento.

Hay que señalar también que la terminología tal como la estación base (también referida como NodoB, eNodoB, o Node B evolucionado) y el terminal inalámbrico o terminal móvil (también referido como nodo de equipo de usuario o UE) debería considerarse no limitativa y no implica una cierta relación jerárquica entre los dos. En general, una estación base (por ejemplo, un "nodo B" o "eNodoB") y un terminal inalámbrico (por ejemplo, un "UE") pueden considerarse como ejemplos de respectivos dispositivos de comunicaciones diferentes que se comunican entre sí a través de un canal de radio inalámbrico.

Aunque las realizaciones discutidas en este documento pueden centrarse en realizaciones de ejemplo en las que las soluciones descritas se aplican en redes heterogéneas que incluyen una mezcla de estaciones base de potencia relativamente mayor (por ejemplo, "macro" estaciones base, que también pueden ser referidas como estaciones base de área ancha se describe o nodos de red de área ancha) y nodos de potencia relativamente menor (por ejemplo, las "pico" estaciones base, que también pueden ser referidas como las estaciones base de área local o como nodos de red de área local), las técnicas descritas se puede aplicar en cualquier tipo de red adecuado, incluyendo configuraciones tanto homogéneas como heterogéneas. Por lo tanto, las estaciones base involucradas en las configuraciones descritas pueden ser similares o idénticas entre sí, o pueden diferir en términos de potencia de transmisión, número de antenas de transmisor-receptor, potencia de procesamiento, características de receptor y transmisor, y/o cualquier otra capacidad funcional o física.

La red de acceso de radio terrestre UMTS evolucionada (E-UTRAN) incluye estaciones base llamadas NodosB mejorados (los eNB) o los eNodeB, proporcionando las terminaciones de protocolo de plano de control y plano de usuario E-UTRA hacia el UE. Los eNB son interconectados entre sí usando la interfaz X2. Los eNB también están conectados usando la interfaz SI al EPC (núcleo de paquetes evolucionado), más específicamente a la MME (entidad de gestión de movilidad) por medio de la interfaz de S1-MME y a la pasarela de servicio (S-GW) por medio de la interfaz S1-T. La interfaz S1 apoya la relación de muchos a muchos entre las MME/las S-GW y los eNB. Una vista simplificada de la arquitectura E-UTRAN se ilustra en la figura 2.

El eNB 210 aloja funcionalidades tales como la gestión de recursos de radio (RRM), control de portadores de radio, control de admisión, compresión de cabecera de los datos de plano de usuario hacia la pasarela de servicio, y/o enrutado de datos de plano de usuario hacia la pasarela de servicio. La MME 220 es el nodo de control que procesa la señalización entre el UE y la CN (red del núcleo). Las funciones significativas de la MME 220 están relacionadas con la gestión de conexión y la gestión de soportes, que se manejan a través de protocolos de estrato de no acceso (NAS). La S-GW 230 es el punto de anclaje para la movilidad del UE, y también incluye otras funcionalidades tales como almacenamiento de datos de DL (enlace descendente) temporal, mientras que el UE está siendo localizado, el enrutamiento de paquetes y remisión al eNB correcto, y/o la recopilación de información para la carga y la interceptación legal. La pasarela PDN (P-GW, no mostrada en la figura 2) es el nodo responsable de la localización de direcciones IP de UE, así como la aplicación de calidad de servicio (QoS) (como se discute más adelante). El lector es referido a TS 36.300 de 3GPP y las referencias en él para más detalles de las funciones de los diferentes nodos.

En la descripción de diversas realizaciones de las técnicas divulgadas en la presente, el término no limitativo nodo de red de radio puede ser usado para referirse cualquier tipo de nodo de red que sirve al UE y/o esté conectado a otro nodo de red o elemento de red o cualquier nodo de radio desde donde el UE recibe la señal. Los ejemplos de nodos de red de radio son los Nodos B, estaciones base (BS), radio multiestándar (MSR), nodos de radio como las BS de MSR, los eNodoB, controladores de red, controladores de red de radio (los RNC), controladores de estaciones base, relés, nodos de donantes que controlan relés, estaciones transceptoras base (BTS), puntos de acceso (AP), enrutadores inalámbricos, puntos de transmisión, nodos de transmisión, unidades de radio remotas (las RRU), cabeceras de radio remotas (las RRH), nodos en un sistema de antenas distribuido (DAS), etc.

En algunos casos se usa un término más general "nodo de red"; este término puede corresponder a cualquier tipo de nodo de red de radio o cualquier nodo de red que se comunica con al menos un nodo de red de radio. Los ejemplos de nodos de red son cualquier nodo de red de radio indicado anteriormente, los nodos de red de núcleo (por ejemplo, MSC, MME, etc.), O&M, OSS, SON, nodos de posicionamiento (por ejemplo, E-SMLC), MDT, etc.

En la descripción de algunas realizaciones, se usa el término equipo de usuario (UE), y se refiere a cualquier tipo de dispositivo inalámbrico que comunica con un nodo de red de radio en un sistema de comunicación celular o móvil. Los ejemplos de los UE son dispositivos de destino, los UE de dispositivo a dispositivo, los UE de tipo máquina o los UE capaces de comunicación de máquina a máquina, las PDA, ordenadores de mesa con capacidad inalámbrica, terminales móviles, teléfonos inteligentes, portátil integrado equipado (LEE), portátil de equipo montado (LME), llaves electrónicas USB, equipo de premisas del cliente (CPE), etc. El término "terminal móvil", como se usa en este documento debe entenderse como que es generalmente intercambiable con el término UE tal como se usa aquí y en las diversas especificaciones promulgadas por el 3GPP, pero no debería entenderse como que está limitada a los dispositivos en conformidad con las normas 3GPP.

Las realizaciones de ejemplo presentadas en este documento están dirigidas específicamente a la generación de

claves cuando la pila de protocolo Uu de LTE se divide entre una macro célula y una célula de eNB auxiliar. Las técnicas y los aparatos son más aplicables generalmente para la generación de claves en otros escenarios de conectividad dual.

Como se señaló anteriormente, una opción para dividir los portadores de radio de datos (los DRB) entre dos estaciones base en un escenario de conectividad dual es mantener el plano de control, que es gestionado por el protocolo de control de recursos de radio (RRC), en el eNB de anclaje, mientras la distribución de las entidades de protocolo de convergencia de datos de paquete (PDCP), que están asociadas con portadores de radio individuales, de manera que una o más se terminan en el eNB de anclaje y una o más en el eNB auxiliar.

La capa RRC configura todas las entidades PDCP con las que está asociada. Esto se ilustra en la figura 3, que muestra un ejemplo de una arquitectura de protocolo para conectividad múltiple.

Más particularmente, RRC configura las entidades PDCP con las claves de cifrado y los datos de configuración, como datos que indican qué algoritmos de seguridad deberían ser aplicados en conexión con el correspondiente portador de radio. Para conexiones asociadas con un terminal móvil dado, RRC configura todas las entidades PDCP para el tráfico de plano de usuario (DRB) con una y la misma clave de cifrado, KUP-enc, y todas las entidades PDCP para el tráfico de plano de control (SRB) con una y la misma clave de cifrado, KRRC-enc, y una y la misma clave de protección de integridad, KRRC-int. Para el DRB usado para proteger los datos entre un donante-eNB y un nodo de relé, RRC también configura los DRB con una clave de protección de integridad, KUP-int.

Puesto que el eNB de anclaje y el eNB auxiliar pueden ser implementados en nodos físicos separados, la suposición de que el RRC puede configurar las entidades PDCP a través de interfaces de programa de aplicación interna (las API) ya no se sostiene. Es decir, la situación actual en la que se puede asumir que los datos de configuración de seguridad se mantienen de forma segura en el interior del entorno físicamente seguro del eNB ya no se sostiene. En lugar de ello, la entidad RRC en el eNB de anclaje tiene que configurar las entidades PDCP en el eNB auxiliar, que está fuera del entorno seguro del eNB de anclaje.

El eNB de anclaje y el eNB auxiliar se usan aquí para definir los diferentes papeles de los eNB desde una perspectiva de terminal inalámbrico o UE. Se reconoce que esto es solo un nombre de ejemplo y que podrías así ser llamados de otra forma, como anclaje y refuerzo, maestro y esclavo, o simplemente eNB_1 y eNB_2.

El diseño de seguridad de LTE proporciona generalmente la compartimentación de funciones de seguridad. Esta compartimentación está destinada a asegurar que si un intruso irrumpe la seguridad de una función, únicamente esa función se ve comprometida. Por ejemplo, hay una clave usada para el cifrado del protocolo RRC y otra clave usada para la protección de la integridad del protocolo RRC. Si un intruso rompe la clave de cifrado, puede descifrar y leer todos los mensajes de RRC. Sin embargo, puesto que la clave de integridad es diferente de la clave de cifrado, el intruso no puede modificar o inyectar mensajes RRC.

Otro aspecto del enfoque de compartimentación usado en LTE es que cada eNB usa un conjunto separado de claves. La razón de esto es que este enfoque asegura que un intruso que irrumpe en una eNB no consigue ninguna información sobre los datos transmitidos entre un terminal móvil y otro eNB físicamente diferente. En un escenario de conectividad dual, entonces, para mantener la propiedad que irrumpe en un nodo RAN físico, es decir, un eNB, no ayuda en el ataque a otro nodo RAN, el eNB auxiliar debería usar su propio juego de claves, separados del conjunto de clave usado en el eNB de anclaje.

Una arquitectura de conectividad dual puede abrir tres nuevas trayectorias para los ataques potenciales de seguridad, dependiendo de las técnicas adoptadas para manejar claves y parámetros de seguridad. En primer lugar, el transporte de la configuración de seguridad y las claves de cifrado desde el eNB de anclaje al eNB auxiliar proporciona un punto en el que un intruso puede interceptar o puede modificar las claves y los datos de configuración. En segundo lugar, un intruso puede irrumpir físicamente en un eNB auxiliar e interceptar o modificar las claves y los datos de configuración allí. Además, un intruso que irrumpe físicamente en un eNB puede leer, modificar o inyectar datos del plano de usuario para cualquier terminal inalámbrico conectado al eNB auxiliar. En tercer lugar, el intruso puede acceder y modificar los datos del plano de usuario cuando el eNB auxiliar los envía y recibe. Esto es cierto independientemente de si los datos del plano de usuario fluyen entre el eNB auxiliar y el eNB de anclaje, entre el eNB auxiliar y la S-GW, o si los datos salen a Internet de forma local en el eNB auxiliar.

Las realizaciones de ejemplo divulgadas en este documento están dirigidas a la generación segura de un conjunto de claves de cifrado para ser usadas para la comunicación entre un terminal inalámbrico en la conectividad dual y un eNB auxiliar. En algunas realizaciones, una clave de base para el eNB auxiliar se genera a partir de la clave de seguridad del eNB de anclaje. La clave de base se puede usar entonces para generar las claves para la comunicación segura entre el terminal inalámbrico y el eNB auxiliar.

Establecimiento de clave para el eNB auxiliar

En LTE, la clave situada en un eNB comprende la K_{eNB}, y $K_{UP\text{-}enc}$ y $K_{RRC\text{-}enc}$ y $K_{RRC\text{-}int}$. Dependiendo de qué funciones

el eNB auxiliar ofrezca, el conjunto de claves que necesita el eNB auxiliar será diferente. Puesto que el eNB auxiliar al menos terminará el cifrado del plano de usuario, es útil establecer una clave de cifrado que el eNB auxiliar comparta con el terminal inalámbrico. Si el eNB auxiliar proporcionará servicios para los nodos de relé, también hay una necesidad de una clave de integridad para proteger los DRB que llevan el tráfico de plano de control del nodo de relé. Es por lo tanto útil establecer una clave de base para el eNB auxiliar, similar a la K_{eNB}, a partir de la cual otras claves se pueden derivar. De aquí en adelante la discusión será sobre el establecimiento de una clave de base, llamada $K_{assisting\_eNB}$, pero el mismo razonamiento puede aplicarse obviamente al caso en que, por ejemplo, solo se establece una clave de cifrado.

La figura 4 muestra cómo $K_{assisting\_eNB}$ puede ser generada a partir de la K_{eNB} del eNB de anclaje. La figura muestra una posible jerarquía de claves para el eNB auxiliar. En este ejemplo, el eNB auxiliar y el terminal inalámbrico comparten las claves $K_{assisting\_eNB}$, $K_{assisting\_eNB\text{-}enc}$ y $K_{assisting\_eNB\text{-}int}$, las cuales se derivan directa o indirectamente de la K_{eNB} para el eNB de anclaje.

Las flechas en la figura 4 indican las aplicaciones de las funciones de derivación de claves (KDF). Una KDF puede, a todos los efectos prácticos, se considera una función unidireccional. Como es bien conocido para los familiarizados con las técnicas criptográficas, las funciones unidireccionales son fáciles de calcular en la dirección de avance (la dirección de la flecha), pero computacionalmente imposible de invertir. La implicación de esto es que el acceso a una clave menor en la jerarquía de claves no da ninguna información útil sobre una clave más arriba en la jerarquía. Un ejemplo de una KDF es la función HMAC-SHA256, que es la KDF usada en LTE y en muchos otros sistemas 3GPP.

Un ejemplo concreto está en la figura 4. Si la clave $K_{assisting\_eNB}$ se genera en el eNB de anclaje y se envía al eNB auxiliar, entonces el eNB auxiliar tiene acceso a $K_{assisting\_eNB}$ y el cifrado y las claves de integridad que deriva. No tendrá, sin embargo, acceso a la K_{eNB}.

Debido a que se supone que se conocen las KDF, el nodo eNB de anclaje, por otro lado, tendrá acceso a todas las claves usadas por el eNB auxiliar. Esto rompe el principio de compartimentación si se interpreta en su sentido más estricto. Sin embargo, el nivel de seguridad en este escenario es similar al obtenido en un traspaso X2, que es un traspaso en LTE que se maneja sin la participación de la entidad de gestión de movilidad (MME). En un traspaso X2, la fuente eNB calcula una nueva clave basada en la K_{eNB} usada actualmente y proporciona la nueva clave en el eNB de destino. Otro ejemplo de una situación similar se presenta en el contexto de nodos de relé. En el caso de nodos de relé, el donante eNB actúa como un SI-proxy para el nodo relé. Como resultado, el donante eNB tiene acceso a todas las claves usadas por el nodo de relé. Debido a que la situación de seguridad es similar a varias que ya surgen en las redes LTE, usando K_{eNB} como el material de claves base para la $K_{assisting\_eNB}$ pueden considerarse aceptables desde el punto de vista de la seguridad.

La jerarquía de claves mostrada en la figura 4 se puede emplear ventajosamente en un escenario de conectividad dual en el que el eNB de anclaje controla las entidades PDCP en el eNB auxiliar, es decir, el eNB de anclaje puede establecer nuevas entidades PDCP, borrarlas y volver a empezar entidades PDCP que hayan sido borradas previamente. El eNB de anclaje y el terminal móvil (por ejemplo, el UE de LTE) derivarán cada uno la $K_{assisting\_eNB}$ de la K_{eNB} así: $K_{assisting\_eNB}$ = KDF (KeNB, other_params).

Para evitar la posibilidad de ataques conocidos que explotan la transmisión repetida de datos cifrados que transportan datos subyacentes conocidos, se debería asegurar que la $K_{assisting\_eNB}$ es "actualizada" cada vez que una entidad PDCP vuelve a usar los mismos valores de RECUENTO. Por lo tanto, la derivación de $K_{assisting\_eNB}$ debería comprender preferentemente parámetros apropiados de actualización. Una forma de lograr actualización es usar los números de secuencia de RECUENTO PDCP que se asocian con algún mensaje RRC predeterminado, tal como el último mando de modo de seguridad RRC u orden de traspaso, o una de las peticiones de reconfiguración RRC o mensajes completos que se usaron para establecer las entidades PDCP en el eNB auxiliar. Los números de secuencia asociados con otros mensajes de RRC se pueden usar en su lugar, por supuesto. Otras opciones para la incorporación de actualización en la generación de $K_{assisting\_eNB}$ incluye enviar una "semilla" actualizada desde el terminal inalámbrico al eNB de anclaje o eNB auxiliar, desde el eNB de anclaje o eNB auxiliar al terminal inalámbrico (o ambos direcciones) en algún mensaje(s) RRC predeterminado u otros mensajes de protocolo. Una semilla es una (pseudo-) número generado aleatoriamente que, con una probabilidad suficientemente alta, será único con respecto a la K_{eNB} .

Sean cual sean los parámetros de actualización, a continuación, se incluyen en la derivación $K_{assisting\_eNB}$ o en la derivación de las claves derivadas de $K_{assisting\ eNB}$. También es posible volver a usar elementos de información existentes en mensajes RRC y la información que se transmite desde el eNB de anclaje o eNB auxiliar en bloques de información del sistema. Cualquier información puede ser usada siempre que proporcione una entrada (estadísticamente) única con una probabilidad suficientemente alta.

Otro diseño posible es que el eNB de anclaje deriva la $K_{assisting\_eNB}$ de la K_{eNB} sin ningún parámetro de actualización. De acuerdo con este enfoque alternativo, si el eNB auxiliar o eNB de anclaje detecta que un RECUENTO PDCP en el eNB auxiliar está a punto de plegarse, el eNB de anclaje inicia una actualización de la clave K_{eNB} a través de un

traspaso entre células. Un resultado del traspaso intracelular es que el terminal inalámbrico y el eNB de anclaje no solo actualizan la K_{eNB}, sino también las $K_{assisting\_eNB}$; la $K_{assisting\_eNB}$ podría ser re-calculada de la misma forma en que fue derivada la primera vez. Este enfoque puede requerir que el eNB auxiliar tiene que informar al eNB de anclaje sobre los RECUENTOS PDCP que están a punto de ser usados de nuevo.

Transportar la $K_{assisting\_eNB}$ desde el eNB de anclaje a al eNB auxiliar puede hacerse a través del canal de control entre los dos. El canal de control tiene que ser protegido confidencial e íntegramente como ya se ha indicado.

Otros parámetros distintos a los mencionados explícitamente también pueden ser de entrada a la KDF, en diversas realizaciones de las técnicas descritas anteriormente. Los parámetros se pueden poner en cualquiera de varios órdenes diferentes. Además, uno cualquiera o más de los parámetros para la KDF pueden transformarse antes de ser introducidos en la KDF. Por ejemplo, un conjunto de parámetros P1, P2, …, Pn, para algún entero no negativo n, podría ser transformado primero siendo ejecutado a través de una función de transformación f, y el resultado de eso, es decir, _f (P1, P2, …, Pn), siendo introducido en la KDF.

En un ejemplo de la derivación de la clave, el parámetro P1 se transforma primero antes de ser introducido en la KDF para calcular una clave llamada "output_key": output_key = KDF (f (P1), P2), donde f es alguna función o cadena de funciones arbitraria y P1 y P2 son parámetros de entrada. El parámetro P2, por ejemplo, podría ser 0, 1 o más de otros parámetros, por ejemplo, usados para unir la clave a cierto contexto. Los parámetros pueden ser introducidos como parámetros separados o se pueden concatenar juntos y luego introducirlos en una entrada única a la KDF. Incluso cuando se usan variantes de la KDF como estos, el núcleo de la idea sigue siendo el mismo.

Independientemente del enfoque de establecimiento de clave que se use, los procedimientos de traspaso existentes no se ven afectados generalmente en la entrega del terminal móvil con conectividad dual a otra estación base, independientemente del tipo de estación base de destino. El eNB de anclaje puede derribar las DRB en el eNB auxiliar y realizar el traspaso a la estación base de destino de acuerdo a las especificaciones existentes.

Cuando la entrega de un terminal inalámbrico a un eNB de destino y un eNB auxiliar de destino, la derivación de la K_{eNB} y la clave $K_{assisting\_eNB}$ se pueden realizar de forma individual.

Derivación de claves basada en K_{ASME}

En lugar de usar la clave de base del nodo de anclaje como la base para la generación de $K_{assisting\_eNB}$, una clave asociada a otro nodo en la red inalámbrica y conocido para el terminal móvil puede ser usado en su lugar. Por ejemplo, usando la K_{ASME} como base material de clave para $K_{assisting\_eNB}$, como se muestra en la figura 5, permite un mayor nivel de seguridad, en comparación con el uso de K_{eNB} descrito anteriormente. Como se ve en la figura 5, la $K_{assisting\_eNB}$ puede derivarse de la K_{ASME}, y el cifrado y las claves de integridad para el eNB auxiliar derivados de la $K_{assisting\_eNB}$ resultante.

K_{ASME} es la clave establecida a través de la autenticación de abonado en LTE, y se comparte entre la MME y el terminal inalámbrico. Si la $K_{assisting\_eNB}$ se deriva de la K_{ASME} y la MME proporciona el eNB auxiliar con esta $K_{assisting\_eNB}$ directamente, a continuación, el nodo de anclaje no tiene acceso a la $K_{assisting\_eNB}$ o las claves de cifrado e integridad derivadas de este. En este caso, entonces, el principio de compartimentación discutido anteriormente se adhiere en un sentido más estricto.

Basando la derivación de la $K_{assisting\_eNB}$ en K_{ASME} requiere que la MME se haga consciente de cuándo el eNB auxiliar necesita tener acceso a las claves, y requiere, además, que exista una trayectoria de comunicación entre los dos. Ya sea que la MME es consciente de cuándo el terminal inalámbrico está conectado al eNB auxiliar (y por lo tanto se necesitan claves) y si hay una trayectoria de señalización entre la MME y el eNB auxiliar depende de cómo se controla el eNB auxiliar. Si no se cumplen estas condiciones, el uso de la K_{ASME} como base de material de clave es menos útil, aunque todavía es posible, porque la MME tendría que enviar la $K_{assisting\_eNB}$ al nodo de anclaje, el cual, a su vez, lo proporciona al eNB auxiliar. En este escenario, por supuesto, el nodo de anclaje tiene acceso al $K_{assisting\_eNB}$.

El uso de K_{ASME} como base de material de claves significa que la $K_{assisting\_eNB}$ es derivada de K_{ASME} usando una función de derivación de claves $K_{assisting\_eNB}$ = KDF (K_{ASME}, [other_params]), donde los [other_params] opcionales pueden incluir uno o más parámetros de actualización.

Como se ha descrito anteriormente, cuando los contadores de paquetes PDCP (RECUENTO PDCP) se resetean, las claves de cifrado e integridad deberían ser renovadas. Si se usa la misma clave con los mismos RECUENTOS PDCP, habrá reutilización de transmisión de claves, y potencialmente, posibles ataques de repetición. Por lo tanto, la MME y el terminal inalámbrico podrían incluir un parámetro de actualización en la derivación de claves. Por ejemplo, el mismo parámetro de actualización que se usa cuando la K_{eNB} se deriva para el nodo de anclaje (el eNB). Qué parámetro de actualización se usa para la derivación K_{eNB} puede depender de la situación. Posibles parámetros de actualización incluyen semillas (números aleatorios usados una vez) que la MME y el terminal inalámbrico intercambian. Otras posibilidades son contadores de paquetes, tales como el enlace ascendente NAS o enlace

descendente RECUENTO, o un contador de reciente introducción que se transmite ya sea desde el terminal inalámbrico a la MME o desde la MME al terminal inalámbrico. Un inconveniente con un contador de reciente introducción es que si se pone fuera de sincronización, tiene que ser re-sincronizado por algún mecanismo de resincronización nuevo.

Otros parámetros pueden ser incluidos en la derivación $K_{assisting\_eNB}$ también. Por ejemplo, la identidad del eNB auxiliar o la célula que el eNB auxiliar usa puede ser usada como entrada. Esto es similar a cómo el K_{eNB} está unido a la identidad de la célula. El propósito podría ser además compartimentar las brechas de seguridad potenciales.

Una vez que la MME ha derivado $K_{assisting\_eNB}$, la MME también tiene que transferirlo al eNB auxiliar. La transferencia de la $K_{assisting\_eNB}$ al eNB auxiliar puede proceder de una estas dos maneras, ya sea directamente al eNB auxiliar, o indirectamente, transfiriendo primero $K_{assisting\_eNB}$ al eNB y luego permitiendo que el eNB lo transfiera al eNB auxiliar cuando sea necesario.

En general, es una ventaja de seguridad transferir la $K_{assisting\_eNB}$ directamente desde la MME al eNB auxiliar. De esta manera, solo la MME, el eNB auxiliar y el terminal inalámbrico conocen la clave. Si la señalización para el establecimiento de la conexión entre el eNB auxiliar y el terminal inalámbrico es tal que la MME está involucrada, entonces esto es preferible.

La otra alternativa es que la MME envíe la $K_{assisting\_eNB}$ al eNB, que simplemente reenvía $K_{assisting\_eNB}$ al eNB auxiliar. Este enfoque tiene una desventaja de seguridad en que el eNB ahora también es consciente de la $K_{assisting\_eNB.}$ El enfoque puede ser útil, sin embargo, si no existe una trayectoria de señalización directa entre la MME y el eNB auxiliar y la K_{ASME} es el material clave usado como base para la derivación $K_{assisting\_eNB}$.

Métodos de ejemplo

En vista de los ejemplos detallados que se describen anteriormente, se apreciará que las figuras 6 y 7 son diagramas de flujo que representan operaciones de ejemplo que pueden ser tomadas por un nodo de red y el terminal inalámbrico, respectivamente, donde la red puede ser una estación base de anclaje o una MME, en varias realizaciones. Los diagramas de flujo de los procesos ilustrados incluyen algunas operaciones que se ilustran con un borde continuo y algunas operaciones que se ilustran con un borde discontinuo. Las operaciones que se componen de un borde continuo son operaciones que se incluyen en las realizaciones de ejemplo más amplias. Las operaciones que se componen de un borde discontinuo son realizaciones de ejemplo que pueden estar comprendidas, o parte de, o son otras operaciones que se pueden tener, además de las operaciones de las realizaciones de ejemplo más amplias. Por lo tanto, estas operaciones mostradas en contornos discontinuos pueden ser consideradas "opcionales" en el sentido de que no pueden aparecer en cada ejemplo de cada realización del proceso ilustrado. También debería apreciarse que las operaciones de las figuras 6 y 7 están provistas simplemente como ejemplo.

Más particularmente, la figura 6 ilustra un proceso para generar una clave de seguridad auxiliar para usar por una estación base auxiliar en un escenario de conectividad dual. El proceso mostrado en la figura 6 puede ser implementado en un nodo de red, tal como en una estación base de anclaje (por ejemplo, un eNB de anclaje de LTE) o en algún otro nodo de red, tal como una MME. Como se muestra en el bloque 10, el nodo de red determina primero una necesidad de que una clave de seguridad auxiliar se genere. Esto puede ser provocado por el establecimiento de un escenario de conectividad dual, por ejemplo. En respuesta a esta determinación, el nodo de red genera una clave de seguridad auxiliar, basándose al menos en parte en una clave de seguridad principal. Esto se muestra en el bloque 12. Como se ha explicado en detalle anteriormente, esta clave de seguridad principal puede ser, en varias realizaciones, una clave de base de nodo de anclaje (por ejemplo, K_{eNB}) u otra clave que es conocida en el nodo de red y en el terminal móvil de interés, tal como una clave de MME (por ejemplo, K_{ASME}) ·

La generación de la clave de seguridad auxiliar puede incorporar el uso de una KDF, por ejemplo, una función criptográfica unidireccional, así como uno o más parámetros de actualización, como se muestra en los bloques 12 y 16. Una lista de parámetros de actualización que ya han sido usados puede mantenerse en algunas realizaciones, como se muestra en el bloque 17.

Como se muestra en el bloque 18, la clave de seguridad auxiliar generada se envía a la estación base auxiliar. En algunos casos, como se detalla anteriormente, la clave de seguridad auxiliar se usa entonces para generar una o más claves de protección de datos transferidos hacia y desde el terminal móvil, aunque la clave de seguridad auxiliar podría ser usada directamente para tales propósitos en algunas realizaciones.

La figura 7 ilustra un método correspondiente tal como podría ser llevado a cabo en un terminal móvil. Como se muestra en el bloque 30, el terminal móvil genera la clave de seguridad auxiliar, basándose al menos en parte en la misma clave de seguridad principal usada por el nodo de red en la figura 6. Una vez más, esta clave de seguridad principal puede ser, en varias realizaciones, una clave de base de nodo de anclaje (por ejemplo, K_{eNB}) u otra clave que es conocida en el nodo de red y en el terminal móvil de interés, tal como una clave de MME (por ejemplo, K_{ASME}). La generación de la clave de seguridad auxiliar puede incorporar el uso de una KDF, por ejemplo, una función

criptográfica unidireccional, así como uno o más parámetros de actualización, como se muestra en los bloques 32 y 34. Una lista de parámetros de actualización que ya han sido usados puede ser mantenida en algunas realizaciones, como se muestra en el bloque 17.

Como se muestra en el bloque 36, se aplica entonces la clave de seguridad auxiliar generada a la protección de los datos enviados desde y hacia la estación base auxiliar. En algunos casos, como se detalla anteriormente, la clave de seguridad auxiliar se usa para generar una o más claves de protección de datos transferidos hacia y desde el terminal móvil, aunque la clave de seguridad auxiliar podría ser usada directamente para tales propósitos en algunas realizaciones.

Como se discutió anteriormente, la clave de seguridad auxiliar puede generarse a partir de una clave de nodo de anclaje o de una clave de seguridad correspondiente a otro nodo, tal como una MME, en diversas realizaciones. Las figuras 8 y 9 son diagramas de flujo del proceso que corresponden respectivamente a estos dos escenarios. Estos métodos pueden llevarse a cabo en una red de LTE, por ejemplo, pero también se pueden aplicar a otras redes inalámbricas que emplean la conectividad dual.

La figura 8 ilustra por tanto un método, adecuado para la implementación en un nodo de red, para la generación de claves de seguridad para comunicaciones seguras entre un terminal inalámbrico y una estación base de anclaje y entre el terminal inalámbrico y una estación base auxiliar, en el que el terminal inalámbrico es o está a punto de ser conectado dualmente a la estación base de anclaje y a la estación base auxiliar. Como se muestra en el bloque 810, el método ilustrado incluye la generación de una clave de seguridad auxiliar para la estación base auxiliar, basándose, al menos en parte, en una clave de estación base de anclaje. Como se muestra en el bloque 820, la clave de seguridad auxiliar generada se envía a la estación base auxiliar, para su uso por la estación base auxiliar en el cifrado del tráfico de datos enviado al terminal inalámbrico o en la generación de una o más claves de seguridad auxiliares adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base auxiliar mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base auxiliar. Como se muestra en el bloque 830, la clave de estación base de anclaje, o una clave derivada de la clave de estación base de anclaje, se usa para cifrar los datos enviados al terminal inalámbrico por la estación base de anclaje mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base auxiliar.

En algunas realizaciones del método ilustrado en la figura 8, la clave de seguridad auxiliar generada comprende una clave de seguridad auxiliar de base para su uso en la generación de una o más claves de seguridad auxiliares adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base auxiliar. En algunas de estas realizaciones, la estación base de anclaje y el terminal móvil pueden cada derivar una clave de cifrado, o una clave de integridad, o ambos, de la clave de estación base de anclaje, y usar la clave o claves derivadas para la protección de datos enviados o recibidos desde el terminal inalámbrico por la estación base de anclaje mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base auxiliar.

En algunos de las realizaciones mostradas en la figura 8, la generación de la clave de seguridad auxiliar comprende derivar la clave de seguridad auxiliar a partir de la clave de estación base de anclaje usando una función unidireccional. La función unidireccional puede ser una función criptográfica HMAC-SHA-256, en algunas realizaciones. En algunos de estas y en algunas otras realizaciones, la generación de la clave de seguridad auxiliar se basa además en un parámetro de actualización.

En algunas realizaciones, el método ilustrado puede incluir además la detección de que un parámetro RECUENTO de un protocolo de convergencia de datos de paquetes (PDCP) en la estación base auxiliar está a punto de plegarse y, en respuesta, iniciar una actualización de la clave de estación base de anclaje y volver a calcular la clave de seguridad auxiliar.

En algunas realizaciones, una única clave de seguridad auxiliar se usa para generar un juego de claves para su uso en todos los portadores de radio de datos. En otras realizaciones, múltiples claves de seguridad auxiliares pueden ser usadas, en cuyo caso se repite la operación de generación descrita anteriormente para cada una de una pluralidad portadores de radio de datos establecidos entre el terminal inalámbrico y la estación base auxiliar, de manera que las claves de seguridad auxiliares resultantes difieren para cada portador de radio de datos. Múltiples de las distintas claves resultantes pueden ser enviadas al mismo tiempo, en algunas realizaciones.

La figura 9 es un diagrama de flujo del proceso que ilustra otro método para generar una clave de seguridad auxiliar para una estación base auxiliar. Al igual que el método mostrado en la figura 8, el proceso de la figura 9 es adecuado para la implementación en un nodo de red, para la generación de claves de seguridad para comunicaciones seguras entre un terminal inalámbrico y una estación base de anclaje y entre el terminal inalámbrico y una estación base auxiliar, donde el terminal inalámbrico es o está a punto de ser conectado dualmente a la estación base de anclaje y a la estación base auxiliar. En este método, sin embargo, el método puede llevarse a cabo en un nodo de red que no sea la estación base de anclaje, usando una clave principal que puede ser desconocida para la estación base de anclaje.

Como se muestra en el bloque 910, el método ilustrado incluye compartir una clave de seguridad principal con el terminal inalámbrico. Esta clave puede ser desconocida para la estación base de anclaje, en algunas realizaciones. Un ejemplo es la clave K_{ASME} discutida anteriormente, que es compartida entre la MME de LTE y el terminal móvil.

Como se muestra en el bloque 920, el método continúa con la generación de una clave de seguridad auxiliar para la estación base auxiliar, basándose, al menos en parte, en la clave de seguridad principal. La clave de seguridad auxiliar generada se envía a la estación base auxiliar, como se muestra en el bloque 930, para su uso por la estación base auxiliar en el cifrado del tráfico de datos enviado al terminal inalámbrico o en la generación de una o más claves de seguridad auxiliares adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base auxiliar mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base auxiliar. En algunas realizaciones, la clave de seguridad auxiliar generada se envía directamente a la estación base auxiliar de tal manera que la estación base de anclaje no tiene conocimiento de la clave, mientras que en otras realizaciones la clave de seguridad auxiliar generada se envía a la estación base auxiliar indirectamente, a través de la estación base de anclaje.

En algunas realizaciones, la clave de seguridad auxiliar generada comprende una clave de seguridad auxiliar de base para su uso en la generación de una o más claves de seguridad auxiliares adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base auxiliar. En algunos de estas y en algunas otras realizaciones, la generación de la clave de seguridad comprende derivar la clave de seguridad auxiliar a partir de la clave de estación base de anclaje usando una función unidireccional. La función unidireccional puede ser una función criptográfica HMAC-SHA 256, por ejemplo. Como se discutió en detalle anteriormente, la generación de la clave de seguridad auxiliar puede basarse además en un parámetro de actualización, en algunas realizaciones.

Implementaciones de equipo físico de ejemplo

Varias de las técnicas y métodos descritos anteriormente pueden implementarse usando circuitería de procesamiento electrónico de datos y circuitería de radio u otra circuitería de interfaz provista en un nodo de red, tal como una estación base de anclaje o en una MME, mientras que otros pueden ser implementados usando circuitería de radio y circuitería de procesamiento electrónico de datos provista en un terminal inalámbrico.

La figura 10 ilustra una configuración de nodos de ejemplo de una estación base 401A de anclaje que puede realizar algunas de las realizaciones de ejemplo descritas en este documento. La estación base 401A de anclaje puede comprender circuitería de radio o un puerto 410A de comunicación que puede ser configurada para recibir y/o transmitir mediciones, datos, instrucciones y/o mensajes de comunicación. La estación base 401A de anclaje puede comprender además un circuito 440A de interfaz de red que puede estar configurado para recibir o enviar comunicaciones de red, por ejemplo, hacia y desde otros nodos de red. Debería apreciarse que la circuitería de radio o puerto de comunicación 410A puede estar compuesto de cualquier número de circuitería o unidades de transcepción, de recepción y/o de transmisión. Además, debe apreciarse que la circuitería o comunicación 410A de radio puede tener la forma de cualquier puerto de comunicaciones de entrada o salida conocido en la técnica. La circuitería o comunicación 410A de radio y/o la interfaz 440A de red pueden comprender circuitería de RF y circuitería de procesamiento de banda base, cuyos detalles son bien conocidos por los expertos que están familiarizados con el diseño de la estación base.

La estación base 401A de anclaje puede comprender también una unidad o circuitería 420A de procesamiento que puede ser configurada para realizar las operaciones relacionadas con la generación de claves de seguridad auxiliares (por ejemplo, claves de seguridad para un eNB auxiliar), como se describe en el presente documento. La circuitería 420A de procesamiento puede ser cualquier tipo adecuado de unidad de cálculo, por ejemplo un microprocesador, procesador de señal digital (DSP), matriz de puertas programable de campo (FPGA), o circuito integrado de aplicación específica (ASIC), o cualquier otra forma de circuitería. La estación base 401A de anclaje puede comprender además una unidad o circuitería 430A de memoria que puede ser cualquier tipo adecuado de memoria legible por ordenador y puede ser de tipo volátil y/o no volátil. La memoria 430A puede configurarse para almacenar información recibida, transmitida, y/o relacionada con la generación de claves de seguridad o parámetros de actualización, parámetros de dispositivo, prioridades de comunicación, y/o instrucciones de programas ejecutables.

Las funciones típicas del circuito 420A de procesamiento, por ejemplo, cuando se configura con código de programa adecuado almacenado en la memoria 430A, incluyen la modulación y la codificación de las señales transmitidas y la demodulación y decodificación de las señales recibidas. En varias realizaciones de la presente invención, el circuito 420A de procesamiento se adapta, usando el código de programa adecuado almacenado en la memoria 430A de almacenamiento de programas, por ejemplo, para llevar a cabo una de las técnicas descritas anteriormente para la manipulación de claves de seguridad en un escenario de conectividad dual. Por supuesto, se apreciará que no todos los pasos de estas técnicas se realizan necesariamente en un único microprocesador o incluso en un único módulo.

Se apreciará que el circuito 420A de procesamiento, adaptado con código de programa almacenado en el programa y memoria 430A de datos, puede implementar el flujo del proceso de la figura 8 (o una variante de la misma) usando una disposición de "módulos" funcionales, donde los módulos son programas de ordenador o porciones de los

programas de ordenador que se ejecutan en el circuito 420A de procesador. Por lo tanto, el aparato 401A puede entenderse como que comprende una interfaz 440A de comunicaciones configurada para comunicarse con la estación base auxiliar, y que comprende además varios módulos funcionales implementados en circuitería 420A de procesamiento. Estos módulos funcionales incluyen: un módulo de generación para generar una clave de seguridad auxiliar para la estación base auxiliar, basándose, al menos en parte, en una clave de estación base de anclaje; un módulo de envío para enviar a la estación base auxiliar, usando la circuitería de interfaz, la clave de seguridad auxiliar generada, para su uso por la estación base auxiliar en el cifrado del tráfico de datos enviado al terminal inalámbrico o en la generación de una o más claves de seguridad auxiliares adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base auxiliar mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base auxiliar; y un módulo de cifrado para el uso de la clave de estación base de anclaje, o una clave derivada de la clave de estación base de anclaje, para cifrar los datos enviados al terminal inalámbrico por la estación base de anclaje mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base auxiliar.

La figura 11 ilustra una configuración de nodo de ejemplo de un nodo 505A de gestión de movilidad (por ejemplo, una MME, SGSN, S4-SGSN) que puede realizar algunas de las realizaciones de ejemplo descritas en este documento. El nodo 505A de gestión de movilidad puede comprender circuitería de interfaz o un puerto de comunicación 510A que puede ser configurado para recibir y/o transmitir mediciones, datos, instrucciones y/o mensajes de comunicación. Se debe apreciar que la circuitería de radio o el puerto de comunicación 510A pueden estar compuestos como cualquier número de unidades o circuitería de transcepción, de recepción, y/o de transmisión. Además, debe apreciarse que la circuitería 510A de radio o comunicación puede tener la forma de cualquier puerto de comunicaciones de entrada o salida conocido en la técnica. La comunicación o circuitería de interfaz 510A puede comprender circuitería de RF y circuitería de procesamiento de banda base (no mostrado).

El nodo 505A de gestión de movilidad también puede comprender una unidad o circuitería 520A de procesamiento que puede ser configurada para realizar las operaciones relacionadas con la generación de claves de seguridad auxiliares (por ejemplo, claves de seguridad para un eNB auxiliar), como se describe en el presente documento. La circuitería 520A de procesamiento puede ser cualquier tipo adecuado de unidad de cálculo, por ejemplo un microprocesador, procesador de señal digital (DSP), matriz de puertas programable de campo (FPGA), o circuito integrado de aplicación específica (ASIC), o cualquier otra forma de circuitería. El nodo 505A de gestión de movilidad puede comprender además una unidad o circuitería 530A de memoria que puede ser cualquier tipo adecuado de memoria legible por ordenador y puede ser de tipo volátil y/o no volátil. La memoria 530A puede configurarse para almacenar información recibida, transmitida, y/o relacionada con la generación de claves de seguridad o parámetros de actualización, parámetros de dispositivo, prioridades de comunicación, y/o instrucciones de programas ejecutables para su uso por circuitería 520A de procesamiento.

En varias realizaciones de la presente invención, el circuito 520A de procesamiento se adapta, usando el código de programa adecuado almacenado en la memoria 530A de almacenamiento de programas, por ejemplo, para llevar a cabo una de las técnicas descritas anteriormente para la manipulación de claves de seguridad en un escenario de conectividad dual. Por supuesto, se apreciará que no todos los pasos de estas técnicas se realizan necesariamente en un solo microprocesador o incluso en un único módulo.

Se apreciará que el circuito 520A de procesamiento, adaptado con código de programa almacenado en el programa y memoria 530A de datos, puede implementar el flujo del proceso de la figura 9 (o una variante de la misma) usando una disposición de "módulos" funcionales, donde los módulos son programas de ordenador o porciones de los programas de ordenador que se ejecutan en el circuito 520A de procesador. Por lo tanto, el aparato 501A puede entenderse como que comprende una interfaz 540A de comunicaciones configurada para comunicarse con la estación base auxiliar, y que comprende además varios módulos funcionales implementados en circuitería 520A de procesamiento. Estos módulos funcionales incluyen: un módulo de intercambio para compartir una clave de seguridad principal con el terminal inalámbrico; un módulo de generación para generar una clave de seguridad auxiliar para la estación base auxiliar, basándose, al menos en parte, en la clave de seguridad principal; y un módulo de envío para enviar a la estación base auxiliar, a través de circuitería de interfaz, la clave de seguridad auxiliar generada, para su uso por la estación base auxiliar en el cifrado del tráfico de datos enviado al terminal inalámbrico o en la generación de una o más claves de seguridad auxiliares adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base auxiliar mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base auxiliar. La figura 12 ilustra una configuración de nodo de ejemplo de un terminal inalámbrico 505B que puede ser configurado para llevar a cabo algunos de los métodos de ejemplo descritos en el presente documento. El terminal inalámbrico 505B puede comprender circuitería de interfaz o un puerto 510B de comunicación que se puede configurar para recibir y/o transmitir las mediciones de comunicación, datos, instrucciones, y/o mensajes. Debería apreciarse que la circuitería de radio o puerto 510B de comunicación puede estar compuesto como cualquier número de unidades o circuitería de transcepción, de recepción y/o de transmisión. Debería ser además apreciado que la circuitería de radio o puerto 510B de comunicación puede tener la forma de cualquier puerto de comunicaciones de entrada o salida conocido en la técnica. La circuitería o comunicación 510B de interfaz puede comprender circuitería de RF y circuitería de procesamiento de banda base (no mostrados).

El terminal inalámbrico 505B también puede comprender una unidad o circuitería 520B de procesamiento que puede ser configurada para realizar las operaciones relacionadas con la generación de claves de seguridad auxiliares (por ejemplo, claves de seguridad para un eNB auxiliar), como se describe en el presente documento. La circuitería 520B de procesamiento puede ser cualquier tipo adecuado de unidad de cálculo, por ejemplo un microprocesador, procesador de señal digital (DSP), matriz de puertas programable de campo (FPGA), o circuito integrado de aplicación específica (ASIC), o cualquier otra forma de circuitería. El terminal inalámbrico 505B puede comprender además una unidad o circuitería 530B de memoria que puede ser cualquier tipo adecuado de memoria legible por ordenador y puede ser de tipo volátil y/o no volátil. La memoria 530B puede configurarse para almacenar información recibida, transmitida, y/o relacionada con la generación de claves de seguridad o parámetros de actualización, parámetros de dispositivo, prioridades de comunicación, y/o instrucciones de programas ejecutables.

En consecuencia, en diversas realizaciones de la invención, unos circuitos de procesamiento, tales como los circuitos 520A y 520B de procesamiento y sus circuitos 530A y 530B de memoria correspondientes, están configurados para llevar a cabo una o más de las técnicas descritas en detalle anteriormente. Otras realizaciones pueden incluir estaciones base y/u otros nodos de red que incluyen uno o más de tales circuitos de procesamiento. En algunos casos, estos circuitos de procesamiento se configuran con código de programa apropiado, almacenado en uno o más dispositivos de memoria adecuados, para implementar una o más de las técnicas descritas en el presente documento. Por supuesto, se apreciará que no todos los pasos de estas técnicas se realizan necesariamente en un único microprocesador o incluso en un único módulo.

Se apreciará por la persona experta en la técnica que pueden hacerse diversas modificaciones a las realizaciones descritas anteriormente sin apartarse del alcance de la presente invención. Por ejemplo, aunque las realizaciones de la presente invención han sido descritas con ejemplos que incluyen un sistema de comunicación conforme a las normas LTE especificadas de 3GPP, hay que señalar que las soluciones presentadas pueden ser igualmente bien aplicables a otras redes que soportan la conectividad dual. Por consiguiente, las realizaciones específicas descritas anteriormente deberían considerarse a modo de ejemplo en lugar de limitar el alcance de la invención. Debido a que no es posible, por supuesto, describir cada combinación concebible de componentes o técnicas, los expertos en la técnica apreciarán que la presente invención puede ser implementada de otras maneras que las establecidas específicamente en este documento, sin apartarse de las características esenciales de la invención. Las presentes realizaciones por lo tanto han de ser consideradas en todos los aspectos como ilustrativas y no restrictivas.

En la presente descripción de diversas realizaciones de presentes conceptos de la invención, ha de entenderse que la terminología usada en este documento tiene el propósito de describir solamente realizaciones particulares y no se pretende que sea limitativa de los presentes conceptos de la invención. A menos que se defina lo contrario, todos los términos (incluyendo términos técnicos y científicos) usados aquí tienen el mismo significado que se entiende comúnmente por una experiencia ordinaria en la técnica a la que presentan conceptos de la invención pertenece. Se entenderá además que los términos, tales como los definidos en los diccionarios usados comúnmente, deberían ser interpretados como que un significado que es consistente con su significado en el contexto de esta especificación y la técnica relevante y no serán interpretados en un sentido idealizado o demasiado formal expresamente a lo definido en este documento.

Cuando un elemento es referido como que es "conectado", "acoplado", "sensible", o variantes del mismo a otro elemento, puede ser directamente conectado, acoplado o sensible al otro elemento o elementos de intervención pueden estar presentes. Por el contrario, cuando un elemento se denomina como que es “conectado directamente", "acoplado directamente", "sensible directamente", o variantes del mismo a otro elemento, no hay elementos intermedios presentes. Los números iguales se refieren a elementos iguales en todo. Además, "acoplado", "conectado", "sensible", o variantes de los mismos, como se usa en el presente documento pueden incluir de forma acoplado, conectado, o sensible inalámbricamente. Tal como se usa en el presente documento, las formas singulares "un", "una" y "el", “la” pretenden incluir las formas plurales, a menos que el contexto indique claramente lo contrario. Las funciones o construcciones bien conocidas no pueden ser descritas en detalle por razones de brevedad y/o claridad. El término "y/o" incluye cualquiera y todas las combinaciones de uno o más de los elementos enumerados asociados.

Se entenderá que aunque los términos primero, segundo, tercero, etc., pueden ser usados en el presente documento para describir diversos elementos/operaciones, estos elementos/operaciones no deberían ser limitados por estos términos. Estos términos solo se usan para distinguir un elemento/operación de otro elemento/operación. Así, un primer elemento/operación en algunas realizaciones podría denominarse un segundo elemento/operación en otras realizaciones sin apartarse de las enseñanzas de los actuales conceptos de la invención. Los mismos números de referencia o los mismos designadores de referencia denotan los mismos o similares elementos a lo largo de la especificación.

Tal como se usa en el presente documento, los términos "comprenden", "que comprende", "comprende", "incluyen", "que incluye", “incluye”, "comprende", "tienen", "tiene", "que tiene", o variantes de los mismos son indefinidos, e incluyen una o más características establecidas, números enteros, elementos, etapas, componentes o funciones pero no excluyen la presencia o adición de una o más de otras características, números enteros, elementos, etapas, componentes, funciones o grupos de los mismos. Además, como se usa aquí, la abreviatura común "por ejemplo",

que se deriva de la frase latina *exempli gratia*, puede ser usada para introducir o especificar un ejemplo general o ejemplos de un elemento mencionado anteriormente, y no se pretende que sea limitado a este elemento. La abreviatura común "es decir", que se deriva de la frase latina *id est*, se puede usar para especificar un elemento determinado de una recitación más general.

Aquí se describen realizaciones de ejemplo con referencia a diagramas de bloques y/o ilustraciones de diagramas de flujo de métodos implementados por ordenador, aparatos (sistemas y/o dispositivos) y/o productos de programas de ordenador. Se entiende que un bloque de los diagramas de bloques y/o ilustraciones de organigramas, y combinaciones de bloques en los diagramas de bloques y/o ilustraciones de diagramas de flujo, pueden ser implementados por las instrucciones de programas de ordenador que son realizadas por uno o más circuitos de ordenador. Estas instrucciones de programas de ordenador pueden ser proporcionadas a un circuito de procesador de un circuito de ordenador de propósito general, un circuito de ordenador de propósito especial, y/u otro circuito de procesamiento de datos programable para producir una máquina, de tal manera que las instrucciones, que se ejecutan a través del procesador del ordenador y/u otro aparato de procesamiento de datos programable, transforman y controlan transistores, valores almacenados en posiciones de memoria y otros componentes de equipo físico en tal circuitería para implementar las funciones/actos especificados en los diagramas de bloques y/o bloque o bloques de diagrama de flujo, y de ese modo crear medios (funcionalidad) y/o la estructura para implementar las funciones/actos especificados en los diagramas de bloques y/o bloques(s) de diagrama de flujo.

Estas instrucciones de programa informático también se pueden almacenar en un medio legible por ordenador tangible que puede dirigir un ordenador u otro aparato de procesamiento de datos programable para funcionar de una manera particular, de manera que las instrucciones almacenadas en el medio legible por ordenador producen un artículo de fabricación que incluye instrucciones que implementan las funciones/actos especificados en los diagramas de bloques y/o bloque o bloques de diagrama de flujo. En consecuencia, las realizaciones de los conceptos de la invención presentes pueden ser incluidas en el equipo físico y/o en el equipo lógico (incluyendo soporte lógico inalterable, equipo lógico residente, micro-código, etc.) que se ejecutan en un procesador tal como un procesador de señal digital, que en conjunto puede ser denominado "circuitería", "un módulo" o variantes de ellos.

También hay que señalar que en algunas implementaciones alternativas, las funciones/actos señaladas en los bloques pueden producirse fuera del orden señalado en los diagramas de flujo. Por ejemplo, dos bloques mostrados en sucesión pueden de hecho ser ejecutados sustancialmente de manera concurrente o los bloques pueden a veces ser ejecutados en orden inverso, dependiendo de la funcionalidad/actos involucrados. Además, la funcionalidad de un bloque dado de los diagramas de flujo y/o diagramas de bloques puede separarse en varios bloques y/o la funcionalidad de dos o más bloques de los diagramas de flujo y/o diagramas de bloques puede ser al menos parcialmente integrada. Finalmente, otros bloques se pueden añadir/insertar entre los bloques que se ilustran, y/o los bloques/operaciones pueden omitirse sin apartarse del alcance de los conceptos de la invención. Además, aunque algunos de los diagramas incluyen flechas en las trayectorias de comunicación para mostrar una dirección principal de comunicación, se ha de entender que la comunicación puede ocurrir en la dirección opuesta a las flechas representadas.

Muchas variaciones y modificaciones se pueden hacer a las realizaciones sin apartarse sustancialmente de los principios de los presentes conceptos de la invención. Todas estas variaciones y modificaciones están destinadas a ser incluidas en el presente documento dentro del alcance de los actuales conceptos de la invención. De acuerdo con ello, el objeto divulgado anteriormente se ha de considerar ilustrativo, y no restrictivo, y los ejemplos adjuntos de las realizaciones están destinados a cubrir todas las modificaciones, mejoras y otras realizaciones que caen dentro del espíritu y alcance de los presentes conceptos de la invención. Por lo tanto, en la medida máxima permitida por la ley, el alcance de los actuales conceptos de la invención se debe determinar por la más amplia interpretación admisible de la presente divulgación, y no podrá ser restringido o limitado por la descripción detallada anterior.

REIVINDICACIONES

1.- Un método, en una estación base de anclaje, para la generación de claves de seguridad para comunicaciones seguras entre un terminal inalámbrico y una estación base auxiliar, en el que el terminal inalámbrico es o está a punto de ser conectado dualmente a la estación base de anclaje y a la estación base auxiliar, en el que una clave de seguridad principal es conocida para la estación base de anclaje y el terminal inalámbrico, comprendiendo el método:

generar (920) una clave de seguridad auxiliar para la estación base auxiliar, basándose, al menos en parte, en la clave de seguridad principal;

enviar (930), a la estación base auxiliar, la clave de seguridad auxiliar generada, para su uso por la estación base auxiliar en la generación de una o más claves de seguridad auxiliares adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base auxiliar mientras el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base auxiliar.

2.- El método de la reivindicación 1, en el que la clave de seguridad auxiliar generada comprende una clave de seguridad auxiliar de base para su uso en la generación de una o más claves de seguridad auxiliares adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base auxiliar.

3.- El método de la reivindicación 1 ó 2, en el que la generación (920) de la clave de seguridad auxiliar comprende derivar la clave de seguridad auxiliar a partir de la clave principal usando una función unidireccional.

4.- El método de la reivindicación 3, en el que la función unidireccional es una función criptográfica HMAC-SHA-256

5.- El método de las reivindicaciones 1-4, en el que la generación (920) de la clave de seguridad auxiliar se basa además en un parámetro de actualización.

6.- Una estación base (505A) de anclaje para la generación de claves de seguridad para comunicaciones seguras entre un terminal inalámbrico y una estación base auxiliar, en la que el terminal inalámbrico es, o está a punto de ser, conectado dualmente a la estación base de anclaje y a la estación base auxiliar, y en el que una clave de seguridad principal es conocida para la estación base (505A) de anclaje y el terminal inalámbrico, comprendiendo la estación base (505A) de anclaje circuitería (510A) de interfaz configurada para comunicarse con la estación base auxiliar y que comprende además circuitería (520A, 530A) de procesamiento, caracterizada porque la circuitería (520A, 530A) de procesamiento está configurada para:

generar una clave de seguridad auxiliar para la estación base auxiliar, basándose, al menos en parte, en la clave de seguridad principal;

enviar a la estación base auxiliar, a través de la circuitería (510A) de interfaz, la clave de seguridad auxiliar generada, para su uso por la estación base auxiliar en la generación de una o más claves de seguridad auxiliares adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base auxiliar mientras el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base auxiliar.

7.- La estación base (505A) de anclaje de la reivindicación 6, en la que la clave de seguridad auxiliar generada comprende una clave de seguridad auxiliar de base para su uso en la generación de una o más claves de seguridad auxiliares adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base auxiliar.

8.- La estación base (505A) de anclaje de la reivindicación 6 ó 7, en la que la circuitería (520A, 530A) de procesamiento está configurada para generar la clave de seguridad auxiliar derivando la clave de seguridad auxiliar a partir de la clave principal usando una función unidireccional.

9.- La estación base (505A) de anclaje de la reivindicación 8, en la que la función unidireccional es una función criptográfica HMAC-SHA-256.

10.- La estación base (505A) de anclaje de cualquiera de las reivindicaciones 6-9, en la que la circuitería (520A, 530A) está configurada para generar la clave de seguridad auxiliar basándose además en un parámetro de actualización.

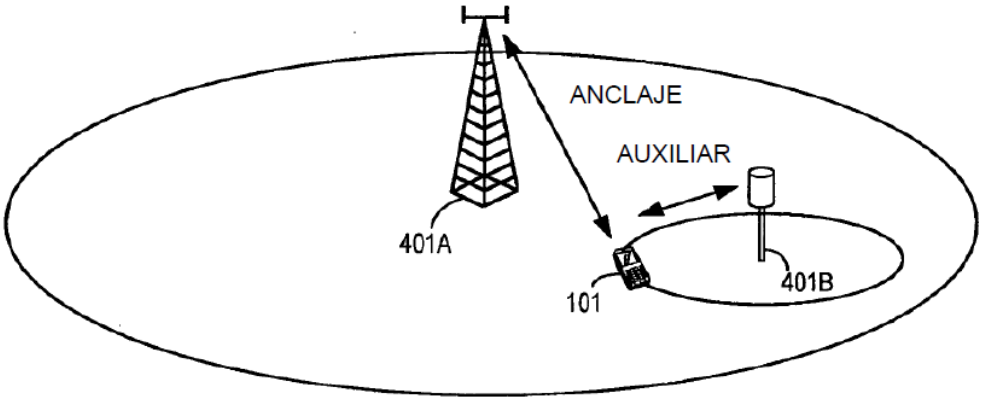

FIG. 1

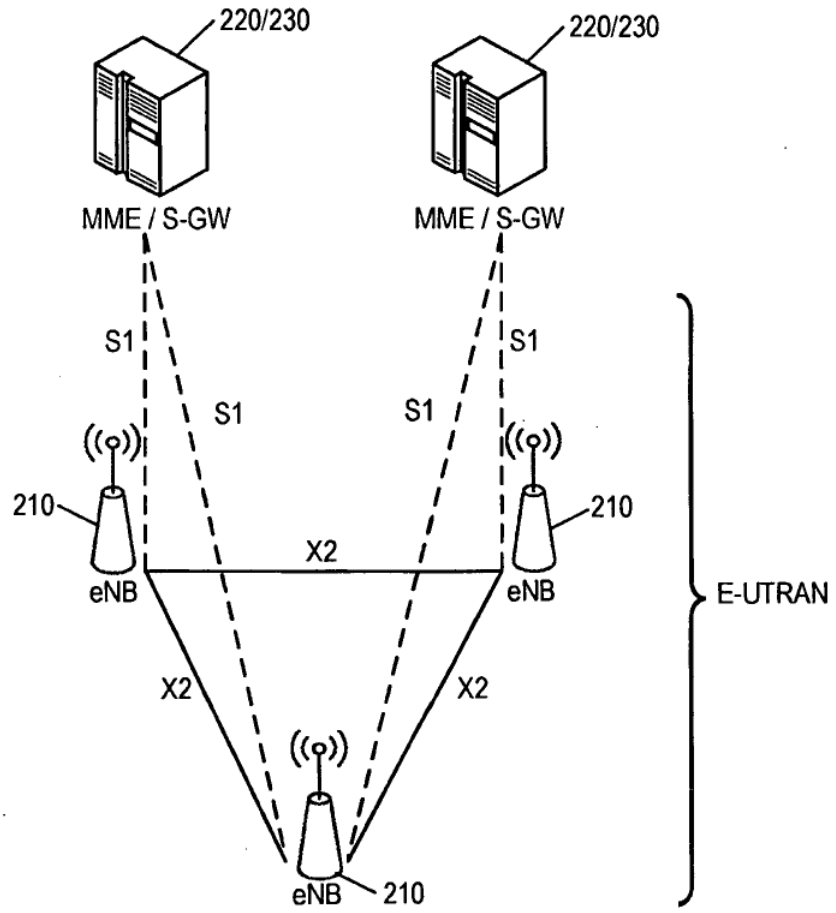
220/230
220/230
MME / S-GW
MME / S-GW
S1
S1
S1
S1
210
210
X2
eNB
eNB
E-UTRAN
X2
X2
eNB
210

FIG. 2

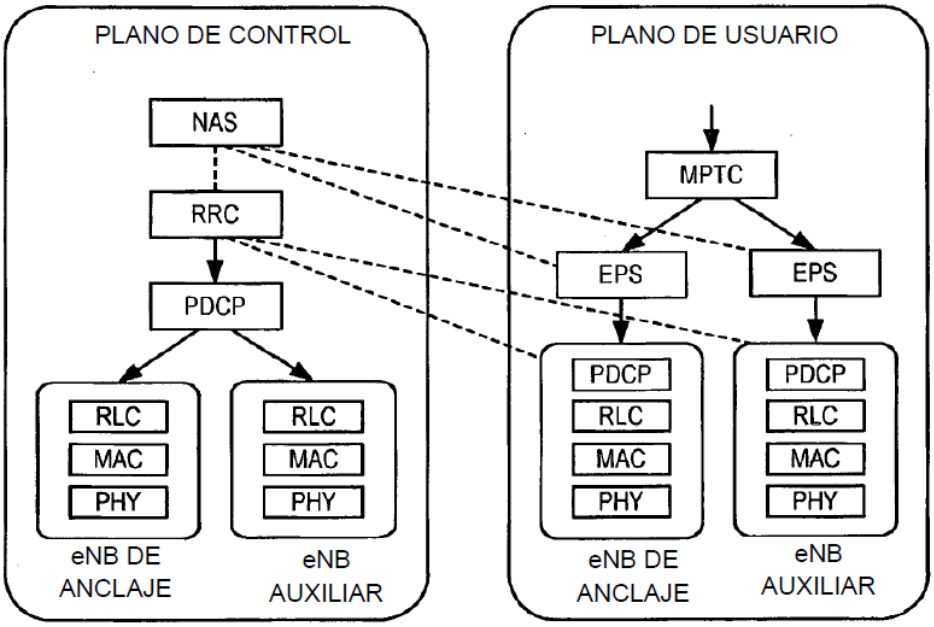
PLANO DE CONTROL
NAS
RRC
PDCP
RLC
MAC
PHY
RLC
MAC
PHY
eNB DE ANCLAJE
eNB AUXILIAR
PLANO DE USUARIO
MPTC
EPS
EPS
PDCP
RLC
MAC
PHY
PDCP
RLC
MAC
PHY
eNB DE ANCLAJE
eNB AUXILIAR

FIG. 3

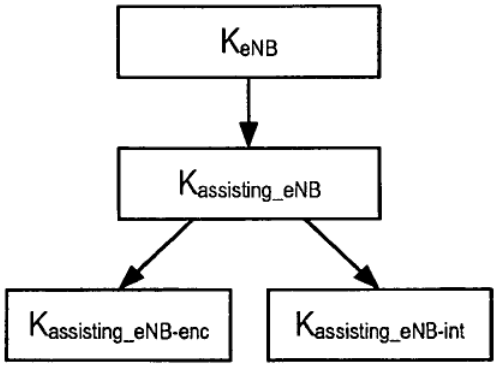
K_{eNB}
$K_{assisting\_eNB}$
$K_{assisting\_eNB\text{-}enc}$
$K_{assisting\_eNB\text{-}int}$

FIG. 4

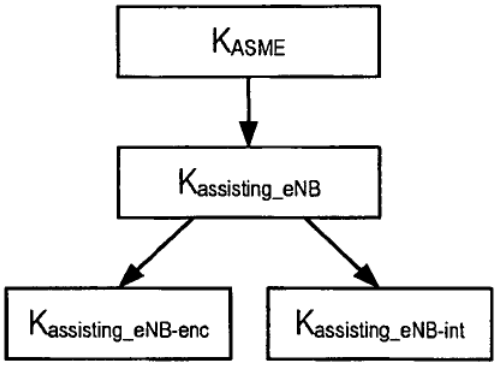
K_{ASME}
$K_{assisting\_eNB}$
$K_{assisting\_eNB\text{-}enc}$
$K_{assisting\_eNB\text{-}int}$

FIG. 5

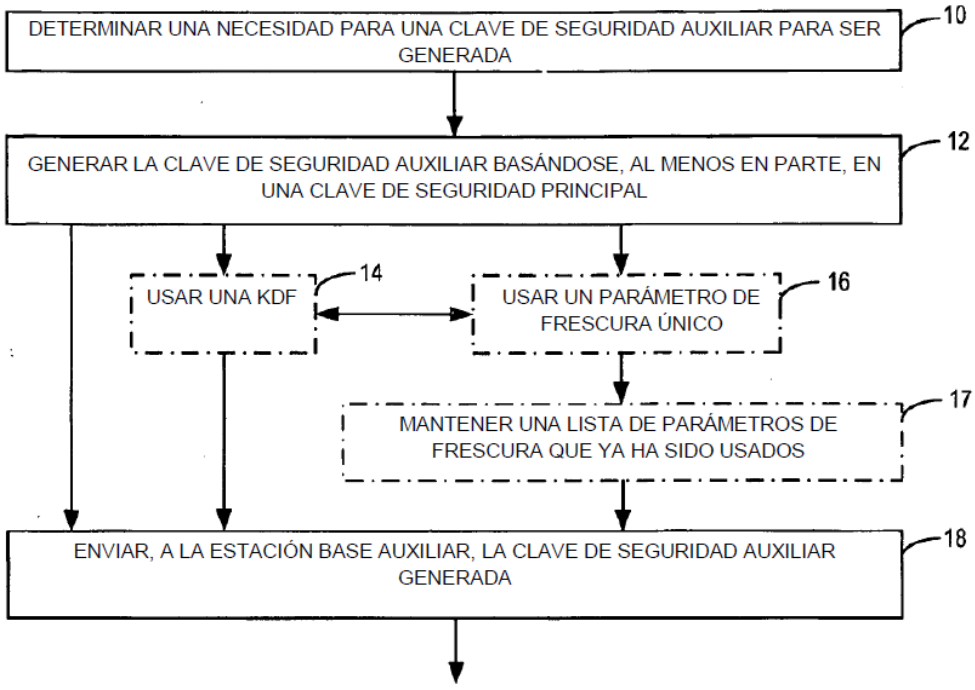
DETERMINAR UNA NECESIDAD PARA UNA CLAVE DE SEGURIDAD AUXILIAR PARA SER GENERADA
10
GENERAR LA CLAVE DE SEGURIDAD AUXILIAR BASÁNDOSE, AL MENOS EN PARTE, EN UNA CLAVE DE SEGURIDAD PRINCIPAL
12
USAR UNA KDF
14
USAR UN PARÁMETRO DE FRESCURA ÚNICO
16
MANTENER UNA LISTA DE PARÁMETROS DE FRESCURA QUE YA HA SIDO USADOS
17
ENVIAR, A LA ESTACIÓN BASE AUXILIAR, LA CLAVE DE SEGURIDAD AUXILIAR GENERADA
18

FIG. 6

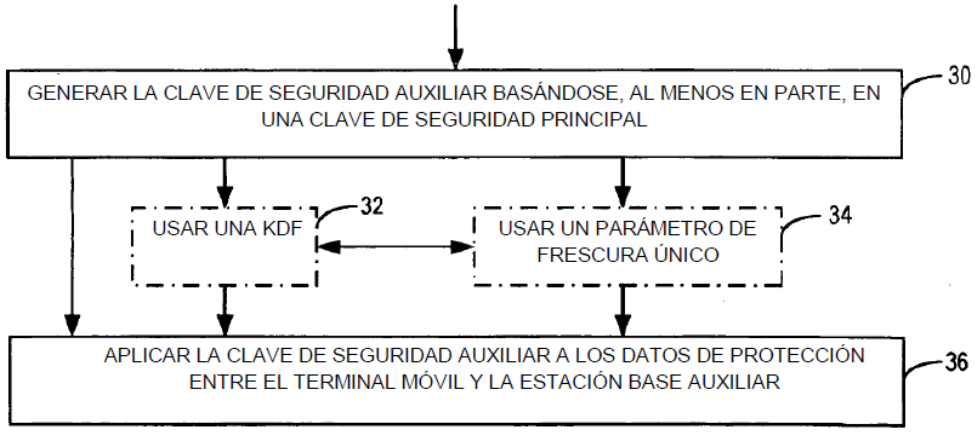
GENERAR LA CLAVE DE SEGURIDAD AUXILIAR BASÁNDOSE, AL MENOS EN PARTE, EN UNA CLAVE DE SEGURIDAD PRINCIPAL
30
USAR UNA KDF
32
USAR UN PARÁMETRO DE FRESCURA ÚNICO
34
APLICAR LA CLAVE DE SEGURIDAD AUXILIAR A LOS DATOS DE PROTECCIÓN ENTRE EL TERMINAL MÓVIL Y LA ESTACIÓN BASE AUXILIAR
36

FIG. 7

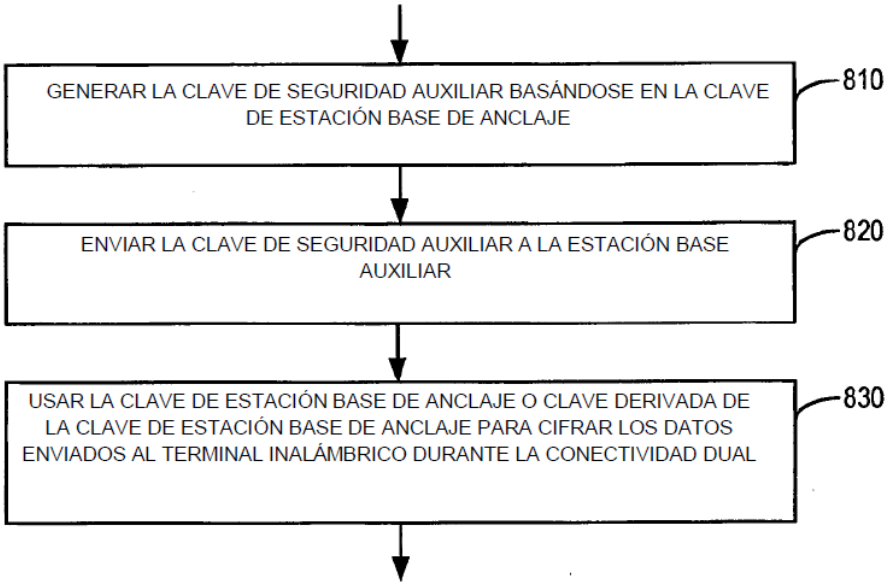
GENERAR LA CLAVE DE SEGURIDAD AUXILIAR BASÁNDOSE EN LA CLAVE DE ESTACIÓN BASE DE ANCLAJE
810
ENVIAR LA CLAVE DE SEGURIDAD AUXILIAR A LA ESTACIÓN BASE AUXILIAR
820
USAR LA CLAVE DE ESTACIÓN BASE DE ANCLAJE O CLAVE DERIVADA DE LA CLAVE DE ESTACIÓN BASE DE ANCLAJE PARA CIFRAR LOS DATOS ENVIADOS AL TERMINAL INALÁMBRICO DURANTE LA CONECTIVIDAD DUAL
830

FIG. 8

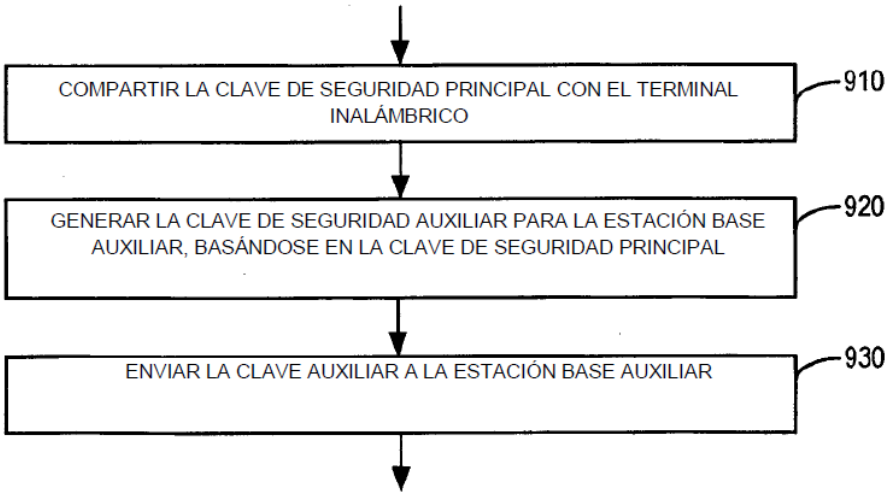
COMPARTIR LA CLAVE DE SEGURIDAD PRINCIPAL CON EL TERMINAL INALÁMBRICO
910
GENERAR LA CLAVE DE SEGURIDAD AUXILIAR PARA LA ESTACIÓN BASE AUXILIAR, BASÁNDOSE EN LA CLAVE DE SEGURIDAD PRINCIPAL
920
ENVIAR LA CLAVE AUXILIAR A LA ESTACIÓN BASE AUXILIAR
930

FIG. 9

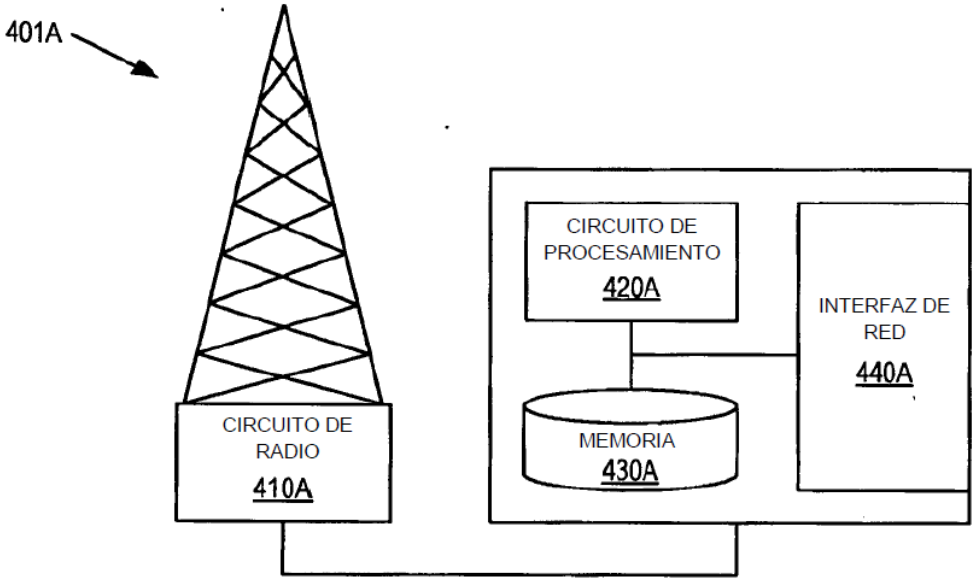
401A
CIRCUITO DE RADIO
410A
CIRCUITO DE PROCESAMIENTO
420A
MEMORIA
430A
INTERFAZ DE RED
440A

FIG. 10

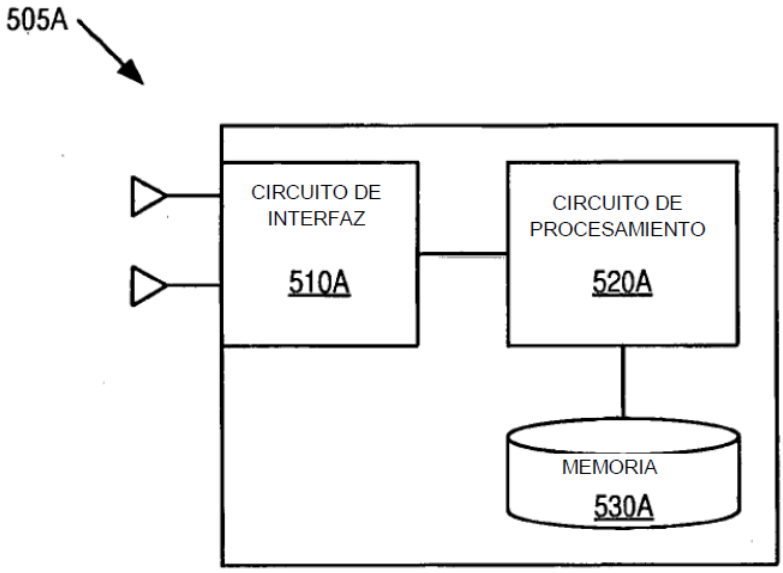
505A
CIRCUITO DE INTERFAZ
510A
CIRCUITO DE PROCESAMIENTO
520A
MEMORIA
530A

FIG. 11

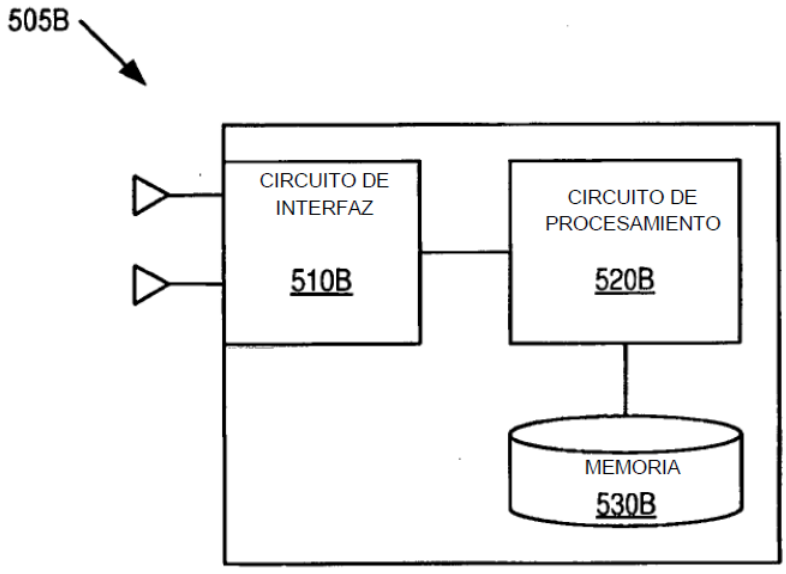
505B
CIRCUITO DE INTERFAZ
510B
CIRCUITO DE PROCESAMIENTO
520B
MEMORIA
530B

FIG. 12