(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 637 320**

(51) Int. CI.:

H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.01.2014 E 15193250 (6)**

(97) Fecha y número de publicación de la concesión europea: **10.05.2017 EP 3018850**

(54) Título: **Generación de clave 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:
11.10.2017

(73) Titular/es:

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

(72) Inventor/es:

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

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Generación de clave de seguridad para conectividad dual

Campo técnico

La tecnología descrita en el presente documento se refiere en general a redes de telecomunicaciones inalámbricas, y se refiere más particularmente a técnicas para manejar claves de seguridad en escenarios de conectividad dual, es decir, escenarios en los que un terminal móvil está conectado a múltiples estaciones base simultáneamente.

Antecedentes

En un sistema de radio celular típico, los terminales móviles (también denominados equipos de usuario, UE, terminales inalámbricos y/o estaciones móviles) se comunican a través de una red de acceso por radio (RAN) con una o más redes centrales que proporcionan acceso a redes de datos, como Internet, y/o la red de telecomunicaciones pública conmutada (RTPC). Una RAN cubre un área geográfica que se divide en áreas de células, con cada área de célula siendo servida por una estación base de radio (también referida como una estación base, un nodo RAN, un "NodoB" y/o un NodoB mejorado o "eNodoB"). Un área de célula es un área geográfica sobre la cual la cobertura de radio es proporcionada por el equipo de estación base en un sitio de estación base. Las estaciones base se comunican a través de canales de comunicación de radio con terminales inalámbricos dentro del alcance de las estaciones base.

Los operadores de sistemas de comunicaciones celulares han comenzado a ofrecer servicios de datos de banda ancha móvil basados, por ejemplo, en tecnologías inalámbricas de acceso por división múltiple de código de banda ancha (WCDMA), acceso de paquetes de alta velocidad (HSPA) y evolución a largo plazo (LTE). Impulsados por la introducción de nuevos dispositivos diseñados para aplicaciones de datos, los requisitos de rendimiento del usuario final continúan aumentando. El aumento de la adopción de la banda ancha móvil ha dado lugar a un crecimiento significativo del tráfico gestionado por las redes inalámbricas de datos de alta velocidad. En consecuencia, se desean técnicas que permitan a los operadores celulares 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), comunicaciones de flujo múltiple, despliegue de portadoras múltiples, etc. Dado que las eficacias espectrales por enlace pueden aproximarse a los límites teóricos, los siguientes pasos pueden incluir la mejora de las eficiencias espectrales por unidad de área. Pueden conseguirse eficiencias adicionales para las redes inalámbricas, por ejemplo, cambiando una topología de las redes tradicionales para proporcionar una mayor uniformidad de las experiencias del usuario a través de una célula. Un enfoque es a través del despliegue de las llamadas redes heterogéneas.

Una red homogénea es una red de estaciones base (también denominada NodoB, NodoB mejorado o eNB) en un diseño planificado, que proporciona servicios de comunicaciones para una colección de terminales de usuario (también denominados nodos de equipo de usuario, UE y/o terminales inalámbricos), en los que todas las estaciones base tienen típicamente similares niveles de potencia de transmisión, patrones de antena, niveles de ruido de receptor y/o conectividad de red de retorno a la red de datos. Además, todas las estaciones base en una red homogénea pueden, en general, ofrecer acceso sin restricciones a terminales de usuario en la red, y cada estación base puede servir aproximadamente a un mismo número de terminales de usuario. Los actuales sistemas de comunicaciones inalámbricas celulares de esta categoría pueden incluir, por ejemplo, GSM (sistema global para comunicaciones móviles), WCDMA, HSDPA (acceso de paquetes 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 unidades de radio remotos, nodos RRU, células pequeñas, RRU, etc.) pueden ser desplegadas junto con o como una superposición a las macro estaciones base planificadas y/o regularmente colocadas. Una macro estación base (MBS) puede proporcionar así servicio a través de un área de macro célula relativamente grande, y cada LPN puede proporcionar servicio para un área de células LPN relativamente pequeña respectiva dentro del área de macro células 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 macro estación base típica. Un LPN puede desplegarse, por ejemplo, para reducir/eliminar un agujero o agujeros de cobertura en la cobertura proporcionada por las macro estaciones base, y/o para descargar el tráfico de las macro estaciones base, tales como aumentar la capacidad en una localización de tráfico alto o el llamado punto caliente. Debido a su menor potencia de transmisión y menor tamaño físico, un LPN puede ofrecer una mayor flexibilidad para la adquisición del sitio.

Por lo tanto, una red heterogénea presenta un despliegue multicapa de nodos de alta potencia (HPN), tales como macro estaciones base, y nodos de baja potencia (LPN), tales como las llamadas pico estaciones base o pico nodos.

Los LPN y HPN en una región dada de una red heterogénea pueden funcionar en la misma frecuencia, en cuyo caso el despliegue puede ser referido como un despliegue heterogéneo de co-canal, o en frecuencias diferentes, en cuyo caso el despliegue puede referirse como un despliegue heterogéneo inter-frecuencia o portadora múltiple o frecuencia múltiple.

El proyecto asociación de tercera generación (3GPP) continúa desarrollando especificaciones para características avanzadas y mejoradas en el contexto del sistema de telecomunicaciones inalámbricas de cuarta generación conocido como LTE (evolución a largo plazo). En la versión 12 de las especificaciones LTE y más allá, se considerarán mejoras adicionales relacionadas con nodos de baja potencia y despliegues heterogéneos bajo el paraguas 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 las capas de baja potencia, incluso mediante el uso de un conjunto de técnicas y tecnologías denominadas "conectividad de doble capa" o simplemente "conectividad dual".

Como se muestra en la figura 1, la conectividad dual implica que el dispositivo tiene conexiones simultáneas tanto a macro capas como a capas de baja potencia. La figura 1 ilustra un ejemplo de una red heterogénea en la que un terminal móvil 101 utiliza múltiples flujos, por ejemplo, un flujo de anclaje desde la macro estación base (o "eNB de anclaje") 401A y un flujo de asistencia desde una pico estación base (o un "eNB de asistencia") 401B. Obsérvese que la terminología puede variar - la estación base de anclaje y la estación base de asistencia en una configuración como la mostrada en la figura 1 pueden algunas veces denominarse estaciones base "maestras" y "esclavas" o de acuerdo con otros nombres. Cabe señalar además que, si bien los términos "ancla/ asistencia" y "maestro/esclavo" sugieren una relación jerárquica entre las estaciones base implicadas en un escenario de conectividad dual, muchos de los principios y técnicas asociados con la conectividad dual pueden aplicarse a escenarios de despliegue donde no existe tal relación jerárquica, por ejemplo, entre estaciones base de pares. En consecuencia, aunque los términos "estación base de anclaje" y "estación base de asistencia" se utilizan en el presente documento, debe entenderse que las técnicas y el aparato descritos aquí no se limitan a realizaciones que utilizan esa terminología, ni se limitan necesariamente a realizaciones que tengan la relación jerárquica sugerida por la figura 1.

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

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

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

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

La macro asistencia, incluida la conectividad dual, puede proporcionar varios beneficios:

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

- Transmisiones de baja sobrecarga desde la capa de baja potencia- al transmitir sólo la información requerida para la experiencia del usuario individual, es posible evitar la sobrecarga que proviene de soportar la movilidad en modo inactivo dentro de la capa de área local, por ejemplo.

- Equilibrio de carga eficiente en energía- al desactivar 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- al seleccionar el punto de terminación para enlace ascendente y enlace descendente por separado, se puede optimizar la selección de nodos para cada enlace.

Uno de los problemas en el uso de conectividad dual es cómo mapear los portadores de radio de datos (DRB) sobre el flujo de anclaje y el flujo de asistencia, respectivamente. Una opción para dividir 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 eNB de anclaje y algunas de ellas en el eNB de asistencia. Como se explica con mayor detalle a continuación, este enfoque puede producir algunos beneficios importantes de eficiencia del sistema. Sin embargo, este enfoque crea problemas relacionados con el manejo de claves de seguridad que se utilizan para la protección de la confidencialidad e integridad de los datos transmitidos hacia y desde el terminal móvil.

La solicitud de patente europea EP 2320592 A1 es una técnica anterior adicional.

Sumario

En los sistemas LTE, la capa de control de recursos de radio (RRC) configura las entidades del protocolo de convergencia de datos de paquetes (PDCP) con claves criptográficas y datos de configuración, tales como datos que indican qué algoritmos de seguridad deben aplicarse en relación con el portador de radio correspondiente. En un escenario de conectividad dual, la capa de RRC puede ser manejada exclusivamente por el nodo de anclaje, mientras que las entidades PDCP pueden ser gestionadas en cada uno de los nodos de la estación base de anclaje y de asistencia. Dado que la estación base de anclaje y la estación base de asistencia pueden implementarse en nodos físicamente separados, la suposición de que RRC puede configurar las entidades PDCP a través de interfaces de programa de aplicación (API) internas ya no es válida.

Las realizaciones de ejemplo divulgadas en el presente documento están dirigidas hacia la generación segura de un conjunto de claves de cifrado que se utilizarán para la comunicación entre un terminal inalámbrico en conectividad dual y un eNB de asistencia. En algunas realizaciones, una clave de base para el eNB de asistencia se genera a partir de la clave de seguridad del eNB de anclaje. La clave de base se puede utilizar entonces para generar claves para una comunicación segura entre el terminal inalámbrico y el eNB de asistencia.

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 comunicaciones seguras entre un terminal inalámbrico y una estación base de anclaje y entre el terminal inalámbrico y una estación base de asistencia, donde el terminal inalámbrico es o está a punto de ser conectado de forma dual a la estación base de anclaje y la estación base de asistencia. El método de ejemplo incluye generar una clave de seguridad de asistencia para la estación base de asistencia, basada, al menos en parte, en una clave de estación base de anclaje. La clave de seguridad de asistencia generada se envía entonces a la estación base de asistencia, para su uso por la estación base de asistencia para cifrar el tráfico de datos enviado al terminal inalámbrico o para generar una o más claves de seguridad de asistencia para cifrar el tráfico de datos enviado al terminal inalámbrico o para generar una o más claves de seguridad de asistencia adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico mediante la estación base de asistencia mientras el terminal inalámbrico se conecta de forma dual a la estación base de anclaje y la estación base de asistencia. La clave de estación base de anclaje, o una clave derivada de la clave de estación base de anclaje, se utiliza para cifrar los datos enviados al terminal inalámbrico por la estación base de anclaje mientras el terminal inalámbrico se conecta de forma dual a la estación base de anclaje y la estación base de asistencia.

También se divulga en el presente documento otro método para generar una clave de seguridad de asistencia para una estación base de asistencia. Como el método resumido anteriormente, este método es también 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 de asistencia, donde el terminal inalámbrico es o está a punto de ser conectado de forma dual a la estación base de anclaje y la estación base de asistencia. Sin embargo, en este método, el método puede llevarse a cabo en un nodo de red distinto de la estación base de anclaje, utilizando una clave primaria que puede ser desconocida para la estación base de anclaje.

De acuerdo con este segundo método de ejemplo, una clave de seguridad primaria 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 generando una clave de seguridad de asistencia para la estación base de asistencia, basada, al menos en parte, en la clave de seguridad primaria. La clave de seguridad de asistencia generada se envía entonces a la estación base de asistencia, para su uso por la estación base de asistencia para cifrar el tráfico de datos enviado al terminal inalámbrico o para generar una o más claves de seguridad de asistencia para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base de asistencia mientras el terminal inalámbrico está conectado de forma dual a la estación base de anclaje y la estación base de asistencia. En algunas realizaciones, la clave de seguridad de asistencia generada se envía directamente a la estación base de asistencia de tal manera que la estación base de anclaje no es consciente de la clave, mientras que en otras realizaciones la clave de seguridad de asistencia generada se envía indirectamente a la estación base de asistencia, Base de anclaje.

Otras realizaciones de la tecnología divulgada en el presente documento incluyen aparatos de nodos de red y aparatos de terminales móviles, configurados cada uno 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 heterogéneo de conectividad dual con flujos de anclajes y de asistencia simultáneos en un terminal móvil.

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

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

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

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

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

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

La figura 8 y la figura 9 ilustran cada una un diagrama de flujo de proceso correspondiente realizaciones de ejemplo de las técnicas actualmente divulgadas.

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

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

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

Descripción detallada

Los conceptos de la invención se describirán ahora más completamente a continuación con referencia a los dibujos adjuntos, en los que se muestran ejemplos de realizaciones de los conceptos de la invención. Sin embargo, estos conceptos de la invención pueden ser realizados de muchas formas diferentes y no deben interpretarse como limitados a las realizaciones expuestas en el presente documento. Más bien, estas realizaciones se proporcionan de manera que esta descripción sea exhaustiva y completa y transmita completamente el alcance de los conceptos de la invención presentes a los expertos en la técnica. También debe observarse que estas realizaciones no son mutuamente excluyentes. Se puede suponer tácitamente que los componentes de una realización están presentes o se utilizan en otra realización.

Con fines ilustrativos y explicativos solamente, estas y otras realizaciones de los conceptos actuales de la invención se describen aquí en el contexto de funcionar en una red de acceso por radio (RAN) que comunica a través de canales de comunicación de radio con terminales móviles (también denominados terminales inalámbricos o UE). Como se utiliza en el presente documento, un terminal móvil, terminal inalámbrico o UE puede incluir cualquier dispositivo que reciba datos de una red de comunicación, y puede incluir, pero no está limitado a ello, un teléfono móvil (teléfono "celular"), ordenador portátil/portátil, ordenador de bolsillo, ordenador de mano, ordenador de sobremesa, dispositivo de máquina a máquina (M2M) o MTC, sensor con interfaz de comunicación inalámbrica, etc.

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

El proyecto asociación de tercera generación (3GPP) se ha comprometido a seguir desarrollando las tecnologías de red de acceso por radio basadas en UTRAN y GSM. A este respecto, en el 3GPP se están llevando a cabo las especificaciones de la red de acceso por radio terrestre universal evolucionada (E-UTRAN). La red de acceso por radio terrestre universal evolucionada (E-UTRAN) comprende la evolución a largo plazo (LTE) y la evolución de la arquitectura del sistema (SAE).

Obsérvese que aunque la terminología de LTE se utiliza generalmente en esta divulgación para ejemplificar realizaciones de los conceptos de la invención, esto no debe ser visto como que limita el alcance de los conceptos de la invención solamente a estos sistemas. Otros sistemas inalámbricos, incluyendo variaciones y sucesores de los sistemas LTE y WCDMA de 3GPP, WiMAX (interoperabilidad mundial para acceso por microondas), UMB (ancho de banda ultra móvil), HSDPA (acceso de paquetes de enlace descendente de alta velocidad), GSM (sistema global para comunicaciones móviles), etc., también pueden beneficiarse de explotar realizaciones de los actuales conceptos de la invención divulgados en el presente documento.

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

Aunque las realizaciones aquí discutidas pueden enfocarse en realizaciones de ejemplo en las que las soluciones descritas se aplican en redes heterogéneas que incluyen una mezcla de estaciones base de relativa mayor potencia (por ejemplo, "macro" estaciones base, que también pueden denominarse estaciones base de área amplia o nodos de red de área amplia) y nodos de potencia relativamente baja (por ejemplo, "pico" estaciones base, que también pueden denominarse estaciones base de área local o nodos de red de área local), las técnicas descritas pueden aplicarse en cualquier tipo adecuado de red, incluyendo configuraciones tanto homogéneas como heterogéneas. Por lo tanto, las estaciones base implicadas en las configuraciones descritas pueden ser similares o idénticas entre sí, o pueden diferir en términos de potencia de transmisión, número de antenas transmisor-receptor, potencia de procesamiento, características del receptor y del transmisor y/o cualquier otra capacidad física o funcional.

La red de acceso por radio terrestre UMTS evolucionada (E-UTRAN) incluye estaciones base llamadas Nodos B mejorados (los eNB o eNodoB), proporcionando terminaciones de protocolo de plano de usuario y de plano de control E-UTRA hacia el UE. Los eNB están interconectados entre sí utilizando la interfaz X2. Los eNB también están conectados utilizando la interfaz S1 al EPC (centro de paquetes evolucionado), más específicamente a la MME (entidad de gestión de movilidad) mediante la interfaz S1-MME y a la pasarela de servicio (S-GW) por medio de la interfaz S1-U. La interfaz S1 soporta la relación muchos-a-muchos entre las MME/S-GW y los eNB. En la figura 2 se ilustra una vista simplificada de la arquitectura E-UTRAN.

El eNB 210 aloja funcionalidades tales como gestión de recursos de radio (RRM), control de portador de radio, control de admisión, compresión de cabecera de datos de plano de usuario hacia 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 de núcleo). Las funciones importantes de la MME 220 están relacionadas con la gestión de las conexiones y la gestión del portador, 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 temporal de datos temporales de DL (enlace descendente) mientras el UE está siendo llamado, enrutado de paquetes y enviado al eNB correcto, y/o recopilación de información para la carga y la intercepción legal. La pasarela de enlace de PDN (P-GW, no mostrada en la figura 2) es el nodo responsable de la asignación de direcciones IP del UE, así como la aplicación de la calidad de servicio (QoS). El lector es referido al 3GPP TS 36.300 y las referencias en el mismo para más detalles de las funcionalidades de los diferentes nodos.

En la descripción de diversas realizaciones de las técnicas actualmente divulgadas, el nodo de red de radio de término no limitativo puede utilizarse para referirse a cualquier tipo de nodo de red que sirve al UE y/o conectado a otro nodo de red o elemento de red o a cualquier nodo de radio desde donde el UE recibe señal. Ejemplos de nodos de red de radio son Nodos B, estaciones base (BS), nodos de radio de radio multiestándar (MSR) como las BS de MSR, eNodos B, controladores de red, controladores de red de radio (RNC), controladores de estación base, relés, nodos donantes que controlan relés, estaciones de transceptor base (BTS), puntos de acceso (AP), enrutadores inalámbricos, puntos de transmisión, nodos de transmisión, unidades de radio remotas (RRU), cabeceras de radio remotas (RRH), nodos en un sistema de antena distribuida (DAS), etc.

En algunos casos se utiliza 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 comunique con al menos un nodo de red de radio. Ejemplos de nodos de red son cualquier nodo de red de radio mencionado anteriormente, nodos de red centrales (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 utiliza el término equipo de usuario (UE) y se refiere a cualquier tipo de dispositivo inalámbrico que se comunica con un nodo de red de radio en un sistema de comunicación celular o móvil. Ejemplos de los UE son dispositivos de destino, los UE de dispositivo a dispositivo, los UE de tipo de máquina o los UE capaces de comunicación de máquina a máquina, las PDA, ordenadores inalámbricos de mesa, terminales móviles, teléfonos inteligentes, equipo embebido de portátil (LEE), equipo montado de portátil (LME), dongles de USB, equipo de premisas de cliente (CPE), etc. El término “terminal móvil” tal como se utiliza en el presente documento debe entenderse que es generalmente intercambiable con el término UE tal como se utiliza en el presente documento y en las diversas especificaciones promulgadas por el 3GPP, pero no debe entenderse que está limitado a dispositivos compatibles con los estándares de 3GPP.

Las realizaciones de ejemplo presentadas en el presente documento están dirigidas específicamente hacia la generación de claves cuando la pila de protocolo Uu de LTE está dividida entre una macro célula y una célula eNB de asistencia. Las técnicas y aparatos son generalmente más aplicables a la generación de claves en otros escenarios de conectividad dual.

Como se ha indicado anteriormente, una opción para dividir los portadores de radio de datos (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 que se distribuyen las entidades del protocolo de convergencia de datos de paquetes (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 de asistencia

La capa de 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 claves criptográficas y datos de configuración, tales como datos que indican qué algoritmos de seguridad deben aplicarse en conexión con el portador de radio correspondiente. Para las conexiones asociadas con un terminal móvil dado, RRC configura todas las entidades PDCP para tráfico de plano de usuario (DRB) con una y la misma clave de cifrado, KUP-enc y todas las entidades PDCP para 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 los DRB utilizados para proteger datos entre un donante-eNB y un nodo de relé, RRC también configura los DRB con una clave de protección de integridad, KUP-int.

Dado que el eNB de anclaje y el eNB de asistencia se pueden implementar en nodos físicos separados, la suposición de que RRC puede configurar las entidades de PDCP a través de interfaces de programa de aplicación (API) internas ya no es válida. Es decir, la situación actual en la que se puede suponer que los datos de configuración de seguridad se mantienen de forma segura dentro del entorno físicamente seguro del eNB ya no se sostiene. En su lugar, la entidad RRC en el eNB de anclaje tiene que configurar las entidades PDCP en el eNB de asistencia, que está fuera del entorno seguro del eNB de anclaje.

El eNB de anclaje y el eNB de asistencia se utilizan aquí para definir diferentes papeles de los eNB desde una perspectiva de UE o terminal inalámbrico. Se reconoce que esto es sólo una nomenclatura de ejemplo y que también podría ser llamado de otra forma, como ancla e intensificador de señal, maestro y esclavo, o simplemente eNB_1 y eNB_2.

El diseño de seguridad de LTE generalmente proporciona la compartimentación de funciones de seguridad. Esta compartimentación tiene la intención de asegurar que si un atacante penetra la seguridad de una función, sólo esa función está comprometida. Por ejemplo, hay una clave utilizada para el cifrado del protocolo RRC y otra clave utilizada para la protección de integridad del protocolo de RRC. Si un atacante descifra la clave de cifrado, puede descifrar y leer todos los mensajes de RRC. Sin embargo, como la clave de integridad es diferente de la clave de cifrado, el atacante no puede modificar o inyectar mensajes de RRC.

Otro aspecto del enfoque de compartimentación utilizado en LTE es que cada eNB utiliza un conjunto separado de claves. La razón de esto es que este enfoque asegura que un atacante que penetre en un eNB no obtenga información sobre los datos transmitidos entre un terminal inalámbrico y otro eNB físicamente diferente. En un escenario de conectividad dual, entonces, para mantener la propiedad que se penetra en un nodo RAN físico, es decir, un eNB, no ayuda a atacar otro nodo RAN, el eNB de asistencia debe utilizar su propio juego de claves, separado del conjunto de claves utilizado en el eNB de anclaje.

Una arquitectura de conectividad dual puede abrir tres nuevos caminos para posibles ataques de seguridad, dependiendo de las técnicas adoptadas para el manejo de claves y parámetros de seguridad. En primer lugar, el transporte de la configuración de seguridad y las claves criptográficas desde el eNB de anclaje al eNB de asistencia proporciona un punto en el que un atacante puede interferir o puede modificar las claves y los datos de configuración. En segundo lugar, un atacante puede penetrar físicamente en un eNB de asistencia, y escuchar o modificar las claves y datos de configuración allí. Además, un atacante que penetra físicamente en un eNB de asistencia puede leer, modificar o inyectar datos de plano de usuario para cualquier terminal inalámbrico conectado al eNB de asistencia. En tercer lugar, el atacante puede acceder y modificar los datos del plano de usuario cuando el eNB de asistencia lo envía y lo recibe. Esto es cierto independientemente de si los datos del plano de usuario fluyen entre el eNB de asistencia y el eNB de anclaje, entre el eNB de asistencia y la S-GW, o si los datos aparecen en Internet localmente en el eNB de asistencia.

Las realizaciones de ejemplo divulgadas en el presente documento están dirigidas hacia la generación segura de un conjunto de claves de cifrado que se utilizarán para la comunicación entre un terminal inalámbrico en conectividad dual y un eNB de asistencia. En algunas realizaciones, una clave de base para el eNB de asistencia se genera a partir de la clave de seguridad del eNB de anclaje. La clave de base se puede utilizar entonces para generar claves para una comunicación segura entre el terminal inalámbrico y el eNB de asistencia.

Establecimiento de clave para eNB de asistencia

En LTE, la clave establecida en un eNB comprende la K_{eNB}, y $K_{UP\text{-}enc}$, $K_{RRC\text{-}enc}$ y $K_{RRC\text{-}int}$. Dependiendo de las funciones que el eNB de asistencia proporcione, el conjunto de claves necesario para el eNB de asistencia será diferente. Dado que el eNB de asistencia al menos terminará el cifrado del plano de usuario, es útil establecer una

clave de cifrado que el eNB de asistencia comparta con el terminal inalámbrico. Si el eNB de asistencia proporcionase servicios para los nodos de relé, también existe la necesidad de una clave de integridad para proteger los DRB que llevan el tráfico del plano de control del nodo de relé. Por lo tanto, es útil establecer una clave de base para el eNB de asistencia, similar a la K_{eNB}, del que pueden derivarse otras claves. A partir de ahora la discusión será sobre el establecimiento de una clave de base, llamada $K_{assisting\_eNB}$, pero el mismo razonamiento puede obviamente aplicarse al caso en el que, por ejemplo, sólo se establece una clave de cifrado.

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

Las flechas de la figura 4 indican aplicaciones de funciones de derivación de claves (KDF). Una KDF puede, a todos los efectos prácticos, ser considerada una función unidireccional. Como es bien conocido para aquellos familiarizados con las técnicas criptográficas, las funciones unidireccionales son fáciles de calcular en la dirección de avance (la dirección de la flecha), pero computacionalmente inviables de invertir. La implicación de esto es que el acceso a una clave inferior en la jerarquía de claves no proporciona ninguna información útil sobre una clave más arriba en la jerarquía. Un ejemplo de KDF es la función HMAC-SHA256, que es la KDF utilizada 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 de asistencia, entonces el eNB de asistencia tiene acceso a $K_{assisting\_eNB}$ y las claves de cifrado e integridad que deriva. Sin embargo, no tendrá acceso a la K_{eNB}.

Debido a que se supone que las KDF son conocidas, el nodo eNB de anclaje, por otro lado, tendrá acceso a todas las claves utilizadas por el eNB de asistencia. 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 realiza sin la participación de la entidad de gestión de movilidad (MME). En un traspaso X2, el eNB de origen calcula una nueva clave basada en la K_{eNB} utilizada actualmente y proporciona la nueva clave al eNB de destino. Otro ejemplo de una situación similar surge en el contexto de los nodos de relé. En el caso de los nodos de relé, el eNB donante actúa como un proxy S1 para el nodo de relé. Como resultado, el eNB donante tiene acceso a todas las claves utilizadas por el nodo de relé. Debido a que la situación de seguridad es similar a varias que ya surgen en las redes LTE, utilizando K_{eNB} como el material de clave de base para la $K_{assisting\_eNB}$ puede considerarse aceptable desde un punto de vista de seguridad.

La jerarquía de claves mostrada en la figura 4 puede ser ventajosamente empleada en un escenario de conectividad dual en el que el eNB de anclaje controla las entidades PDCP en el eNB de asistencia, es decir, el eNB de anclaje puede establecer nuevas entidades PDCP, borrarlas y reiniciar entidades PDCP borradas anteriormente. 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} de esta manera: $K_{assisting\_eNB}$ = KDF (KeNB, other_params).

Para evitar la posibilidad de ataques bien conocidos que explotan la transmisión repetida de datos cifrados que lleva datos subyacentes conocidos, debe asegurarse que la $K_{assisting\_eNB}$ esté "actualizada" cada vez que una entidad PDCP reutilice los mismos valores COUNT. Por lo tanto, la derivación de $K_{assisting\_eNB}$ debe comprender preferentemente parámetros de actualización apropiados. Una manera de lograr actualización es utilizar los números de secuencia COUNT de PDCP que están asociados con algún mensaje RRC predeterminado, como el último comando de modo de seguridad RRC o comando de traspaso, o uno de la solicitud de reconfiguración de RRC o mensajes completos que se utilizaron para establecer el PDCP en el eNB de asistencia. Por supuesto, pueden utilizarse números de secuencia asociados con otros mensajes RRC. Otras opciones para incorporar actualización en la generación de $K_{assisting\_eNB}$ incluyen enviar un nuevo "nonce" desde el terminal inalámbrico al eNB de anclaje o eNB de asistencia, desde el eNB de anclaje o eNB de asistencia al terminal inalámbrico (o ambas direcciones) en algún mensaje o mensajes de RRC predeterminado/s u otros mensajes de protocolo. Un nonce es un número (pseudo-) aleatoriamente generado que, con una probabilidad suficientemente alta, será único con respecto al KeNB.

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

Otro posible diseño 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 de asistencia o eNB de anclaje detecta que un COUNT de PDCP en el eNB de asistencia está a punto de envolverse, el eNB de anclaje inicia una actualización de clave de K_{eNB} a través de un traspaso intra-celular. Un resultado del traspaso intracelular es que el terminal inalámbrico y el eNB de anclaje no sólo actualizan la K_{eNB}, sino también la $K_{assisting\_eNB}$; la $K_{assisting\_eNB}$ podría ser recalculada de la misma

manera que se derivó la primera vez. Este enfoque puede requerir que el eNB de asistencia tenga que informar al eNB de anclaje acerca de los COUNT de PDCP que están a punto de ser reutilizados.

Transportar el $K_{assisting\_eNB}$ desde el eNB de anclaje al eNB de asistencia se puede hacer 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 de los mencionados explícitamente también pueden introducirse en la KDF, en diversas realizaciones de las técnicas descritas anteriormente. Los parámetros se pueden poner en cualquiera de varios órdenes diferentes. Además, uno o más de los parámetros para la KDF pueden transformarse antes de ser introducidos en la KDF. Por ejemplo, se podría transformar un conjunto de parámetros P1, P2, ..., Pn, para un número entero n no negativo, transformándose primero mediante una función de transformación f y el resultado de esto, es decir, f (P1, P2 , ..., Pn), siendo introducido en la KDF.

En un ejemplo de la derivación de clave, el parámetro P1 se transforma primero antes de ser introducido en la KDF para calcular una clave llamada "clave_de_alta": output_key = KDF (f (P1), P2), donde f es alguna función arbitraria o cadena de funciones y P1 y P2 son parámetros de entrada. El parámetro P2, por ejemplo, puede ser 0, 1 o más parámetros adicionales, por ejemplo, utilizado para enlazar la clave a un contexto determinado. Los parámetros se pueden introducir como parámetros independientes o pueden concatenarse juntos y luego ingresar en una sola entrada a la KDF. Incluso cuando se utilizan variantes de la KDF como éstas, el núcleo de la idea sigue siendo el mismo.

Independientemente de qué enfoque de establecimiento de clave se utilice, los procedimientos de traspaso existentes generalmente no se ven afectados al entregar el terminal móvil con conectividad dual a otra estación base, independientemente del tipo de estación base de destino. El eNB de anclaje puede arrancar los DRB en el eNB de asistencia y realizar el traspaso a la estación base de destino de acuerdo con las especificaciones existentes.

Cuando se entrega un terminal inalámbrico a un eNB de destino y a un eNB de asistencia de destino, la derivación de las claves K_{eNB} y $K_{assisting\_eNB}$ se pueden realizar individualmente.

Derivación de clave basada en K_{ASME}

En lugar de utilizar la clave de base del nodo de anclaje como base para generar $K_{assisting\_eNB}$, se puede utilizar una clave asociada con otro nodo en la red inalámbrica y conocida por el terminal móvil. Por ejemplo, el uso de K_{ASME} como base de material de clave para la $K_{assisting\_eNB}$, 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 las claves de cifrado e integridad para el eNB de asistencia derivadas de la $K_{assisting\_eNB}$ resultante.

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

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

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

Como se describió anteriormente, cuando se restablecen los contadores de paquetes PDCP (COUNT de PDCP), se deben renovar las claves de cifrado e integridad. Si se utiliza la misma clave con los mismos COUNT de PDCP, habrá reutilización de secuencias de claves y, potencialmente, ataques de repetición posibles. Por lo tanto, el MME y el terminal inalámbrico podrían incluir un parámetro de actualización en la derivación clave. Por ejemplo, el mismo parámetro de actualización que ese se utiliza cuando la K_{eNB} es derivada para el nodo de anclaje (el eNB). El parámetro de actualización que se utiliza para la derivación de K_{eNB} puede depender de la situación. Parámetros posibles de actualización incluyen nonces (números aleatorios utilizados una vez) que el MME y el terminal inalámbrico intercambian. Otras posibilidades son los contadores de paquetes tales como el COUNT de enlace

ascendente o descendente de NAS o un contador recién introducido que se transmite desde el terminal inalámbrico al MME o desde el MME al terminal inalámbrico. Un inconveniente con un contador recién introducido es que si sale fuera de sincronización, tiene que ser re-sincronizado por algún nuevo mecanismo de resincronización.

Otros parámetros pueden ser incluidos en la derivación de $K_{assisting\_eNB}$ también. Por ejemplo, la identidad del eNB de asistencia o la célula que el eNB de asistencia utiliza puede ser utilizada como entrada. Esto es similar a cómo la K_{eNB} se une a la identidad de la célula. El propósito podría ser compartimentar aún más posibles brechas de seguridad.

Una vez que el MME ha derivado la $K_{assisting\_eNB}$, el MME también tiene que transferirlo al eNB de asistencia. Transferir la $K_{assisting\_eNB}$ al eNB de asistencia puede realizarse de dos maneras, ya sea directamente al eNB de asistencia, o indirectamente, transfiriendo primero la $K_{assisting\_eNB}$ al eNB y luego dejando que el eNB lo transfiera al eNB de asistencia cuando sea necesario.

Generalmente es una ventaja de seguridad transferir la $K_{assisting\_eNB}$ directamente del MME al eNB de asistencia. De esta manera, sólo el MME, el eNB de asistencia y el terminal inalámbrico conocen la clave. Si la señalización para establecer la conexión entre el eNB de asistencia y el terminal inalámbrico es tal que el MME está implicado, entonces esto es preferible.

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

Métodos de ejemplo

A la vista de los ejemplos detallados descritos 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 un terminal inalámbrico, respectivamente, donde la red puede ser una estación base de anclaje o un MME, en diversas realizaciones. Los diagramas de flujo del proceso ilustrado incluyen algunas operaciones que se ilustran con un borde continuo y algunas operaciones que se ilustran con un borde discontinuo. Las operaciones que están comprendidas en un borde sólido son operaciones que se incluyen en las más amplias realizaciones de ejemplo. Las operaciones que están comprendidas en un borde discontinuo son ejemplos de realización que pueden estar comprendidos, o ser una parte, o son operaciones adicionales que se pueden tomar además de las operaciones de las realizaciones de ejemplo más amplias. Por lo tanto, las operaciones mostradas en líneas discontinuas pueden considerarse "opcionales" en el sentido de que pueden no aparecer en cada caso en cada realización del proceso ilustrado. También debe apreciarse que las operaciones de las figuras 6 y 7 se proporcionan meramente como un ejemplo.

Más particularmente, la figura 6 ilustra un proceso para generar una clave de seguridad de asistencia para su uso por una estación base de asistencia en un escenario de conectividad dual. El proceso mostrado en la figura 6 puede implementarse 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 un MME. Como se muestra en el bloque 10, el nodo de red determina primero la necesidad de que se genere una clave de seguridad de asistencia. 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 de asistencia, basada al menos en parte en una clave de seguridad primaria. Esto se muestra en el bloque 12. Como se ha explicado con detalle anteriormente, esta clave de seguridad primaria puede ser, en diversas realizaciones, una clave de base de nodo de anclaje (por ejemplo, K_{eNB}) u otra clave que es conocida por el nodo de red y el terminal móvil de interés, tal como una clave MME (por ejemplo, K_{ASME}).

La generación de la clave de seguridad de asistencia 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 los parámetros de actualización que ya se han utilizado puede mantenerse en algunas realizaciones, como se muestra en el bloque 17.

Como se muestra en el bloque 18, la clave de seguridad de asistencia generada se envía entonces a la estación base de asistencia. En algunos casos, como se ha detallado anteriormente, la clave de seguridad de asistencia se utiliza entonces para generar una o más claves adicionales para proteger los datos transferidos hacia y desde el terminal móvil, aunque la clave de seguridad de asistencia puede utilizarse directamente para tales propósitos en algunas realizaciones.

La figura 7 ilustra un método correspondiente tal que podría llevarse a cabo en un terminal móvil. Como se muestra en el bloque 30, el terminal móvil genera la clave de seguridad de asistencia, basada al menos en parte en la misma clave de seguridad primaria utilizada por el nodo de red en la figura 6. Una vez más, esta clave de seguridad primaria puede ser, en diversas realizaciones, una clave de base de nodo de anclaje (por ejemplo, K_{eNB}) u otra clave que es conocida por el nodo de red y el terminal móvil de interés, tal como una clave MME (por ejemplo, K_{ASME}). La

generación de la clave de seguridad de asistencia 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 los parámetros de actualización que ya se han utilizado puede mantenerse en algunas realizaciones, como se muestra en el bloque 17.

Como se muestra en el bloque 36, la clave de seguridad de asistencia generada se aplica entonces a la protección de los datos enviados hacia y desde la estación base de asistencia. En algunos casos, como se ha detallado anteriormente, la clave de seguridad de asistencia se utiliza para generar una o más claves adicionales para proteger los datos transferidos hacia y desde el terminal móvil, aunque la clave de seguridad de asistencia puede utilizarse directamente para tales propósitos en algunas realizaciones.

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

La figura 8 ilustra así 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 de asistencia, en el que el terminal inalámbrico es o está a punto de ser conectado de forma dual a la estación base de anclaje y la estación base de asistencia. Como se muestra en el bloque 810, el método ilustrado incluye generar una clave de seguridad de asistencia para la estación base de asistencia, basada, al menos en parte, en una clave de estación base de anclaje. Como se muestra en el bloque 820, la clave de seguridad de asistencia generada se envía entonces a la estación base de asistencia para su uso por la estación base de asistencia para cifrar el tráfico de datos enviado al terminal inalámbrico o para generar una o más claves de seguridad de asistencia para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base de asistencia mientras que el terminal inalámbrico está conectado de forma dual a la estación base de anclaje y la estación base de asistencia. 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 utiliza para cifrar los datos enviados al terminal inalámbrico por la estación base de anclaje mientras que el terminal inalámbrico está conectado de forma dual a la estación base de anclaje y la estación base de asistencia.

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

En algunas de las realizaciones mostradas en la figura 8, generar la clave de seguridad de asistencia comprende derivar la clave de seguridad de asistencia desde la clave de estación base de anclaje utilizando una función unidireccional. La función unidireccional puede ser una función criptográfica HMAC-SHA-256, en algunas realizaciones. En algunas de estas y en algunas otras realizaciones, la generación de la clave de seguridad de asistencia se basa adicionalmente en un parámetro de actualización.

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

En algunas realizaciones, se utiliza una clave de seguridad de asistencia única para generar un conjunto de claves para su uso en todos los portadores de radio de datos. En otras realizaciones, pueden utilizarse múltiples claves de seguridad de asistencia, en cuyo caso la operación de generación descrita anteriormente se repite para cada uno de una pluralidad de portadores de radio de datos establecidos entre el terminal inalámbrico y la estación base de asistencia, de tal manera que las claves de seguridad de asistencia resultantes difieren para cada portador de radio de datos. Múltiples de las varias claves resultantes pueden enviarse al mismo tiempo, en algunas realizaciones.

La figura 9 es un diagrama de flujo de proceso que ilustra otro método para generar una clave de seguridad de asistencia para una estación base de asistencia. 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 de asistencia, el terminal inalámbrico es o está a punto de ser conectado de forma dual a la estación base de anclaje y la estación base de asistencia. Sin embargo, en este método, el método puede llevarse a cabo en un nodo de red distinto de la estación base de anclaje, utilizando una clave primaria 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 primaria 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 el MTE de LTE y el terminal móvil.

Como se muestra en el bloque 920, el método continúa generando una clave de seguridad de asistencia para la estación base de asistencia, basada, al menos en parte, en la clave de seguridad primaria. La clave de seguridad de asistencia generada se envía entonces a la estación base de asistencia, tal como se muestra en el bloque 930, para ser utilizada por la estación base de asistencia para cifrar el tráfico de datos enviado al terminal inalámbrico o para generar una o más claves de seguridad de asistencia para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base de asistencia mientras que el terminal inalámbrico está conectado de forma dual a la estación base de anclaje y la estación base de asistencia. En algunas realizaciones, la clave de seguridad de asistencia generada se envía directamente a la estación base de asistencia de tal manera que la estación base de anclaje no es consciente de la clave, mientras que en otras realizaciones la clave de seguridad de asistencia generada se envía indirectamente a la estación base de asistencia, a través de la estación base de anclaje.

En algunas realizaciones, la clave de seguridad de asistencia generada comprende una clave de seguridad de asistencia base para su uso en la generación de una o más claves de seguridad de asistencia adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base de asistencia. En algunas de estas y en algunas otras realizaciones, generar la clave de seguridad de asistencia comprende derivar la clave de seguridad de ayuda desde la clave de estación base de anclaje utilizando 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 de asistencia se puede basar además en un parámetro de actualización, en algunas realizaciones.

Implementaciones de equipo físico de ejemplo

Varias de las técnicas y métodos descritos anteriormente se pueden implementar utilizando circuitería electrónica de procesamiento de datos y circuitería de radio u otra circuitería de interfaz proporcionada en un nodo de red, tal como una estación base de anclaje o en un MME, mientras que otros se pueden implementar utilizando circuitería de radio y circuitería de procesamiento de datos electrónicos proporcionada en un terminal inalámbrico.

La figura 10 ilustra una configuración de nodo de ejemplo de una estación base 401A de anclaje que puede realizar algunas de las realizaciones de ejemplo descritas en el presente documento. La estación base 401A de anclaje puede comprender circuitería de radio o un puerto 410A de comunicación que puede estar configurado para recibir y/o transmitir mediciones de comunicación, datos, instrucciones y/o mensajes. La estación base 401A de anclaje puede comprender además una circuitería 440A de interfaz de red que puede estar configurada para recibir o enviar comunicaciones de red, por ejemplo, hacia y desde otros nodos de red. Debe apreciarse que la circuitería de radio o el puerto 410A de comunicación pueden estar comprendidos como cualquier número de unidades o circuitería transceptor, receptora y/o transmisora. Debe apreciarse además 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 interfaz 440A de red pueden comprender circuitería de RF y circuitería de procesamiento de banda base, cuyos detalles son bien conocidos para aquellos familiarizados con el diseño de estación base.

La estación 401A de base de anclaje también puede comprender una unidad o circuitería 420A de procesamiento que puede configurarse para realizar operaciones relacionadas con la generación de claves de seguridad de asistencia (por ejemplo, claves de seguridad para un eNB de asistencia), 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 pasarela programable por campo (FPGA) o circuito integrado específico de aplicación (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 cualquier información relacionada con la generación de claves de seguridad o parámetros de actualización, parámetros de dispositivo, prioridades de comunicación y/o instrucciones de programa ejecutables.

Las funciones típicas del circuito 420A de procesamiento, por ejemplo, cuando se configuran con el código de programa apropiado almacenado en la memoria 430A, incluyen modulación y codificación de señales transmitidas y la demodulación y decodificación de señales recibidas. En varias realizaciones de la presente invención, el circuito 420A de procesamiento está adaptado, utilizando un código de programa adecuado almacenado en la memoria 430A de almacenamiento de programa, por ejemplo, para llevar a cabo una de las técnicas descritas anteriormente para manejar 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 solo módulo.

Se apreciará que el circuito 420A de procesamiento, adaptado con el código de programa almacenado en la memoria 430A de programa y de datos, puede implementar el flujo de proceso de la figura 8 (o una variante del mismo) utilizando una disposición de "módulos" funcionales donde los módulos son programas informáticos o porciones de programas informáticos que se ejecutan en el circuito 420A de procesamiento. Por lo tanto, el aparato 401A puede entenderse que comprende una interfaz 440A de comunicaciones configurada para comunicarse con la estación base de asistencia, y que comprende además varios módulos funcionales implementados en el circuito 420A de procesamiento. Estos módulos funcionales incluyen: un módulo generador para generar una clave de seguridad de asistencia para la estación base de asistencia, basada, al menos en parte, en una clave de estación base de anclaje; un módulo de envío para enviar a la estación base de asistencia, utilizando la circuitería de interfaz, la clave de seguridad de asistencia generada, para su uso por la estación base de asistencia en cifrar el tráfico de datos enviado al terminal inalámbrico o en generar una o más claves de seguridad de asistencia para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base de asistencia mientras el terminal inalámbrico está conectado de forma dual a la estación base de anclaje y la estación base de asistencia; y un módulo de cifrado para utilizar 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 el terminal inalámbrico está conectado de forma dual a la estación base de anclaje y la estación base de asistencia.

La figura 11 ilustra una configuración de nodo de ejemplo de un nodo 505A de gestión de movilidad (por ejemplo, un MME, SGSN, S4-SGSN) que puede realizar algunas de las realizaciones de ejemplo descritas en el presente documento. El nodo 505A de gestión de movilidad puede comprender una circuitería de interfaz o un puerto 510A de comunicación que puede estar configurado para recibir y/o transmitir mediciones de comunicación, datos, instrucciones y/o mensajes. Debe apreciarse que la circuitería de radio o el puerto 510A de comunicación pueden estar comprendidos como cualquier número de unidades o circuitería transceptora, receptora y/o transmisora. Debe apreciarse además que la circuitería o comunicación 510A de radio puede tener la forma de cualquier puerto de comunicaciones de entrada o salida conocido en la técnica. La circuitería o comunicación 510A de interfaz puede comprender circuitería de RF y circuitería de procesamiento de banda base (no mostrada).

El nodo 505A de gestión de movilidad también puede comprender una unidad o circuitería 520A de procesamiento que puede configurarse para realizar operaciones relacionadas con la generación de claves de seguridad de asistencia (por ejemplo, claves de seguridad para un eNB de asistencia), 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 pasarela programable por campo (FPGA) o circuito integrado específico de aplicación (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 estar configurada para almacenar información recibida, transmitida y/o cualquier información relacionada con la generación de claves de seguridad o parámetros de actualización, parámetros de dispositivo, prioridades de comunicación y/o instrucciones de programa ejecutables para su uso mediante circuitería 520A de procesamiento.

En varias realizaciones de la presente invención, el circuito 520A de procesamiento está adaptado, utilizando un código de programa adecuado almacenado en la memoria de almacenamiento de programa 530A, por ejemplo, para llevar a cabo una de las técnicas descritas anteriormente para manejar 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 solo módulo.

Se apreciará que el circuito 520A de procesamiento, adaptado con código de programa almacenado en la memoria 530A de programa y de datos, puede implementar el flujo de proceso de la figura 9 (o una variante del mismo) utilizando una disposición de "módulos" funcionales, donde los módulos son programas informáticos o porciones de programas informáticos que se ejecutan en el circuito 520A de procesamiento. Por lo tanto, el aparato 501A puede entenderse que comprende una interfaz 540A de comunicaciones configurada para comunicarse con la estación base de asistencia, y que comprende además varios módulos funcionales implementados en el circuito 520A de procesamiento. Estos módulos funcionales incluyen: un módulo de compartición para compartir una clave de seguridad primaria con el terminal inalámbrico; un módulo generador para generar una clave de seguridad de asistencia para la estación base de asistencia, basada, al menos en parte, en la clave de seguridad primaria; y un módulo de envío para enviar a la estación base de asistencia, a través de la circuitería de interfaz, la clave de seguridad de asistencia generada, para su uso por la estación base de asistencia para cifrar el tráfico de datos enviado al terminal inalámbrico o generar una o más claves de seguridad de asistencia adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base de asistencia mientras el terminal inalámbrico está conectado de forma dual a la estación base de anclaje y la estación base de asistencia. La figura 12 ilustra una configuración de nodo de ejemplo de un terminal inalámbrico 505B que puede estar configurado para llevar a cabo algunos de los métodos de ejemplo descritos en el presente documento. El terminal inalámbrico 505B puede comprender una circuitería de interfaz o un puerto 510B de comunicación que puede estar configurado para recibir y/o transmitir medidas, datos, instrucciones y/o mensajes de comunicación. Debe apreciarse que la circuitería de radio o el puerto 510B de comunicación pueden estar comprendidos como cualquier número de unidades o circuitos transceptores, receptores y/o transmisores. Debe apreciarse además que la circuitería o comunicación 510B de radio 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 mostrada).

El terminal inalámbrico 505B también puede comprender una unidad o circuitería 520B de procesamiento que puede configurarse para realizar operaciones relacionadas con la generación de claves de seguridad de asistencia (por ejemplo, claves de seguridad para un eNB de asistencia), 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 pasarela programable por campo (FPGA) o circuito integrado específico de aplicación (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 estar configurada para almacenar información recibida, transmitida y/o cualquier información relacionada con la generación de claves de seguridad o parámetros de actualización, parámetros de dispositivo, prioridades de comunicación y/o instrucciones de programa ejecutables.

Por consiguiente, en diversas realizaciones de la invención, los circuitos de procesamiento, tales como los circuitos 520A y 520B de procesamiento y sus correspondientes circuitos 530A y 530B de memoria, están configurados para llevar a cabo una o más de las técnicas descritas con detalle anteriormente. Otras realizaciones pueden incluir estaciones base y/u otros nodos de red que incluyen uno o más de dichos circuitos de procesamiento. En algunos casos, estos circuitos de procesamiento están configurados con un 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 solo microprocesador o incluso en un solo módulo.

La persona experta en la técnica apreciará que se pueden hacer diversas modificaciones a las realizaciones descritas anteriormente sin apartarse del alcance de la presente invención. Por ejemplo, aunque se han descrito realizaciones de la presente invención con ejemplos que incluyen un sistema de comunicación que cumple los estándares LTE especificados para 3GPP, debe observarse que las soluciones presentadas pueden ser igualmente aplicables a otras redes que soportan conectividad dual. Por lo tanto, las realizaciones específicas descritas anteriormente deben considerarse ejemplares en lugar de limitar el alcance de la invención. Como no es posible, por supuesto, describir todas las combinaciones concebibles de componentes o técnicas, los expertos en la técnica apreciarán que la presente invención se puede implementar de otras formas distintas a las específicamente expuestas en este documento, sin apartarse de las características esenciales de la invención. Por lo tanto, las presentes realizaciones deben considerarse en todos los aspectos como ilustrativas y no restrictivas.

En la presente descripción de varias realizaciones de los presentes conceptos de la invención, debe entenderse que la terminología utilizada en el presente documento es con el propósito de describir únicamente realizaciones particulares y no pretende limitar los presentes conceptos de la invención. A menos que se defina lo contrario, todos los términos (incluidos los términos técnicos y científicos) utilizados en el presente documento tienen el mismo significado que comúnmente entiende un experto en la técnica a la que pertenecen los presentes conceptos de la invención. Se entenderá además que los términos, tales como los definidos en los diccionarios comúnmente utilizados, deberían interpretarse como que tienen un significado que es consistente con su significado en el contexto de esta memoria descriptiva y la técnica relevante y no se interpretarán en un sentido idealizado o excesivamente formal expresamente definido en el presente documento.

Cuando se hace referencia a un elemento como "conectado", "acoplado", "sensible" o variantes de los mismos a otro elemento, puede estar conectado directamente, acoplado o sensible al otro elemento o pueden estar presentes elementos interpuestos. Por el contrario, cuando se hace referencia a un elemento como "directamente conectado", "directamente acoplado", "directamente sensible" o variantes de los mismos a otro elemento, no hay elementos intermedios presentes. Los números semejantes se refieren a elementos semejantes. Además, "acoplado", "conectado", "sensible", o sus variantes, tal como se utilizan en el presente documento, pueden incluir acoplamiento, conexión o respuesta inalámbrica. Tal como se utiliza en el presente documento, las formas singulares "un", "una" y "el" y “ella” pretenden incluir también las formas plurales, a menos que el contexto indique claramente lo contrario. Las funciones o construcciones bien conocidas pueden no ser descritas en detalle para mayor brevedad y/o claridad. El término "y/o" incluye todas y cada una de las combinaciones de uno o más de los elementos enumerados asociados.

Se entenderá que aunque los términos primero, segundo, tercero, etc. se pueden utilizar aquí para describir varios elementos/operaciones, estos elementos/operaciones no deberían estar limitados por estos términos. Estos términos sólo se utilizan 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 presentes conceptos de la invención. Los mismos números de referencia o los mismos designadores de referencia indican los mismos elementos o elementos similares a lo largo de la memoria descriptiva.

Tal como se utiliza en el presente documento, los términos "comprender", "comprendiendo", "comprende", "incluir", "incluyendo", "incluye", "tener", "tiene”, “teniendo”, o variantes de los mismos son abiertos, e incluyen una o más

características, enteros, elementos, pasos, componentes o funciones expresados, pero no excluye la presencia o adición de una o más características, enteros, elementos, pasos, componentes, funciones o grupos de los mismos. Además, tal como se utiliza en el presente documento, la abreviatura común "eg", que deriva de la frase latina "exempli gratia", puede utilizarse para introducir o especificar un ejemplo general o ejemplos de un elemento mencionado anteriormente, y no pretende ser limitativo de tal elemento. La abreviatura común "i.e.", que deriva de la frase latina "id est", puede utilizarse para especificar un elemento particular de una recitación más general.

En el presente documento 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 informáticos. Se entiende que un bloque de los diagramas de bloques y/o ilustraciones de diagrama de flujo, y combinaciones de bloques en los diagramas de bloques y/o ilustraciones de diagrama de flujo, puede implementarse mediante instrucciones de programa informático que son realizadas por uno o más circuitos informáticos. Estas instrucciones de programa informático pueden proporcionarse a un circuito de procesador de un circuito informático de propósito general, un circuito informático de propósito especial y/o 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, transforme y controle transistores, valores almacenados en ubicaciones de memoria y otros componentes de equipo físico dentro de tal circuitería para implementar las funciones/actos especificados en los diagramas de bloques y/o bloques o bloques de diagrama de flujo, y por ello cree medios (funcionalidad) y/o estructura para implementar las funciones/actos especificados en los diagramas de bloques y/o bloque/s de diagrama de flujo.

Estas instrucciones del programa informático también pueden almacenarse en un medio legible por ordenador tangible que puede dirigir un ordenador u otro aparato de procesamiento de datos programable para que funcione de una manera particular, de tal manera que las instrucciones almacenadas en el medio legible por ordenador produzcan un artículo de fabricación que incluye instrucciones que implementan las funciones/actos especificados en los diagramas de bloques y/o bloques de diagrama de flujo. Por consiguiente, las realizaciones de los presentes conceptos de la invención pueden realizarse en equipo físico y/o en equipo lógico (incluyendo microprogama, equipo lógico residente, microcódigo, etc.) que se ejecutan en un procesador tal como un procesador de señal digital, que se puede denominar colectivamente como "circuitería", "un módulo" o sus variantes.

También debe observarse que en algunas implementaciones alternativas, las funciones/actos observados en los bloques pueden ocurrir fuera del orden indicado en los diagramas de flujo. Por ejemplo, dos bloques mostrados en sucesión pueden de hecho ejecutarse de forma sustancialmente concurrente o los bloques a veces pueden ejecutarse en el orden inverso, dependiendo de la funcionalidad/los actos implicados. Además, la funcionalidad de un bloque dado de los diagramas de flujo y/o diagramas de bloques se puede separar en múltiples 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, se pueden añadir/insertar otros bloques entre los bloques que se ilustran, y/o pueden omitirse bloques/operaciones sin apartarse del alcance de los conceptos de la invención. Además, aunque algunos de los diagramas incluyen flechas en trayectos de comunicación para mostrar una dirección primaria de comunicación, debe entenderse que la comunicación puede producirse en la dirección opuesta a las flechas representadas.

Se pueden hacer muchas variaciones y modificaciones 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 aquí dentro del alcance de los presentes conceptos de la invención. Por consiguiente, se ha de considerar que la materia descrita anteriormente es ilustrativa, y no restrictiva, y los ejemplos de realizaciones adjuntas están destinados a cubrir todas dichas 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 presentes conceptos de la invención se determinará por la interpretación permisible más amplia de la presente divulgación y no se restringirá ni limitará por la descripción detallada anterior.

A continuación se describen algunas realizaciones no limitativas.

Realización 1. Un método, 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 de asistencia, en el que el terminal inalámbrico es o está a punto de ser conectado de forma dual a la estación base de anclaje y la estación base de asistencia, comprendiendo el método:

generar (810) una clave de seguridad de asistencia para la estación base de asistencia, basada, al menos en parte, en una clave de estación base de anclaje;

enviar (820), a la estación base de anclaje, la clave de seguridad de asistencia generada, para su uso por la estación base de asistencia para cifrar el tráfico de datos enviado al terminal inalámbrico o para generar una o más claves de seguridad de asistencia adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base de asistencia mientras el terminal inalámbrico está conectado de forma dual a la estación base de anclaje y la estación base de asistencia; y

utilizar (830) 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 el terminal inalámbrico está conectado de forma dual a la estación base de anclaje y la estación base de asistencia.

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

Realización 3. El método de la realización 2, en el que utilizar (830) la clave de estación base de anclaje comprende derivar una clave de cifrado, o una clave de integridad, o ambas, desde la clave de estación base de anclaje y utilizar la clave o claves derivadas para proteger los datos enviados al terminal inalámbrico por la estación base de anclaje mientras que el terminal inalámbrico está conectado de forma dual a la estación base de anclaje y la estación base de asistencia.

Realización 4. El método de cualquiera de las realizaciones 1-3, en el que generar (810) la clave de seguridad de asistencia comprende derivar la clave de seguridad de asistencia desde la clave de estación base de anclaje utilizando una función unidireccional.

Realización 5. El método de la realización 4, en el que la función unidireccional es una función criptográfica HMAC-SHA-256.

Realización 6. El método de cualquiera de las realizaciones 1-5, en el que generar (810) la clave de seguridad de asistencia se basa además en un parámetro de actualización.

Realización 7. El método de cualquiera de las realizaciones 1-6, que comprende además:

detectar que un parámetro COUNT de protocolo de convergencia de datos de paquetes, PDCP, en la estación base de asistencia está a punto de envolverse; en respuesta a dicha detección, iniciar una actualización de la clave de estación base de anclaje y volver a calcular la clave de seguridad de asistencia.

Realización 8. El método de cualquiera de las realizaciones 1-7, en el que el nodo de red es un eNodoB de evolución a largo plazo, LTE.

Realización 9. El método de cualquiera de las realizaciones 1-8, en el que dicha generación (810) se repite para cada uno de una pluralidad de portadores de radio de datos establecidos entre el terminal inalámbrico y la estación base de asistencia, de tal manera que las claves de seguridad de asistencia resultantes difieren para cada portador de radio de datos.

Realización 10. Un método, 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 de asistencia, en el que el terminal inalámbrico es o está a punto de ser conectado de forma dual a la estación base de anclaje y la estación base de asistencia, comprendiendo el método:

compartir (910) una clave de seguridad primaria con el terminal inalámbrico;

generar (920) una clave de seguridad de asistencia para la estación base de asistencia, basada, al menos en parte, en la clave de seguridad primaria;

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

Realización 11. El método de la realización 10, en el que la clave de seguridad de asistencia generada comprende una clave de seguridad de asistencia base para su uso en la generación de una o más claves de seguridad de asistencia adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base de asistencia.

Realización 12. El método de la realización 10 u 11, en el que generar (920) la clave de seguridad de asistencia comprende derivar la clave de seguridad de asistencia desde la clave de estación base de anclaje utilizando una función unidireccional.

Realización 13. El método de la realización 12, en el que la función unidireccional es una función criptográfica HMAC-SHA-256.

Realización 14. El método de cualquiera de las realizaciones 10-13, en el que generar (920) la clave de seguridad de asistencia se basa adicionalmente en un parámetro de actualización.

Realización 15. El método de cualquiera de las realizaciones 10-14, en el que enviar (930) la clave de seguridad de asistencia generada a la estación base de asistencia comprende enviar la clave de seguridad de asistencia generada a la estación base de asistencia indirectamente, a través de la estación base de anclaje.

Realización 16. El método de cualquiera de las realizaciones 10-15, en el que el nodo de red es un nodo de gestión de movilidad.

Realización 17. Un nodo (401A) de red para la generación de claves de seguridad para comunicaciones seguras entre un terminal inalámbrico y una estación base de asistencia, en el que el terminal inalámbrico es o está a punto de ser conectado de forma dual con la estación base de anclaje y la estación base de asistencia, el nodo (401A) de red comprendiendo circuitería (440A) de interfaz configurada para comunicar con la estación base de asistencia y que comprende además circuitería (420A, 430A) de procesamiento, caracterizado porque la circuitería (420A, 430A) de procesamiento está configurada para:

generar una clave de seguridad de asistencia para la estación base de asistencia, basada, al menos en parte, en una clave de estación base de anclaje;

enviar a la estación base de asistencia, utilizando la circuitería de interfaz, la clave de seguridad de asistencia generada, para su uso por la estación base de asistencia para cifrar el tráfico de datos enviado al terminal inalámbrico o para generar una o más claves de seguridad de asistencia adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base de asistencia mientras el terminal inalámbrico está conectado de forma dual a la estación base de anclaje y la estación base de asistencia; y

utilizar 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 el terminal inalámbrico está conectado de forma dual a la estación base de anclaje y la estación base de asistencia.

Realización 18. El nodo (401A) de red de la realización 17, en el que la clave de seguridad de asistencia generada comprende una clave de seguridad de asistencia base para su uso en la generación de una o más claves de seguridad de asistencia adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base de asistencia.

Realización 19. El nodo (401A) de red de la realización 18, en el que la circuitería (420A, 430A) de procesamiento está configurada para utilizar la clave de estación base de anclaje para derivar una clave de cifrado, o una clave de integridad, o ambas, desde la clave de estación base de anclaje y para utilizar la clave o claves derivadas para proteger los datos enviados al terminal inalámbrico por la estación base de anclaje mientras el terminal inalámbrico está conectado de forma dual a la estación base de anclaje y la estación base de asistencia.

Realización 20. El nodo (401A) de red de cualquiera de las realizaciones 17-19, en el que la circuitería (420A, 430A) de procesamiento está configurada para generar la clave de seguridad de asistencia derivando la clave de seguridad de asistencia desde la clave de estación base de anclaje utilizando una función unidireccional.

Realización 21. El nodo (401A) de red de la realización 20, en el que la función unidireccional es una función criptográfica HMAC-SHA-256.

Realización 22. El nodo (401A) de red de cualquiera de las realizaciones 17-21, en el que la circuitería (420A, 430A) de procesamiento está configurada para generar la clave de seguridad de asistencia basándose además en un parámetro de actualización.

Realización 23. El nodo (401A) de red de cualquiera de las realizaciones 17-22, en el que la circuitería (420A, 430A) de procesamiento está configurada además para:

detectar que un parámetro de COUNT de protocolo de convergencia de datos de paquetes, PDCP, en la estación base de asistencia está a punto de envolverse ;

en respuesta a dicha detección, iniciar una actualización de la clave de estación base de anclaje y volver a calcular la clave de seguridad de asistencia.

Realización 24. El nodo (401A) de red de cualquiera de las realizaciones 17-23, en el que el nodo (401A) de red es un eNodoB de evolución a largo plazo, LTE.

Realización 25. El nodo (401A) de red de cualquiera de las realizaciones 17-24, en el que la circuitería (420A, 430A)

de procesamiento está configurada para repetir dicha generación para cada uno de una pluralidad de portadores de radio de datos establecidos entre el terminal inalámbrico y la estación base de asistencia, de tal manera que las claves de seguridad de asistencia resultantes difieren para cada portador de radio de datos.

Realización 26. Un nodo (505A) de red para la generación de claves de seguridad para comunicaciones seguras entre un terminal inalámbrico y una estación base de asistencia, en el que el terminal inalámbrico es o está a punto de ser conectado de forma dual a la estación base de anclaje y la estación base de asistencia, el nodo (505A) de red comprendiendo una circuitería (510A) de interfaz configurada para comunicarse con la estación base de asistencia y que comprende además una circuitería (520A, 530A) de procesamiento, caracterizado porque el circuito de procesamiento está configurado para:

compartir una clave de seguridad primaria con el terminal inalámbrico;

generar una clave de seguridad de asistencia para la estación base de asistencia, basada, al menos en parte, en la clave de seguridad primaria;

enviar a la estación base de asistencia, a través de la circuitería (510A) de interfaz, la clave de seguridad de asistencia generada, para su uso por la estación base de asistencia para cifrar el tráfico de datos enviado al terminal inalámbrico o para generar una o más claves de seguridad de asistencia para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base de asistencia mientras el terminal inalámbrico está conectado de forma dual a la estación base de anclaje y la estación base de asistencia.

Realización 27. El nodo (505A) de red de la realización 26, en el que la clave de seguridad de asistencia generada comprende una clave de seguridad de asistencia base para su uso en la generación de una o más claves de seguridad de asistencia adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base de asistencia.

Realización 28. El nodo (505A) de red de la realización 26 ó 27, en el que la circuitería (520A, 530A) de procesamiento está configurada para generar la clave de seguridad de asistencia derivando la clave de seguridad de asistencia desde la clave de estación base de anclaje utilizando una función unidireccional.

Realización 29. El nodo (505A) de red de la realización 28, en el que la función unidireccional es una función criptográfica HMAC-SHA-256.

Realización 30. El nodo (505A) de red de cualquiera de las realizaciones 26-29, en el que la circuitería (520A, 530A) de procesamiento está configurada para generar la clave de seguridad de asistencia basándose además en un parámetro de actualización.

Realización 31. El nodo (505A) de red de cualquiera de las realizaciones 26-30, en el que la circuitería (520A, 530A) de procesamiento está configurada para enviar la clave de seguridad de asistencia generada a la estación base de asistencia indirectamente, a través de la estación base de anclaje.

Realización 32. El nodo (505A) de red de cualquiera de las realizaciones 26-31, en el que el nodo (505A) de red es un nodo de gestión de movilidad.

REIVINDICACIONES

1.- Un método en un terminal inalámbrico (505B) para la generación de claves de seguridad para comunicaciones seguras entre el terminal inalámbrico (505B) y una estación base de asistencia, en el que el terminal inalámbrico (505B) es o está a punto de ser conectado de forma dual a una estación base de anclaje y la estación base de asistencia, en el que una clave de seguridad primaria es conocida por la estación base de anclaje y el terminal inalámbrico (505B), comprendiendo el método:

generar una clave de seguridad de asistencia, basada al menos en parte en la clave de seguridad primaria;

utilizar la clave de seguridad de asistencia en la generación de una o más claves de seguridad de asistencia adicionales para cifrar el tráfico de datos;

en el que el tráfico de datos es enviado desde el terminal inalámbrico (505B) a la estación base de asistencia mientras el terminal inalámbrico (505B) está conectado de forma dual a la estación base de anclaje y la estación base de asistencia.

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

3.- El método de la reivindicación 1 ó 2, en el que la generación de la clave de seguridad de asistencia comprende derivar la clave de seguridad de asistencia desde la clave primaria utilizando 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 cualquiera de las reivindicaciones 1-4, en el que la generación de la clave de seguridad de asistencia se basa adicionalmente en un parámetro de actualización.

6.- Un terminal inalámbrico (505B), para la generación de claves de seguridad para comunicaciones seguras entre el terminal inalámbrico (505B) y una estación base de asistencia, comprendiendo el terminal inalámbrico (505B) circuitería (510B) de interfaz, circuitería (520B) de procesamiento y una memoria (530B), en el que el terminal inalámbrico (505B) está configurado para conectarse de forma dual a una estación base de anclaje y la estación base de asistencia, y en el que la circuitería (520B) de procesamiento está configurada para:

generar una clave de seguridad de asistencia, basada al menos en parte en una clave de seguridad primaria que es conocida por la estación base de anclaje y el terminal inalámbrico (505B);

utilizar la clave de seguridad de asistencia en la generación de una o más claves de seguridad de asistencia adicionales para cifrar el tráfico de datos;

en el que el tráfico de datos es enviado desde el terminal inalámbrico (505B) a la estación base de asistencia mientras el terminal inalámbrico (505B) está conectado de forma dual a la estación base de anclaje y la estación base de asistencia.

7.- El terminal inalámbrico (505B) de la reivindicación 6, en el que la circuitería (520B) de procesamiento está configurada además para generar la clave de seguridad de asistencia derivando la clave de seguridad de asistencia desde la clave primaria utilizando una función unidireccional.

8.- El terminal inalámbrico (505B) de la reivindicación 7, en el que la función unidireccional es una función criptográfica HMAC-SHA-256.

9.- El terminal inalámbrico (505B) de cualquiera de las reivindicaciones 6-8, en el que la circuitería (520B) de procesamiento está configurada además para generar la clave de seguridad de asistencia basándose en un parámetro de actualización.

10.- El terminal inalámbrico (505B) de cualquiera de las reivindicaciones 6-9, configurado adicionalmente para almacenar la clave primaria y/o la clave de seguridad de asistencia en la memoria (530B).

11.- El terminal inalámbrico (505B) de la reivindicación 9 ó 10, configurado adicionalmente para almacenar el parámetro de actualización en la memoria (530B).

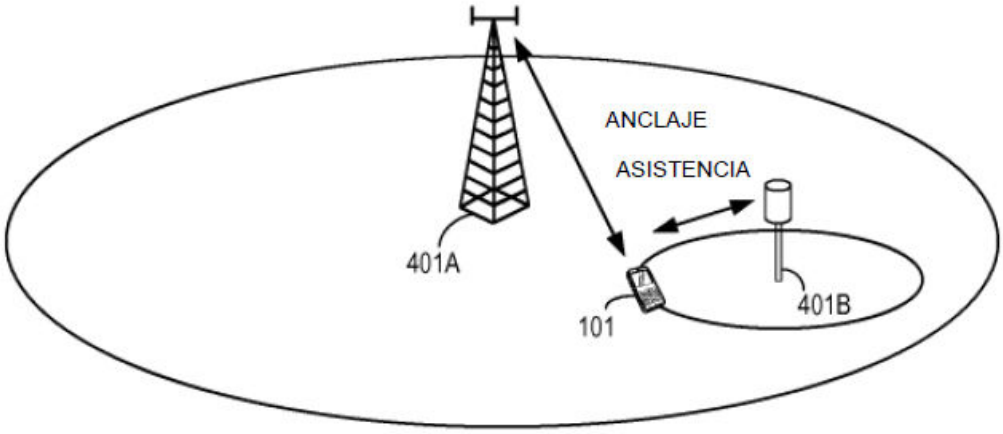

FIG. 1

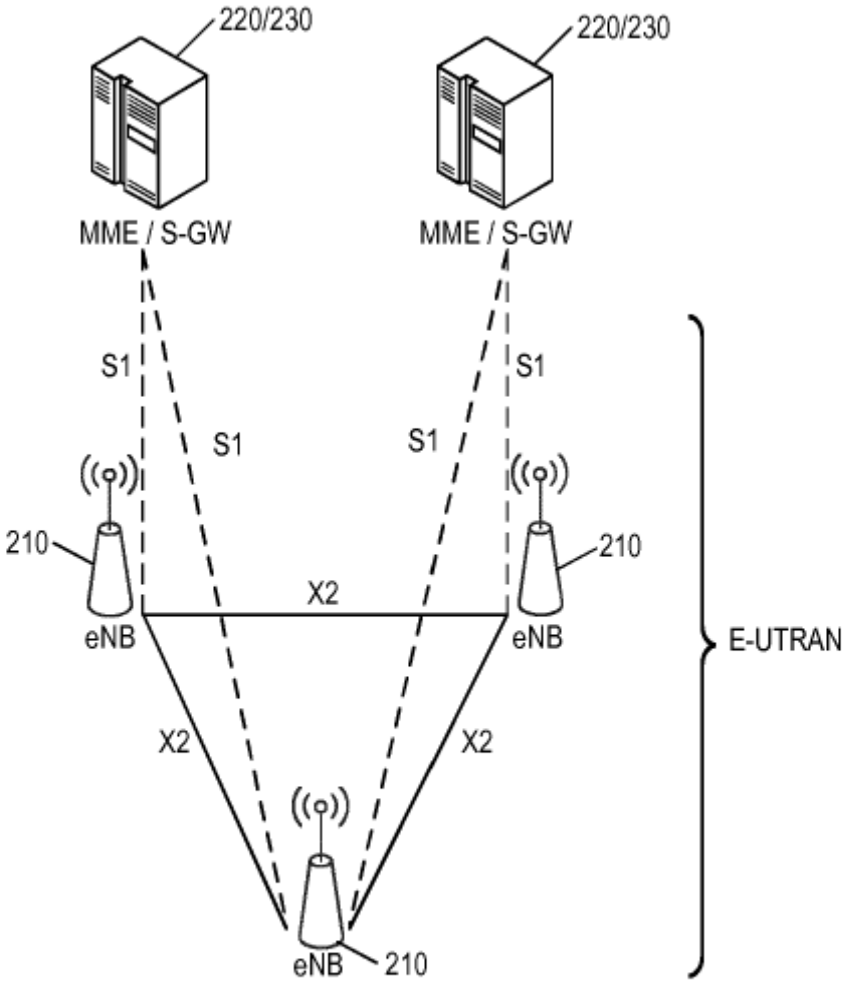
220/230
220/230
MME / S-GW
MME / S-GW
S1
S1
S1
S1
210
210
X2
eNB
eNB
E-UTRAN
X2
X2
eNB
210

FIG. 2

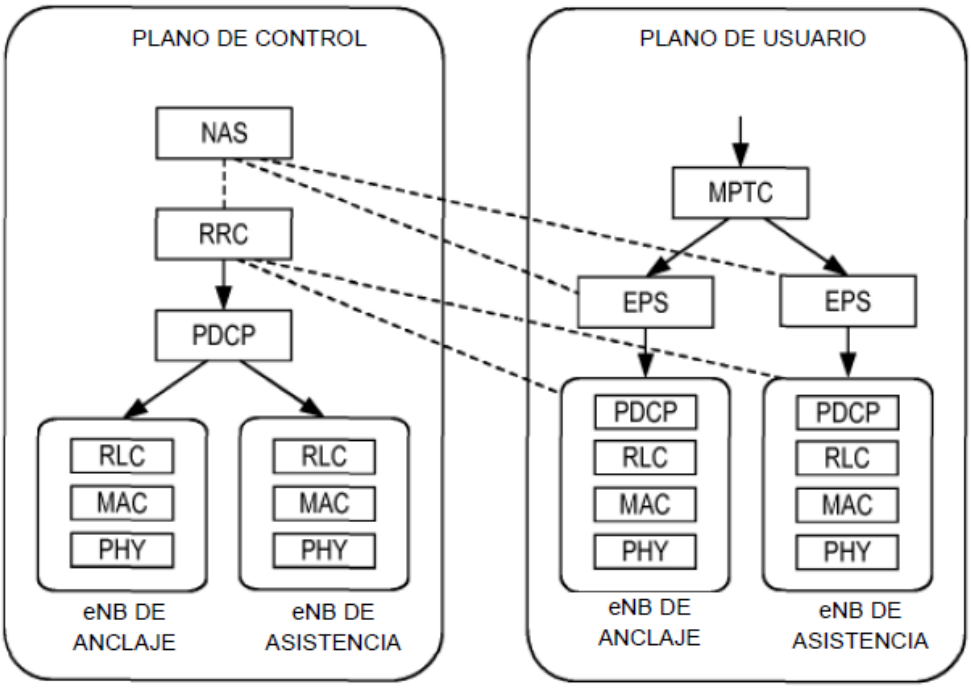
PLANO DE CONTROL
PLANO DE USUARIO
NAS
RRC
PDCP
RLC
MAC
PHY
RLC
MAC
PHY
eNB DE ANCLAJE
eNB DE ASISTENCIA
MPTC
EPS
EPS
PDCP
RLC
MAC
PHY
PDCP
RLC
MAC
PHY
eNB DE ANCLAJE
eNB DE ASISTENCIA

FIG. 3

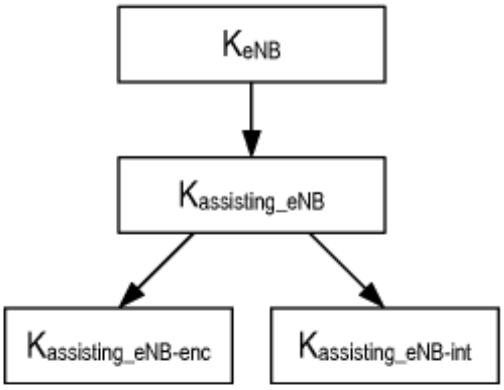
KeNB
Kassisting_eNB
Kassisting_eNB-enc
Kassisting_eNB-int

FIG. 4

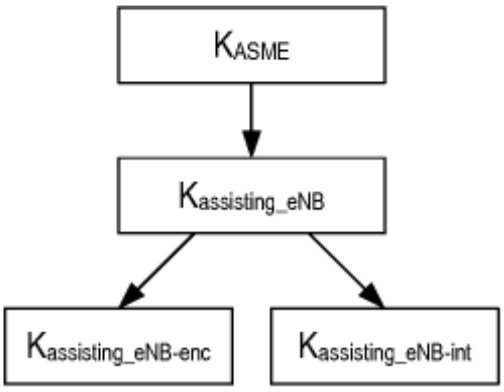
KASME
Kassisting_eNB
Kassisting_eNB-enc
Kassisting_eNB-int

FIG. 5

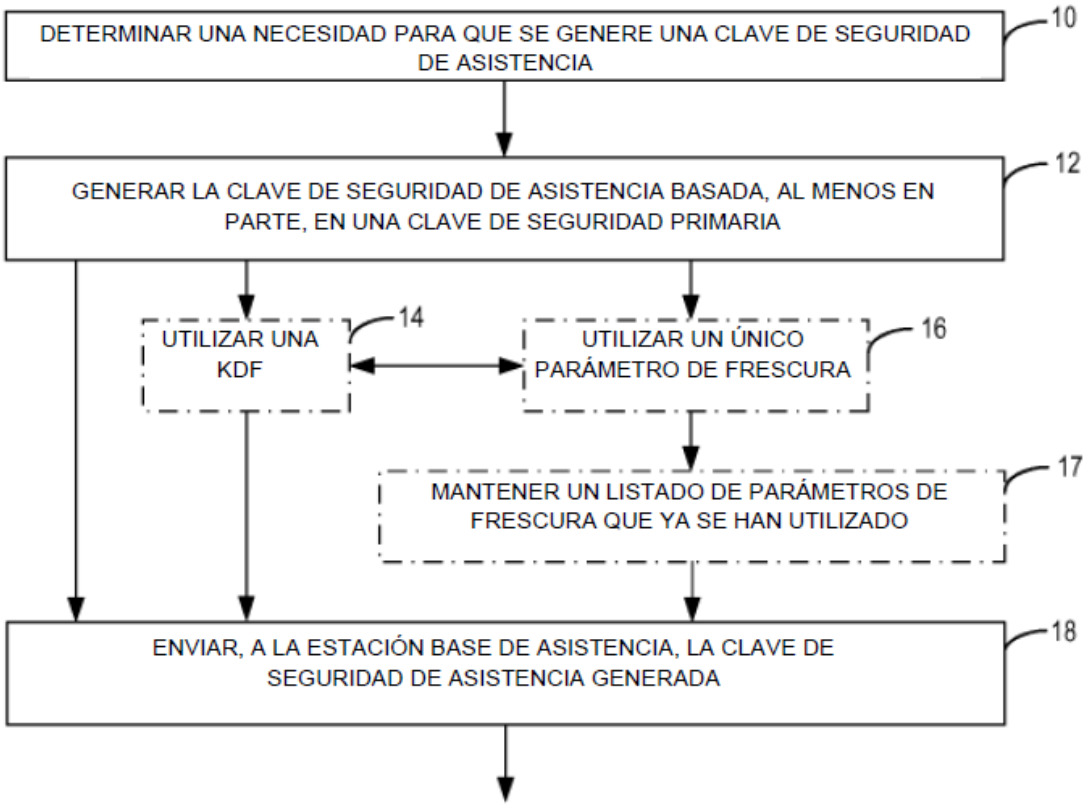
DETERMINAR UNA NECESIDAD PARA QUE SE GENERE UNA CLAVE DE SEGURIDAD DE ASISTENCIA
10
GENERAR LA CLAVE DE SEGURIDAD DE ASISTENCIA BASADA, AL MENOS EN PARTE, EN UNA CLAVE DE SEGURIDAD PRIMARIA
12
UTILIZAR UNA KDF
14
UTILIZAR UN ÚNICO PARÁMETRO DE FRESCURA
16
MANTENER UN LISTADO DE PARÁMETROS DE FRESCURA QUE YA SE HAN UTILIZADO
17
ENVIAR, A LA ESTACIÓN BASE DE ASISTENCIA, LA CLAVE DE SEGURIDAD DE ASISTENCIA GENERADA
18

FIG. 6

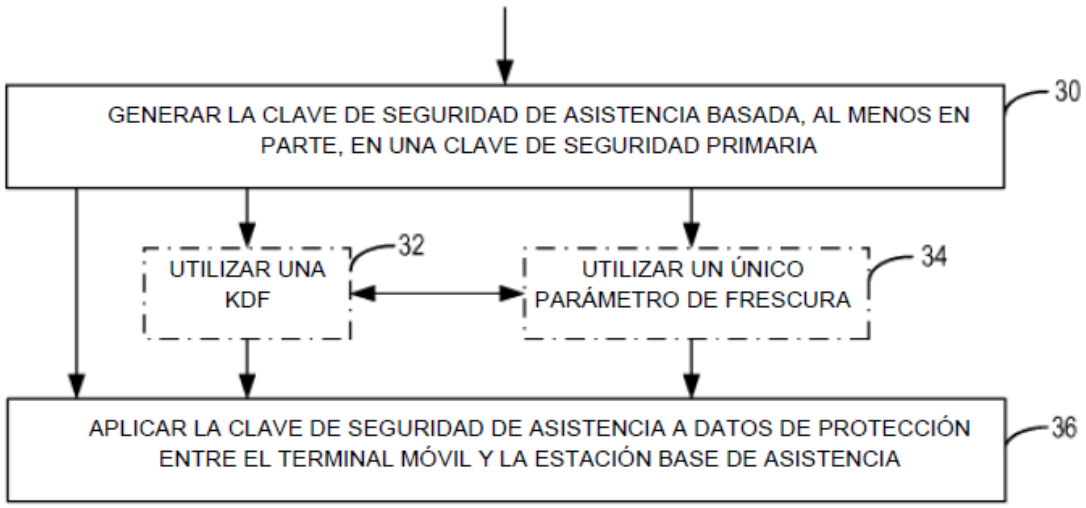
GENERAR LA CLAVE DE SEGURIDAD DE ASISTENCIA BASADA, AL MENOS EN PARTE, EN UNA CLAVE DE SEGURIDAD PRIMARIA
30
UTILIZAR UNA KDF
32
UTILIZAR UN ÚNICO PARÁMETRO DE FRESCURA
34
APLICAR LA CLAVE DE SEGURIDAD DE ASISTENCIA A DATOS DE PROTECCIÓN ENTRE EL TERMINAL MÓVIL Y LA ESTACIÓN BASE DE ASISTENCIA
36

FIG. 7

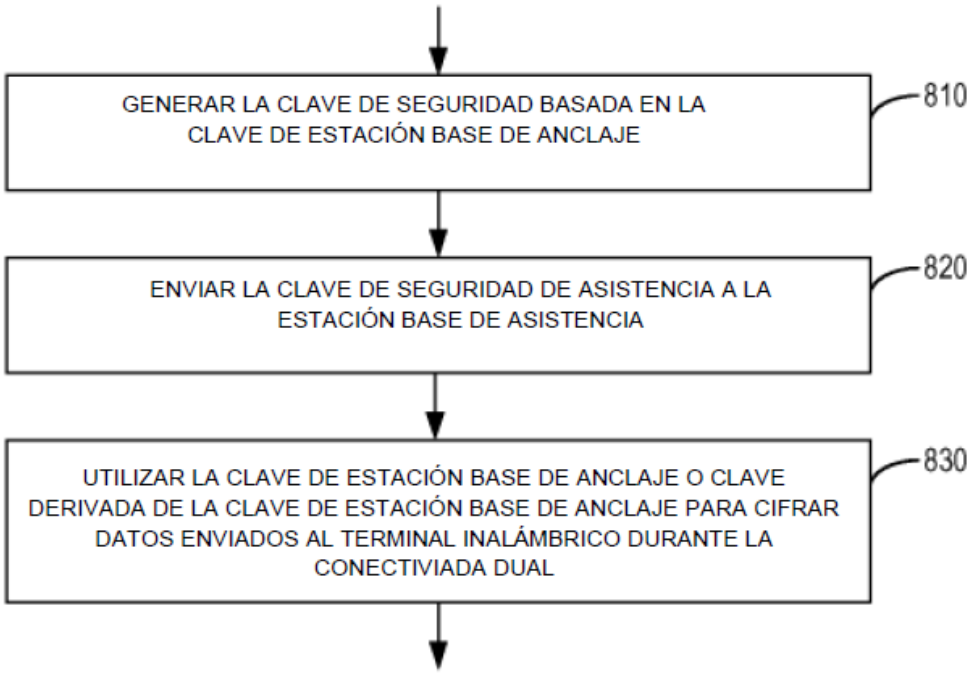
GENERAR LA CLAVE DE SEGURIDAD BASADA EN LA CLAVE DE ESTACIÓN BASE DE ANCLAJE
810
ENVIAR LA CLAVE DE SEGURIDAD DE ASISTENCIA A LA ESTACIÓN BASE DE ASISTENCIA
820
UTILIZAR LA CLAVE DE ESTACIÓN BASE DE ANCLAJE O CLAVE DERIVADA DE LA CLAVE DE ESTACIÓN BASE DE ANCLAJE PARA CIFRAR DATOS ENVIADOS AL TERMINAL INALÁMBRICO DURANTE LA CONECTIVIADA DUAL
830

FIG. 8

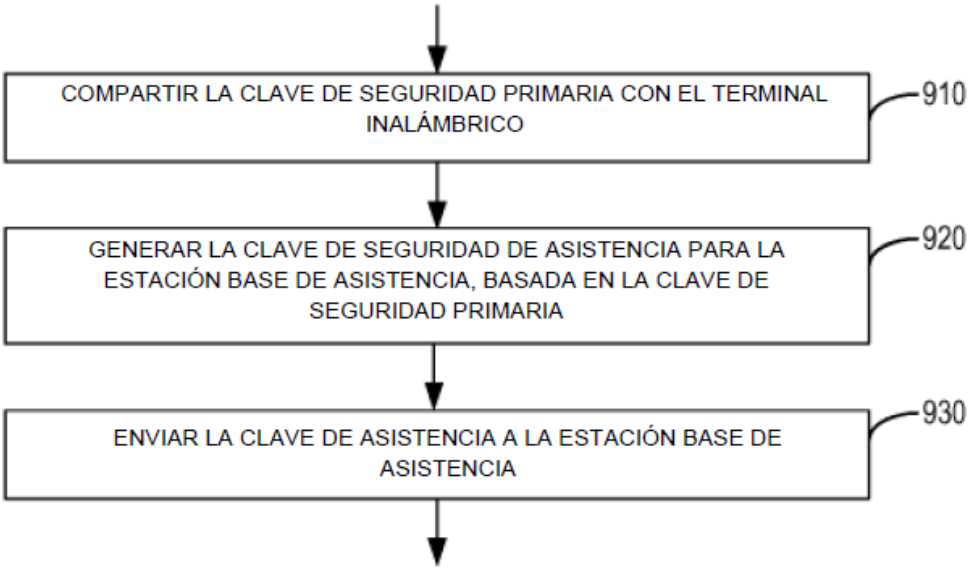
COMPARTIR LA CLAVE DE SEGURIDAD PRIMARIA CON EL TERMINAL INALÁMBRICO
910
GENERAR LA CLAVE DE SEGURIDAD DE ASISTENCIA PARA LA ESTACIÓN BASE DE ASISTENCIA, BASADA EN LA CLAVE DE SEGURIDAD PRIMARIA
920
ENVIAR LA CLAVE DE ASISTENCIA A LA ESTACIÓN BASE DE ASISTENCIA
930

FIG. 9

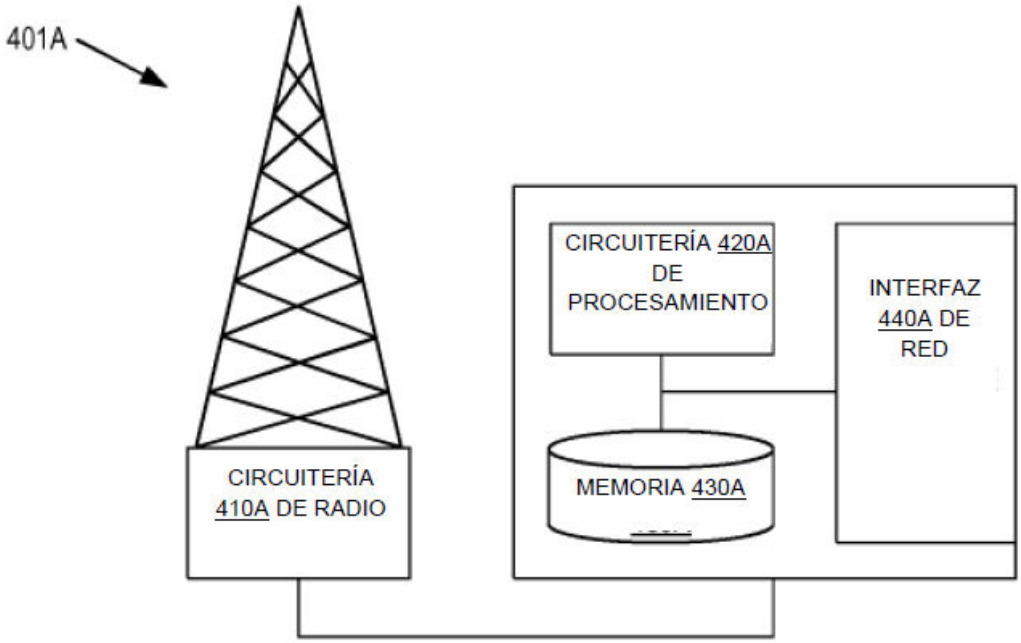
401A
CIRCUITERÍA 420A DE PROCESAMIENTO
INTERFAZ 440A DE RED
MEMORIA 430A
CIRCUITERÍA 410A DE RADIO

FIG. 10

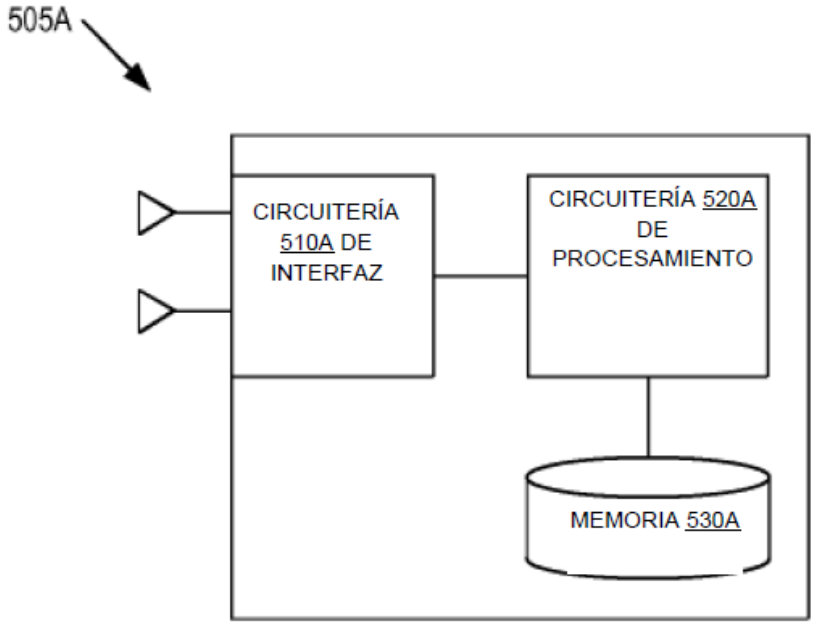
505A
CIRCUITERÍA 510A DE INTERFAZ
CIRCUITERÍA 520A DE PROCESAMIENTO
MEMORIA 530A

FIG. 11

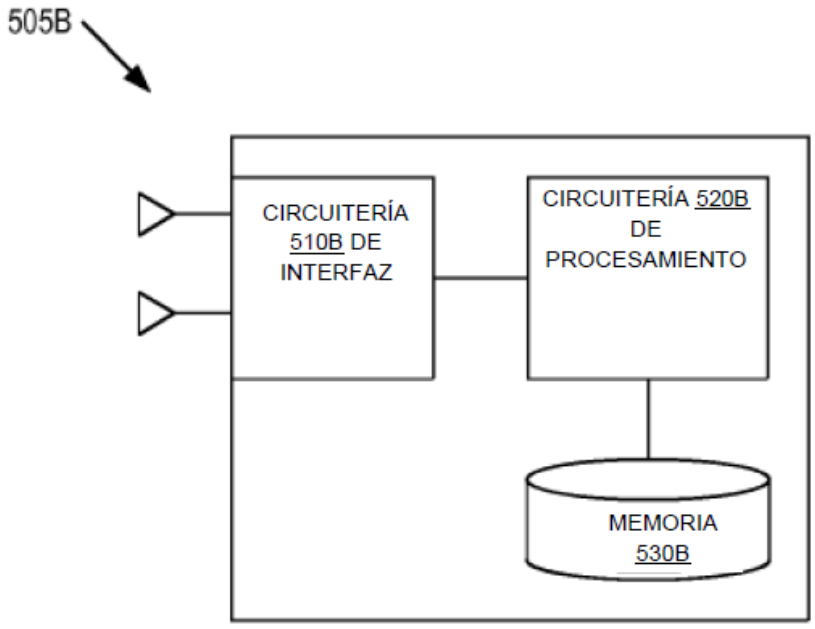
505B
CIRCUITERÍA 510B DE INTERFAZ
CIRCUITERÍA 520B DE PROCESAMIENTO
MEMORIA 530B

FIG. 12