(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 715 784**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04L 29/06 (2006.01)
H04L 9/14 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.01.2014 E 17169974 (7)**

(97) Fecha y número de publicación de la concesión europea: **12.12.2018 EP 3261374**

(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:
06.06.2019

(73) Titular/es:

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

(72) Inventor/es:

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

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Generación de clave de seguridad para conectividad dual

CAMPO TÉCNICO

La tecnología descrita en la presente memoria se refiere de manera general a redes de telecomunicaciones inalámbricas, y más particularmente se refiere 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 celular por radio típico, los terminales móviles (a los que también se hace referencia como 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, tales como Internet, y/o a la red de telecomunicaciones pública conmutada (PSTN). Una RAN cubre un área geográfica que se divide en áreas de celda, con cada área de celda que está servida por una estación base de radio (a la que también se hace referencia como una estación base, un nodo RAN, un "NodoB" y/o un NodoB mejorado o "eNodoB"). Un área de celda es un área geográfica sobre la cual se proporciona cobertura de radio por el equipo de la estación base en un sitio de estación base. Las estaciones base se comunican a través de canales de radiocomunicación 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 WCDMA (Acceso Múltiple por División de Código de Banda Ancha), HSPA (Acceso de Paquetes de Alta Velocidad) y Evolución a Largo Plazo (LTE). Alimentados 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 banda ancha móvil ha dado como resultado un crecimiento significativo en el tráfico manejado por las redes de datos inalámbricas de alta velocidad. Por consiguiente, se desean técnicas que permitan a los operadores celulares gestionar redes de manera más eficiente.

Técnicas para mejorar el rendimiento de enlace descendente pueden incluir técnicas de transmisión de múltiples antenas de Entrada Múltiple Salida Múltiple (MIMO), comunicaciones de múltiples flujos, despliegue de múltiples portadoras, etc. Dado que las eficiencias espectrales por enlace se pueden aproximar a los límites teóricos, los siguientes pasos pueden incluir mejorar las eficiencias espectrales por unidad de área. Se pueden lograr eficiencias adicionales para redes inalámbricas, por ejemplo, cambiando una topología de redes tradicionales para proporcionar un aumento de uniformidad de las experiencias de usuario en toda una celda. Un planteamiento es a través del despliegue de las llamadas redes heterogéneas.

Una red homogénea es una red de estaciones base (a las que también se hace referencia como NodoB, NodoB mejorados o eNB) en un diseño planificado, que proporciona servicios de comunicación para una colección de terminales de usuario (a los que también se hace referencia como nodos de equipos de usuario, UE, y/o terminales inalámbricos), en la que todas las estaciones base tienen típicamente niveles similares de potencia de transmisión, diagramas de antena, niveles mínimos de ruido del receptor y/o conectividad de enlace de retroceso a la red de datos. Además, todas las estaciones base en una red homogénea pueden ofrecer generalmente acceso no restringido a los terminales de usuario en la red, y cada estación base puede servir aproximadamente a un mismo número de terminales de usuario. Los sistemas de comunicaciones inalámbricos celulares actuales en esta categoría pueden incluir, por ejemplo, GSM (Sistema Global para Comunicaciones Móviles), WCDMA, HSDPA (Acceso de Paquetes de Enlace Descendente de Alta Velocidad), LTE (Evolución a Largo Plazo), WiMAX (Interoperabilidad Mundial para Acceso por Microondas), etc.

En una red heterogénea, se pueden desplegar estaciones base de baja potencia (a las que también se hace referencia como nodos de baja potencia (LPN), micro nodos, pico nodos, femto nodos, nodos de retransmisión, nodos de unidades de radio remotas, nodos RRU, celdas pequeñas, RRU, etc.) junto con o como una superposición a macro estaciones base planificadas y/o colocadas regularmente. Una macro estación base (MBS) puede proporcionar, de este modo, servicio sobre un área de macro celda relativamente grande, y cada LPN puede proporcionar servicio para un área de celda LPN relativamente pequeña respectiva dentro del área de macro celda 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 40 vatios para una macro estación base típica. Se puede desplegar un LPN, por ejemplo, para reducir/eliminar un agujero o agujeros de cobertura en la cobertura proporcionada por las macro estaciones base, y/o para descargar tráfico de las macro estaciones base, tal como para aumentar la capacidad en una ubicación de alto tráfico o los denominados puntos calientes. Debido a su menor potencia de transmisión y menor tamaño físico, un LPN puede ofrecer una mayor flexibilidad para la adquisición del sitio.

De este modo, una red heterogénea presenta un despliegue de múltiples capas de nodos de alta potencia (HPN), tales como macro estaciones base, y nodos de baja potencia (LPN), tales como las denominadas pico estaciones base o pico nodos. Los LPN y los HPN en una región dada de una red heterogénea pueden operar en la misma frecuencia, en cuyo caso se puede hacer referencia al despliegue como despliegue heterogéneo cocanal, o en diferentes frecuencias, en cuyo caso se puede hacer referencia al despliegue como un despliegue heterogéneo entre frecuencias o multiportadora o multifrecuencia.

El Proyecto de Cooperación de Tercera Generación (3GPP) está continuamente desarrollando especificaciones para características avanzadas y mejoradas en el contexto del sistema de telecomunicaciones inalámbrico de cuarta generación conocido como LTE (Evolución a Largo Plazo). En la Versión 12 de las especificaciones LTE y posteriores, se considerarán mejoras adicionales relacionadas con nodos de baja potencia y despliegues heterogéneos bajo el paraguas de las actividades de “mejoras de celdas pequeñas”. Algunas de estas actividades se centrarán en lograr un grado incluso mayor de interfuncionamiento entre las capas macro y de baja potencia, incluyendo a través del uso de un conjunto de técnicas y tecnologías a las que se hace referencia como “conectividad de capa dual” o simplemente “conectividad dual”. Como se muestra en la Figura 1, la conectividad dual implica que el dispositivo tiene conexiones simultáneas tanto a las capas macro como de baja potencia. La Figura 1 ilustra un ejemplo de una red heterogénea en la que un terminal móvil 101 usa múltiples flujos, por ejemplo, un flujo de anclaje desde la macro estación base (o “eNB de anclaje”) 401A y un flujo de asistencia desde una pico estación base (o un “eNB de asistencia”) 401B. Obsérvese que la terminología puede variar – se puede hacer referencia a la estación base de anclaje y la estación base de asistencia en una configuración que se muestra en la Figura 1 algunas veces como estaciones base “maestra” y “esclava” o según otros nombres. Se debería observar además que, mientras que los términos “anclaje/asistencia” y “maestra/esclava” 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 se pueden aplicar a escenarios de despliegue donde no hay tal relación jerárquica, por ejemplo, entre estaciones base iguales. Por consiguiente, aunque se usan en la presente memoria los términos “estación base de anclaje” y “estación base de asistencia”, se debería entender que las técnicas y el aparato descritos en la presente memoria no se limitan a las realizaciones que usan esa terminología, ni están necesariamente limitados a las realizaciones que tienen la relación jerárquica sugerida por la Figura 1.

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

- Control y separación de datos donde, por ejemplo, la señalización de control para movilidad se proporciona a través de la macro capa al mismo tiempo que se proporciona conectividad de datos de alta velocidad a través de la capa de baja potencia.
- Una separación entre el enlace descendente y el 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) se puede proporcionar a través de múltiples enlaces, mejorando aún más el rendimiento de movilidad.

La macro asistencia que incluye conectividad dual puede proporcionar diversos beneficios:

- Soporte mejorado para la movilidad - manteniendo el punto de anclaje de movilidad en la macro capa, como se ha descrito anteriormente, es posible mantener una movilidad sin discontinuidad entre las capas macro y de baja potencia, así como entre nodos de baja potencia.
- Transmisiones de baja sobrecarga desde la capa de baja potencia - transmitiendo solamente la información requerida para experiencia de usuario individual, es posible evitar una sobrecarga que proviene de soportar movilidad en modo inactivo dentro de la capa de área local, por ejemplo.
- Equilibrio de carga eficiente en energía - apagando los nodos de baja potencia cuando no hay transmisión de datos en curso, es posible reducir el consumo de energía de la capa de baja potencia.
- Optimización por enlace - seleccionando el punto de terminación para enlace ascendente y enlace descendente por separado, la selección del nodo se puede optimizar para cada enlace.

Uno de los problemas en el uso de conectividad dual es cómo correlacionar los Portadores de Radio de Datos (DRB) en 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 el eNB de anclaje y algunas de ellas en el eNB de asistencia. Como se trata con más detalle a continuación, este planteamiento puede producir algunos beneficios importantes de eficiencia del sistema. No obstante, este planteamiento crea problemas relacionados con el manejo de las claves de seguridad que se usan para confidencialidad y protección de integridad de los datos transmitidos hacia y desde el terminal móvil.

COMPENDIO

En los sistemas LTE, la capa de Control de Recursos de Radio (RRC) configura las entidades de Protocolo de Convergencia de Paquetes de Datos (PDCP) con claves criptográficas y datos de configuración, tales como datos que indican qué algoritmos de seguridad se deberían aplicar en conexión con el portador de radio correspondiente.

En un escenario de conectividad dual, la capa RRC se puede manejar exclusivamente por el nodo de anclaje, mientras que las entidades PDCP se pueden gestionar en cada uno de los nodos de estación base de anclaje y de asistencia. Dado que la estación base de anclaje y la estación base de asistencia se pueden implementar 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 se mantiene.

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

Las realizaciones de las técnicas descritas 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 está o está a punto de ser conectado dualmente a la estación base de anclaje y a 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 en el cifrado del tráfico de datos enviado al terminal inalámbrico o en la generación de una o más claves de seguridad de asistencia adicionales para cifrar tráfico de datos enviado al terminal inalámbrico por la estación base de asistencia, mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia. La clave de estación base de anclaje, o una clave derivada a partir de la clave de estación base de anclaje, se usa para cifrar los datos enviados al terminal inalámbrico por la estación base de anclaje mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia.

También se describe en la presente memoria otro método para generar una clave de seguridad de asistencia para una estación base de asistencia. Como el método resumido anteriormente, este método también es adecuado para su implementación en un nodo de red, para 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 está o está a punto de ser conectado dualmente a la estación base de anclaje y a la estación base de asistencia. En este método, no obstante, el método se puede llevar a cabo en un nodo de red distinto de la estación base de anclaje, usando una clave primaria que puede ser desconocida por la estación base de anclaje.

Según este segundo método de ejemplo, una clave de seguridad primaria se comparte entre el nodo de red y el terminal inalámbrico. Esta clave puede ser desconocida por la estación base de anclaje, en algunas realizaciones. El método continúa con la generación de una clave de seguridad de asistente 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 en el cifrado del tráfico de datos enviado al terminal inalámbrico o 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 mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a 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 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 a la estación base de asistencia indirectamente, a través de la estación base de anclaje.

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

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es un diagrama esquemático que ilustra un ejemplo de un despliegue heterogéneo de conectividad dual con flujos de anclaje y de asistencia simultáneos para un terminal móvil.
La Figura 2 ilustra componentes de la arquitectura del sistema E-UTRAN.
La Figura 3 ilustra detalles de la arquitectura de protocolo de estación base en un escenario de conectividad dual.
La Figura 4 ilustra una jerarquía de derivación de claves basada en una clave de estación base de anclaje.
La Figura 5 ilustra una jerarquía de derivación de claves basada en una clave MME.
La Figura 6 es un diagrama de flujo de proceso que ilustra un método de ejemplo como se implementa por un nodo de red de ejemplo.
La Figura 7 es un diagrama de flujo de proceso que ilustra un método de ejemplo como se implementa por un terminal inalámbrico.

La Figura 8 y la Figura 9 ilustran cada una un diagrama de flujo de proceso correspondiente a realizaciones de ejemplo de las técnicas descritas actualmente.
La Figura 10 es un diagrama de bloques que ilustra un aparato de estación base de anclaje de ejemplo, según las técnicas descritas actualmente.
La Figura 11 es un diagrama de bloques que ilustra otro aparato de nodo de red de ejemplo, según las técnicas descritas actualmente.
La Figura 12 ilustra componentes de un terminal inalámbrico de ejemplo configurado según algunas de las realizaciones descritas actualmente.

DESCRIPCIÓN DETALLADA

Los conceptos inventivos se describirán ahora más plenamente en lo sucesivo con referencia a los dibujos que se acompañan, en los que se muestran ejemplos de realizaciones de los conceptos inventivos. Estos conceptos inventivos, no obstante, se pueden incorporar de muchas formas diferentes y no se deberían interpretar como limitados a las realizaciones expuestas en la presente memoria. Más bien, estas realizaciones se proporcionan de modo que esta descripción sea minuciosa y completa, y transmita plenamente el alcance de los presentes conceptos inventivos a los expertos en la técnica. También se debería observar que estas realizaciones no son mutuamente exclusivas. Se puede suponer tácitamente que los componentes de una realización estén presentes o se usen en otra realización.

Con propósitos de ilustración y explicación solamente, estas y otras realizaciones de los presentes conceptos inventivos se describen en la presente memoria en el contexto de operación en una Red de Acceso por Radio (RAN) que se comunica sobre canales de comunicación de radio con terminales móviles (a los que también se hace referencia como terminales inalámbricos o UE). Como se usa en la presente memoria, un terminal móvil, terminal inalámbrico o UE puede incluir cualquier dispositivo que reciba datos de una red de comunicación, y puede incluir, pero no se limita a, un teléfono móvil (teléfono “celular”), ordenador portátil/portable, ordenador de bolsillo, ordenador de mano, ordenador de sobremesa, un dispositivo tipo máquina a máquina (M2M) o MTC, un sensor con una interfaz de comunicación inalámbrico, etc.

El Sistema Universal de Telecomunicaciones Móviles (UMTS) es un sistema de comunicación móvil de tercera generación, que evolucionó a partir del Sistema Global para Comunicaciones Móviles (GSM), y está destinado a proporcionar servicios de comunicaciones móviles mejorados basados en la tecnología de Acceso Múltiple por División de Código de Banda Ancha (WCDMA), UTRAN, abreviatura de Red de Acceso por Radio Terrestre UMTS, es un término colectivo para los Nodos B y los Controladores de Red de Radio que componen la red de acceso por radio UMTS. De este modo, UTRAN es esencialmente una red de acceso por radio que usa acceso múltiple por división de código de banda ancha (WCDMA) para los UE.

El Proyecto de Cooperación de Tercera Generación (3GPP) se ha encargado de evolucionar aún más las tecnologías de red de acceso por radio basadas en UTRAN y GSM. A este respecto, las especificaciones para Red de Acceso por Radio Terrestre Universal Evolucionada (E-UTRAN) están en curso dentro del 3GPP. La Red de Acceso por Radio Terrestre Universal Evolucionada (E-UTRAN) comprende la Evolución a Largo Plazo (LTE) y la Evolución de Arquitectura de Sistema (SAE).

Obsérvese que aunque la terminología de LTE se usa generalmente en esta descripción para ejemplificar realizaciones de los conceptos inventivos, esto no se debería ver como limitante del alcance de los conceptos inventivos a solamente estos sistemas. Otros sistemas inalámbricos, incluyendo variaciones y sucesores de los sistemas LTE del 3GPP y WCDMA, WiMAX (Interoperabilidad Mundial para Acceso por Microondas), UMB (Banda Ancha Ultra Móvil), HSDPA (Acceso de Paquetes de Enlace Descendente de Alta Velocidad), GSM (Sistema Global para Comunicaciones Móviles), etc., también pueden beneficiarse de la explotación de las realizaciones de los presentes conceptos inventivos descritos en la presente memoria.

Obsérvese también que terminología tal como estación base (a la que también se hace referencia como NodoB, eNodoB, o Nodo B Evolucionado) y terminal inalámbrico o terminal móvil (al que también se hace referencia como nodo de Equipo de Usuario o UE) se debería considerar no limitante 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”) se pueden considerar como ejemplos de diferentes dispositivos de comunicaciones respectivos que se comunican unos con otros sobre un canal de radio inalámbrico.

Mientras que las realizaciones tratadas en la presente memoria pueden centrarse en realizaciones de ejemplo en las cuales se aplican las soluciones descritas en redes heterogéneas que incluyen una mezcla de estaciones base de potencia relativamente mayor (por ejemplo, “macro” estaciones base, a las que también se hace referencia como estaciones base de área amplia o nodos de red de área amplia) y nodos de potencia relativamente menor (por ejemplo, “pico” estaciones base, a las que también se puede hacer referencia como estaciones base de área local o nodos de red de área local), las técnicas descritas se pueden aplicar en cualquier tipo de red adecuada, incluyendo configuraciones tanto homogéneas como heterogéneas. De este modo, las estaciones base implicadas en las configuraciones descritas pueden ser similares o idénticas unas a otras, o pueden diferir en términos de potencia de

transmisión, número de antenas transmisor-receptor, potencia de procesamiento, características de receptor y transmisor, y/o cualquier otra capacidad funcional o física.

La Red de Acceso por Radio Terrestre UMTS Evolucionada (E-UTRAN) incluye estaciones base llamadas NodosB mejorados (eNB o eNodosB), que proporcionan el plano de usuario E-UTRA y las terminaciones de protocolo de plano de control hacia el UE. Los eNB se interconectan unos con otros usando la interfaz X2. Los eNB también se conectan usando la interfaz S1 al EPC (Núcleo de Paquetes Evolucionado), más específicamente a la MME (Entidad de Gestión de Movilidad) por medio de la interfaz S1-MME y a la Pasarela de Servicio (S-GW) por medio de la interfaz S1-U. La interfaz S1 soporta relaciones de muchos a muchos entre las MME/S-GW y los eNB. Se ilustra una vista simplificada de la arquitectura E-UTRAN en la Figura 2.

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 la pasarela de servicio y/o encaminamiento 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 central). Las funciones significativas de la MME 220 están relacionadas con gestión de conexión y gestión de portadores, que se manejan a través de los protocolos de Estrato Sin 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 de DL (enlace descendente) temporal mientras que el UE está siendo buscado, encaminamiento de paquetes y reenvío al eNB correcto, y/o recopilación de información para tarificación e interceptación legal. La Pasarela PDN (P-GW, no mostrada en la Figura 2) es el nodo responsable de la asignación de direcciones IP de UE, así como de la aplicación de Calidad de Servicio (QoS) (como se trata además a continuación). Se hace referencia al lector a la especificación TS 36.300 del 3GPP y a las referencias dentro la misma para obtener detalles adicionales de las funcionalidades de los diferentes nodos.

En la descripción de diversas realizaciones de las técnicas descritas actualmente, el término no limitante nodo de red de radio se puede usar para hacer referencia a cualquier tipo de nodo de red que sirve al UE y/o está conectado a otro nodo de red o elemento de red o cualquier nodo de radio desde donde el UE recibe una señal. Ejemplos de nodos de red de radio son los Nodos B, las estaciones base (BS), los nodos de radio de radio multiestándar (MSR) tales como las BS de MSR, los eNodosB, los controladores de red, los controladores de red de radio (RNC), los controladores de estación base, los retransmisores, los nodos de donantes que controlan los retransmisores, las estaciones base transceptoras (BTS), los puntos de acceso (AP), los encaminadores inalámbricos, los puntos de transmisión, los nodos de transmisión, las unidades de radio remotas (RRU), las cabeceras de radio remotos (RRH), los nodos en un sistema de antenas distribuidas (DAS), etc.

En algunos casos, se usa un término más general “nodo de red”; este término puede corresponder a cualquier tipo de nodo de red de radio o cualquier nodo de red que se comunique con al menos un nodo de red de radio. Ejemplos de nodos de red son cualquier nodo de red de radio indicado anteriormente, nodos de red central (por ejemplo, MSC, MME, etc.), O y M, OSS, SON, nodos de posicionamiento (por ejemplo, E-SMLC), MDT, etc.

En la descripción de algunas realizaciones, se usa el término equipo de usuario (UE), y se refiere a cualquier tipo de dispositivo inalámbrico que se comunica con un nodo de red de radio en un sistema de comunicación móvil o celular. Ejemplos de UE son dispositivos de destino, UE de dispositivo a dispositivo, UE de tipo máquina o UE capaces de comunicación máquina a máquina, PDA, ordenadores de mesa habilitados inalámbricamente, terminales móviles, teléfonos inteligentes, ordenadores portátiles equipados integrados (LEE), equipos montados en ordenadores portátiles (LME), mochilas USB, equipos en las instalaciones del cliente (CPE), etc. El término “terminal móvil” como se usa en la presente memoria se debería entender como que es intercambiable de manera general con el término UE como se usa en la presente memoria y en las diversas especificaciones promulgadas por el 3GPP, pero no se debería entender como que está limitado a dispositivos compatibles con los estándares del 3GPP.

Las realizaciones de ejemplo presentadas en la presente memoria se dirigen específicamente hacia la generación de claves cuando la pila de protocolo Uu de LTE se divide entre una macro celda y una celda de eNB de asistencia. Las técnicas y el aparato son aplicables de manera más general a generación de claves en otros escenarios de conectividad dual.

Como se ha señalado anteriormente, una opción para dividir Portadores de Radio de Datos (DRB) entre dos estaciones base en un escenario de conectividad dual es mantener el plano de control, que se gestiona 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 Paquetes de Datos (PDCP), que están asociadas con portadores de radio individuales, de modo que una o más se terminan en el eNB de anclaje y una o más en el eNB de asistencia.

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

Más particularmente, RRC configura las entidades PDCP con claves criptográficas y datos de configuración, tales como datos que indican qué algoritmos de seguridad se deberían aplicar en conexión con el portador de radio correspondiente. Para conexiones asociadas con un terminal móvil dado, RRC configura todas las entidades PDCP

para el tráfico de plano de usuario (DRB) con una y la misma clave de cifrado, KUP-enc, y todas las entidades PDCP para el tráfico del 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 usados para proteger datos entre un eNB donante y un nodo de retransmisión, 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 PDCP a través de interfaces de programa de aplicación (API) internas ya no se mantiene. Es decir, ya no se sostiene la situación actual donde se puede suponer que los datos de configuración de seguridad se guarden de manera segura dentro del entorno físicamente seguro del eNB. 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.

Se usan aquí el eNB de anclaje y el eNB de asistencia para definir diferentes papeles de los eNB desde una perspectiva de UE o de terminal inalámbrico. Se reconoce que esto es sólo una denominación de ejemplo y que también se podrían llamar algo más, como anclaje y amplificador, maestro y esclavo, o simplemente eNB_1 y eNB_2.

El diseño de seguridad de LTE proporciona generalmente compartimentación de las funciones de seguridad. Esta compartimentación se destina a asegurar que si un atacante rompe la seguridad de una función, solamente se compromete esa función. Por ejemplo, hay una clave usada para el cifrado del protocolo RRC y otra clave usada para protección de integridad del protocolo RRC. Si un atacante rompe la clave de cifrado, puede descifrar y leer todos los mensajes RRC. No obstante, dado que la clave de integridad es diferente de la clave de cifrado, el atacante no puede modificar o inyectar mensajes RRC.

Otro aspecto del planteamiento de compartimentación usado en LTE es que cada eNB usa un conjunto de claves separadas. La razón de esto es que este planteamiento asegura que un atacante que irrumpa en un eNB no obtenga ninguna información acerca de datos transmitidos entre un terminal inalámbrico y otro eNB físicamente diferente. En un escenario de conectividad dual, entonces, para mantener la propiedad de que irrumpir en un nodo RAN físico, es decir, un eNB, no ayuda en el ataque a otro nodo RAN, el eNB de asistencia debería usar su propio conjunto de claves, separado del conjunto de claves usado en el eNB de anclaje.

Una arquitectura de conectividad dual puede abrir tres nuevos caminos para ataques de seguridad potenciales, dependiendo de las técnicas adoptadas para manejar claves y parámetros de seguridad. En primer lugar, el transporte de la configuración de seguridad y las claves criptográficas desde el eNB de anclaje al eNB de asistencia proporciona un punto en el que un atacante puede espiar o puede modificar las claves y los datos de configuración. En segundo lugar, un atacante puede irrumpir físicamente en un eNB de asistencia, y espiar o modificar las claves y los datos de configuración allí. Además, un atacante que irrumpe 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 de plano de usuario cuando el eNB de asistencia los envía y los recibe. Esto es cierto independientemente de si los datos de 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 salen a Internet localmente en el eNB de asistencia.

Las realizaciones de ejemplo descritas en la presente memoria están dirigidas hacia la generación segura de un conjunto de claves de cifrado a ser usadas para la comunicación entre un terminal inalámbrico en conectividad dual y un eNB de asistencia. En algunas realizaciones, una clave base para el eNB de asistencia se genera a partir de la clave de seguridad del eNB de anclaje. La clave base se puede usar 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, el conjunto de claves en un eNB comprende la K_{eNB}, y K_{UP-enc}, $K_{RRC-enc}$ y $K_{RRC-int}$. Dependiendo de qué funciones proporciona el eNB de asistencia, el conjunto de claves necesitado por el eNB de asistencia diferirá. Dado que el eNB de asistencia terminará al menos el cifrado de plano de usuario, es útil para establecer una clave de cifrado que el eNB de asistencia comparte con el terminal inalámbrico. Si el eNB de asistencia proporcionase servicios para nodos de retransmisión, también hay una necesidad de una clave de integridad para proteger los DRB que transportan el tráfico de plano de control del nodo de retransmisión. Por lo tanto, es útil establecer una clave base para el eNB de asistencia, similar a la K_{eNB}, a partir de la cual se pueden derivar otras claves. De ahora en adelante, la discusión será acerca del establecimiento de una clave base, llamada $K_{assisting\_eNB}$, pero el mismo razonamiento se puede aplicar obviamente al caso donde, por ejemplo, solamente se establece una clave de cifrado.

La Figura 4 muestra cómo se puede generar $K_{assisting\_eNB}$ basada en el 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 $K_{assisting\_eNB}$, $K_{assisting\_eNB-enc}$ y $K_{assisting\_eNB-int}$, todas las cuales se derivan directa o indirectamente de la K_{eNB} para el eNB de anclaje.

Las flechas en la Figura 4 indican aplicaciones de Funciones de Derivación de Claves (KDF). Una KDF se puede considerar, a todos los efectos prácticos, una función unidireccional. Como es bien sabido por los familiarizados con las técnicas criptográficas, las funciones unidireccionales son fáciles de calcular en la dirección hacia adelante (la dirección de la flecha), pero imposibles de invertir computacionalmente. La implicación de esto es que el acceso a una clave inferior en la jerarquía de claves no da ninguna información útil sobre una clave más alta en la jerarquía. Un ejemplo de una KDF es la función HMAC-SHA256, que es la KDF usada en LTE y en muchos otros sistemas del 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 al cifrado y a las claves de integridad que deriva. No obstante, no tendrá acceso a la K_{eNB}.

Debido a que se supone que las KDF son conocidas, el nodo de eNB de anclaje, por otra parte, tendrá acceso a todas las claves usadas por el eNB de asistencia. Esto rompe el principio de compartimentación si se interpreta en su sentido más estricto. No obstante, el nivel de seguridad en este escenario es similar al obtenido en un traspaso X2, que es un traspaso en LTE que se maneja sin implicación de la Entidad de Gestión de la Movilidad (MME). En un traspaso X2, el eNB de origen calcula una nueva clave basada en la K_{eNB} usada actualmente y proporciona la nueva clave al eNB de destino. Otro ejemplo de una situación similar surge en el contexto de nodos de retransmisión. En el caso de nodos de retransmisión, el eNB Donante actúa como un intermediario S1 para el nodo de retransmisión. Como resultado, el eNB Donante tiene acceso a todas las claves usadas por el nodo de retransmisión. Debido a que la situación de seguridad es similar a varias que ya surgen en redes LTE, usar la K_{eNB} como material de codificación base para la $K_{assisting\_eNB}$ se puede considerar aceptable desde un punto de vista de seguridad.

La jerarquía de claves mostrada en la Figura 4 se puede emplear ventajosamente en un escenario de conectividad dual en el que el eNB de anclaje controla las entidades PDCP en el eNB de asistencia, es decir, el eNB de anclaje puede establecer nuevas entidades PDCP, eliminarlas y reiniciar las entidades PDCP eliminadas previamente. El eNB de anclaje y el terminal móvil (por ejemplo, UE de LTE) derivarán cada uno la $K_{assisting\_eNB}$ a partir de la K_{eNB} como esta: $K_{assisting\_eNB}$ = KDF (KeNB, other_params).

Para evitar la posibilidad de ataques bien conocidos que explotan la transmisión repetida de datos cifrados que transportan datos subyacentes conocidos, se debería asegurar que la $K_{assisting\_eNB}$ está “fresca” cada vez que una entidad PDCP reutilice los mismos valores COUNT. De este modo, la derivación de $K_{assisting\_eNB}$ debería comprender preferiblemente los parámetros de refresco adecuados. Una forma de lograr el refresco es usar los números de secuencia PDCP COUNT que están asociados con algún mensaje RRC predeterminado, tal como el último Comando de Modo de Seguridad RRC o el Comando de Traspaso, o uno de los mensaje de Solicitud de Reconfiguración RRC o Reconfiguración RRC Completa que se usaron para establecer las entidades PDCP en el eNB de asistencia. Los números de secuencia asociados con otros mensajes RRC se pueden usar en su lugar, por supuesto. Otras opciones para incorporar refresco en la generación de $K_{assisting\_eNB}$ incluyen el envío de un “valor de uso único” fresco desde el terminal inalámbrico al eNB de anclaje o al eNB de asistencia, desde el eNB de anclaje o el eNB de asistencia hasta el terminal inalámbrico (o ambas direcciones) en algún mensaje o mensajes RRC predeterminados u otros mensajes de protocolo. Un valor de uso único es un número generado (pseudo) aleatoriamente que, con una probabilidad suficientemente alta, será único con respecto al K_{eNB}.

Cualquiera que sean los parámetros de refresco, entonces 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. Se puede usar cualquier información siempre que proporcione una entrada (estadísticamente) única con una probabilidad suficientemente alta.

Otro diseño posible es que el eNB de anclaje deriva la $K_{assisting\_eNB}$ a partir de la K_{eNB} sin ningún parámetro de refresco. Según este planteamiento alternativo, si el eNB de asistencia o el eNB de anclaje detecta que un PDCP COUNT en el eNB de asistencia está a punto de envolverse, el eNB de anclaje inicia una actualización de la clave K_{eNB} a través de un traspaso dentro de la celda. Un resultado del traspaso dentro de la celda es que el terminal inalámbrico y el eNB de anclaje no solamente refrescan la K_{eNB}, sino también la $K_{assisting\_eNB}$; la $K_{assisting\_eNB}$ se podría volver a calcular de la misma manera que se derivó la primera vez. Este planteamiento puede requerir que el eNB de asistencia tenga que informar al eNB de anclaje sobre los PDCP COUNT que están a punto de ser reutilizados.

Transportar la $K_{assisting\_eNB}$ desde el eNB de anclaje al eNB de asistencia se puede hacer sobre el canal de control entre los dos. El canal de control ha de ser protegido por confidencialidad e integridad como ya se ha indicado.

Parámetros distintos de los mencionados explícitamente también se pueden introducir en la KDF, en diversas realizaciones de las técnicas descritas anteriormente. Los parámetros se pueden poner en cualquiera de varios órdenes diferentes. Además, uno cualquiera o más de los parámetros para la KDF se pueden transformar antes de ser introducidos a la KDF. Por ejemplo, un conjunto de parámetros P1, P2, ..., Pn, para algunos números enteros no

negativos n, se podría transformar siendo primero ejecutado a través de una función de transformación f y el resultado de eso, es decir, f(P1, P2, ..., Pn), siendo introducido a la KDF.

En un ejemplo de la derivación de claves, el parámetro P1 se transforma primero antes de entrar en la KDF para calcular una clave llamada “output_key”: 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, podría ser 0, 1 o más otros parámetros, por ejemplo, usados para enlazar la clave a un cierto contexto. Los parámetros se pueden introducir como parámetros separados o se pueden concatenar juntos y luego introducir en una única entrada a la KDF. Incluso cuando se usan variantes de la KDF tales como éstas, el núcleo de la idea sigue siendo el mismo.

Independientemente de qué planteamiento de establecimiento de claves se use, los procedimientos de traspaso existentes generalmente no se ven afectados cuando se traspasa el terminal móvil con conectividad dual a otra estación base, independientemente del tipo la de estación base de destino. El eNB de anclaje puede echar abajo los DRB en el eNB de asistencia y realizar el traspaso a la estación base de destino según las especificaciones existentes.

Cuando se traspasa 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 claves basada en K_{ASME}

En lugar de usar la clave base del nodo de anclaje como la base para generar $K_{assisting\_eNB}$, se puede usar en su lugar una clave asociada con otro nodo en la red inalámbrica y conocida por el terminal móvil. Por ejemplo, usar la K_{ASME} como base material de codificación para la $K_{assisting\_eNB}$, como se muestra en la Figura 5, permite un nivel de seguridad más alto, en comparación con el uso de la K_{eNB} descrita anteriormente. Como se ve en la Figura 5, la $K_{assisting\_eNB}$ se puede derivar de la K_{ASME}, y las claves de cifrado e integridad para el eNB de asistencia derivadas a partir 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 la MME y el terminal inalámbrico. Si la $K_{assisting\_eNB}$ se deriva a partir de la K_{ASME} y la MME dota al eNB de asistencia con esta $K_{assisting\_eNB}$ directamente, entonces el nodo de anclaje no tiene acceso a la $K_{assisting\_eNB}$ ni a las claves de cifrado e integridad derivadas a partir de ella. En este caso, entonces, el principio de compartimentación tratado anteriormente se adhiere en un sentido más estricto.

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

El uso de la K_{ASME} como la base material de claves significa que $K_{assisting\_eNB}$ se deriva a partir de la K_{ASME} usando una función de derivación de claves $K_{assisting\_eNB}$ = KDF (K_{ASME}, [other_params]), donde los other_params opcionales pueden Incluir uno o más parámetros de refresco.

Como se ha descrito anteriormente, cuando se reinician los contadores de paquetes PDCP (PDCP COUNT), se deberían renovar las claves de cifrado e integridad. Si se usa la misma clave con los mismos PDCP COUNT, habrá una reutilización de la secuencia de claves y, potencialmente, posibles ataques de repetición. Por lo tanto, la MME y el terminal inalámbrico podrían incluir un parámetro de refresco en la derivación de claves. Por ejemplo, el mismo parámetro de refresco como el que se usa cuando se deriva la K_{eNB} para el nodo de anclaje (el eNB). Qué parámetro de refresco se usa para la derivación de la K_{eNB} puede depender de la situación. Posibles parámetros de refresco incluyen valores usados una sola vez (números aleatorios usados una vez) que intercambian la MME y el terminal inalámbrico. Otras posibilidades son los contadores de paquetes tales como el COUNT de enlace ascendente o de enlace descendente del NAS, o un contador recién introducido que se transmite o bien desde el terminal inalámbrico a la MME o bien desde la MME al terminal inalámbrico. Un inconveniente con un contador recién introducido es que si se sale de sincronización, ha de ser vuelto a sincronizar mediante algún nuevo mecanismo de vuelta a sincronizar.

También se pueden incluir otros parámetros en la derivación de $K_{assisting\_eNB}$. Por ejemplo, se pueden usar como entrada la identidad del eNB de asistencia o la celda que usan el eNB de asistencia. Esto es similar a cómo la K_{eNB} está unida a la identidad de la celda. El propósito podría ser compartimentar aún más posibles violaciones de seguridad.

Una vez que la MME ha derivado la $K_{assisting\_eNB}$, la MME también tiene que transferirla al eNB de asistencia. La transferencia de la $K_{assisting\_eNB}$ al eNB de asistencia puede proceder de una de dos formas, o bien directamente al

eNB de asistencia, o bien indirectamente, transfiriendo primero la $K_{assisting\_eNB}$ al eNB y luego permitiendo que el eNB la transfiera al eNB de asistencia cuando sea necesario.

En general, es una ventaja de seguridad transferir la $K_{assisting\_eNB}$ directamente desde la MME al eNB de asistencia. De esta forma, solamente la 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 de manera que está implicada la MME, entonces esto es preferible.

La otra alternativa es para que la MME envíe la $K_{assisting\_eNB}$ al eNB, que simplemente reenvía la $K_{assisting\_eNB}$ al eNB de asistencia. Este planteamiento tiene un inconveniente de seguridad en que el eNB ahora también es consciente de la $K_{assisting\_eNB}$. El planteamiento puede ser útil, no obstante, si no hay un camino de señalización directo entre la MME y el eNB de asistencia y la K_{ASME} es el material de codificación usado como base para la derivación de la $K_{assisting\_eNB}$.

Métodos de ejemplo

En 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 una MME, en diversas realizaciones. Los diagramas de flujo del proceso ilustrados incluyen algunas operaciones que se ilustran con un borde sólido 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 realizaciones de ejemplo más amplias. Las operaciones que están comprendidas en un borde discontinuo son realizaciones de ejemplo que pueden estar comprendidas en, o una parte de, o son operaciones adicionales que se pueden tomar además de las operaciones de las realizaciones de ejemplo de borde. De este modo, las operaciones mostradas en contornos discontinuos se pueden considerar “opcionales” en el sentido de que pueden no aparecer en todas las instancias o en todas las realizaciones del proceso ilustrado. También se debería apreciar que las operaciones de las Figuras 6 y 7 se proporcionan meramente como 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 se puede implementar en un nodo de red, tal como en una estación base de anclaje (por ejemplo, un eNB de anclaje LTE) o en algún otro nodo de red, tal como una MME. Como se muestra en el bloque 10, el nodo de la red primero determina la necesidad de que una clave de seguridad de asistencia sea generada. Esto se puede desencadenar mediante 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 en detalle anteriormente, esta clave de seguridad primaria puede ser, en diversas realizaciones, una clave base de nodo de anclaje (por ejemplo, K_{eNB}) u otra clave que es conocida por el nodo de red y por 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 refresco, como se muestra en los bloques 12 y 16. Una lista de parámetros de refresco que ya se han usado se puede mantener 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 usa entonces para generar una o más claves adicionales para proteger datos transferidos a y desde el terminal móvil, aunque la clave de seguridad de asistencia se podría usar directamente para tales propósitos en algunas realizaciones.

La Figura 7 ilustra un método correspondiente tal como se podría llevar 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 usada por el nodo de red en la Figura 6. Una vez más, esta clave de seguridad primaria puede ser, en diversas realizaciones, una clave base de nodo de anclaje (por ejemplo, K_{eNB}) u otra clave que es conocida por el nodo de red y por 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 refresco, como se muestra en los bloques 32 y 34. Una lista de parámetros de refresco que ya se han usado se puede mantener 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 a y desde la estación base de asistencia. En algunos casos, como se ha detallado anteriormente, la clave de seguridad de asistencia se usa para generar una o más claves adicionales para proteger los datos transferidos a y desde el terminal móvil, aunque la clave de seguridad de asistencia se podría usar directamente para tales propósitos en algunas realizaciones.

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

La Figura 8 ilustra de este modo un método, adecuado para su 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 donde el terminal inalámbrico está o está a punto de ser conectado dualmente a la estación base de anclaje y a la estación base de asistencia. Como se muestra en el bloque 810, el método ilustrado incluye la generación de 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 en el cifrado del tráfico de datos enviado al terminal inalámbrico o 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 mientras el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia. Como se muestra en el bloque 830, la clave de estación base de anclaje, o una clave derivada a partir de la clave de estación base de anclaje, se usa para cifrar los datos enviados al terminal inalámbrico por la estación base de anclaje mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base 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 uno una clave de cifrado, o una clave de integridad, o ambas, a partir de la clave de estación base de anclaje, y usar 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 dualmente a la estación base de anclaje y a 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 a partir de la clave de estación base de anclaje usando una función unidireccional. La función unidireccional puede ser una función criptográfica HMAC-SHA-256, en algunas realizaciones. En algunas de éstas y en algunas otras realizaciones, la generación de la clave de seguridad de asistencia se basa además en un parámetro de refresco.

En algunas realizaciones, el método ilustrado puede incluir además detectar que un parámetro COUNT del Protocolo de Convergencia de Paquetes de Datos (PDCP) en la estación base de asistencia está a punto de envolverse y, en respuesta, iniciar un refresco de la clave de estación base de anclaje y volver a calcular la clave de seguridad de asistencia.

En algunas realizaciones, se usa una única clave de seguridad de asistencia para generar un conjunto de claves para su uso en todos los Portadores de Radio de Datos. En otras realizaciones, se pueden usar múltiples claves de seguridad de asistencia, en cuyo caso se repite la operación de generación descrita anteriormente para cada uno de una pluralidad de Portadores de Radio de Datos establecida entre el terminal inalámbrico y la estación base de asistencia, de manera que las claves de seguridad de asistencia resultantes difieren para cada Portador de Radio de Datos. Se pueden enviar al mismo tiempo múltiples de las diversas claves resultantes, 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. Como el método mostrado en la Figura 8, el proceso de la Figura 9 es adecuado para su implementación en un nodo de red, para 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 está o está a punto de ser conectado dualmente a la estación base de anclaje y a la estación base de asistencia. En este método, no obstante, el método se puede llevar a cabo en un nodo de red distinto de la estación base de anclaje, usando una clave primaria que puede ser desconocida por 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 por la estación base de anclaje, en algunas realizaciones. Un ejemplo es la clave K_{ASME} tratada anteriormente, que se comparte entre la MME de LTE y el terminal móvil.

Como se muestra en el bloque 920, el método continúa con la generación de una clave de seguridad 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, como se muestra en el bloque 930, para su uso por la estación base de asistencia en el cifrado del tráfico de datos enviado al terminal inalámbrico o 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 mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a 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 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 a la estación base de asistencia indirectamente, 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 éstas y en algunas otras realizaciones, la generación de la clave de seguridad de asistencia comprende derivar la clave de seguridad de asistencia a partir de la clave de estación base de anclaje usando una función unidireccional. La función unidireccional puede ser una función criptográfica HMAC-SHA-256, por ejemplo. Como se ha tratado en detalle anteriormente, la generación de la clave de seguridad de asistencia se puede basar además en un parámetro de refresco, en algunas realizaciones.

Ejemplo de implementaciones de hardware

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

La Figura 10 ilustra una configuración de nodo de ejemplo de una estación base de anclaje 401A que puede realizar algunas de las realizaciones de ejemplo descritas en la presente memoria. La estación base de anclaje 401A puede comprender circuitería de radio o un puerto de comunicación 410A que se puede configurar para recibir y/o transmitir mediciones de comunicación, datos, instrucciones y/o mensajes. La estación base de anclaje 401A puede comprender además un circuito de interfaz de red 440A que se puede configurar para recibir o enviar comunicaciones de red, por ejemplo, a y desde otros nodos de red. Se debería apreciar que la circuitería de radio o el puerto de comunicación 410A puede estar comprendido como cualquier número de unidades o circuitería de transmisión/recepción, recepción y/o transmisión. Además, se debería apreciar que la circuitería de radio o la comunicación 410A pueden ser en forma de cualquier puerto de comunicaciones de entrada o salida conocido en la técnica. La circuitería de radio o la comunicación 410A y/o la interfaz de red 440A pueden comprender circuitería de RF y circuitería de procesamiento en banda base, los detalles de las cuales son bien conocidos por los familiarizados con el diseño de estaciones base.

La estación base de anclaje 401A también puede comprender una unidad o circuitería de procesamiento 420A que se puede configurar 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 la presente memoria. La circuitería de procesamiento 420A puede ser cualquier tipo adecuado de unidad de cálculo, por ejemplo, un microprocesador, procesador digital de señal (DSP), agrupación de puertas programables en campo (FPGA), o circuito integrado de aplicaciones específicas (ASIC), o cualquier otra forma de circuitería. La estación base de anclaje 401A puede comprender además una unidad o circuitería de memoria 430A que puede ser cualquier tipo adecuado de memoria legible por ordenador y puede ser de tipo volátil y/o no volátil. La memoria 430A se puede configurar para almacenar información recibida, transmitida y/o cualquiera relacionada con la generación de claves de seguridad o parámetros de refresco, parámetros de dispositivo, prioridades de comunicación, y/o instrucciones de programa ejecutables.

Las funciones típicas de la circuitería de procesamiento 420A, 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 diversas realizaciones de la presente invención, se adapta el circuito de procesamiento 420A, usando un código de programa adecuado almacenado en la memoria de almacenamiento de programa 430A, 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 único microprocesador o incluso en un único módulo.

Se apreciará que el circuito de procesamiento 420A, que se adapta con el código de programa almacenado en la memoria de programa y de datos 430A, puede implementar el flujo de proceso de la Figura 8 (o una variante del mismo) usando una disposición de “módulos” funcionales, donde los módulos son programas de ordenador o partes de programas de ordenador que se ejecutan en el circuito de procesador 420A. De este modo, el aparato 401A se puede entender como que comprende una interfaz de comunicaciones 440A configurada para comunicarse con la estación base de asistencia, y que comprende además diversos módulos funcionales implementados en la circuitería de procesamiento 420A. Estos módulos funcionales incluyen: un módulo de generación 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, usando la circuitería de interfaz, la clave de seguridad de asistencia generada, para su uso por la estación de base de asistencia en el cifrado del tráfico de datos enviado al terminal inalámbrico o 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 mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia; y un módulo de cifrado para usar la clave de estación base de anclaje, o una clave derivada de la clave de estación base de anclaje, para cifrar los datos enviados al terminal inalámbrico por la estación base de anclaje mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia.

La Figura 11 ilustra una configuración de nodo de ejemplo de un nodo de gestión de movilidad 505A (por ejemplo, una MME, un SGSN, un S4-SGSN) que puede realizar algunas de las realizaciones descritas en la presente memoria. El nodo de gestión de movilidad 505A puede comprender circuitería de interfaz o un puerto de comunicación 510A que se puede configurar para recibir y/o transmitir mediciones de comunicación, datos, instrucciones y/o mensajes. Se debería apreciar que la circuitería de radio o el puerto de comunicación 510A puede estar comprendido como cualquier número de unidades o circuitería de transmisión/recepción, recepción y/o transmisión. Se debería apreciar además que la circuitería de radio o la comunicación 510A puede ser en forma de cualquier puerto de comunicaciones de entrada o salida conocido en la técnica. La circuitería de interfaz o la comunicación 510A puede comprender circuitería de RF y circuitería de procesamiento en banda base (no mostradas).

El nodo de gestión de movilidad 505A también puede comprender una unidad o circuitería de procesamiento 520A que se puede configurar 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 la presente memoria. La circuitería de procesamiento 520A puede ser cualquier tipo adecuado de unidad de cálculo, por ejemplo, un microprocesador, procesador digital de señal (DSP), agrupación de puertas programables en campo (FPGA), o circuito integrado de aplicaciones específicas (ASIC), o cualquier otra forma de circuitería. El nodo de gestión de movilidad 505A puede comprender además una unidad o circuitería de memoria 530A que puede ser cualquier tipo adecuado de memoria legible por ordenador y puede ser de tipo volátil y/o no volátil. La memoria 530A se puede configurar para almacenar información recibida, transmitida y/o cualquiera relacionada con la generación de claves de seguridad o parámetros de refresco, parámetros de dispositivo, prioridades de comunicación y/o instrucciones de programa ejecutables para su uso por la circuitería de procesamiento 520A.

En diversas realizaciones de la presente invención, el circuito de procesamiento 520A se adapta, usando un código de programa adecuado almacenado en una memoria de almacenamiento de programas 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 único microprocesador o incluso en un único módulo.

Se apreciará que el circuito de procesamiento 520A, en la medida que se adapta con el código de programa almacenado en la memoria de programa y de datos 530A, puede implementar el flujo de proceso de la Figura 9 (o una variante del mismo) usando una disposición de “módulos” funcionales, donde los módulos son programas de ordenador o partes de programas de ordenador que se ejecutan en el circuito de procesador 520A. De esta manera, el aparato 501A se puede entender como que comprende una interfaz de comunicaciones 540A configurada para comunicarse con la estación base de asistencia, y que comprende además diversos módulos funcionales implementados en la circuitería de procesamiento 520A. Estos módulos funcionales incluyen: un módulo de compartición para compartir una clave de seguridad primaria con el terminal inalámbrico; un módulo de generación 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 en el cifrado del tráfico de datos enviado al terminal inalámbrico o 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 mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia. La Figura 12 ilustra una configuración de nodo de ejemplo de un terminal inalámbrico 505B que se puede configurar para llevar a cabo algunos de los métodos de ejemplo descritos en la presente memoria. El terminal inalámbrico 505B puede comprender circuitería de interfaz o un puerto de comunicación 510B que se puede configurar para recibir y/o transmitir mediciones de comunicación, datos, instrucciones y/o mensajes. Se debería apreciar que la circuitería de radio o el puerto de comunicación 510B puede estar comprendido como cualquier número de unidades o circuitería de transmisión/recepción, recepción, y/o transmisión. Además, se debería apreciar que la circuitería de radio o la comunicación 510B pueden ser en forma de cualquier puerto de comunicaciones de entrada o salida conocido en la técnica. La circuitería de interfaz o la comunicación 510B pueden comprender circuitería de RF y circuitería de procesamiento en banda base (no mostradas).

El terminal inalámbrico 505B también puede comprender una unidad o circuitería de procesamiento 520B que se puede configurar 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 la presente memoria. La circuitería de procesamiento 520B puede ser cualquier tipo adecuado de unidad de cálculo, por ejemplo, un microprocesador, procesador digital de señal (DSP), agrupación de puertas programables en campo (FPGA) o circuito integrado de aplicaciones específicas (ASIC), o cualquier otra forma de circuitería. El terminal inalámbrico 505B puede

comprender además una unidad o circuitería de memoria 530B que puede ser cualquier tipo adecuado de memoria legible por ordenador y puede ser de tipo volátil y/o no volátil. La memoria 530B se puede configurar para almacenar información recibida, transmitida y/o cualquiera relacionada con la generación de claves de seguridad o parámetros de refresco, parámetros de dispositivo, prioridades de comunicación. y/o instrucciones de programa ejecutables.

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

Se apreciará por las personas expertas en la técnica 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 compatible con los estándares LTE especificados por el 3GPP, se debería observar que las soluciones presentadas pueden ser igualmente bien aplicables a otras redes que soporten conectividad dual. Las realizaciones específicas descritas anteriormente, por lo tanto, se deberían considerar ejemplares más que limitantes del alcance de la invención. Debido a que no es posible, por supuesto, describir cada combinación concebible de componentes o técnicas, los expertos en la técnica apreciarán que la presente invención se puede implementar de otras formas distintas a las expuestas específicamente en la presente memoria, sin apartarse de las características esenciales de la invención. Las presentes realizaciones han de ser consideradas, de este modo, en todos los aspectos como ilustrativas y no restrictivas.

En la presente descripción de diversas realizaciones de los presentes conceptos inventivos, ha de ser entendido que la terminología usada en la presente memoria es con el propósito de describir realizaciones particulares solamente y no se pretende que sea limitante de los presentes conceptos inventivos. A menos que se defina de otro modo, todos los términos (incluyendo términos técnicos y científicos) usados en la presente memoria tienen el mismo significado que se entiende comúnmente por un experto en la técnica a la que pertenecen los presentes conceptos inventivos. Se entenderá además que términos, tales como los definidos en los diccionarios comúnmente usados, se deberían interpretar como que tienen un significado que es coherente con su significado en el contexto de esta especificación y la técnica relevante y no se interpretarán en un sentido idealizado o demasiado formal expresamente definido así en la presente memoria.

Cuando se hace referencia a un elemento como que está “conectado”, “acoplado”, es “sensible”, o variantes de los mismos a otro elemento, puede ser directamente conectado, acoplado o sensible al otro elemento o pueden estar presentes elementos de intervención. Por el contrario, cuando se hace referencia a un elemento como que está “conectado directamente”, “acoplado directamente”, es “sensible directamente”, o variantes de los mismos a otro elemento, no hay presentes elementos de intervención. Números similares se refieren a elementos similares en todo. Además, “acoplado”, “conectado”, “sensible”, o variantes de los mismos, como se usan en la presente memoria, pueden incluir acoplado, conectado o sensible inalámbricamente. Como se usa en la presente memoria, las formas singulares “un”, “uno”, “una”, “el” y “la” se pretende que incluyan las formas plurales también, a menos que el contexto lo indique claramente de otro modo. Funciones o construcciones bien conocidas pueden no ser descritas en detalle por 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 usar en la presente memoria para describir diversos elementos/operaciones, estos elementos/operaciones no deberían estar limitados por estos términos. Estos términos se usan solamente para distinguir un elemento/operación de otro elemento/operación. De este modo, un primer elemento/operación en algunas realizaciones se podría denominar un segundo elemento/operación en otras realizaciones sin apartarse de las enseñanzas de los presentes conceptos inventivos. Los mismos números de referencia o los mismos indicadores de referencia denotan los mismos elementos o similares en toda la especificación.

Como se usa en la presente memoria, los términos “comprenden”, “que comprende”, “comprende”, “incluyen”, “que incluye”, “incluye”, “tienen”, “tiene”, “que tiene”, o variantes de los mismos son abiertos, e incluyen una o más características, enteros, elementos, pasos, componentes o funciones establecidos, pero no excluyen la presencia o adición de una o más de otras características, enteros, elementos, pasos, componentes, funciones o grupos de los mismos. Además, como se usa en la presente memoria, la abreviatura común “por ejemplo” (en inglés “e.g.”), que se deriva de la frase en latín “ejempli gratia”, se puede usar para introducir o especificar un ejemplo o ejemplos generales de un elemento mencionado anteriormente, y no pretende ser limitante de tal elemento. La abreviatura común “es decir” (en inglés “i.e.”), que se deriva de la frase en latín “id est”, se puede usar para especificar un elemento particular de una enumeración más general.

Las realizaciones de ejemplo se describen en la presente memoria con referencia a ilustraciones de diagramas de bloques y/o diagramas de flujo de métodos implementados por ordenador, aparatos (sistemas y/o dispositivos) y/o productos de programas de ordenador. Se entiende que un bloque de las ilustraciones de diagramas de bloques y/o diagramas de flujo, y combinaciones de bloques en las ilustraciones de diagramas de bloques y/o diagramas de flujo, se pueden implementar mediante instrucciones de programa de ordenador que son realizadas por uno o más circuitos de ordenador. Estas instrucciones de programa de ordenador se pueden proporcionar a un circuito de procesador de un circuito de ordenador de propósito general, circuito de ordenador de propósito especial y/u otro circuito de procesamiento de datos programable para producir una máquina, de manera que las instrucciones, que se ejecutan a través del procesador del ordenador y/u otro aparato de procesamiento de datos programable, transistores de transformación y control, valores almacenados en ubicaciones de memoria y otros componentes de hardware dentro de tal circuitería implementen las funciones/actos especificados en los diagramas de bloques y/o bloque o bloques de diagrama de flujo, y por ello creen medios (funcionalidad) y/o estructura para implementar las funciones/actos especificados en los diagramas de bloques y/o bloque o bloques de diagrama de flujo.

Estas instrucciones de programa de ordenador también se pueden almacenar en un medio tangible legible por ordenador que puede dirigir un ordenador u otro aparato de procesamiento de datos programable para funcionar de una manera particular, de manera que las instrucciones almacenadas en el medio legible por ordenador producen un artículo de fabricación que incluye instrucciones que implementan las funciones/actos especificados en los diagramas de bloques y/o bloque o bloques de diagrama de flujo. Por consiguiente, las realizaciones de los presentes conceptos inventivos se pueden incorporar en hardware y/o en software (incluyendo microprograma, software residente, microcódigo, etc.) ejecutándose en un procesador tal como un procesador digital de señal, al que se puede hacer referencia colectivamente como “circuitería”, “un módulo” o variantes de los mismos.

También se debería observar que en algunas implementaciones alternativas, las funciones/actos señalados en los bloques pueden ocurrir fuera del orden señalado en los diagramas de flujo. Por ejemplo, dos bloques que se muestran en sucesión se pueden ejecutar de hecho de manera sustancialmente concurrente o los bloques se pueden ejecutar algunas veces en el orden inverso, dependiendo de la funcionalidad/actos implicados. Además, la funcionalidad de un bloque dado de los diagramas de flujo y/o los 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 los diagramas de bloques se pueden integrar al menos parcialmente. Finalmente, se pueden añadir/insertar otros bloques entre los bloques que se ilustran, y/o se pueden omitir bloques/operaciones sin apartarse del alcance de los conceptos inventivos. Además, aunque algunos de los diagramas incluyen flechas en los caminos de comunicación para mostrar una dirección primaria de comunicación, ha de ser entendido que la comunicación puede ocurrir 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 inventivos. Todas de tales variaciones y modificaciones se pretende que estén incluidas en la presente memoria dentro del alcance de los presentes conceptos inventivos. Por consiguiente, la materia objeto descrita anteriormente ha de ser considerada ilustrativa y no restrictiva, y los ejemplos de realizaciones adjuntos se pretende que cubran todas de tales modificaciones, mejoras y otras realizaciones, que caen dentro del espíritu y alcance de los presentes conceptos inventivos. De este modo, en la máxima medida permitida por la ley, el alcance de los presentes conceptos inventivos ha de ser determinado por la interpretación más amplia admisible de la presente descripción, y no se restringirá o limitará por la descripción detallada precedente.

Se describen a continuación algunas realizaciones no limitantes.

Realización 1. Un método, en un nodo de red, para 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 donde el terminal inalámbrico está o está a punto de ser conectado dualmente a la estación base de anclaje y a la estación base de asistencia, el método que comprende:

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 asistencia, la clave de seguridad de asistencia generada, para su uso por la estación base de asistencia en el cifrado del tráfico de datos enviado al terminal inalámbrico o 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 mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia; y
usar (830) la clave de estación base de anclaje, o una clave derivada a partir de la clave de estación base de anclaje, para cifrar los datos enviados al terminal inalámbrico por la estación base de anclaje mientras que el terminal inalámbrico está conectado dualmente a la estación base del anclaje y a la estación base de asistencia.

Realización 2. El método de la realización 1, en donde 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 donde usar (830) la clave de estación base de anclaje comprende derivar una clave de cifrado, o una clave de integridad, o ambas, a partir de la clave de estación base de anclaje, y usar 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 dualmente a la estación base de anclaje y a la estación base de asistencia.

Realización 4. El método de cualquiera de las realizaciones 1-3, en donde la generación (810) de la clave de seguridad de asistencia comprende derivar la clave de seguridad de asistencia a partir de la clave de estación base de anclaje usando una función unidireccional.

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

Realización 6. El método de cualquiera de las realizaciones 1-5, en donde la generación (810) de la clave de seguridad de asistencia se basa además en un parámetro de refresco.

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

detectar de que un parámetro COUNT del Protocolo de Convergencia de Paquetes de Datos, PDCP, en la estación base de asistencia está a punto de envolverse;
en respuesta a dicha detección, iniciar un refresco 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 donde 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 donde 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 manera que las claves de seguridad de asistencia resultantes difieran 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 donde el terminal inalámbrico está o está a punto de ser conectado dualmente a la estación base de anclaje y a la estación base de asistencia, el método que comprende:

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 en el cifrado del tráfico de datos enviado al terminal inalámbrico o 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 mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia.

Realización 11. El método de la realización 10, en donde 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 donde la generación (920) de la clave de seguridad de asistencia comprende derivar la clave de seguridad de asistencia a partir de la clave de estación base de anclaje usando una función unidireccional.

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

Realización 14. El método de cualquiera de las realizaciones 10-13, en donde la generación (920) de la clave de seguridad de asistencia se basa además en un parámetro de refresco.

Realización 15. El método de cualquiera de las realizaciones 10-14, en donde el envío (930) de 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 donde el nodo de red es un nodo de gestión de movilidad.

Realización 17. Un nodo de red (401A) para la generación de claves de seguridad para comunicaciones seguras entre un terminal inalámbrico y una estación base de asistencia, en donde el terminal inalámbrico está, o está a punto de ser, conectado dualmente a la estación base de anclaje y la estación base de asistencia, el nodo de red (401A) que comprende circuitería de interfaz (440A) configurada para comunicarse con la estación base de asistencia y que comprende además circuitería de procesamiento (420A, 430A), caracterizada por que la circuitería de procesamiento (420A, 430A) 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, usando la circuitería de interfaz, la clave de seguridad de asistencia generada, para su uso por la estación base de asistencia en el cifrado del tráfico de datos enviado al terminal inalámbrico o 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 mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia; y
usar la clave de estación base de anclaje, o una clave derivada a partir de la clave de estación base de anclaje, para cifrar los datos enviados al terminal inalámbrico por la estación base de anclaje mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia.

Realización 18. El nodo de red (401A) de la realización 17, en donde 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 de red (401A) de la realización 18, en donde la circuitería de procesamiento (420A, 430A) está configurada para usar la clave de estación base de anclaje para derivar una clave de cifrado o una clave de integridad, o ambas, a partir de la clave de estación base de anclaje, y para usar 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 dualmente a la estación base de anclaje y a la estación base de asistencia.

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

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

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

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

detectar que un parámetro COUNT de Protocolo de Convergencia de Paquetes de Datos, PDCP, en la estación base de asistencia está a punto de envolverse;
en respuesta a dicha detección, iniciar un refresco de la clave de estación base de anclaje y volver a calcular la clave de seguridad de asistencia.

Realización 24. El nodo de red (401A) de cualquiera de las realizaciones 17-23, en donde el nodo de red (401A) es un eNodoB de Evolución a Largo Plazo, LTE.

Realización 25. El nodo de red (401A) de cualquiera de las realizaciones 17-24, en donde la circuitería de procesamiento (420A, 430A) 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 manera que las claves de seguridad de asistencia resultantes difieran para cada Portador de Radio de Datos.

Realización 26. Un nodo de red (505A) para generación de claves de seguridad para comunicaciones seguras entre un terminal inalámbrico y una estación base de asistencia, en donde el terminal inalámbrico está, o está a punto de ser, conectado dualmente a la estación base de anclaje y a la estación base de asistencia, el nodo de red (505A) que comprende circuitería de interfaz (510A) configurada para comunicarse con la estación base de asistencia y que comprende además circuitería de procesamiento (520A, 530A), caracterizada por que la circuitería de procesamiento está configurada 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 de interfaz (510A), la clave de seguridad de asistencia generada, para su uso por la estación base de asistencia en el cifrado del tráfico de datos enviado al terminal inalámbrico o 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, mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia.

Realización 27. El nodo de red (505A) de la realización 26, en donde 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 de red (505A) de la realización 26 o 27, en donde la circuitería de procesamiento (520A, 530A) está configurada para generar la clave de seguridad de asistencia derivando la clave de seguridad de asistencia a partir de la clave de estación base de anclaje usando una función unidireccional.

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

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

Realización 31. El nodo de red (505A) de cualquiera de las realizaciones 26-30, en donde la circuitería de procesamiento (520A, 530A) 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 de red (505A) de cualquiera de las realizaciones 26-31, en donde el nodo de red (505A) es un nodo de gestión de movilidad.

REIVINDICACIONES

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 donde el terminal inalámbrico está o está a punto de ser conectado dualmente a la estación base de anclaje y a la estación base de asistencia, el método que comprende:

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 asistencia, la clave de seguridad de asistencia generada, para su uso por la estación base de asistencia en el cifrado del tráfico de datos enviado al terminal inalámbrico o en la generación de una o más de claves de seguridad de asistencia adicionales para cifrar el tráfico de datos enviado al terminal inalámbrico por la estación base de asistencia, en donde el tráfico de datos se envía mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia; y
usar (830) la clave de estación base de anclaje, o una clave derivada a partir de la clave de estación base de anclaje, para cifrar los datos enviados al terminal inalámbrico por la estación base de anclaje, mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia.

2. El método de la reivindicación 1, en donde la clave de seguridad de asistencia generada comprende una clave de seguridad de asistencia de 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 2, en donde usar (830) la clave de estación base de anclaje comprende derivar una clave de cifrado, o una clave de integridad, o ambas, a partir de la clave de estación base de anclaje, y usar 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 dualmente a la estación base de anclaje y a la estación base de asistencia.

4. El método de cualquiera de las reivindicaciones 1-3, en donde la generación (810) de la clave de seguridad de asistencia comprende derivar la clave de seguridad de asistencia a partir de la clave de estación de base de anclaje usando una función unidireccional.

5. El método de la reivindicación 4, en donde la función unidireccional es una función criptográfica HMAC-SHA-256.

6. El método de cualquiera de las reivindicaciones 1-4, en donde 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 manera que las claves de seguridad de asistencia resultantes difieren para cada Portador de Datos de Radio.

7. Un nodo de red para la generación de claves de seguridad para comunicaciones seguras entre un terminal inalámbrico y una estación base de asistencia, en donde el terminal inalámbrico está, o está a punto de ser, conectado dualmente a la estación base de anclaje y a la estación base de asistencia, el nodo de red (401A) que comprende circuitería de interfaz (440A) configurada para comunicarse con la estación base de asistencia y que comprende además circuitería de procesamiento (420A, 430A) que 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, la clave de seguridad de asistencia generada, para su uso por la estación base de asistencia en el cifrado del tráfico de datos enviado al terminal inalámbrico o 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 donde el tráfico de datos se envía mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia; y
usar la clave de estación base de anclaje, o una clave derivada a partir de la clave de estación base de anclaje, para cifrar los datos enviados al terminal inalámbrico por la estación base de anclaje mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia.

8. El nodo de red de la reivindicación 7, en donde la circuitería de procesamiento está configurada además para realizar los pasos de cualquiera de las reivindicaciones 2-6.

9. Un producto de programa de ordenador que comprende instrucciones de programa para un procesador en un nodo de red, en donde un terminal inalámbrico está, o está a punto de ser, conectado dualmente a una estación

base de anclaje y a una estación base de asistencia, en donde dichas instrucciones de programa están configuradas para hacer que el nodo de red, cuando las instrucciones de programa se ejecutan por el procesador:

genere 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;
envíe, a la estación base de asistencia, la clave de seguridad de asistencia generada para su uso por la estación base de asistencia en el cifrado del tráfico de datos enviado al terminal inalámbrico o 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 donde el tráfico de datos se envía mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia; y
use la clave de estación base de anclaje, o una clave derivada de la clave de estación base de anclaje, para cifrar los datos enviados al terminal inalámbrico por la estación base de anclaje mientras que el terminal inalámbrico está conectado dualmente a la estación base de anclaje y a la estación base de asistencia.

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

generar una clave de seguridad de asistencia, basada al menos en parte en la clave de seguridad primaria;
usar la clave de seguridad de asistencia para cifrar tráfico de datos, o en la generación de una o más claves de seguridad de asistencia adicionales para cifrar tráfico de datos, donde el tráfico de datos se envía desde el terminal inalámbrico (505B) a la estación base de asistencia, mientras que el terminal inalámbrico (505B) está conectado dualmente a la estación base de anclaje y a la estación base asociada.

11. Un terminal inalámbrico (505B), para generación de claves de seguridad para comunicaciones seguras entre el terminal inalámbrico (505B) y una estación base de asistencia, el terminal inalámbrico (505B) que comprende circuitería de interfaz (510B), circuitería de procesamiento (520B) y una memoria (530B), en donde el terminal inalámbrico (505B) está configurado para ser conectado dualmente a una estación base de anclaje y a la estación base de asistencia, y en donde la circuitería de procesamiento (520B) 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);
usar la clave de seguridad de asistencia para cifrar tráfico de datos, o en la generación de una o más claves de seguridad de asistencia adicionales para cifrar tráfico de datos, en donde el tráfico de datos se envía desde el terminal inalámbrico (505B) a la estación base de asistencia mientras que el terminal inalámbrico (505B) está conectado dualmente a la estación base de anclaje y a la estación base de asistencia.

12. El terminal inalámbrico de la reivindicación 11, configurado además para generar la clave de seguridad de asistencia comprende derivar la clave de seguridad de asistencia a partir de la clave primaria usando una función unidireccional.

13. El terminal inalámbrico de la reivindicación 12, en donde la función unidireccional es una función criptográfica HMAC-SHA-256.

14. El terminal inalámbrico de cualquiera de las reivindicaciones 12-13, configurado además para generar la clave de seguridad de asistencia basada en un parámetro de refresco.

15. Un producto de programa de ordenador que comprende instrucciones de programa para un procesador en un terminal inalámbrico que está configurado para ser conectado dualmente a una estación base de anclaje y a una estación base de asistencia, en donde dichas instrucciones de programa están configuradas para hacer que el terminal inalámbrico, cuando las instrucciones del programa se ejecutan por el procesador:

genere 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);
use la clave de seguridad de asistencia para cifrar tráfico de datos, o en la generación de una o más claves de seguridad de asistencia adicionales para cifrar tráfico de datos, en donde el tráfico de datos se envía desde el terminal inalámbrico (505B) a la estación base de asistencia mientras que el terminal inalámbrico (505B) está conectado dualmente a la estación base de anclaje y a la estación base de asistencia.

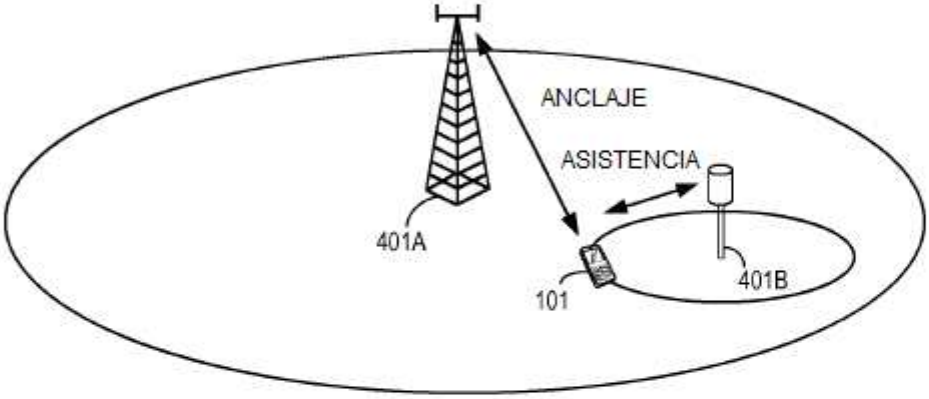

FIG. 1

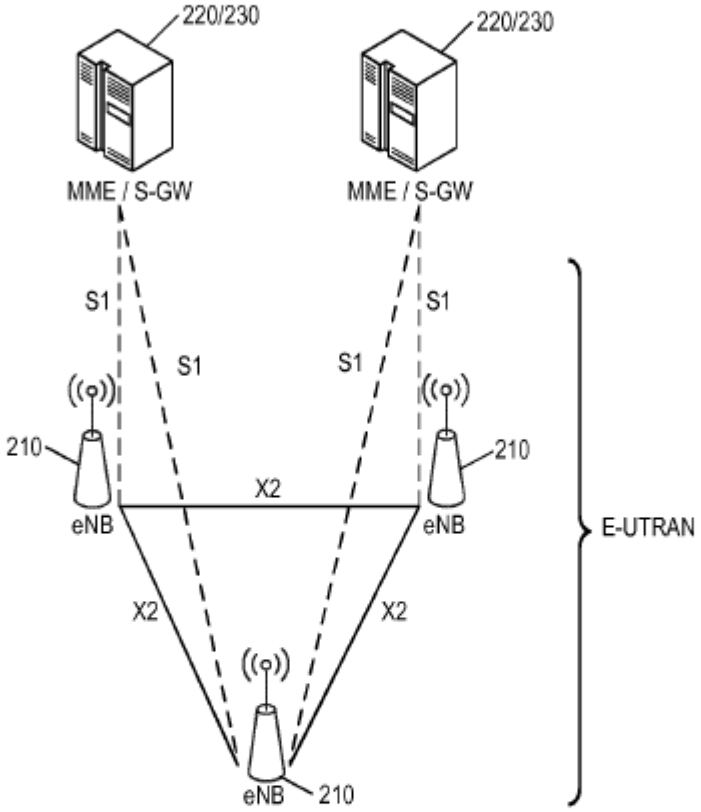
220/230
220/230
MME / S-GW
MME / S-GW
S1
S1
S1
S1
210
210
X2
eNB
eNB
E-UTRAN
X2
X2
eNB
210

FIG. 2

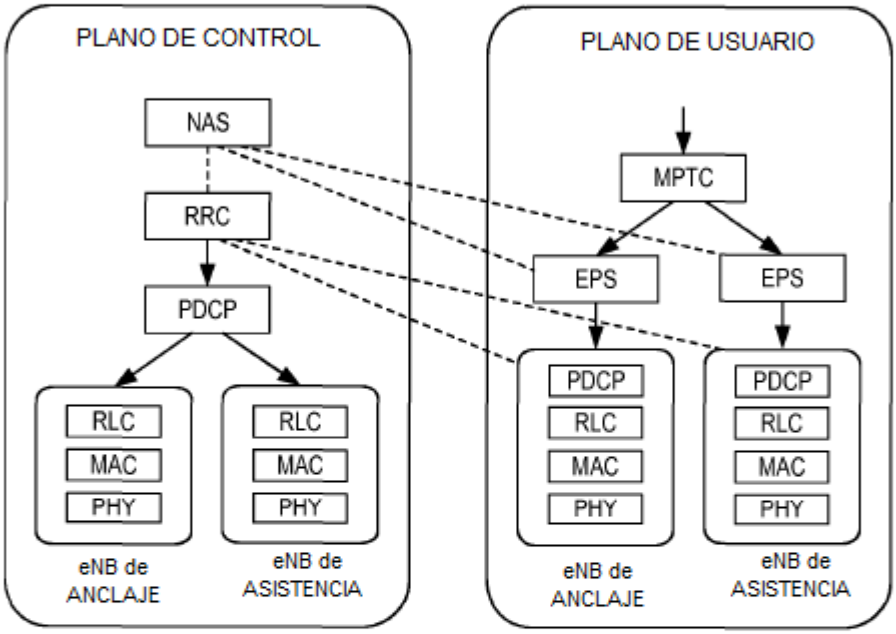
PLANO DE CONTROL
NAS
RRC
PDCP
RLC
MAC
PHY
RLC
MAC
PHY
eNB de ANCLAJE
eNB de ASISTENCIA
PLANO DE USUARIO
MPTC
EPS
EPS
PDCP
RLC
MAC
PHY
PDCP
RLC
MAC
PHY
eNB de ANCLAJE
eNB de ASISTENCIA

FIG. 3

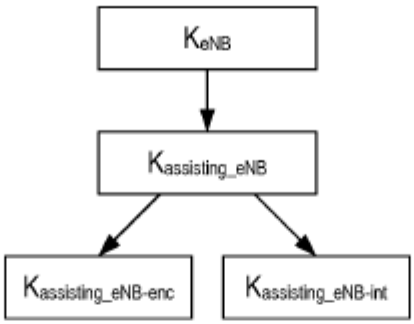
KeNB
Kassisting_eNB
Kassisting_eNB-enc
Kassisting_eNB-int

FIG. 4

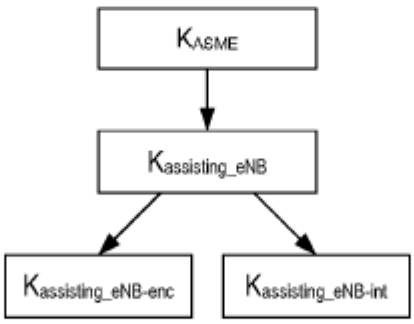
KASME
Kassisting_eNB
Kassisting_eNB-enc
Kassisting_eNB-int

FIG. 5

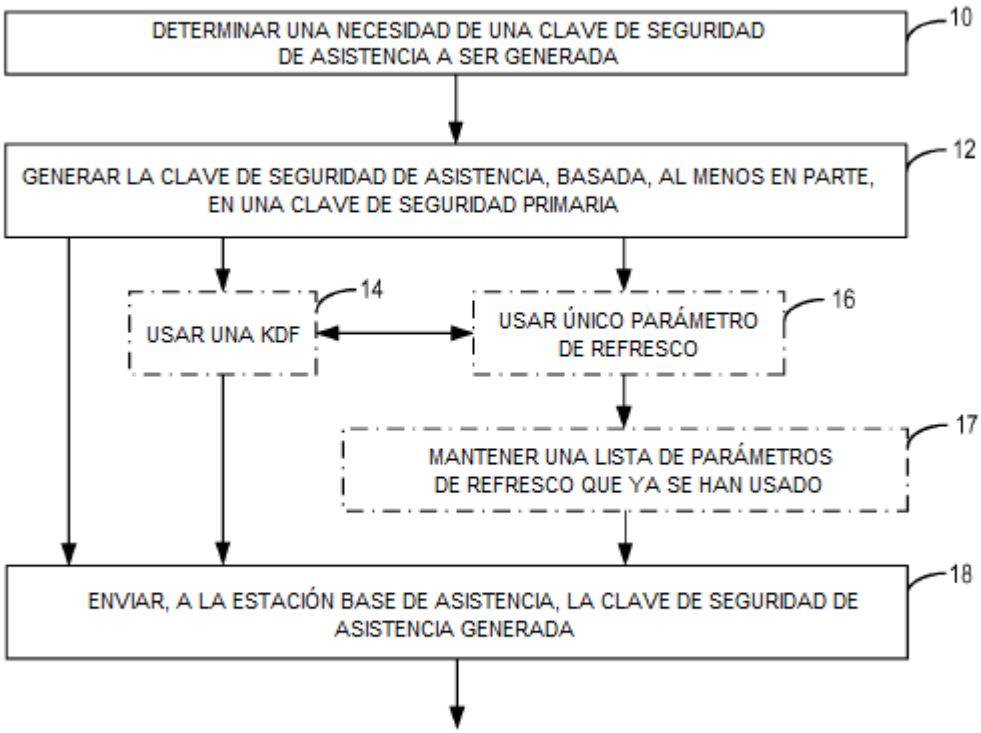
DETERMINAR UNA NECESIDAD DE UNA CLAVE DE SEGURIDAD DE ASISTENCIA A SER GENERADA
10
GENERAR LA CLAVE DE SEGURIDAD DE ASISTENCIA, BASADA, AL MENOS EN PARTE, EN UNA CLAVE DE SEGURIDAD PRIMARIA
12
USAR UNA KDF
14
USAR ÚNICO PARÁMETRO DE REFRESCO
16
MANTENER UNA LISTA DE PARÁMETROS DE REFRESCO QUE YA SE HAN USADO
17
ENVIAR, A LA ESTACIÓN BASE DE ASISTENCIA, LA CLAVE DE SEGURIDAD DE ASISTENCIA GENERADA
18

FIG. 6

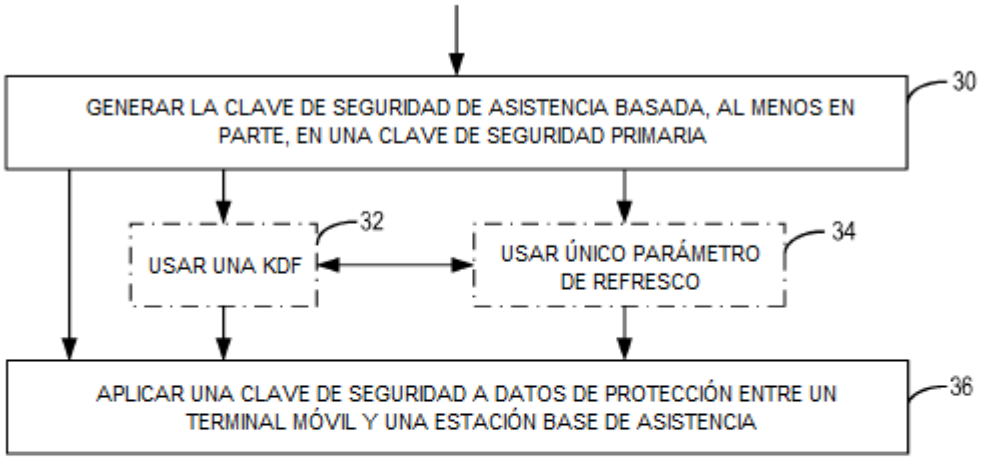
GENERAR LA CLAVE DE SEGURIDAD DE ASISTENCIA BASADA, AL MENOS EN PARTE, EN UNA CLAVE DE SEGURIDAD PRIMARIA
30
USAR UNA KDF
32
USAR ÚNICO PARÁMETRO DE REFRESCO
34
APLICAR UNA CLAVE DE SEGURIDAD A DATOS DE PROTECCIÓN ENTRE UN TERMINAL MÓVIL Y UNA ESTACIÓN BASE DE ASISTENCIA
36

FIG. 7

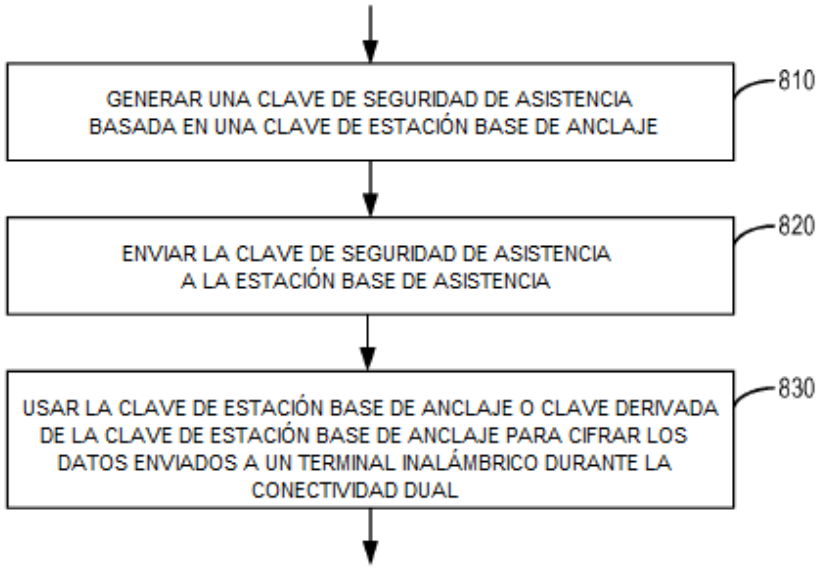
GENERAR UNA CLAVE DE SEGURIDAD DE ASISTENCIA BASADA EN UNA CLAVE DE ESTACIÓN BASE DE ANCLAJE
810
ENVIAR LA CLAVE DE SEGURIDAD DE ASISTENCIA A LA ESTACIÓN BASE DE ASISTENCIA
820
USAR LA CLAVE DE ESTACIÓN BASE DE ANCLAJE O CLAVE DERIVADA DE LA CLAVE DE ESTACIÓN BASE DE ANCLAJE PARA CIFRAR LOS DATOS ENVIADOS A UN TERMINAL INALÁMBRICO DURANTE LA CONECTIVIDAD DUAL
830

FIG. 8

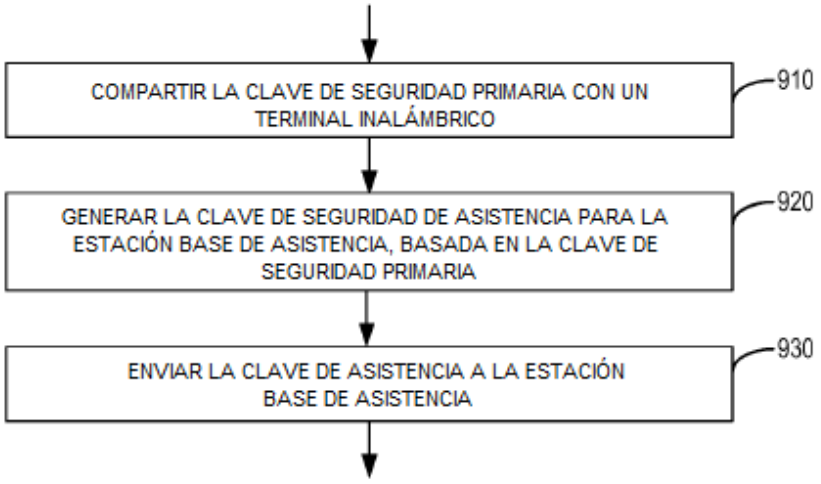
COMPARTIR LA CLAVE DE SEGURIDAD PRIMARIA CON UN TERMINAL INALÁMBRICO
910
GENERAR LA CLAVE DE SEGURIDAD DE ASISTENCIA PARA LA ESTACIÓN BASE DE ASISTENCIA, BASADA EN LA CLAVE DE SEGURIDAD PRIMARIA
920
ENVIAR LA CLAVE DE ASISTENCIA A LA ESTACIÓN BASE DE ASISTENCIA
930

FIG. 9

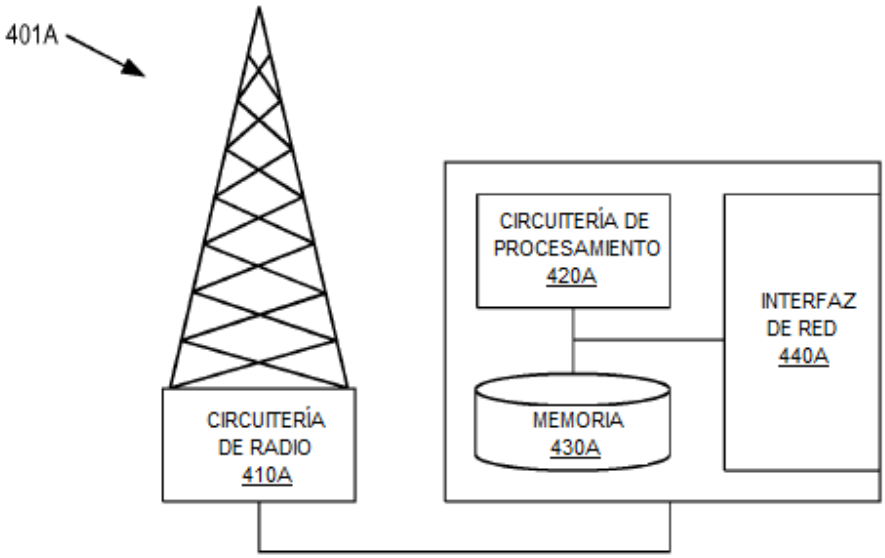
401A
CIRCUITERÍA DE PROCESAMIENTO 420A
INTERFAZ DE RED 440A
MEMORIA 430A
CIRCUITERÍA DE RADIO 410A

FIG. 10

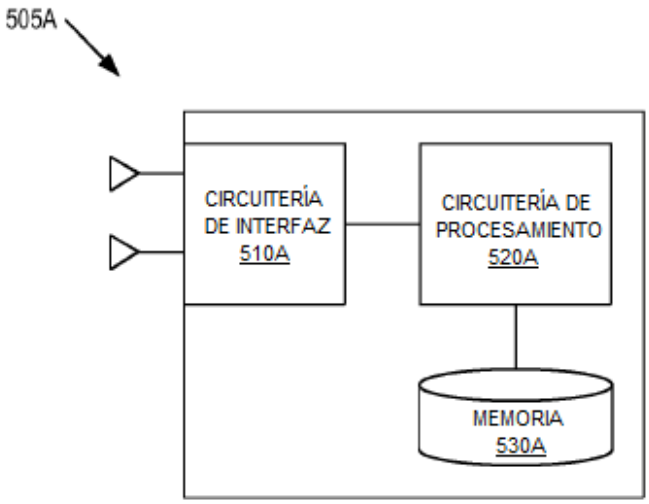
505A
CIRCUITERÍA DE INTERFAZ 510A
CIRCUITERÍA DE PROCESAMIENTO 520A
MEMORIA 530A

FIG. 11

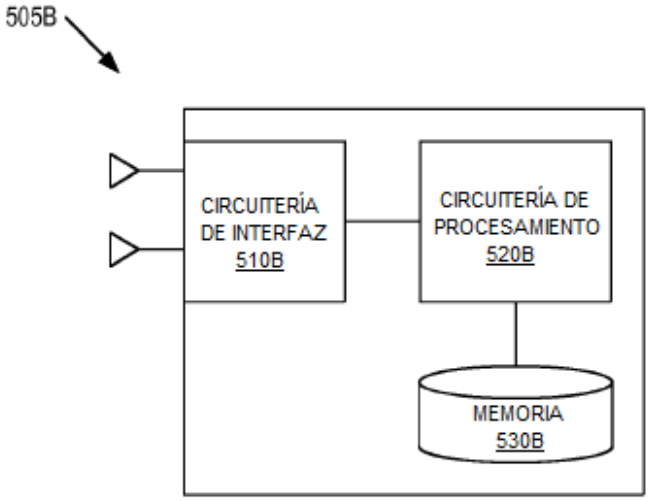
505B
CIRCUITERÍA DE INTERFAZ 510B
CIRCUITERÍA DE PROCESAMIENTO 520B
MEMORIA 530B

FIG. 12