(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 797 598**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 84/04 (2009.01)
H04W 36/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.12.2013 PCT/JP2013/083535**

(87) Fecha y número de publicación internacional: **24.07.2014 WO14112262**

(96) Fecha de presentación y número de la solicitud europea: **10.12.2013 E 13812187 (6)**

(97) Fecha y número de publicación de la concesión europea: **25.03.2020 EP 2946581**

(54) Título: **Comunicaciones seguras en un sistema celular con usuarios y planos de control divididos**

(30) Prioridad:

17.01.2013 GB 201300884

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.12.2020

(73) Titular/es:

NEC CORPORATION (100.0%)
7-1, Shiba 5-chome Minato-ku
Tokyo 108-8001, JP

(72) Inventor/es:

SHARMA, VIVEK

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Comunicaciones seguras en un sistema celular con usuarios y planos de control divididos

Campo técnico:
La presente invención se refiere a dispositivos y redes de comunicación móviles, particularmente, pero no exclusivamente, a aquellos que operan según los estándares del Proyecto de Asociación de 3ª generación (3GPP) o equivalentes o derivados de los mismos. La invención tiene una relevancia particular, aunque no exclusiva, para un mayor desarrollo de la llamada Evolución a Largo Plazo (LTE) / LTE avanzado (LTE-Avanzado (LTE-A)) de UTRAN (llamada Red de Acceso Radio Terrestre Universal Evolucionada (E-UTRAN)).

Antecedentes de la técnica:
Se ha decidido, como parte del proceso de estandarización del 3GPP, que el funcionamiento del enlace descendente para anchos de banda del sistema por encima de 20MHz se basará en la agregación de una pluralidad de portadoras de componente a diferentes frecuencias. Dicha agregación de portadora puede utilizarse para soportar el funcionamiento en un sistema tanto con, como sin, un espectro contiguo (por ejemplo, un sistema no contiguo puede comprender portadoras de componente a 800MHz, 2 GHz, y 3,5GHz). Mientras que un dispositivo móvil heredado solo puede comunicarse utilizando una única portadora de componente, compatible con versiones anteriores, un terminal más avanzado con capacidad para múltiples portadoras podría utilizar simultáneamente múltiples portadoras de componente.

A medida que la tecnología de comunicación móvil (celular) se ha desarrollado, ha habido propuestas para proporcionar una comunicación mejorada en regiones geográficas relativamente pequeñas teniendo celdas pequeñas (p. ej., “pico” o “femto” celdas) que coexisten con una celda mayor (“macro”) y proporcionan capacidades de comunicación mejoradas en la región geográfica localizada que cubre las celdas pequeñas. Estas celdas pequeñas pueden proporcionarse en la misma portadora que la macro celda, o pueden proporcionarse en una portadora dedicada diferente (p. ej., de mayor frecuencia).

Más recientemente, se ha propuesto permitir que los datos de usuario para un dispositivo de usuario particular, como un teléfono móvil u otro dispositivo de comunicación móvil (también referido como “equipo de usuario” o “UE”) se comuniquen a través de una celda diferente a la celda a través de la cual se comunican los datos de control para ese usuario. Específicamente, se ha propuesto permitir que el plano de usuario (plano U) y el plano de control (plano C) para un dispositivo de usuario particular se divida entre la celda pequeña y la macro celda de manera que los datos del plano U se comunican a través de la celda pequeña y los datos del plano C se comunican a través de la macro celda.

La celda pequeña de esta propuesta es, efectivamente, una “pseudo” celda o celda “fantasma” porque no proporciona las señales específicas de celda y/o canales convencionales como señales de referencia de portadora, emisiones de información maestra/información del sistema, señales de sincronización primaria/secundaria, etc.

En teoría, la división del plano C/plano U de esta propuesta proporciona una optimización de: los beneficios de la mejor conectividad normalmente ofrecida por una macro celda para la señalización de control crítica; y los beneficios de un mayor rendimiento y una comunicación más flexible, eficiente en energía y rentable ofrecida por una celda pequeña utilizando una banda de frecuencia más alta o más ancha para datos de usuario de mayor volumen.

Sin embargo, la división del plano C/plano U presenta un número de desafíos que deben abordarse si dicho propuesta se implementa prácticamente en la red de comunicación global.

Uno de dichos desafíos es la provisión de seguridad de comunicación apropiada donde diferentes estaciones base son responsables de la señalización del plano U y de la señalización del plano C respectivamente, asegurando al mismo tiempo que el dispositivo de usuario puede cifrar / descifrar los datos de usuario y datos de control correctamente. Esto tiene el potencial de añadir una complejidad significativa no deseada a la señalización entre la red central, la estación base, y el dispositivo de usuario.

Además, para asegurar una seguridad apropiada, es beneficio poder, de vez en cuando, regenerar las claves de seguridad utilizadas para la encriptación y la protección de la integridad (“restablecimiento de clave” o “refresco de clave”). Dichos cambios de clave dinámicos pueden ser el resultado de procedimientos de restablecimiento de clave explícitos o de refresco de clave implícitos. Para asegurar que los parámetros de seguridad utilizados para el cifrado y la protección de la integridad siguen siendo únicos, por ejemplo, normalmente se requiere refresco de clave cuando el contador del Protocolo de Convergencia de Datos en Paquetes (PDCP) (“CONTADOR PDCP”), que se utiliza como entrada de cifrado, alcanza su límite y ‘se envuelve’ o 'se da la vuelta’ hasta su valor inicial. El restablecimiento de clave / refresco de clave evita el riesgo de que valores del CONTADOR PDCP previamente utilizados se reutilicen, en combinación con la misma clave de seguridad, como entradas para el cifrado evitando así la reutilización cíclica de los parámetros de seguridad anteriores.

Sin embargo, actualmente, dicho refresco de clave dinámico no es posible cuando el plano U y el plano C está divididos porque el contador PDCP se mantiene en el plano U mientras que la señalización de control requerida para el restablecimiento de clave ocurre en el plano C.

WO 2011/137775 describe un sistema de comunicación celular que incluye una macro estación base y una micro estación base dentro de la cobertura de la macro estación base. El plano de control del usuario servido por la micro estación base puede separarse del plano de datos del usuario, para que los recursos de la micro estación base puedan utilizarse para comunicación de datos.

CN 102740289 describe un método en el que una femtocelda monitoriza valores del CONTADOR (PDCP) del protocolo de convergencia de datos en paquetes del enlace ascendente y del enlace descendente de la interfaz de usuario de cada equipo de usuario (UE) conectado con la femto-celda, y envía información sobre los valores del CONTADOR PDCP del enlace ascendente y del enlace descendente de la interfaz de usuario a una macro estación base.

Compendio de la Invención:
La invención, por lo tanto, tiene como objetivo superar o al menos mitigar los problemas anteriores.

La invención se expone en las reivindicaciones independientes adjuntas a la misma, y las realizaciones preferidas se indican en las reivindicaciones dependientes que siguen.

Según un ejemplo se proporciona un dispositivo de comunicación móvil para la comunicación de datos del plano de usuario a través de un primer aparato de comunicación, de una red de comunicación, que opera una primera celda de comunicación, y para la recepción de señalización del plano de control relacionada con una comunicación del plano de usuario de un segundo aparato de comunicación, de la red de comunicación, que opera una segunda celda de comunicación, comprendiendo dicho dispositivo de comunicación móvil: medios para recibir información de seguridad; medios para obtener, a partir de dicha información de seguridad, al menos un parámetro de seguridad del plano de usuario para proporcionar seguridad del plano de usuario para dicha comunicación del plano de usuario, a través de dicho primer aparato de comunicación, y al menos un parámetro de seguridad del plano de control para proporcionar la seguridad del plano de control para la comunicación del plano de control a través de dicho segundo aparato de comunicación; y medios para aplicar dicho, al menos uno, parámetro de seguridad del plano de usuario en dicha comunicación del plano de usuario a través de dicho primer aparato de comunicación y para aplicar dicho, al menos uno, parámetro de seguridad del plano de control en dicha comunicación de plano de control a través de dicho segundo aparato de comunicación.

Opcionalmente, dicho dispositivo de comunicación móvil puede funcionar para recibir un indicador de que el plano de usuario y el plano de control pueden ser proporcionados por diferentes aparatos de comunicación respectivos.

Opcionalmente, dicho dispositivo de comunicación móvil puede funcionar para recibir un indicador de que dicho plano de usuario y dicho plano de control pueden ser proporcionados por diferentes aparatos de comunicación respectivos a partir de dicho segundo aparato de comunicación.

Opcionalmente, dicho dispositivo de comunicación móvil puede funcionar para recibir un indicador de que dicho plano de usuario y dicho plano de control pueden ser proporcionados por diferentes aparatos de comunicación respectivos a partir de una entidad de comunicación de dicha red de comunicación (p. ej., una entidad de la red central, p. ej., una entidad de gestión de la movilidad 'MME').

Opcionalmente, dicho, al menos uno, parámetro de seguridad del plano de usuario puede comprender una clave de seguridad 'K_{UPenc}' para el cifrado y/o descifrado de la comunicación del plano de usuario.

Opcionalmente, dichos medios de obtención pueden funcionar para obtener dicha clave de seguridad 'K_{UPenc}' para el cifrado y/o descifrado de la comunicación del plano de usuario derivándola de la utilización de una clave de seguridad adicional (p. ej., 'K_{eNB}' o 'K_{eNB}*') obtenida a partir de dicha información de seguridad.

Opcionalmente, dichos medios de obtención pueden funcionar para obtener dicha clave de seguridad 'K_{UPenc}' para el cifrado y/o descifrado sin la derivación que requiere una calve de seguridad adicional.

Opcionalmente, dicho, al menos uno, parámetro de seguridad del plano de usuario puede comprender una clave de seguridad 'K_{UPint}' para la protección de la integridad de la comunicación del plano de usuario.

Opcionalmente, dicho, al menos uno, parámetro de seguridad del plano de control puede comprender una clave de seguridad 'K_{RRCenc}' para el cifrado y/o descifrado de la comunicación del plano de control.

Opcionalmente, dicho, al menos uno, parámetro de seguridad del plano de control puede comprender una clave de seguridad '$KRRC_{int}$' para la protección de la integridad de la comunicación del plano de control.

Según un ejemplo adicional, se proporciona un aparato de comunicación para operar una celda de comunicación a través de la cual un dispositivo de comunicación móvil que puede participar en la comunicación del plano de usuario, en una red de comunicación en la que un aparato de comunicación adicional opera una celda adicional y proporciona la señalización del plano de control relacionada con dicha comunicación del plano de usuario, comprendiendo el aparato de comunicación: medios para operar dicha celda de comunicación a través de la cual dicho dispositivo de comunicación móvil puede participar en la comunicación del plano de usuario; medios para recibir la información de seguridad; medios para obtener, a partir de dicha información de seguridad, al menos un parámetro de seguridad del plano de usuario para proporcionar seguridad del plano de usuario para dicha comunicación del plano de usuario; y medios para aplicar dicho parámetro de seguridad del plano de usuario a la comunicación del plano de usuario a través de dicho primer aparato de comunicación.

Opcionalmente, dichos medios para recibir dicha información de seguridad pueden funcionar para recibir dicha información de seguridad de dicho aparato de comunicación adicional.

Opcionalmente, dichos medios para recibir dicha información de seguridad pueden funcionar para recibir dicha información de seguridad sobre un interfaz X2.

Opcionalmente, dichos medios para recibir dicha información de seguridad pueden funcionar para recibir dicha información de seguridad de una entidad de comunicación de dicha red de comunicación (p. ej., una entidad de la red central, p. ej., una entidad de gestión de la movilidad 'MME').

Opcionalmente, dichos medios para recibir dicha información de seguridad pueden funcionar para recibir dicha información de seguridad sobre un interfaz S1.

Opcionalmente, dichos medios para operar dicha celda de comunicación pueden configurarse para operar una celda que es pequeña en relación con la celda adicional operada por el aparato de comunicación adicional.

Opcionalmente, dicho, al menos uno, parámetro de seguridad del plano de usuario puede comprender una clave de seguridad 'K_{UPenc}' para el cifrado y/o descifrado de la comunicación del plano de usuario.

Opcionalmente, dichos medios de obtención pueden funcionar para obtener dicha clave de seguridad 'K_{UPenc}' para el cifrado y/o descifrado de la comunicación del plano de usuario directamente a partir de dicha información de seguridad.

Opcionalmente, dichos medios de obtención pueden funcionar para obtener dicha clave de seguridad 'K_{UPenc}' derivándola utilizando una clave de seguridad adicional (p. ej., 'K_{eNB}' o 'K_{eNB}*') obtenida a partir de dicha información de seguridad.

Opcionalmente, el aparato de comunicación puede comprender además medios para transmitir un indicador a dicho aparato de comunicación adicional de que dicho parámetro de seguridad del plano de usuario para proporcionar seguridad del plano de usuario requiere cambio (p. ej., en un procedimiento de restablecimiento de clave o de refresco de clave).

Opcionalmente, dicho aparato de comunicación puede comprender una estación base.

Opcionalmente, dicha estación base puede comprender una estación base de la Red de Acceso Radio Terrestre Universal Evolucionada (E-UTRAN).

Según otro ejemplo adicional se proporciona un aparato de comunicación para operar una celda de comunicación a través de la cual se proporciona la señalización del plano de control a un dispositivo de comunicación móvil, en una red de comunicación en la que el aparato de comunicación adicional opera una celda adicional a través de la cual dicho dispositivo de comunicación móvil puede participar en la comunicación del plano de usuario a la que se refiere dicha señalización del plano de control, comprendiendo el aparato de comunicación: medios para operar dicha celda de comunicación a través de la cual se proporciona dicha señalización del plano de control a un dispositivo de comunicación móvil; medios para recibir información de seguridad de una entidad de comunicación de dicha red de comunicación; medios para obtener, a partir de dicha información de seguridad, al menos un parámetro de seguridad del plano de control para proporcionar seguridad del plano de control para dicha señalización del plano de control proporcionada a dicho dispositivo de comunicación móvil, y al menos un parámetro de seguridad adicional; medios para proporcionar información de seguridad que comprende dicho parámetro de seguridad adicional para dicho aparato de comunicación adicional; y medios para aplicar dicho, al menos uno, parámetro de seguridad del plano de control cuando se proporciona dicha señalización del plano de control a dicho dispositivo de comunicación móvil.

Opcionalmente, dicho aparato de comunicación puede funcionar para transmitir, a dicho dispositivo de comunicación móvil, un indicador de que el plano de usuario y el plano de control son proporcionados por diferentes aparatos de comunicación respectivos.

Opcionalmente, el aparato de comunicación puede comprender además medios para recibir un indicador de dicho aparato de comunicación adicional de que un parámetro de seguridad del plano de usuario para proporcionar seguridad del plano de usuario requiere cambio (p. ej., en un procedimiento de restablecimiento de clave o de refresco de clave).

Opcionalmente, el aparato de comunicación puede comprender además medios para iniciar, en respuesta a la recepción de dicho indicador de que dicho parámetro de seguridad del plano de usuario para proporcionar seguridad del plano de usuario requiere cambio, un traspaso intracelular a través del cual, proporcionar un cambio en dicho parámetro de seguridad del plano de usuario para proporcionar seguridad del plano de usuario.

Opcionalmente, dicho aparato de comunicación comprende una estación base.

Opcionalmente, dicha estación base comprende una estación base de la Red de Acceso Radio Terrestre Universal Evolucionada (E-UTRAN).

Según otro ejemplo adicional se proporciona una entidad de comunicación para una red de comunicación en la que un dispositivo de comunicación móvil participa en la comunicación del plano de usuario a través de un primer aparato de comunicación que opera una primera celda de comunicación, y en la que el dispositivo de comunicación móvil recibe señalización del plano de control relacionada con dicha comunicación del plano de usuario de un segundo aparato de comunicación que opera una segunda celda de comunicación, comprendiendo dicha entidad de comunicación: medios para recibir información de seguridad de una entidad de comunicación adicional de dicha red de comunicación; medios para obtener, a partir de dicha información de seguridad, al menos un parámetro de seguridad raíz que puede ser utilizado en la derivación de: al menos un parámetro de seguridad del plano de usuario para proporcionar seguridad del plano de usuario para dicha comunicación del plano de usuario a través de dicho primer aparato de comunicación; y al menos un parámetro de seguridad del plano de control para proporcionar seguridad del plano de control para la comunicación del plano de control a través de dicho segundo aparato de comunicación; y medios para proporcionar información de seguridad que comprende dicho parámetro de seguridad raíz para dicho primer aparato de comunicación en un primer mensaje y para dicho segundo aparato de comunicación en un segundo mensaje.

Opcionalmente, la entidad de comunicación puede comprender una entidad de la red central.

Opcionalmente, la entidad de comunicación puede comprender una entidad de gestión de la movilidad (MME).

Opcionalmente, dichos medios de provisión pueden funcionar para proporcionar dichos primer y segundo mensaje sobre un interfaz S1.

Opcionalmente, dichos medios de provisión pueden funcionar para proporcionar dichos primer y segundo mensaje utilizando un protocolo de aplicación S1 ‘S1-AP’.

Según otro ejemplo adicional se proporciona un aparato de comunicación para operar una celda de comunicación a través de la cual se proporciona la señalización del plano de control a un dispositivo de comunicación móvil, en una red de comunicación en la que el aparato de comunicación adicional opera una celda adicional a través de la cual dicho dispositivo de comunicación móvil puede participar en la comunicación del plano de usuario a la que se refiere dicha señalización del plano de control, comprendiendo el aparato de comunicación: medios para operar dicha celda de comunicación a través de la cual se proporciona dicha señalización del plano de control a un dispositivo de comunicación móvil; medios para recibir información de seguridad de una entidad de comunicación de dicha red de comunicación; medios para obtener, a partir de dicha información de seguridad, al menos un parámetro de seguridad del plano de control para proporcionar seguridad del plano de control para dicha señalización del plano de control proporcionada a dicho dispositivo de comunicación móvil; medios para transmitir, a dicho dispositivo de comunicación móvil, un indicador de que el plano de usuario y el plano de control son proporcionados por diferentes aparatos de comunicación respectivos; y medios para aplicar dicho, al menos uno, parámetro de seguridad del plano de control cuando se proporciona dicha señalización del plano de control a dicho dispositivo de comunicación móvil.

Opcionalmente, dichos medios de obtención pueden funcionar para obtener, a partir de dicha información de seguridad, al menos un parámetro de seguridad adicional; y puede comprender además medios para proporcionar información de seguridad que comprende dicho parámetro de seguridad adicional para dicho aparato de comunicación adicional.

Según otro ejemplo adicional se proporciona un dispositivo de comunicación móvil para comunicar datos del plano de usuario a través de un primer aparato de comunicación, de una red de comunicación, que opera una primera celda de comunicación, y para recibir señalización del plano de control relacionada con una comunicación del plano de usuario de un segundo aparato de comunicación, de la red de comunicación, que opera una segunda celda de comunicación, comprendiendo dicho dispositivo de comunicación móvil: medios para obtener un primer conjunto de parámetros de seguridad para dicha comunicación del plano de usuario, de un primer procedimiento de acuerdo de clave autenticada

(AKA) con respecto a dicho primer aparato de comunicación, y para generar un primer contexto de seguridad asociado; medios para obtener un segundo conjunto de parámetros de seguridad para la comunicación del plano de control, de un segundo procedimiento de acuerdo de clave autenticada (AKA) con respecto a dicho segundo aparato de comunicación, y para generar un segundo contexto de seguridad asociado; y medios para mantener dicho primer contexto de seguridad y dicho segundo contexto de seguridad.

Según otro ejemplo adicional se proporciona una entidad de comunicación para una red de comunicación en la que un dispositivo de comunicación móvil puede participar en la comunicación del plano de usuario a través de un primer aparato de comunicación que opera una primera celda de comunicación, y en la que el dispositivo de comunicación móvil puede recibir señalización del plano de control relacionada con dicha comunicación del plano de usuario de un segundo aparato de comunicación que opera una segunda celda de comunicación, comprendiendo dicha entidad de comunicación: medios para realizar un primer procedimiento de acuerdo de clave autenticada (AKA), con respecto a dicho primer aparato de comunicación, para la comunicación del plano de usuario y para generar un primer contexto de seguridad asociado; medios para realizar un segundo procedimiento de acuerdo de clave autenticada (AKA), con respecto a dicho segundo aparato de comunicación, para la comunicación del plano de control y para generar un segundo contexto de seguridad asociado; y medios para mantener dicho primer contexto de seguridad y dicho segundo contexto de seguridad.

Según otro ejemplo adicional se proporciona un método realizado por un dispositivo de comunicación móvil que puede comunicar datos del plano de usuario a través de un primer aparato de comunicación, de una red de comunicación, que opera una primera celda de comunicación, y puede recibir señalización del plano de control relacionada con una comunicación del plano de usuario de un segundo aparato de comunicación, de la red de comunicación, que opera una segunda celda de comunicación, comprendiendo dicho método: recibir información de seguridad; obtener, a partir de dicha información de seguridad, al menos un parámetro de seguridad del plano de usuario para proporcionar seguridad del plano de usuario para dicha comunicación del plano de usuario a través de dicho primer aparato de comunicación y al menos un parámetro de seguridad del plano de control para proporcionar seguridad del plano de control para la comunicación del plano de control a través de dicho segundo aparato de comunicación; y aplicar dicho, al menos uno, parámetro de seguridad del plano de usuario en dicha comunicación del plano de usuario a través de dicho primer aparato de comunicación y aplicar dicho, al menos uno, parámetro de seguridad del plano de control en dicha comunicación del plano de control a través de dicho segundo aparato de comunicación.

Según otro ejemplo adicional se proporciona un método realizado por un aparato de comunicación cuando se opera una celda a través de la cual un dispositivo de comunicación móvil puede participar en la comunicación del plano de usuario, en una red de comunicación en la que el aparato de comunicación adicional opera una celda adicional y proporciona señalización del plano de control relacionada con dicha comunicación del plano de usuario, comprendiendo el método: recibir información de seguridad; obtener, a partir de dicha información de seguridad, al menos un parámetro de seguridad del plano de usuario para proporcionar seguridad del plano de usuario para dicha comunicación del plano de usuario; y aplicar dicho parámetro de seguridad del plano de usuario a dicha comunicación del plano de usuario a través de dicho primer aparato de comunicación.

Según otro ejemplo adicional se proporciona un método realizado por un aparato de comunicación cuando se opera una celda a través de la cual se proporciona señalización del plano de control a un dispositivo de comunicación móvil, en una red de comunicación en la que el aparato de comunicación adicional opera una celda adicional a través de la cual dicho dispositivo de comunicación móvil puede participar en la comunicación del plano de usuario a la que se refiere dicha señalización del plano de control, comprendiendo el método: recibir información de seguridad de una entidad de comunicación de dicha red de comunicación; obtener, a partir de dicha información de seguridad, al menos un parámetro de seguridad del plano de control para proporcionar seguridad del plano de control para dicha señalización del plano de control proporcionada a dicho dispositivo de comunicación móvil, y al menos un parámetro de seguridad adicional; proporcionar información de seguridad que comprende dicho parámetro de seguridad adicional para dicho aparato de comunicación adicional; y aplicar dicho, al menos uno, parámetro de seguridad del plano de control cuando se proporciona dicha señalización del plano de control a dicho dispositivo de comunicación móvil.

Según otro ejemplo adicional se proporciona un método realizado por una entidad de comunicación en una red de comunicación en la que un dispositivo de comunicación móvil participa en la comunicación del plano de usuario a través de un primer aparato de comunicación que opera una primera celda de comunicación, y en la que el dispositivo de comunicación móvil recibe señalización del plano de control relacionada con dicha comunicación del plano de usuario de un segundo aparato de comunicación que opera una segunda celda de comunicación, comprendiendo dicho método: recibir información de seguridad de una entidad de comunicación adicional de dicha red de comunicación; obtener, a partir de dicha información de seguridad, al menos un parámetro de seguridad raíz que puede ser utilizado en la derivación de:

al menos un parámetro de seguridad del plano de usuario para proporcionar seguridad del plano de usuario para dicha comunicación del plano de usuario a través de dicho primer aparato de comunicación; y al menos un parámetro de seguridad del plano de control para proporcionar seguridad del plano de control para la comunicación del plano de control a través de dicho segundo aparato de comunicación; y proporcionar información de seguridad que comprende

dicho parámetro de seguridad raíz para dicho primer aparato de comunicación en un primer mensaje y para dicho segundo aparato de comunicación en un segundo mensaje.

Según otro ejemplo adicional se proporciona un método realizado por un aparato de comunicación cuando se opera una celda de comunicación a través de la cual se proporciona señalización del plano de control a un dispositivo de comunicación móvil, en una red de comunicación en la que un aparato de comunicación adicional opera una celda adicional a través de la cual dicho dispositivo de comunicación móvil puede participar en la comunicación del plano de usuario a la que se refiere dicha señalización del plano de usuario, comprendiendo el método: operar dicha celda de comunicación a través de la cual se proporciona dicha señalización del plano de control a un dispositivo de comunicación móvil; recibir información de seguridad de una entidad de comunicación de dicha red de comunicación; obtener, a partir de dicha información de seguridad, al menos un parámetro de seguridad del plano de control para proporciona seguridad del plano de control para dicha señalización del plano de control proporcionada a dicho dispositivo de comunicación móvil; transmitir, a dicho dispositivo de comunicación móvil, un indicador de que el plano de usuario y el plano de control son proporcionados por diferentes aparatos de comunicación respectivos; y aplicar dicho, al menos uno, parámetro de seguridad del plano de control cuando se proporciona dicha señalización del plano de control a dicho dispositivo de comunicación móvil.

Según otro ejemplo adicional se proporciona un método realizado por un dispositivo de comunicación móvil que puede comunicar datos del plano de usuario a través de un primer aparato de comunicación, de una red de comunicación, que opera una primera celda de comunicación, y que puede recibir señalización del plano de control relacionada con una comunicación del plano de usuario de un segundo aparato de comunicación, de la red de comunicación, que opera una segunda celda de comunicación, comprendiendo dicho método: obtener un primer conjunto de parámetros de seguridad para dicha comunicación del plano de usuario, a partir de un primer procedimiento de acuerdo de clave autenticada (AKA) con respecto a dicho primer aparato de comunicación, y generar un primer contexto de seguridad asociado; obtener un segundo conjunto de parámetros de seguridad para la comunicación del plano de control, a partir de un segundo procedimiento de acuerdo de clave autenticada (AKA) con respecto a dicho segundo aparato de comunicación, y generar un segundo contexto de seguridad asociado; y mantener dicho primer contexto de seguridad y dicho segundo contexto de seguridad.

Según otro ejemplo adicional se proporciona un método realizado por una entidad de comunicación en una red de comunicación en la que un dispositivo de comunicación móvil puede participar en una comunicación del plano de usuario a través de un primer aparato de comunicación que opera una primera celda de comunicación, y en la que el dispositivo de comunicación móvil puede recibir señalización del plano de control relacionada con dicha comunicación del plano de usuario de un segundo aparato de comunicación que opera una segunda celda de comunicación, comprendiendo dicho método: realizar un primer procedimiento de acuerdo de clave autenticada (AKA), con respecto a dicho primer aparato de comunicación, para dicha comunicación del plano de usuario y para generar un primer contexto de seguridad asociado; realizar un segundo procedimiento de acuerdo de clave autenticada (AKA), con respecto a dicho segundo aparato de comunicación, para la comunicación del plano de control y para generar un segundo contexto de seguridad asociado; y mantener dicho primer contexto de seguridad y dicho segundo contexto de seguridad.

Según otro ejemplo adicional se proporciona un sistema de comunicación que comprende un dispositivo de comunicación móvil según un aspecto anterior, un primer aparato de comunicación según un aspecto anterior, y un segundo aparato de comunicación según un aspecto anterior, en donde dicho dispositivo de comunicación móvil se configura para comunicar datos del plano de usuario a través del primer aparato de comunicación y para recibir señalización del plano de control relacionada con dicha comunicación del plano de usuario del segundo aparato de comunicación.

Según otro ejemplo adicional se proporciona un sistema de comunicación que comprende un dispositivo de comunicación móvil según un aspecto anterior, un primer aparato de comunicación según un aspecto anterior, un segundo aparato de comunicación, y una entidad de comunicación según un aspecto anterior, en donde dicho dispositivo de comunicación móvil se configura para comunicar datos del plano de usuario a través del primer aparato de comunicación y para recibir señalización del plano de control relacionada con dicha comunicación del plano de usuario del segundo aparato de comunicación.

Los ejemplos se extienden a productos de programas informáticos como un medio de almacenamiento legible por ordenador que tiene instrucciones almacenadas en el mismo que son operables para programar un procesador programable para llevar a cabo un método como se describe en los aspectos y las posibilidades establecidas anteriormente o mencionadas en las reivindicaciones y/o para programar un ordenador adecuadamente adaptado para proporcionar el apartado mencionado en cualquiera de las reivindicaciones.

Cada característica descrita en esta especificación (cuyo término incluye las reivindicaciones) y/o mostrada en los dibujos puede incorporarse en la invención independientemente de (o en combinación con) cualesquiera otras características descritas y/o ilustradas. En particular, pero sin limitación, las características de cualquiera de las

reivindicaciones dependientes de una reivindicación independiente particular pueden introducirse en esa reivindicación independiente en cualquier combinación o individualmente.

Breve descripción de los dibujos

Las realizaciones de la invención se describirán ahora por medio de ejemplos con referencia solo a las figuras adjuntas en las que:

La Figura 1 ilustra esquemáticamente un sistema de telecomunicación;
La Figura 2 ilustra una jerarquía de claves de encriptación / integridad utilizada en el sistema de telecomunicación de la Figura 1;
La Figura 3 ilustra un esquema de derivación de clave utilizado por una estación base en el sistema de telecomunicación de la Figura 1;
La Figura 4 ilustra un esquema de derivación de clave utilizado por un dispositivo de comunicación móvil en el sistema de telecomunicación de la Figura 1;
La Figura 5 muestra un diagrama de bloques simplificado de un dispositivo de comunicación móvil para el sistema de telecomunicación de la Figura 1;
La Figura 6 muestra un diagrama de bloques simplificado de una “macro” estación base para el sistema de telecomunicación de la Figura 1;
La Figura 7 muestra un diagrama de bloques simplificado de una “pico” estación base para el sistema de telecomunicación de la Figura 1;
La Figura 8 muestra un diagrama de bloques simplificado de una entidad de gestión de la movilidad para el sistema de telecomunicación de la Figura 1;
La Figura 9 muestra un cronograma simplificado que ilustra el funcionamiento del sistema de telecomunicación de la Figura 1 en la realización de un primer procedimiento de seguridad;
La Figura 10 muestra un cronograma simplificado que ilustra el funcionamiento del sistema de telecomunicación de la Figura 1 en la realización de un segundo procedimiento de seguridad;
La Figura 11 muestra un cronograma simplificado que ilustra el funcionamiento del sistema de telecomunicación de la Figura 1 en la realización de un tercer procedimiento de seguridad;
La Figura 12 muestra un cronograma simplificado que ilustra el funcionamiento del sistema de telecomunicación de la Figura 1 en la realización de un cuarto procedimiento de seguridad; y
La Figura 13 muestra un cronograma simplificado que ilustra el funcionamiento del sistema de telecomunicación de la Figura 1 en la realización de un procedimiento de autenticación y acuerdo de clave.

Descripción de las realizaciones

Resumen

La Figura 1 ilustra esquemáticamente un sistema de telecomunicación móvil (celular) 1 en el que un usuario de cualquiera de una pluralidad de dispositivos de comunicación móviles 3-1, 3-2, 3-3 pueden comunicarse con otros usuarios a través de una o más de una pluralidad de estaciones base 5-1, 5-2 y 5-3 y de una red central 110. En el sistema ilustrado en la Figura 1, cada estación base 5 mostrada es una estación base (o ‘eNB’) de la Red de Acceso Radio Terrestre Universal Evolucionada (E-UTRAN) capaz de operar en un entorno de portadora múltiple.

La red central 110 comprende una pluralidad de entidades funcionales/lógicas que incluye una Entidad de Gestión de la Movilidad (MME) 112, un Servidor de Abonado Local (HSS) 114, y un Centro de Autenticación (AuC) 116.

La MME 112 es un nodo de control de clave para la red de acceso LTE. Es responsable, entre otras cosas, de autenticar al usuario (interactuando con el HSS 114). La señalización del Estrato de No Acceso (NAS) termina en la MME 112. La MME 112 es también el punto de terminación en la red para el cifrado / protección de la integridad para la señalización NAS y maneja la gestión de claves de seguridad.

El HSS 114 comprende una base de datos central que contiene información relacionada con el usuario y relacionada con la suscripción. La función del HSS 114 incluye funcionalidades como gestión de la movilidad, soporte de establecimiento de llamada y de sesión, autenticación de usuario y autorización de acceso. El HSS 114, en esta realización ilustrativa, incluye la funcionalidad del AuC 116 (aunque esta podría proporcionarse por separado). La función del AuC 116 proporciona la autenticación de cada dispositivo de comunicación móvil 3 (o más específicamente la tarjeta del módulo de identidad del abonado (SIM) asociada) que intenta conectarse a la red central 110 (p. ej., cuando el dispositivo de comunicación móvil está encendido). Una vez que la autenticación es exitosa, el HSS 114 gestiona la SIM y los servicios como se describió anteriormente. Como se describe con más detalle a continuación, una clave de encriptación también es generada por la función del AuC 116 que posteriormente se utiliza para encriptar todas las comunicaciones inalámbricas (voz, SMS, etc.) entre el dispositivo de comunicación móvil 3 y la red central 110.

En la Figura 1, la estación base etiquetada 5-1 comprende una llamada ‘macro’ estación base que opera una ‘macro’ celda 10-1 relativamente grande geográficamente utilizando una portadora de componente asociada que tiene una primera frecuencia (F1). Las otras estaciones base 5-2, 5-3 mostradas en la Figura 1, cada una comprende una

llamada 'pico' estación base que opera una 'pico' celda respectiva 10-2, 10-3. Cada pico celda 10-2, 10-3 es operada en una portadora de componente respectiva que tiene una banda de frecuencia correspondiente (F2). La potencia utilizada para proveer las pico celdas 10-2, 10-3 es baja en relación con la potencia utilizada para la macro celda 10-1 y las pico celdas 10-2, 10-3 son, por lo tanto, pequeñas en relación a la macro celda 10-1.

La macro estación base 5-1 proporciona señalización de control 13-1 en un plano de control ('plano C') a los dispositivos de comunicación móviles, como un dispositivo de comunicación móvil 3-1, que están ubicados en la macro celda 10-1 que los opera. La macro estación base 5-1 también comunica datos de usuario 11-1 en un plano de usuario ('plano U') a y desde dispositivos de comunicación móviles, como un dispositivo de comunicación móvil 3-1, que están ubicados en la macro celda que los opera.

En el caso de las pico celdas 10-2, 10-3, sin embargo, la provisión del plano U y del plano C se divide entre la macro estación base 5-1 y la pico estación base 5-2 o 5-3 que opera la pico celda 10-2, 10-3. Específicamente, la macro estación base 5-1 proporciona señalización de control 13-2, 13-3, en el plano de control ('plano C'), a dispositivos de comunicación móviles, como un dispositivo de comunicación móvil 3-2 y 3-3, que están ubicados en las pico celdas 10-2 y 10-3 que son operadas por la pico estaciones base 5-2, 5-3. En contraste, cada pico estación base 5-2, 5-3 comunica datos de usuario 11-2, 11-3 en el plano U, con un dispositivo de comunicación móvil respectivo 3-2, 3-3, en la pico celda 10-2, 10-3, que esa pico estación base 5-2, 5-3 opera.

La señalización del plano C incluye, entre otra señalización de control, señalización relacionada con la comunicación del plano U como, por ejemplo, los recursos de control de señalización utilizados para la comunicación del plano de usuario, señalización para controlar el establecimiento y la liberación de las portadoras de comunicación del plano de usuario, y señalización para controlar la movilidad (p. ej., traspaso) de la comunicación del plano de usuario entre celdas.

Con más detalle, la señalización del plano C comprende señalización de control, que incluye señalización de control del recurso radio (RRC), para: difusión de Información del Sistema; paginación; establecimiento, mantenimiento y liberación de una conexión de RRC entre el dispositivo de comunicación móvil 3 y la red; funciones de seguridad que incluyen la gestión de claves; establecimiento, configuración, mantenimiento y liberación de las portadoras de radio punto a punto; funcionales de movilidad (traspaso y re-selección de celda); funciones de gestión de la calidad del servicio (QoS); reporte de medidas y control del reporte; y asignación de recursos para la comunicación del plano U.

La información de seguridad requerida para el cifrado/descifrado (encriptado/des-encriptado) de los datos del plano C (y para la protección de la integridad en el plano C) para cada pico celda 10-2, 10-3 se proporciona a la macro estación base 5-1. La macro estación base 5-1 utiliza la información de seguridad para derivar claves de seguridad apropiadas para el cifrado/descifrado (encriptado/des-encriptado) de la señalización de control para cada dispositivo de comunicación móvil 3-2, 3-3 que está ubicado en cualquiera de las pico celdas 10-2, 10-3.

La información de seguridad requerida para el cifrado/descifrado (encriptado/desencriptado) de los datos del plano U respectivo (y para cualquier protección de la integridad en el plano U) para cada pico celda 10-2, 10-3 se proporciona a la pico estación base 5-2, 5-3 que opera esa pico celda 10-2, 10-3. Cada pico estación base 5-2, 5-3, determina las claves de seguridad apropiadas para el cifrado/descifrado (encriptado/des-encriptado) de los datos de usuario para cada dispositivo de comunicación móvil 3-2, 3-3, que está ubicado en la pico celda 10-2, 10-3 operada por esa estación base 5-2, 5-3.

La información de seguridad requerida para el cifrado/descifrado (encriptado/desencriptado) de los datos del plano C y de los datos del plano U (y cualquier protección de la integridad) también se proporciona a cada dispositivo de comunicación móvil 3. Cada dispositivo de comunicación móvil 3 determina, a partir de la información de seguridad, claves de seguridad apropiadas para el cifrado/descifrado (encriptado/desencriptado) de los datos de usuario y de los datos de control para ese dispositivo.

Cada dispositivo de comunicación móvil 3-2, 3-3 que se comunica a través de una pico celda 10-2, 10-3 también cuenta con una indicación de que el plano C y el plano U se dividen entre la macro y la pico estación base. Esto ayuda beneficiosamente a asegurar que el dispositivo de comunicación móvil 3-2, 3-3 puede realizar un seguimiento de cual estación base 5 es responsable para el plano C y cual estación base 5 es responsable para el plano U. En consecuencia, el dispositivo de comunicación móvil 3-2, 3-3 puede derivar las claves para el cifrado/descifrado (encriptado/desencriptado) de los datos del plano U respectivos (y para cualquier protección de la integridad en el plano U) correctamente aunque la estación base que maneja la comunicación del plano U es diferente de la estación base que proporciona la comunicación del plano C.

Jerarquía de clave de seguridad y derivación de clave

Las Figuras 2 a 4 ilustran una Jerarquía de Clave de Seguridad y Derivación de Clave en el sistema de telecomunicación móvil de la Figura 1.

Específicamente, la Figura 2 ilustra una jerarquía de clave de encriptación / integridad utilizada en el sistema de telecomunicación móvil de la Figura 1. La Figura 3 ilustra un esquema de derivación de clave utilizado por una estación base en el sistema de telecomunicación de la Figura 1, y la Figura 4 ilustra un esquema de derivación de clave utilizado por un dispositivo de comunicación móvil en el sistema de telecomunicación de la Figura 1.

Las Figuras 2 a 4 se basan en una figura similar del Estándar Técnico (TS) del 3GPP 33.401 v 12.6.0 que, como entendería una persona experta, incluye más detalles de los mecanismos de seguridad que son empleados en el sistema de telecomunicación móvil de la Figura 1.

En referencia a las Figuras 2 a 4, el sistema de telecomunicación móvil 1 utiliza un número de parámetros de clave de seguridad que, con fines ilustrativos, puede considerarse que están organizados en una jerarquía en la que las claves en un nivel inferior en la jerarquía pueden derivarse de claves superiores de la jerarquía (posiblemente en combinación con otros parámetros) utilizando una función de derivación de clave (KDF) apropiada. En esta realización ilustrativa, la KDF que se utiliza para derivar las claves de seguridad es la KDF descrita en el TS del 3GPP 33.220 v. 11.4.0 (Anexo B) con entradas como se describe en el TS del 3GPP 33.401 v 12.6.0 (Anexo A).

Como se ve en las Figuras 2 a 4, la información de seguridad utilizada en el sistema de telecomunicación móvil 1 incluye los siguientes parámetros de clave de seguridad:

Parámetros de clave generales:

- K es una clave permanente almacenada en una USIM o en una UICC en un dispositivo de comunicación móvil 3 y en el AuC 116.
- CK e IK ('clave de cifrado' y 'clave de integridad' respectivamente) son un par de claves derivadas en el AuC 116, y en la USIM/UICC, durante un procedimiento de AKA. CK, IK son manejadas de manera diferente dependiendo de si se utilizan en un contexto de seguridad del Sistema de Paquetes Evolucionado o en un contexto de seguridad heredado, como se describe en la sub-cláusula 6.1.2 del TS del 3GPP 33.401.
- K_{ASME} es una clave intermedia que se deriva en el HSS 114, y en el dispositivo de comunicación móvil 3, a partir de CK e IK (y de la identidad de la red de servicio (SNid)).
- K_{eNB} es una clave derivada por el dispositivo de comunicación móvil 3 y por la MME 112 a partir de K_{ASME} (o posiblemente por el dispositivo de comunicación móvil 3 y por el eNB objetivo durante el traspaso).

Claves para el tráfico NAS:

- K_{NASint} es una clave utilizada para la protección del tráfico NAS con un algoritmo de integridad particular. Esta clave es derivada por el dispositivo de comunicación móvil 3 y por la MME 112 a partir de K_{ASME}, así como un identificador para el algoritmo de integridad utilizando una KDF con entradas según lo especificado en la cláusula A.7 del TS del 3GPP 33.401.
- K_{NASenc} es una clave utilizada para la protección del tráfico NAS con un algoritmo de encriptación particular. Esta clave es derivada por el dispositivo de comunicación móvil 3 y por la MME 112 a partir de K_{ASME}, así como un identificador del algoritmo de encriptación, utilizando una KDF con entradas según lo especificado en la cláusula A.7 del TS del 3GPP 33.401.

Claves para el tráfico del plano de usuario:

- K_{UPenc} es una clave utilizada para la protección del tráfico del Plano U con un algoritmo de encriptación particular. Esta clave es derivada por el dispositivo de comunicación móvil 3 y por la macro estación base 5-1 a partir de K_{eNB}, así como un identificador para el algoritmo de encriptación utilizando una KDF con entradas según lo especificado en la cláusula A.7 del TS del 3GPP 33.401. En el caso de división del plano U / plano C entre pico y macro estaciones base como se describió anteriormente, sin embargo, K_{UPenc} se obtiene en la pico estación base 5-2, 5-3 (como se describe con más detalle más adelante) para su uso en la protección del tráfico del Plano U con un algoritmo de encriptación particular.
- K_{UPint} es una clave utilizada para la protección del tráfico del Plano U entre un Nodo de Retransmisión (RN) y un eNB Donante (DeNB) con un algoritmo de integridad particular. Esta clave es derivada por el RN y por el DeNB a partir de K_{eNB}, así como un identificador para el algoritmo de integridad utilizando una KDF con entradas según lo especificado en la cláusula A.7 del TS del 3GPP 33.401.

Claves para el tráfico del plano de control (RRC):

- K_{RRCint} es una clave utilizada para la protección del tráfico de Control del Recurso Radio (RRC) con un algoritmo de integridad particular. K_{RRCint} es derivada por el dispositivo comunicación móvil 3 y por la macro estación base 5-1 a partir de K_{eNB}, así como un identificador para el algoritmo de integridad utilizando una KDF con entradas según lo especificado en la cláusula A.7 del TS del 3GPP 33.401.
- K_{RRCenc} es una clave utilizada para la protección del tráfico de RRC con un algoritmo de encriptación particular. K_{RRCenc} es derivada por el dispositivo de comunicación móvil 3 y por la macro estación base 5-1 a partir de K_{eNB} así como un identificador para el algoritmo de encriptación utilizando una KDF con entradas según lo especificado en la cláusula A.7 del TS del 3GPP 33.401.

Claves intermedias:

- NH ('Siguiente Salto') es una clave derivada por el dispositivo de comunicación móvil 3 y por la MME 112, utilizando una KDF con entradas según lo especificado en la cláusula A.7 del TS del 3GPP 33.401, para proporcionar seguridad hacia adelante (p. ej., durante el traspaso) según lo especificado en la cláusula 7.2.8 del TS del 3GPP 33.401.
- K_{eNB}* es una clave derivada por el dispositivo de comunicación móvil 3, y por una estación base fuente, a partir de NH o del K_{eNB} activo actualmente para su uso en la derivación de clave durante el traspaso / modificación de contexto, utilizando una KDF con entradas según lo especificado en la cláusula A.5 del TS del 3GPP 33.401. Específicamente, en los traspasos, K_{eNB}* se reenvía a una estación base objetivo desde una estación base origen. La estación base objetivo utiliza la K_{eNB}* recibida directamente como la K_{eNB} que se utiliza con el dispositivo de comunicación móvil 3 que se traspasa. En un método de ejemplo, descrito con más detalle más adelante, este parámetro es, favorablemente, reutilizado durante la división del plano C / plano U.

Una serie de otros parámetros notables también se utilizan en la arquitectura de seguridad de la red de telecomunicación móvil 1. Estos incluyen:

- AMF que es un llamado Campo de Gestión Autenticada en una base de datos en el AuC 116, y en la tarjeta SIM del dispositivo de comunicación móvil 3. El AMF se comparte previamente entre el dispositivo de comunicación móvil 3 y el AuC 116 y se utiliza en el cálculo de ciertos parámetros de seguridad (p. ej., MAC y XMAC descritos a continuación).
- OP que es un llamado Campo de Configuración del Algoritmo Variante de Operador, en la base de datos en el AuC 116, y en la tarjeta SIM del dispositivo de comunicación móvil 3.
- SQN que es un número de secuencia que se incrementa cada vez que la red intenta autenticar un dispositivo de comunicación móvil 3.
- RAND que es un número aleatorio para utilizar en la generación de clave y en la autenticación.
- AK que es una llamada clave de anonimato generada en el AuC 116.
- XRES que es una llamada 'respuesta esperada' generada en el AuC 116.
- RES es un parámetro de respuesta, equivalente a XRES, pero generado en el dispositivo de comunicación móvil 3 para enviar a la MME 112 para su comparación con XRES con fines de autenticación.
- MAC es un código de autenticación de mensaje generado en el AuC 116.
- XMAC es el valor del MAC esperado generado en el dispositivo de comunicación móvil 3 para autenticar un mensaje contra un MAC recibido.
- AUTN es un llamado token de autenticación generado en el AuC 116.

Cuando una MME 112 recibe una solicitud adjunta de un dispositivo de comunicación móvil 3, la MME 112 envía la solicitud de datos de autenticación al AuC/HSS 116/114. Después de la derivación de RAND, XRES, CK, IK, y AUTN el AuC 116 los combina en un llamado vector de autenticación (AV = RAND || XRES || CK || IK || AUTN) que se envía a la MME 112. La MME 112 puede entonces recuperar los parámetros individuales a partir del AV para enviarlos al dispositivo de comunicación móvil durante un proceso de autenticación y de generación de clave como se describe con más detalle a continuación.

Para cifrar / descifrar los datos del plano de usuario se utiliza una función de cifrado que tiene, como entradas: K_{UPenc}; información que identifica la portadora radio utilizada para la comunicación ('PORTADORA'); un indicador de un solo bit de la dirección de la comunicación ('DIRECCIÓN'); la longitud del flujo de claves requerida ('LONGITUD') y un valor de 32-bit específico de portadora, pero dependiente del tiempo y de la dirección, de un contador incremental ('CONTADOR') que corresponde al CONTADOR PDCP de 32-bit mantenido en la capa PDCP para el dispositivo de comunicación móvil 3 y la pico estación base 5-2, 5-3.

Dispositivo de comunicación móvil

La Figura 5 es un diagrama de bloques que ilustra los componentes principales de los dispositivos de comunicación móviles 3 mostrados en la Figura 1. Cada dispositivo de comunicación móvil 3 comprende un teléfono móvil (o 'celda') capaz de operar en un entorno de portadora múltiple. El dispositivo de comunicación móvil 3 comprende un circuito transceptor 510 que es operable para transmitir señales a, y para recibir señales de, las estaciones base 5 a través de al menos una antena 512. El dispositivo de comunicación móvil 3 comprende un interfaz de usuario 514 a través del cual un usuario puede interactuar con el dispositivo (p. ej., una pantalla táctil, teclado, micrófono, altavoz y/o similares).

El dispositivo de comunicación móvil incluye un módulo de identidad del abonado (SIM) 530 en la forma de un SIM Universal (USIM) que se ejecuta en una Tarjeta de Circuito Integrado Universal (UICC). El SIM 530 comprende un módulo de seguridad USIM/UICC 532 para obtener y almacenar la clave permanente 'K' 534-1 que, en funcionamiento, se utiliza para generar los otros parámetros de seguridad utilizados para la seguridad de la comunicación. El módulo de seguridad USIM/UICC 532 es también operable para derivar otros parámetros de seguridad 534-2 como la clave

de cifrado (CK) y la clave de integridad (IK) utilizando 'K' y un valor 'aleatorio' (p. ej., un valor de RAND proporcionado por el AuC 116 a través de la MME 112). El SIM 530 tiene una identidad 536 en la forma de una identidad de abonado móvil internacional (IMSI).

El funcionamiento del circuito transceptor 510 es controlado por un controlador 516 de acuerdo con el software almacenado en la memoria 518.

El software incluye, entre otras cosas, un sistema operativo 520, un módulo de control de comunicación 522 y un módulo de gestión de seguridad 525.

El módulo de control de comunicación 522 se configura para gestionar la comunicación con la macro y/o pico estaciones base 5 en las portadoras de componente asociadas. El módulo de control de comunicación 522 se configura para gestionar la comunicación NAS con la MME 112 (indirectamente a través de la estación base). El módulo de control de comunicación 522 incluye un módulo del plano U 523 para manejar los datos de usuario y un módulo del plano C 524 para manejar la señalización de control como los mensajes de control del recurso radio.

El módulo de gestión de seguridad 525 se configura para gestionar la seguridad de la comunicación incluyendo la realización de procedimientos de autenticación, la generación y utilización de clave y del parámetro de seguridad relacionado, y la autenticación y el acuerdo de clave (AKA) en la medida que son realizados en el dispositivo de comunicación móvil 3. El módulo de gestión de seguridad 525 puede manejar la recuperación/generación de parámetros apropiados 526 para su uso en procedimientos de autenticación / generación de clave. Estos parámetros incluyen: parámetros UICC/USIM 526-1 recuperados del SIM 530 (p. ej., parámetros 534-2 como CK e IK derivados por el SIM 530); parámetros 526-2 recibidos de otras fuentes (p. ej., parámetros como AUTN y RAND recibidos de la MME 112 en la señalización de Estrato Sin Acceso (NAS)); y parámetros 526-3 que pueden ser derivados en el dispositivo de comunicación móvil (p. ej., K_{ASME}, K_{NASint}, K_{NASenc}, K_{eNB}, K_{eNB}*, NH, K_{UPenc}, K_{RRCint}, K_{RRCenc}, etc.). El módulo de gestión de seguridad 525 también incluye un módulo AKA 528 para gestionar procedimientos AKA en la medida en que los realiza el dispositivo de comunicación móvil 3.

Macro estación base

La Figura 6 es un diagrama de bloques que ilustra los componentes principales de la macro estación base 5-1 mostrada en la Figura 1. La macro estación base 5-1 comprende una estación base capaz de portadora múltiple de E-UTRAN que comprende un circuito transceptor 610 que es operable para transmitir señales a, y para recibir señales de, los dispositivos de comunicación móviles 3 a través de al menos una antena 612. La estación base 5-1 también es operable para transmitir señales a, y para recibir señales de: la MME 112 de la red central 110 a través de un interfaz (S1) de la MME 614; y otras estaciones base 5 a través de un interfaz (X2) del eNB 616.

El funcionamiento del circuito transceptor 610 es controlado por un controlador 616 de acuerdo con el software almacenado en la memoria 618.

El software incluye, entre otras cosas, un sistema operativo 620, un módulo de control de comunicación 622 y un módulo de gestión de seguridad 625.

El módulo de control de comunicación 622 se configura para gestionar la comunicación entre la macro estación base 5-1 y los dispositivos de comunicación móviles 3 que operan dentro del área geográfica cubierta por la macro celda 10-1. El módulo de control de comunicación 622 se configura también para gestionar la señalización S1-AP entre la macro estación base 5-1 y la MME 112 y la señalización X2-AP entre la macro estación base 5-1 y otras estaciones base.

El módulo de control de comunicación 622 incluye un módulo del plano U 623 para manejar los datos de usuario para el dispositivo de comunicación móvil 3-1 que se comunica a través de la macro celda 10-1. El módulo de control de comunicación 622 también incluye un módulo del plano C 624 para generar señalización de control, como mensajes de control del recurso radio (RRC), para la transmisión al dispositivo de comunicación móvil 3-1 que se comunica a través de la macro celda 10-1 y para los dispositivo de comunicación móviles 3-2 y 3-3 que comunican los datos de usuario a través de las pico celdas 10-2, 10-3 respectivas.

El módulo de gestión de seguridad 625 se configura para gestionar la seguridad de la comunicación incluyendo la realización de procedimientos de autenticación, la generación y utilización de clave y del parámetro de seguridad relacionado, y procedimientos de autenticación y de acuerdo de clave (AKA) en la medida que son realizados en la macro estación base 5-1.

El módulo de gestión de seguridad 625 puede manejar la recepción/generación de parámetros apropiados 626 para su uso en procedimientos de autenticación / generación de clave. Estos parámetros 626 incluyen parámetros 626-1 recibidos de otras fuentes (p. ej., K_{eNB} o NH recibidos de la MME 112, o K_{eNB}* recibido de una estación base fuente durante el traspaso). Los parámetros 626 también incluyen parámetros 626-2 que pueden ser derivados en la macro estación base 5-1 durante el funcionamiento normal (p. ej., K_{UPenc}, K_{RRCint}, K_{RRCenc}) o durante el traspaso (p. ej., K_{eNB}*

cuando opera como un nodo fuente o K_{eNB} (= K_{eNB}*) cuando opera como un nodo destino etc.). El módulo de gestión de seguridad 625 también incluye un módulo AKA 628 para manejar procedimientos AKA en la medida en que los realiza la macro estación base 5-1.

Pico estación base

La Figura 7 es 7 es un diagrama de bloques que ilustra los componentes principales de una pico estación base 5-2, 5-3 mostrada en la Figura 1. La pico estación base 5-2, 5-3 comprende una estación base capaz de portadora múltiple de E-UTRAN que comprende un circuito transceptor 710 que es operable para transmitir señales a, y para recibir señales de, los dispositivos de comunicación móviles 3 a través de al menos una antena 712. La pico estación base 5-2, 5-3 también es operable para transmitir señales a, y para recibir señales de: la MME 112 de la red central 110 a través de un interfaz (S1) de la MME 714; y otras estaciones base a través de un interfaz (X2) del eNB 716.

El funcionamiento del circuito transceptor 710 es controlado por un controlador 716 de acuerdo con el software almacenado en la memoria 718.

El software incluye, entre otras cosas, un sistema operativo 720, un módulo de control de comunicación 722 y un módulo de gestión de seguridad 725.

El módulo de control de comunicación 722 se configura para gestionar la comunicación entre la pico estación base 5-2, 5-3 y los dispositivos de comunicación móviles 3-2, 3-3 que se comunicación a través de la pico celda 10-2, 10-3. El módulo de control de comunicación 722 se configura también para gestionar la señalización S1-AP entre la pico estación base 5-2, 5-3 y la MME 112 y la señalización X2-AP entre la pico estación base 5-2, 5-3 y otras estaciones base.

El módulo de control de comunicación 722 incluye un módulo del plano U 723 para manejar los datos de usuario para un dispositivo de comunicación móvil 3-2, 3-3 que se comunica a través de la pico celda 10-2, 10-3.

El módulo de gestión de seguridad 725 se configura para gestionar la seguridad de la comunicación incluyendo la realización de procedimientos de autenticación, la generación y utilización de clave y del parámetro de seguridad relacionado, y procedimientos de autenticación y de acuerdo de clave (AKA) en la medida que son realizados en la pico estación base 5-2, 5-3.

El módulo de gestión de seguridad 725 puede manejar la recepción/generación de parámetros apropiados 726 para su uso en procedimientos de autenticación / generación de clave. Estos parámetros 726 incluyen parámetros 726-1 recibidos de otras fuentes (p. ej., K_{eNB} en esta realización). Los parámetros 726 también incluyen parámetros 726-2 que pueden ser derivados en la pico estación base 5-2, 5-3 (p. ej., K_{UPenc}). El módulo de gestión de seguridad 725 también incluye un módulo AKA 728 para manejar los procedimientos AKA en la medida en que los realiza la pico estación base 5-2, 5-3.

MME

La Figura 8 es un diagrama de bloques que ilustra los componentes principales de la entidad de gestión de la movilidad (MME) 112 mostrada en la Figura 1. La MME 112 comprende un circuito transceptor 810 que es operable para transmitir señales a, y para recibir señales de, otros dispositivos de red (como el HSS) a través de un interfaz de entidad de red asociada 812. El circuito transceptor 810 también es operable para transmitir señales a, y para recibir señales de, una estación base 5 a través de un interfaz (S1) del eNB 816 que incluye la señalización S1-AP para la estación base 5, y señalización NAS, que es transparente para la estación base, para el dispositivo de comunicación móvil 3.

El funcionamiento del circuito transceptor 810 es controlado por un controlador 816 de acuerdo con el software almacenado en la memoria 818.

El software incluye, entre otras cosas, un sistema operativo 820, un módulo de control de comunicación 822 y un módulo de gestión de seguridad 825.

El módulo de control de comunicación 822 se configura para gestionar la señalización NAS entre la MME 112 y los dispositivos de comunicación móviles 3 y la señalización S1-AP entre la MME 112 y la estación base 5.

El módulo de gestión de seguridad 825 se configura para gestionar la seguridad de la comunicación incluyendo la realización de procedimientos de autenticación, la generación y utilización de clave y del parámetro de seguridad relacionado, y procedimientos de autenticación y de acuerdo de clave (AKA) en la medida que son realizados en la MME 112.

El módulo de gestión de seguridad 825 puede manejar la recepción/generación de parámetros apropiados 826 para su uso en procedimientos de autenticación / generación de clave. Estos parámetros 826 incluyen parámetros 826-1 recibidos de otras fuentes (p. ej., CK, IK, AUTN, K_{ASME}, RAND, XRES recuperados a partir de un AV recibido del

HSS/AuC 114/116 etc.). Los parámetros 826 también incluyen parámetros 826-2 que pueden ser derivados en la MME (p. ej., K_{NASint}, K_{NASenc}, K_{eNB}, NH etc.). El módulo de gestión de seguridad 825 también incluye un módulo AKA 828 para manejar procedimientos AKA en la medida en que los realiza la MME 112.

Resumen del funcionamiento - provisión de parámetros de seguridad

Las Figuras 9 a 13 muestran cronogramas simplificados cada una ilustrando el funcionamiento del sistema de telecomunicación de la Figura 1 en la realización de una variación respectiva de un procedimiento de seguridad. Como apreciarán los expertos en la técnica, los cronogramas solo muestran la señalización que es particularmente relevante para la seguridad. Generalmente se producirá otra señalización pero, por razones de claridad, se ha omitido de los cronogramas simplificados.

Como se ve en las Figuras 9 a 13, cada procedimiento de seguridad ilustrado utiliza un mecanismo respectivo diferente para asegurar que los parámetros de seguridad apropiados (en particular valores apropiados de K_{UPenc}) se usan de manera consistente para la protección del plano U tanto en el dispositivo de comunicación móvil 3 como en la estación base.

Mientras que los diferentes procedimientos de seguridad ilustrados en las Figuras 9 a 13 se muestran por separado, se apreciará que características clave de los procedimientos de seguridad pueden combinarse, donde sea apropiado, o proporcionarse como opciones de implementación alternativas en un sistema desplegado.

MME basada en la provisión de K_{eNB}

La Figura 9 muestra un cronograma simplificado que ilustra el funcionamiento del sistema de telecomunicación de la Figura 1 en la realización de un primer procedimiento de seguridad en el que parámetros de seguridad apropiados, y en particular valores apropiados de K_{UPenc}, se generan en la pico estación base 5-2, 5-3 en respuesta a la señalización de la MME 112.

Al comienzo del procedimiento de seguridad ilustrado, un dispositivo de comunicación móvil 3 que desea iniciar la comunicación en la pico celda 5-1, 5-2 envía un mensaje de estrato sin acceso (NAS) solicitando conexión (p. ej., un mensaje de 'SOLICITUD DE CONEXIÓN NAS') a la MME 112 (de manera transparente a través de las macro estaciones base 5-1) en S910 que incluye información que identifica la tarjeta SIM 530 del dispositivo de comunicación móvil 3 (p. ej., 'la identidad de abonado móvil internacional (IMSI)').

La MME 112 responde a esta petición, en S912, enviando un mensaje solicitando autenticación e incluyendo información que identifica la tarjeta SIM 530 al HSS 114 (p. ej., un mensaje de 'SOLICITUD DE DATOS DE AUTENTICACIÓN'). La función del AuC 116 del HSS 114 deriva RAND, XRES, CK, IK, AUTN y los combina para formar un vector de autenticación para la tarjeta SIM 530 (AV = RAND || XRES || CK || IK || AUTN) en S914 y envía el AV generado a la MME 112 en S916 (p. ej., en un mensaje de 'RESPUESTA DE DATOS DE AUTENTICACIÓN').

La MME 112 recupera IK, CK, XRES, RAND y AUTN del AV en S918 y envía los parámetros AUTN y RAND al dispositivo de comunicación móvil 3 utilizando señalización NAS en S920 (p. ej., en un mensaje de 'SOLICITUD DE AUTENTICACIÓN NAS').

El dispositivo de comunicación móvil 3 responde, en S922, autenticando la red utilizando el AUTN recibido, y derivando los parámetros relacionados con la seguridad apropiados (IK, CK, RES etc.) utilizando la clave de seguridad permanente almacenada 'K' y los parámetros AUTN y RAND recibidos (y cualquier otro parámetro donde sea necesario - p. ej., AMF para la determinación de XMAC). Suponiendo que la autenticación es exitosa, el dispositivo de comunicación móvil 3 envía el valor calculado de RES a la MME 112 en S924 (p. ej., en un mensaje de 'RESPUESTA DE AUTENTICACIÓN NAS').

La MME 112 comprueba el valor de RES recibido contra XRES en S926, restablece el contador NAS del enlace descendente, y deriva los valores de K_{ASME}, K_{eNB}, K_{NASint} y K_{NASenc}. La MME 112 inicia entonces la seguridad de señalización NAS entre la MME 112 y el dispositivo de comunicación móvil 3, en S928, enviando un mensaje de COMANDO DEL MODO DE SEGURIDAD NAS que informa al dispositivo de comunicación móvil 3 de los algoritmos respectivos a utilizar para la protección de la integridad y el (des)cifrado.

El dispositivo de comunicación móvil 3 responde, en S930, derivando los valores de K_{ASME}, K_{eNB}, K_{NASint} y K_{NASenc} y luego, en S932, enviando un mensaje de respuesta que informa a la MME 112 que la inicialización de seguridad de señalización NAS está completa.

El método continúa iniciando la configuración del contexto de seguridad tanto en la pico estación base 5-2, 5-3, como en la macro estación base 5-1, enviando mensajes de aplicación S1 (S1-AP) sustancialmente duplicados (p. ej., mensajes de 'SOLICITUD DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP') a la pico estación base 5-2, 5-3 en S934, y a la macro estación base 5-1 en S936. Cada uno de los mensajes S1-AP incluye el valor derivado de K_{eNB} y los detalles de las capacidades de seguridad para el dispositivo de comunicación móvil 3.

La pico estación base 5-2, 5-3 luego deriva, en S938, los parámetro(s) de seguridad requeridos para el cifrado/descifrado del plano U (p. ej., K_{UPenc}) a partir del K_{eNB} recibido. De manera similar, la macro estación base 5-1 deriva, en S940, los parámetro(s) de seguridad requeridos para el cifrado/descifrado del plano C (p. ej., K_{RRCint} y K_{RRCenc}) a partir del K_{eNB} recibido.

En S942, suponiendo que la configuración del contexto de seguridad en la pico estación base 5-2, 5-3 es exitosa, la pico estación base 5-2, 5-3 confirma esto a la MME 112 en una mensaje S1-AP apropiado (p. ej., un mensaje 'RESPUESTA DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP').

La macro estación base 5-1 luego inicia, en S944, una configuración del contexto de seguridad RRC (y del plano de usuario) en el dispositivo de comunicación móvil 3 utilizando señalización RRC (p. ej., un mensaje de 'COMANDO DEL MODO DE SEGURIDAD RRC') que incluye información que identifica los algoritmos utilizados para la protección de la integridad y/o el cifrado, y una información que indica que el plano U y el plano C están divididos (p. ej., en la forma de un elemento de información (IE) dedicado, un IE modificado, o reutilización de un IE existente).

El dispositivo de comunicación móvil 3 responde, en S946, inicializando el contexto de seguridad RRC para la comunicación con la macro estación base 5-1 derivando los valores de K_{RRCint}, K_{RRCenc} a partir del valor previamente calculado de K_{eNB} para su uso con la señalización de control de la macro estación base 5-1. El dispositivo de comunicación móvil 3 también inicializa el contexto de seguridad del plano U para la comunicación con la pico estación base 5-2, 5-3 derivando el valor de K_{UPenc} a partir de K_{eNB} para su uso con la señalización del plano de usuario para/de la pico estación base 5-2, 5-3.

Suponiendo que la configuración del contexto de seguridad es exitosa, el dispositivo de comunicación móvil 3 confirma esto, en S932, enviando un mensaje de respuesta apropiado a la macro estación base 5-1 (p. ej., un mensaje de 'MODO DE SEGURIDAD RRC COMPLETO') en S950.

La macro estación base 5-1 confirma, en S952, la exitosa configuración del contexto de seguridad a la MME 112 en un mensaje S1-AP apropiado (p. ej., un mensaje de 'SOLICITUD DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP').

Una vez que los distintos contextos de seguridad (NAS y AS) se han inicializado con éxito en los distintos dispositivos, las conexiones de señalización de control y de usuario se pueden configurar en S954 y el dispositivo de comunicación móvil 3 puede comenzar una comunicación en la que, la señalización del plano de control (S956) es proporcionada por la macro estación base 5-1 y la señalización del plano U es proporcionada a través de la pico estación base 5-2, 5-3 (S958).

Por lo tanto, de manera ventajosa, este método proporciona un modo eficiente de proporcionar una seguridad de la comunicación apropiada, donde diferentes estaciones base son responsables de la señalización del plano U y de la señalización del plano C respectivamente. El dispositivo de usuario puede mantener un contexto de seguridad apropiado tanto para el Plano U como para el plano C permitiendo así cifrar/descifrar los datos de usuario y los datos de control correctamente y hacer seguimiento de los parámetros de seguridad (claves) utilizados en las diferentes estaciones base.

Este enfoque tiene la ventaja sobre los otros métodos descritos en la presente memoria, que evita la necesidad de modificar la señalización de estación base a estación base (sobre el X2 o posiblemente un nuevo interfaz) y el incremento asociado de la complejidad X2-AP. Sin embargo, los otros métodos descritos en la presente memoria tienen la ventaja de que se evita la duplicación de señalización S1 y por lo tanto, se reduce la sobrecarga de señalización S1.

Estación base basada en la provisión de K_{eNB}

La Figura 10 muestra un cronograma simplificado que ilustra el funcionamiento del sistema de telecomunicación de la Figura 1 en la realización de un segundo procedimiento de seguridad en el que se generan parámetros de seguridad apropiados, y en particular valores de K_{UPenc} apropiados, en la pico estación base 5-2, 5-3 en respuesta a la señalización de la macro estación base 5-1.

Al comienzo del procedimiento de seguridad ilustrado en la Figura 10, un dispositivo de comunicación móvil 3 que desea iniciar una comunicación en la pico celda 5-1, 5-2 envía un mensaje de estrato sin acceso (NAS) solicitando conexión (p. ej., un mensaje de 'SOLICITUD DE CONEXIÓN NAS') a la MME 112 (de manera transparente a través de las macro estaciones base 5-1) en S1010 que incluye información que identifica la tarjeta SIM 530 del dispositivo de comunicación móvil 3 (p. ej., 'la identidad de abonado móvil internacional (IMSI)').

La MME 112 responde a esta petición, en S1012, enviando un mensaje solicitando autenticación e incluyendo información que identifica la tarjeta SIM 530 al HSS 114 (p. ej., un mensaje de 'SOLICITUD DE DATOS DE AUTENTICACIÓN'). La función del AuC 116 del HSS 114 deriva RAND, XRES, CK, IK, AUTN y los combina para

formar un vector de autenticación para la tarjeta SIM 530 (AV = RAND || XRES || CK || IK || AUTN) en S1014 y envía el AV generado a la MME 112 en S1016 (p. ej., en un mensaje de 'RESPUESTA DE DATOS DE AUTENTICACIÓN').

La MME 112 recupera IK, CK, XRES, RAND y AUTN del AV en S1018 y envía los parámetros AUTN y RAND al dispositivo de comunicación móvil 3 utilizando señalización NAS en S1020 (p. ej., en un mensaje de 'SOLICITUD DE AUTENTICACIÓN NAS').

El dispositivo de comunicación móvil 3 responde, en S1022, autenticando la red utilizando el AUTN recibido, y derivando los parámetros relacionados con la seguridad apropiados (IK, CK, RES etc.) utilizando la clave de seguridad permanente almacenada 'K' y los parámetros AUTN y RAND recibidos (y cualquier otro parámetro donde sea necesario - p. ej., AMF para la determinación de XMAC). Suponiendo que la autenticación es exitosa, el dispositivo de comunicación móvil 3 envía el valor calculado de RES a la MME 112 en S1024 (p. ej., en un mensaje de 'RESPUESTA DE AUTENTICACIÓN NAS').

La MME 112 comprueba el valor de RES recibido contra XRES en S1026, restablece el contador NAS del enlace descendente, y deriva los valores de K_{ASME}, K_{eNB}, K_{NASint} y K_{NASenc}. La MME 112 inicia entonces la seguridad de señalización NAS entre la MME 112 y el dispositivo de comunicación móvil 3, en S1028, enviando un mensaje de COMANDO DEL MODO DE SEGURIDAD NAS que informa al dispositivo de comunicación móvil 3 de los algoritmos respectivos a utilizar para la protección de la integridad y el (des)cifrado.

El dispositivo de comunicación móvil 3 responde, en S1030, derivando los valores de K_{ASME}, K_{eNB}, K_{NASint} y K_{NASenc} y luego, en S1032, enviando un mensaje de respuesta que informa a la MME 112 que la inicialización de seguridad de señalización NAS está completa.

El método continúa iniciando la configuración del contexto de seguridad en la macro estación base 5-1, enviando un mensaje de aplicación S1 (S1-AP) (p. ej., un mensaje de 'SOLICITUD DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP') a la macro estación base 5-1 en S1034. El mensaje S1-AP incluye el valor derivado de K_{eNB} y los detalles de las capacidades de seguridad para el dispositivo de comunicación móvil 3.

La macro estación base 5-1 inicia la configuración del contexto de seguridad en la pico estación base 5-2, 5-3, enviando un mensaje de aplicación X2 (X2-AP) (p. ej., un nuevo mensaje de 'CONFIGURACIÓN DEL CONTEXTO X2-AP') a la pico estación base 5-2, 5-3 en S1036. El mensaje X2-AP incluye el valor derivado de K_{eNB} y los detalles de las capacidades de seguridad para el dispositivo de comunicación móvil 3.

La pico estación base 5-2, 5-3 luego deriva, en S1038, los parámetro(s) de seguridad requeridos para el cifrado/descifrado del plano U (p. ej., K_{UPenc}) a partir del K_{eNB} recibido de la macro estación base 5-1. De manera similar, la macro estación base 5-1 deriva, en S1040, los parámetro(s) de seguridad requeridos para el cifrado/descifrado del plano C (p. ej., K_{RRCint} y K_{RRCenc}) a partir del K_{eNB} recibido de la MME 112.

En S1042, suponiendo que la configuración del contexto de seguridad en la pico estación base 5-2, 5-3 es exitosa, la pico estación base 5-2, 5-3 confirma esto a la macro estación base 5-1 en un mensaje X2-AP apropiado (p. ej., un mensaje 'RESPUESTA DE CONFIGURACIÓN DEL CONTEXTO X2-AP').

La macro estación base 5-1 luego inicia, en S1044, una configuración del contexto de seguridad RRC (y del plano de usuario) en el dispositivo de comunicación móvil 3 utilizando señalización RRC (p. ej., un mensaje de 'COMANDO DEL MODO DE SEGURIDAD RRC') que incluye información que identifica los algoritmos utilizados para la protección de la integridad y/o el cifrado, y una información que indica que el plano U y el plano C están divididos (p. ej., en la forma de un elemento de información (IE) dedicado, un IE modificado, o reutilización de un IE existente).

El dispositivo de comunicación móvil 3 responde, en S1046, inicializando el contexto de seguridad RRC para la comunicación con la macro estación base 5-1 derivando los valores de K_{RRCint}, K_{RRCenc} a partir del valor previamente calculado de K_{eNB} para su uso con la señalización de control de la macro estación base 5-1. El dispositivo de comunicación móvil 3 también inicializa el contexto de seguridad del plano U para la comunicación con la pico estación base 5-2, 5-3 derivando el valor de K_{UPenc} a partir de K_{eNB} para su uso con la señalización del plano de usuario para/de la pico estación base 5-2, 5-3.

Suponiendo que la configuración del contexto de seguridad es exitosa, el dispositivo de comunicación móvil 3 confirma esto, en S1032, enviando un mensaje de respuesta apropiado a la macro estación base 5-1 (p. ej., un mensaje de 'MODO DE SEGURIDAD RRC COMPLETO') en S1050.

La macro estación base 5-1 confirma, en S1052, la exitosa configuración del contexto de seguridad a la MME 112 en un mensaje S1-AP apropiado (p. ej., un mensaje de 'SOLICITUD DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP').

Una vez que los distintos contextos de seguridad (NAS y AS) se han inicializado con éxito en los distintos dispositivos, las conexiones de señalización de control y de usuario se pueden configurar en S1054 y el dispositivo de comunicación móvil 3 puede comenzar una comunicación en la que, la señalización del plano de control (S1056) es proporcionada por la macro estación base 5-1 y la señalización del plano U es proporcionada a través de la pico estación base 5-2, 5-3 (S1058).

Por lo tanto, de manera ventajosa, este método proporciona otro modo eficiente de proporcionar una seguridad de la comunicación apropiada, donde diferentes estaciones base son responsables de la señalización del plano U y de la señalización del plano C respectivamente. El dispositivo de usuario puede mantener un contexto de seguridad apropiado tanto para el Plano U como para el plano C permitiendo así cifrar/descifrar los datos de usuario y los datos de control correctamente y hacer seguimiento de los parámetros de seguridad (claves) utilizados en las diferentes estaciones base.

Informar al dispositivo de comunicación móvil de la división del plano C/plano U de esta manera, proporciona un modo eficiente de asegurar que el dispositivo de comunicación móvil tiene la información requerida para establecer que se requiere la derivación del parámetro de seguridad del plano de usuario (K_{UPenc}) para la comunicación con la pico celda.

Este enfoque tiene la ventaja sobre el primer método descrito en la presente memoria, que evita la duplicación de señalización S1 y por tanto reduce la sobrecarga de señalización S1. Sin embargo, el primer método tiene la ventaja de que evita la necesidad de modificar la señalización de estación base a estación base (sobre el X2 o posiblemente un nuevo interfaz) y el incremento asociado de la complejidad X2-AP.

Estación base basada en la provisión de K_{UPenc}

La Figura 11 muestra un cronograma simplificado que ilustra el funcionamiento del sistema de telecomunicación de la Figura 1 en la realización de un tercer procedimiento de seguridad, en el que se generan parámetros de seguridad apropiados, y en particular valores de K_{UPenc} apropiados, en la macro estación base 5-1 en respuesta a la señalización de la MME 112, y se reenvían a la pico estación base 5-2, 5-3 sobre el interfaz X2.

Al comienzo del procedimiento de seguridad ilustrado en la Figura 11, un dispositivo de comunicación móvil 3 que desea iniciar una comunicación en la pico celda 5-1, 5-2 envía un mensaje de estrato sin acceso (NAS) solicitando conexión (p. ej., un mensaje de 'SOLICITUD DE CONEXIÓN NAS') a la MME 112 (de manera transparente a través de las macro estaciones base 5-1) en S1110 que incluye información que identifica la tarjeta SIM 530 del dispositivo de comunicación móvil 3 (p. ej., 'la identidad de abonado móvil internacional (IMSI)').

La MME 112 responde a esta petición, en S1112, enviando un mensaje solicitando autenticación e incluyendo información que identifica la tarjeta SIM 530 al HSS 114 (p. ej., un mensaje de 'SOLICITUD DE DATOS DE AUTENTICACIÓN'). La función del AuC 116 del HSS 114 deriva RAND, XRES, CK, IK, AUTN y los combina para formar un vector de autenticación para la tarjeta SIM 530 (AV = RAND || XRES || CK || IK || AUTN) en S1114 y envía el AV generado a la MME 112 en S1116 (p. ej., en un mensaje de 'RESPUESTA DE DATOS DE AUTENTICACIÓN').

La MME 112 recupera IK, CK, XRES, RAND y AUTN del AV en S1118 y envía los parámetros AUTN y RAND al dispositivo de comunicación móvil 3 utilizando señalización NAS en S1120 (p. ej., en un mensaje de 'SOLICITUD DE AUTENTICACIÓN NAS').

El dispositivo de comunicación móvil 3 responde, en S1122, autenticando la red utilizando el AUTN recibido, y derivando los parámetros relacionados con la seguridad apropiados (IK, CK, RES etc.) utilizando la clave de seguridad permanente almacenada 'K' y los parámetros AUTN y RAND recibidos (y cualquier otro parámetro donde sea necesario - p. ej., AMF para la determinación de XMAC). Suponiendo que la autenticación es exitosa, el dispositivo de comunicación móvil 3 envía el valor calculado de RES a la MME 112 en S1124 (p. ej., en un mensaje de 'RESPUESTA DE AUTENTICACIÓN NAS').

La MME 112 comprueba el valor de RES recibido contra XRES en S1126, restablece el contador NAS del enlace descendente, y deriva los valores de K_{ASME}, K_{eNB}, K_{NASint} y K_{NASenc}. La MME 112 inicia entonces la seguridad de señalización NAS entre la MME 112 y el dispositivo de comunicación móvil 3, en S1128, enviando un mensaje de COMANDO DEL MODO DE SEGURIDAD NAS que informa al dispositivo de comunicación móvil 3 de los algoritmos respectivos a utilizar para la protección de la integridad y el (des)cifrado.

El dispositivo de comunicación móvil 3 responde, en S1130, derivando los valores de K_{ASME}, K_{eNB}, K_{NASint} y K_{NASenc} y luego, en S1132, enviando un mensaje de respuesta que informa a la MME 112 que la inicialización de seguridad de señalización NAS está completa.

El método continúa iniciando la configuración del contexto de seguridad en la macro estación base 5-1, enviando un mensaje de aplicación S1 (S1-AP) (p. ej., un mensaje de 'SOLICITUD DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP') a la macro estación base 5-1 en S1134. El mensaje S1-AP incluye el valor derivado de K_{eNB} y los detalles de las capacidades de seguridad para el dispositivo de comunicación móvil 3.

La macro estación base 5-1 deriva, en S1140, los parámetro(s) de seguridad requeridos para la protección del plano C (p. ej., K_{RRCint} y K_{RRCenc}) y para la protección del plano U (p. ej., K_{UPenc}) a partir del K_{eNB} recibido de la MME 112.

La macro estación base 5-1 inicia la configuración del contexto de seguridad en la pico estación base 5-2, 5-3, enviando un mensaje de aplicación X2 (X2-AP) (p. ej., un nuevo mensaje de 'CONFIGURACIÓN DEL CONTEXTO X2-AP') a la pico estación base 5-2, 5-3 en S1136. El mensaje X2-AP incluye el valor derivado de K_{UPenc} y los detalles de las capacidades de seguridad para el dispositivo de comunicación móvil 3.

La pico estación base 5-2, 5-3, al recibir el K_{UPenc} de la macro estación base 5-1, y suponiendo que la configuración del contexto de seguridad en la pico estación base 5-2, 5-3 es exitosa, confirma esto a la macro estación base 5-1 en un mensaje X2-AP apropiado (p. ej., un mensaje de 'RESPUESTA DE CONFIGURACIÓN DEL CONTEXTO X2-AP') en S1142.

La macro estación base 5-1 luego inicia, en S1144, una configuración del contexto de seguridad RRC (y del plano de usuario) en el dispositivo de comunicación móvil 3 utilizando señalización RRC (p. ej., un mensaje de 'COMANDO DEL MODO DE SEGURIDAD RRC') que incluye información que identifica los algoritmos utilizados para la protección de la integridad y/o el cifrado, y una información que indica que el plano U y el plano C están divididos (p. ej., en la forma de un elemento de información (IE) dedicado, un IE modificado, o reutilización de un IE existente).

El dispositivo de comunicación móvil 3 responde, en S1146, inicializando el contexto de seguridad RRC para la comunicación con la macro estación base 5-1 derivando los valores de K_{RRCint}, K_{RRCenc} a partir del valor previamente calculado de K_{eNB} para su uso con la señalización de control de la macro estación base 5-1. El dispositivo de comunicación móvil 3 también inicializa el contexto de seguridad del plano U para la comunicación con la pico estación base 5-2, 5-3 derivando el valor de K_{UPenc} a partir de K_{eNB} para su uso con la señalización del plano de usuario para/de la pico estación base 5-2, 5-3.

Suponiendo que la configuración del contexto de seguridad es exitosa, el dispositivo de comunicación móvil 3 confirma esto, en S1132, enviando un mensaje de respuesta apropiado a la macro estación base 5-1 (p. ej., un mensaje de 'MODO DE SEGURIDAD RRC COMPLETO') en S1150.

La macro estación base 5-1 confirma, en S1152, la exitosa configuración del contexto de seguridad a la MME 112 en un mensaje S1-AP apropiado (p. ej., un mensaje de 'SOLICITUD DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP').

Una vez que los distintos contextos de seguridad (NAS y AS) se han inicializado con éxito en los distintos dispositivos, las conexiones de señalización de control y de usuario se pueden configurar en S1154 y el dispositivo de comunicación móvil puede comenzar una comunicación en la que, la señalización del plano de control (S1156) es proporcionada por la macro estación base 5-1 y la señalización del plano U es proporcionada a través de la pico estación base 5-2, 5-3 (S1158).

Por lo tanto, de manera ventajosa, este método proporciona otro modo eficiente de proporcionar una seguridad de la comunicación apropiada, donde diferentes estaciones base son responsables de la señalización del plano U y de la señalización del plano C respectivamente. El dispositivo de usuario puede mantener un contexto de seguridad apropiado tanto para el Plano U como para el plano C, permitiendo así cifrar/descifrar los datos de usuario y los datos de control correctamente y hacer seguimiento de los parámetros de seguridad (claves) utilizados en las diferentes estaciones base.

Informar al dispositivo de comunicación móvil de la división del plano C/plano U de esta manera proporciona un modo eficiente de asegurar que el dispositivo de comunicación móvil tiene la información requerida para establecer que se requiera la derivación del parámetro de seguridad del plano de usuario (K_{UPenc}) para la comunicación con la pico celda.

Este enfoque tiene la ventaja sobre los otros métodos descritos en la presente memoria, que la pico estación base no tiene que derivar K_{UPenc} ella misma, simplificándolo así aún más, lo que está en consonancia con el deseo general de mantener su complejidad al mínimo. Sin embargo, otros métodos descritos en la presente memoria tienen la ventaja de la seguridad, sobre este método, de que el valor de K_{UPenc} (que también es utilizado por el teléfono móvil 3) no se transmite y por lo tanto no puede verse comprometido fácilmente (p. ej., 'escuchando a escondidas'), lo que puede llevar a comprometer la seguridad de los datos de usuario. Si K_{eNB}, que se transfiere por otros métodos, se ve comprometido, no es un asunto trivial derivar K_{UPenc} a partir de él debido a la necesidad de conocer otras claves de seguridad para hacerlo.

*Estación base basada en la provisión de K_{eNB}**

Se apreciará que, actualmente, la transferencia de K_{eNB} y K_{UPenc} entre estaciones base no se admite en ninguna circunstancia. La Figura 12 muestra un cronograma simplificado que ilustra el funcionamiento del sistema de telecomunicación de la Figura 1 en la realización de un cuarto procedimiento de seguridad en el que, en lugar de

transferir un parámetro para el que, actualmente, no se admite la transferencia entre estaciones base, se transfiere un parámetro de seguridad (K_{eNB}*) para el que, actualmente, se admite la transferencia entre estaciones base, aunque en circunstancias limitadas. Específicamente, actualmente se admite la transferencia de K_{eNB}* entre estaciones base durante el traspaso. En consecuencia, este cuarto procedimiento de seguridad extiende las circunstancias en las que K_{eNB}* se admite para configurar el contexto de seguridad en el caso de una división del plano U/plano C.

Específicamente, K_{eNB}* se genera en la macro estación base 5-1 (como sería durante un traspaso) en respuesta a la señalización de la MME 112, y se reenvía a la pico estación base 5-2, 5-3 sobre un interfaz X2.

Al comienzo del procedimiento de seguridad ilustrado en la Figura 12, un dispositivo de comunicación móvil 3 que desea iniciar una comunicación en la pico celda 5-1, 5-2 envía un mensaje de estrato sin acceso (NAS) solicitando conexión (p. ej., un mensaje de 'SOLICITUD DE CONEXIÓN NAS') a la MME 112 (de manera transparente a través de las macro estaciones base 5-1) en S1210 que incluye información que identifica la tarjeta SIM 530 del dispositivo de comunicación móvil 3 (p. ej., 'la identidad de abonado móvil internacional (IMSI)').

La MME 112 responde a esta petición, en S1212, enviando un mensaje solicitando autenticación e incluyendo información que identifica la tarjeta SIM 530 al HSS 114 (p. ej., un mensaje de 'SOLICITUD DE DATOS DE AUTENTICACIÓN'). La función del AuC 116 del HSS 114 deriva RAND, XRES, CK, IK, AUTN y los combina para formar un vector de autenticación para la tarjeta SIM 530 (AV = RAND || XRES || CK || IK || AUTN) en S1214 y envía el AV generado a la MME 112 en S1216 (p. ej., en un mensaje de 'RESPUESTA DE DATOS DE AUTENTICACIÓN').

La MME 112 recupera IK, CK, XRES, RAND y AUTN del AV en S1218 y envía los parámetros AUTN y RAND al dispositivo de comunicación móvil 3 utilizando señalización NAS en S1220 (p. ej., en un mensaje de 'SOLICITUD DE AUTENTICACIÓN NAS').

El dispositivo de comunicación móvil 3 responde, en S1222, autenticando la red utilizando el AUTN recibido, y derivando los parámetros relacionados con la seguridad apropiados (IK, CK, RES etc.) utilizando la clave de seguridad permanente almacenada 'K' y los parámetros AUTN y RAND recibidos (y cualquier otro parámetro donde sea necesario - p. ej., AMF para la determinación de XMAC). Suponiendo que la autenticación es exitosa, el dispositivo de comunicación móvil 3 envía el valor calculado de RES a la MME 112 en S1224 (p. ej., en un mensaje de 'RESPUESTA DE AUTENTICACIÓN NAS').

La MME 112 comprueba el valor de RES recibido contra XRES en S1226, restablece el contador NAS del enlace descendente, y deriva los valores de K_{ASME}, K_{eNB}, K_{NASint} y K_{NASenc}. La MME 112 inicia entonces la seguridad de señalización NAS entre la MME 112 y el dispositivo de comunicación móvil 3, en S1228, enviando un mensaje de COMANDO DEL MODO DE SEGURIDAD NAS que informa al dispositivo de comunicación móvil 3 de los algoritmos respectivos a utilizar para la protección de la integridad y el (des)cifrado.

El dispositivo de comunicación móvil 3 responde, en S1230, derivando los valores de K_{ASME}, K_{eNB}, K_{NASint} y K_{NASenc} y luego, en S1232, enviando un mensaje de respuesta que informa a la MME 112 que la inicialización de seguridad de la señalización NAS está completa.

El método continúa iniciando la configuración del contexto de seguridad en la macro estación base 5-1, enviando un mensaje de aplicación S1 (S1-AP) (p. ej., un mensaje de 'SOLICITUD DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP') a la macro estación base 5-1 en S1234. El mensaje S1-AP incluye el valor derivado de K_{eNB} y los detalles de las capacidades de seguridad para el dispositivo de comunicación móvil 3.

La macro estación base 5-1 inicia la configuración del contexto de seguridad en la pico estación base 5-2, 5-3, enviando un mensaje de aplicación X2 (X2-AP) (p. ej., un nuevo mensaje de 'CONFIGURACIÓN DEL CONTEXTO X2-AP') a la pico estación base 5-2, 5-3 en S1236. El mensaje X2-AP incluye un valor de K_{eNB}*, derivado del valor de K_{eNB} de la MME 112 (y posiblemente un valor de NH), y detalles de las capacidades de seguridad para el dispositivo de comunicación móvil 3. El valor de K_{eNB}* se deriva, eficazmente, del mismo modo que para el traspaso, aunque se le puede dar otro nombre (p. ej., K_{eNB}**) para permitir que se distinga del caso de traspaso.

La pico estación base 5-2, 5-3, al recibir el K_{eNB}* de la macro estación base 5-1, deriva, en S1238, los parámetro(s) de seguridad requeridos para el cifrado/descifrado del plano U. Específicamente, la pico estación base 5-2, 5-3 deriva un valor de K_{eNB} (en la práctiva un 'pico' K_{eNB}) a partir del K_{eNB}* recibido y un valor de K_{UPenc} a partir del pico K_{eNB} derivado. De manera similar, la macro estación base 5-1 deriva, en S1240, los parámetro(s) de seguridad requeridos para el cifrado/descifrado del plano C (p. ej., K_{RRCint} y K_{RRCenc}) a partir del K_{eNB} recibido de la MME 112.

Suponiendo que la configuración del contexto de seguridad es exitosa, la pico estación base 5-2, 5-3 confirma esto a la macro estación base 5-1 en un mensaje X2-AP apropiado (p. ej., un mensaje de 'RESPUESTA DE CONFIGURACIÓN DEL CONTEXTO X2-AP') en S1242.

La macro estación base 5-1 luego inicia, en S1244, una configuración del contexto de seguridad RRC (y del plano de usuario) en el dispositivo de comunicación móvil 3 utilizando señalización RRC (p. ej., un mensaje de 'COMANDO DEL MODO DE SEGURIDAD RRC') que incluye información que identifica los algoritmos utilizados para la protección de la integridad y/o el cifrado, y una información que indica que el plano U y el plano C están divididos (p. ej., en la forma de un elemento de información (IE) dedicado, un IE modificado, o reutilización de un IE existente).

El dispositivo de comunicación móvil 3 responde, en S1246, inicializando el contexto de seguridad RRC para la comunicación con la macro estación base 5-1 derivando los valores de K_{RRCint}, K_{RRCenc} a partir del valor previamente calculado de ('macro') K_{eNB} para su uso con la señalización de control de la macro estación base 5-1. El dispositivo de comunicación móvil 3 también inicializa el contexto de seguridad del plano U para la comunicación con la pico estación base 5-2, 5-3 derivando el valor de K_{eNB}* y por tanto el 'pico' K_{eNB} a partir del cual se puede encontrar el K_{UPenc} correcto para su uso con la señalización del plano de usuario para/de la pico estación base 5-2, 5-3.

Suponiendo que la configuración del contexto de seguridad es exitosa, el dispositivo de comunicación móvil 3 confirma esto, en S1232, enviando un mensaje de respuesta apropiado a la macro estación base 5-1 (p. ej., un mensaje de 'MODO DE SEGURIDAD RRC COMPLETO') en S1250.

La macro estación base 5-1 confirma, en S1252, la exitosa configuración del contexto de seguridad a la MME 112 en un mensaje S1-AP apropiado (p. ej., un mensaje de 'SOLICITUD DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP').

Una vez que los distintos contextos de seguridad (NAS y AS) se han inicializado con éxito en los distintos dispositivos, las conexiones de señalización de control y de usuario se pueden configurar en S1254 y el dispositivo de comunicación móvil puede comenzar una comunicación en la que, la señalización del plano de control (S1256) es proporcionada por la macro estación base 5-1 y la señalización del plano U es proporcionada a través de la pico estación base 5-2, 5-3 (S1258).

Por lo tanto, de manera ventajosa, este método proporciona otro modo eficiente de proporcionar una seguridad de la comunicación apropiada, donde diferentes estaciones base son responsables de la señalización del plano U y de la señalización del plano C respectivamente. El dispositivo de usuario puede mantener un contexto de seguridad apropiado tanto para el Plano U como para el plano C permitiendo así cifrar/descifrar los datos de usuario y los datos de control correctamente, y hacer seguimiento de los parámetros de seguridad (claves) utilizados en las diferentes estaciones base.

Informar al dispositivo de comunicación móvil de la división del plano C/plano U de esta manera, proporciona un modo eficiente de asegurar que el dispositivo de comunicación móvil tiene la información requerida para establecer que se requiera la derivación del parámetro de seguridad del plano de usuario (K_{UPenc}) para la comunicación con la pico celda.

Este enfoque tiene la ventaja sobre los otros métodos descritos en la presente memoria de que no requiere de la transferencia de parámetros de seguridad entre estaciones base, por lo que dicha transferencia no se admite actualmente. Sin embargo, otros métodos descritos en la presente memoria tienen la ventaja añadida de la complejidad para derivar K_{eNB}* adecuadamente en escenarios de no traspaso.

Procedimientos separados de autenticación y de acuerdo de clave (AKA)

La Figura 13 muestra un diagrama simplificado que ilustra el funcionamiento del sistema de telecomunicación de la Figura 1 en la realización de un procedimiento de seguridad adicional en el que, en lugar de ejecutar un solo procedimiento AKA para la macro estación base 5-1 durante el cual los parámetros de seguridad apropiados son pasados a, y/o derivados en, la pico estación base 5-2, 5-3 (p. ej., como se ilustra en cada una de las Figuras 9 a 11), se ejecutan procedimientos AKA separados para la macro estación base 5-1 y para la pico estación base 5-2, 5-3.

Como se ve en la Figura 13, el procedimiento implica, en S1313, que se ejecuten procedimientos de seguridad AS para las comunicaciones entre la macro estación base 5-1 y el dispositivo de comunicación móvil 3. Durante este procedimiento el dispositivo de comunicación móvil 3, la macro estación base 5-1 y la MME 112, cada una genera y mantiene su propio contexto de seguridad respectivo S1312-1, S1312-2, S1312-3 para la señalización del plano C entre la macro estación base 5-1 y el dispositivo de comunicación móvil 3. La generación de cada contexto de seguridad incluye la derivación de claves de seguridad específicas de macro / plano C apropiadas (p. ej., K_{RRCint}, K_{RRCenc} etc. como se describió anteriormente).

El procedimiento también implica, en S1314, que se ejecuten procedimientos de seguridad AS para las comunicaciones entre la pico estación base 5-2, 5-3 y el dispositivo de comunicación móvil 3. Durante este procedimiento el dispositivo de comunicación móvil 3, la pico estación base 5-2, 5-3 y la MME 112, cada una genera y mantiene su propio contexto de seguridad respectivo S1316-1, S1316-2, S1316-3 para la señalización del plano U entre la pico estación base 5-2, 5-3 y el dispositivo de comunicación móvil 3. La generación de cada contexto de seguridad incluye la derivación de claves de seguridad específicas de pico / plano U apropiadas (p. ej., K_{UPenc} etc. como se describió anteriormente).

Se apreciará que los procedimientos de S1313 y S1314 pueden ejecutarse de manera secuencial en cualquier orden apropiado o en paralelo.

Por lo tanto, puede verse que, como resultado del procedimiento en la Figura 13, la MME 112 y el dispositivo de comunicación móvil 3 cada uno mantiene dos contextos de seguridad activos. Para mantener la presencia de dos contextos de seguridad activos, la señalización de traspaso (para traspaso de macro+pico a otra macro+pico) se modifica en este ejemplo para permitir el intercambio de dos contextos de seguridad. Por ejemplo, la señalización puede modificarse para permitir que se generen y transfieran dos K_{eNB}* (basadas en cada K_{eNB}), que se notifiquen diferentes algoritmos de seguridad (si se utilizan diferentes algoritmos), y la señalización de otra información general relacionada con los dos contextos de seguridad diferentes.

Además, para mantener el procedimiento AKA dual de la Figura 13, se modifican apropiadamente los mensajes RRC y NAS. Por ejemplo, el COMANDO DEL MODO DE SEGURIDAD RRC se modifica para incluir información que identifica el algoritmo de seguridad para cada procedimiento AKA y los mensajes de seguridad NAS se modifican para incluir duplicados de los parámetros de seguridad donde sea necesario.

El dispositivo de comunicación móvil 3 mantiene dos instancias de cifrado (p. ej., en la capa PDCP) cada una con su propio conjunto de claves de seguridad - una para el cifrado del plano de control y otra para el cifrado del plano de usuario.

Se apreciará que, podría aplicarse un procedimiento similar, si fuera necesario, para generar contextos NAS separados para el procedimiento AKA de las estaciones base pico y macro que se está ejecutando. El procedimiento sería similar al descrito con referencia a las Figuras 9 a 12 pero, durante este procedimiento, el dispositivo de comunicación móvil 3 y la MME 112 cada una generaría y mantendría un contexto de seguridad NAS para la macro estación base 5-1 y un contexto de seguridad NAS separado para la pico estación base 5-2, 5-3. La generación y transmisión de los contextos de seguridad NAS puede incluir la derivación y transmisión de parámetros de seguridad duplicados (una copia para cada contexto) donde sea apropiado.

Procedimientos de cambio de clave sobre la marcha

Sin importar cuál de los procedimientos anteriores se implementa, para evitar posibles problemas de seguridad asociados con el vuelco del CONTADOR PDCP, la pico estación base 5-2, 5-3, es operable para informar a la macro estación bar 5-1, cuando se ha producido un vuelco en el CONTADOR PDCP, o está apunto de ocurrir, utilizando un nuevo mensaje X2-AP que incluye un elemento de información que indica que el K_{UPenc} requiere cambios (p. ej., un IE de 'cambio de clave de K_{UPenc}'). En respuesta a la recepción de este mensaje, la macro estación base 5-1 inicia un traspaso entre celdas que, en última instancia, dará como resultado una comunicación que continua en el par de celdas pico/macro actual pero utilizando un valor diferente de K_{UPenc} para el cifrado del plano de usuario.

De manera similar, donde otros parámetros de seguridad, como K_{eNB}, son cambiados dinámicamente y proporcionados por la MME 112 a la macro estación base 5-1 (de acuerdo con los procedimientos actuales), la macro estación base 5-1 se configura para reenviar el nuevo K_{eNB} a la pico estación base 5-2, 5-3 cuando se implementa el procedimiento mostrado en la Figura 10. Según la invención, donde se implementa el procedimiento mostrado en la Figura 12, la macro estación base 5-1 se configura para reenviar un nuevo K_{eNB}* a la pico estación base 5-2, 5-3. Donde se implementa el procedimiento mostrado en la Figura 11, la macro estación base 5-1 se configura para reenviar un nuevo K_{UPenc} a la pico estación base 5-2, 5-3. Donde se implementa el procedimiento mostrado en la Figura 9, la MME 112 se configura para reenviar el nuevo K_{eNB} a la pico estación base 5-2, 5-3 en un mensaje S1 duplicado.

Modificaciones y alternativas

Una realización detallada se ha descrito anteriormente. Como apreciarán los expertos en la técnica, se pueden hacer una serie de modificaciones y alternativas a la realización anterior, y variaciones, mientras se benefician de las invenciones incorporadas en la misma.

En las realizaciones anteriores se describen una macro celda 7 y dos pico celdas 10; las pico celdas se operan utilizando portadoras de componente que tienen la misma banda de frecuencia (F2) y la macro celda se opera utilizando una portadora de componente que tiene una banda de frecuencia diferente (F1). Se apreciará que en un sistema desplegado puede haber cualquier número de pico celdas, cada una de las cuales puede operar en una portadora de componente que tiene una banda de frecuencia respectiva diferente y podría, potencialmente, operar en una portadora de componente que tiene la misma banda de frecuencia que la macro celda.

En las realizaciones anteriores las estaciones base macro y micro pueden tener las mismas capacidades de seguridad. Sin embargo, si son admitidas capacidades de seguridad diferentes, el dispositivo de comunicación móvil es informado (p. ej., en el 'COMANDO DEL MODO DE SEGURIDAD RRC' u otro mensaje similar) de las capacidades apropiadas para cada estación base, permitiendo así al dispositivo de comunicación móvil utilizar los algoritmos correctos.

En los ejemplos anteriores, la clave de cifrado se puede transferir desde la macro estación base o, según la invención, puede ser derivada por la pico estación base basándose en la información de seguridad recibida de la macro estación base. Se apreciará que los otros parámetros requeridos para el cifrado/descifrado del plano U pueden ser derivados como sigue: CONTADOR puede ser mantenido por la pico estación base en el nivel PDCP; la identidad de PORTADORA puede, bien ser transferida desde la macro estación base, o puede ser seleccionada por la pico estación base; y la DIRECCIÓN puede establecerse, bien en la macro, o bien en la pico estación base. Puede proporcionarse sincronización apropiada entre las estaciones base macro y pico para asegurar, por ejemplo, que la identidad de portadora correcta es conocida tanto en la macro como en la pico estación base. En el caso de que ambas estaciones base tengan la información y la capacidad para decidir (p. ej., 'DIRECCIÓN') solo una tomará la decisión y esto será informado a la otra estación base.

La descripción detallada proporcionada para las realizaciones de las Figura 9 a 12 se refiere a procedimientos para establecer la conexión inicial. Se apreciará que puede utilizarse un enfoque similar cuando la decisión de dividir el plano U y el plano C se toma en una etapa posterior. Por ejemplo, donde el dispositivo de comunicación móvil participa en un tipo de comunicación del plano de usuario que es proporcionada por la macro celda (decir voz sobre IP 'VoIP') y luego inicia una forma diferente de comunicación del plano de usuario que es proporciona por la pico celda (decir una sesión de navegación web) una división del plano C/plano U puede necesitar ser iniciada. En este caso una MODIFICACIÓN DEL CONTEXTO DEL UE S1 (con una respuesta correspondiente) puede utilizarse para proporcionar a la pico estación base con la información de seguridad apropiada (análogo al proceso de la Figura 9). De manera similar, un nuevo mensaje X2 (con una respuesta correspondiente) puede proporcionarse (p. ej., un mensaje de MODIFICACIÓN DEL CONTEXTO X2-AP) (análogo a los procesos de cualquiera de las Figura 10 a 12). Además, la señalización RRC utilizada para proporcionar al dispositivo de comunicación móvil con la información de seguridad apropiada (donde los parámetros de seguridad han cambiado) y/o una indicación de que ha sucedido una división puede ser un mensaje como un mensaje de Re-configuración RRC (con una respuesta correspondiente).

Mientras que nuevos mensajes X2-AP específicos (CONFIGURACIÓN DEL CONTEXTO X2-AP o 'RESPUESTA DE CONFIGURACIÓN DEL CONTEXTO X2-AP') se han descrito, se apreciará que cualquier mensaje X2-AP adecuado puede utilizarse, incluyendo la reutilización de un mensaje existente con la incorporación de elementos de información apropiados.

Además, aunque la información como K_{eNB} se describe como siendo intercambiada sobre un interfaz X2 entre las estaciones base pico y macro, se apreciará que el interfaz entre las estaciones base puede ser un nuevo interfaz dedicado (p. ej., un interfaz 'X3').

Aunque el mensaje de COMANDO DEL MODO DE SEGURIDAD RRC se ha descrito como incluyendo información que indica que el plano U y el plano C están divididos (p. ej., en la forma de un elemento de información (IE) dedicado, un IE modificado, o reutilización de un IE existente), una indicación de una división del plano C/plano U podría (alternativamente o adicionalmente) notificarse al dispositivo de comunicación móvil en un mensaje NAS como un mensaje de COMANDO DEL MODO DE SEGURIDAD NAS.

Los elementos de información incluidos en dicho mensaje normalmente incluirán, por ejemplo:

- Un IE de Clave de Seguridad para mensajes desde la macro estación base a la pico estación base (que puede ser utilizado en los procedimientos de las Figuras 10 a 13 o para procedimientos de cambio de clave sobre la marcha)
    - Este puede ser K_{eNB} o Siguiente Salto (NH)
    - En el caso de la implementación de la Figura 10, por ejemplo, puede ser la macro K_{eNB}
    - En el caso de la implementación de la Figura 12, puede ser el K_{eNB}*
    - En el caso de los AKAs duales de la Figura 13, puede ser el Pico K_{eNB} para el nuevo AKA
- Un IE de Capacidades de Seguridad del UE para mensajes desde la macro estación base a la pico estación base (para indicar un cambio en las capacidades de seguridad por ejemplo)
- Un IE de cambio de clave de K_{UPenc} para mensajes desde la macro estación base a la pico estación base (para indicar la necesidad de un procedimiento de traspaso dentro de la celda en el vuelco del CONTADOR PDCP)

En referencia a los cronogramas, se apreciará que en muchos casos el mensaje puede no necesitar seguir el orden específico mostrado, sino que puede seguir cualquier orden lógico.

En referencia a la Figura 9, a modo de ejemplo, se apreciará por aquellos expertos en la técnica que, aunque los mensajes S1-AP enviados a las estaciones base pico y macro para iniciar la configuración del contexto de seguridad AS (S934, S936), y la derivación de clave del plano U y del plano C resultante (S938, S940), se muestran sucediendo en un orden particular (con el propósito de una ilustración clara), pueden ocurrir en cualquier orden apropiado o, donde sea apropiado, en paralelo. Específicamente, por ejemplo, la iniciación de la inicialización del contexto de seguridad y

de la derivación de clave en la pico estación base 5-2, 5-3 (S934, S938) puede ocurrir completamente antes, completamente después, o sustancialmente en paralelo con la correspondiente iniciación de la inicialización del contexto de seguridad y de la derivación de clave (S936, S940) en la macro estación base 5-1. De manera similar, los mensajes de respuesta S1-AP asociados pueden enviarse en cualquier momento apropiado después de la exitosa inicialización del contexto de seguridad.

Además, mientras que, en la Figura 9, se muestra un duplicado de solo un mensaje S1-AP (CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP) siendo enviado a la pico estación base para proporcionar los parámetros de seguridad apropiados. Se apreciará que un duplicado de cualquier mensaje S1-AP adecuado que transporta parámetros de seguridad se puede proporcionar a la pico estación base incluyendo, por ejemplo, un mensaje de MODIFICACIÓN DEL CONTEXTO DEL UE o similar.

En relación al procedimiento AKA dual descrito con referencia a la Figura 13, se apreciará que puede haber un escenario en el que la pico estación base no es una estación base E-UTRAN sino que se conecta a una no EUTRAN o incluso a una red no 3GPP. En este caso la red no 3GPP puede realizar su propio procedimiento de seguridad para el plano de usuario mientras que la macro estación base todavía realiza un procedimiento de seguridad 3GPP, resultando así en un contexto de seguridad no 3GPP para el plano de usuario y un contexto de seguridad 3GPP para el plano de control.

Se apreciará que aunque el sistema de comunicación 1 se describe en términos de estaciones base 5 que operan como estaciones base macro o pico, pueden aplicarse los mismos principios a estaciones base que operan como femto estaciones base, nodos de retransmisión que proporcionan elementos de la funcionalidad de la estación base, u otros nodos de comunicación.

En las realizaciones anteriores, fue descrito un teléfono móvil basado en un sistema de telecomunicaciones. Como apreciarán los expertos en la técnica, las técnicas de señalización descritas en la presente aplicación pueden emplearse en otros sistemas de comunicaciones. Otros nodos o dispositivos de comunicaciones pueden incluir dispositivos de usuario como, por ejemplo, asistentes digitales personales, ordenadores portátiles, navegadores web, etc. Como apreciarán los expertos en la técnica, no es esencial que se utilice el sistema de retransmisión descrito anteriormente por dispositivos de comunicaciones móviles. El sistema puede utilizarse para extender la cobertura de las estaciones bases en una red que tiene uno o más dispositivos informáticos fijos, además de, o en lugar, de los dispositivos de comunicación móviles.

En las realizaciones descritas anteriormente, las estaciones base 5 y los dispositivos de comunicación móviles 3 cada uno incluye un circuito transceptor. Normalmente, este circuito estará formado por circuitos hardware dedicados. Sin embargo, en algunas realizaciones, parte del circuito transceptor puede implementarse como software ejecutado por el correspondiente controlador.

En las realizaciones anteriores, fueron descritos un número de módulos software. Como apreciarán los expertos en la técnica, los módulos software pueden proporcionarse de forma compilado o no compilada y pueden suministrarse a la estación base o a la estación de retransmisión como una señal a través de una red informática, o en un medio de grabación. Además, la funcionalidad realizada por parte, o la totalidad, de este software puede realizarse utilizando uno o más circuitos hardware dedicados.

Otras modificaciones varias serán evidentes para los expertos en la técnica y no se describirán con más detalle aquí.

REIVINDICACIONES

1. Aparato de comunicación (5-2) para operar como un aparato de comunicación secundario (5-2) que proporciona una celda de comunicación secundaria en una red de comunicación que tiene un equipo de usuario (3) y un aparato de comunicación primario (5-1) que proporciona una celda de comunicación primaria y señalización del plano de control al equipo de usuario (3), comprendiendo el aparato de comunicación secundario (5-2):

un medio para proporcionar una comunicación del plano de usuario para el equipo de usuario (3);
un medio para indicar al primer aparato de comunicación (5-1) cuando está a punto de terminar un contador PDCP;
un medio para recibir, del aparato de comunicación primario (5-1), una clave de seguridad del aparato de comunicación secundario (5-2) derivado por el aparato de comunicación primario (5-1) utilizando una clave de seguridad del aparato de comunicación primario (5-1) mientras el equipo de usuario (3) está conectado al aparato de comunicación primario (5-1) y al aparato de comunicación secundario (5-2);
un medio para derivar una clave de seguridad del plano de usuario utilizando dicha clave de seguridad del aparato de comunicación secundario (5-2); y
un medio para utilizar la clave de seguridad del plano de usuario derivada para una comunicación del plano de usuario entre el aparato de comunicación secundario (5-2) y el equipo de usuario (3).

2. Aparato de comunicación según la reivindicación 1, en donde dicho medio para recibir es operable para recibir la clave de seguridad del aparato de comunicación secundario (5-2) sobre un interfaz X2.

3. Aparato de comunicación (5-1) para operar como un aparato de comunicación primario (5-1) que proporciona una celda de comunicación primaria en una red de comunicación que tiene un equipo de usuario (3) y un aparato de comunicación secundario (5-2) que proporciona una celda de comunicación secundaria y comunicación del plano de usuario para el equipo de usuario (3), comprendiendo el aparato de comunicación primario (5-1):

un medio para proporcionar señalización del plano de control al equipo de usuario (3);
un medio para recibir una indicación del aparato de comunicación secundario (5-2) cuando está a punto de terminar un contador PDCP;
un medio para obtener una clave de seguridad del aparato de comunicación primario (5-1), para derivar, utilizando la clave de seguridad del aparato de comunicación primario (5-1), al menos una clave de seguridad del plano de control para una comunicación del plano de control entre el equipo de usuario (3) y el aparato de comunicación primario (5-1), y para derivar, utilizando la clave de seguridad del aparato de comunicación primario, una clave de seguridad para el aparato de comunicación secundario (5-2) mientras el equipo de usuario (3) está conectado al aparato de comunicación primario (5-1) y al aparato de comunicación secundario (5-2), siendo utilizada la clave de seguridad del aparato de comunicación secundario (5-2) para derivar una clave de seguridad del plano de usuario por el aparato de comunicación secundario (5-2); y
un medio para enviar la clave de seguridad del aparato de comunicación secundario (5-2) al aparato de comunicación secundario (5-2).

4. Aparato de comunicación según la reivindicación 3, en donde dicho medio para enviar es operable para enviar la clave de seguridad del aparato de comunicación secundario (5-2) sobre un interfaz X2.

5. Equipo de usuario (3) para una red de comunicación que tiene un aparato de comunicación primario (5-1) que proporciona una celda de comunicación primaria y un aparato de comunicación secundario que proporciona una celda de comunicación secundaria, comprendiendo el equipo de usuario (3):

un medio para recibir señalización del plano de control del aparato de comunicación primario (5-1);
un medio para derivar una clave de seguridad del aparato de comunicación primario;
un medio para derivar, utilizando la clave de seguridad derivada del aparato de comunicación primario, al menos una clave de seguridad del plano de control para una comunicación del plano de control entre el equipo de usuario (3) y el aparato de comunicación primario (5-1);
un medio para derivar, utilizando la clave de seguridad derivada del aparato de comunicación primario, una clave de seguridad del aparato de comunicación secundario mientras el equipo de usuario (3) está conectado al aparato de comunicación primario (5-1) y al aparato de comunicación secundario (5-2);
un medio para derivar, utilizando la clave de seguridad del aparato de comunicación secundario, una clave de seguridad del plano de usuario; y
un medio para utilizar la clave de seguridad del plano de usuario derivada para una comunicación del plano de usuario entre el equipo de usuario (3) y el aparato de comunicación secundario (5-2).

6. Un método realizado por un aparato de comunicación secundario (5-2) que proporciona una celda de comunicación secundaria en una red de comunicación que tiene un equipo de usuario (3) y un aparato de comunicación primario (5-1) que proporciona una celda de comunicación primaria y señalización del plano de control al equipo de usuario (3), comprendiendo el método:

proporcionar comunicación del plano de usuario para el equipo de usuario (3);
indicar al aparato de comunicación primario (5-1) cuando está a punto de terminar un contador PDCP;
recibir, del aparato de comunicación primario (5-1), una clave de seguridad del aparato de comunicación secundario (5-2) derivada por el aparato de comunicación primario (5-1) utilizando una clave de seguridad del aparato de comunicación primero (5-1) mientras el equipo de usuario (3) está conectado al aparato de comunicación primario (5-1) y al aparato de comunicación secundario (5-2);
derivar, utilizando la clave de seguridad del aparato de comunicación secundario (5-2), una clave de seguridad del plano de usuario; y
utilizar la clave de seguridad del plano de usuario derivada para una comunicación del plano de usuario entre el aparato de comunicación secundario (5-2) y el equipo de usuario (3).

7. El método según la reivindicación 6, en donde dicha clave de seguridad del aparato de comunicación secundario (5-2) es recibida sobre un interfaz X2.

8. Un método realizado por un aparato de comunicación primario (5-1) que proporciona una celda de comunicación primaria en una red de comunicación que tiene un equipo de usuario (3) y un aparato de comunicación secundario (5-2) que proporciona una celda de comunicación secundaria y comunicación del plano de usuario para el equipo de usuario (3), comprendiendo el método:

proporcionar señalización de plano de control al equipo de usuario (3);
recibir una indicación del aparato de comunicación secundario (5-2) cuando está a punto de terminar un contador PDCP;
obtener una clave de seguridad del aparato de comunicación primario (5-1);
derivar, utilizando la clave de seguridad del aparato de comunicación primario (5-1), al menos una clave de seguridad del plano de control para una comunicación del plano de control entre el equipo de usuario (3) y el aparato de comunicación primario (5-1);
derivar, utilizando la clave de seguridad del aparato de comunicación primario (5-1), una clave de seguridad del aparato de comunicación secundario (5-2) mientras el equipo de usuario (3) está conectado al aparato de comunicación primario (5-1) y al aparato de comunicación secundario (5-2), siendo utilizada la clave de seguridad del aparato de comunicación secundario (5-2) para derivar una clave de seguridad del plano de usuario por el aparato de comunicación secundario (5-2); y
enviar la clave de seguridad derivada del aparato de comunicación secundario (5-2) al aparato de comunicación secundario (5-2).

9. El método según la reivindicación 8, en donde dicha clave de seguridad del aparato de comunicación secundario (5-2) es enviada sobre un interfaz X2.

10. Un método realizado por un equipo de usuario (3) en una red de comunicación que tiene un aparato de comunicación primario (5-1) que proporciona una celda de comunicación primaria y un aparato de comunicación secundario que proporciona una celda de comunicación secundaria, comprendiendo el método:

recibir señalización del plano de control del aparato de comunicación primario (5-1);
derivar una clave de seguridad del aparato de comunicación primario (5-1);
derivar, utilizando la clave de seguridad derivada del aparato de comunicación primario (5-1), al menos una clave de seguridad del plano de control para una comunicación del plano de control entre el equipo de usuario (3) y el aparato de comunicación primario (5-1);
derivar, utilizando la clave de seguridad derivada del aparato de comunicación primario (5-1), una clave de seguridad del aparato de comunicación secundario (5-2) mientras el equipo de usuario (3) está conectado al aparato de comunicación primario (5-1) y al aparato de comunicación secundario (5-2);
derivar, utilizando la clave de seguridad del aparato de comunicación secundario (5-2), una clave de seguridad del plano de usuario; y
utilizar la clave de seguridad del plano de usuario derivada para una comunicación del plano de usuario entre el equipo de usuario (3) y el aparato de comunicación secundario (5-2).

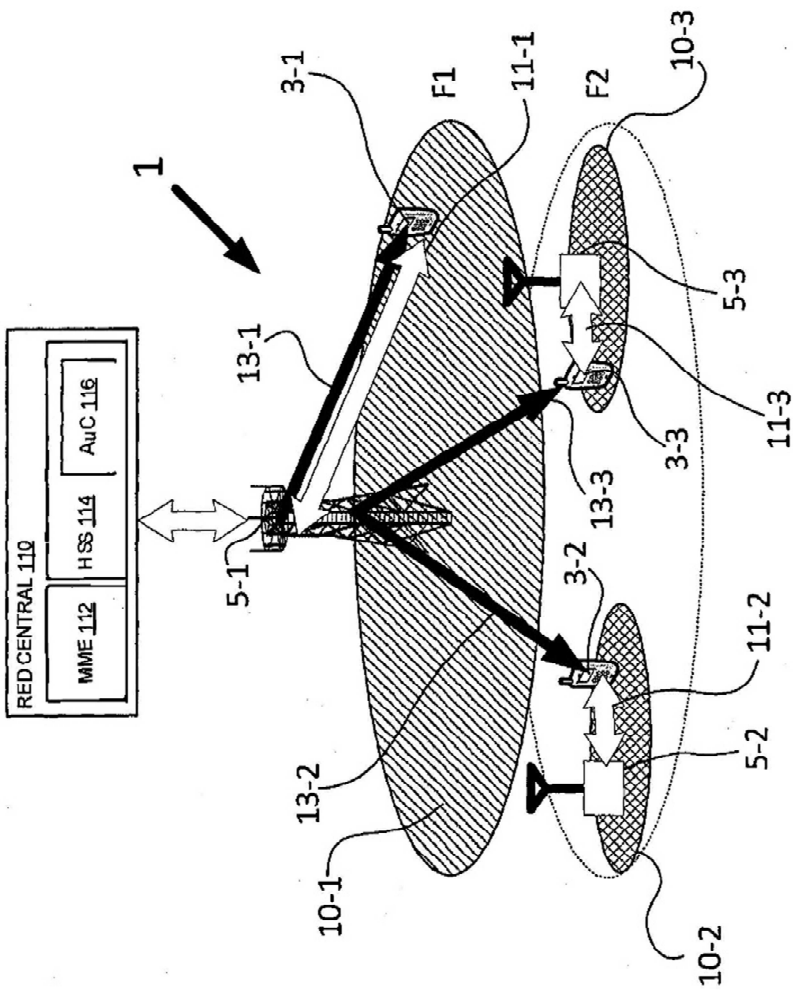
1
RED CENTRAL 110
MME 112
HSS 114
AuC 116
3-1
F1
11-1
F2
10-3
13-1
5-3
11-3
3-3
13-3
5-1
3-2
11-2
5-2
13-2
10-1
10-2

Figura 1

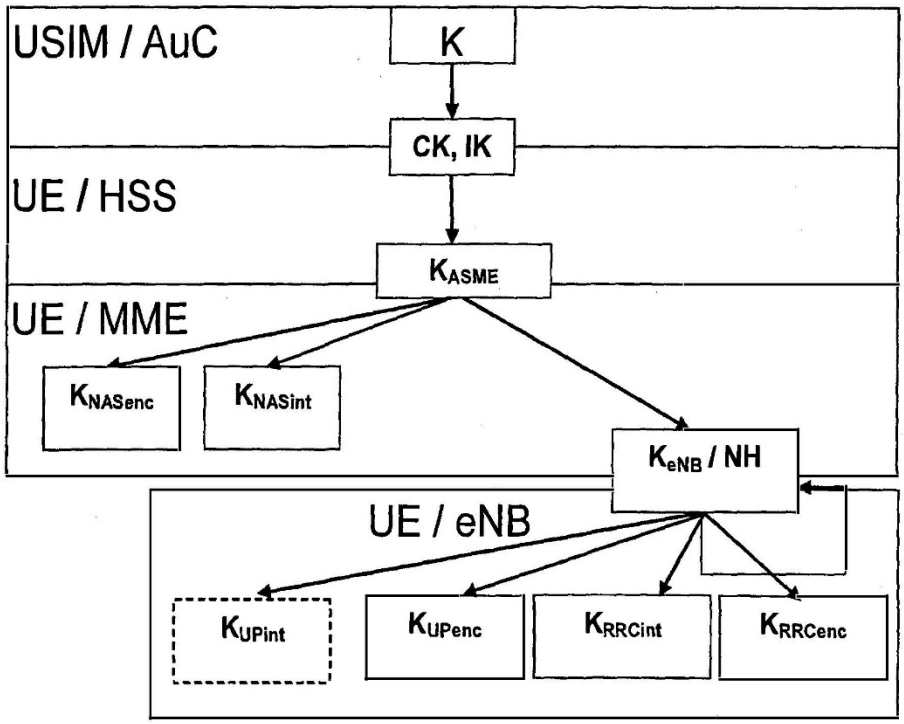
USIM / AuC
K
CK, IK
UE / HSS
KASME
UE / MME
KNASenc
KNASint
KeNB / NH
UE / eNB
KUPint
KUPenc
KRRCint
KRRCenc

Figura 2

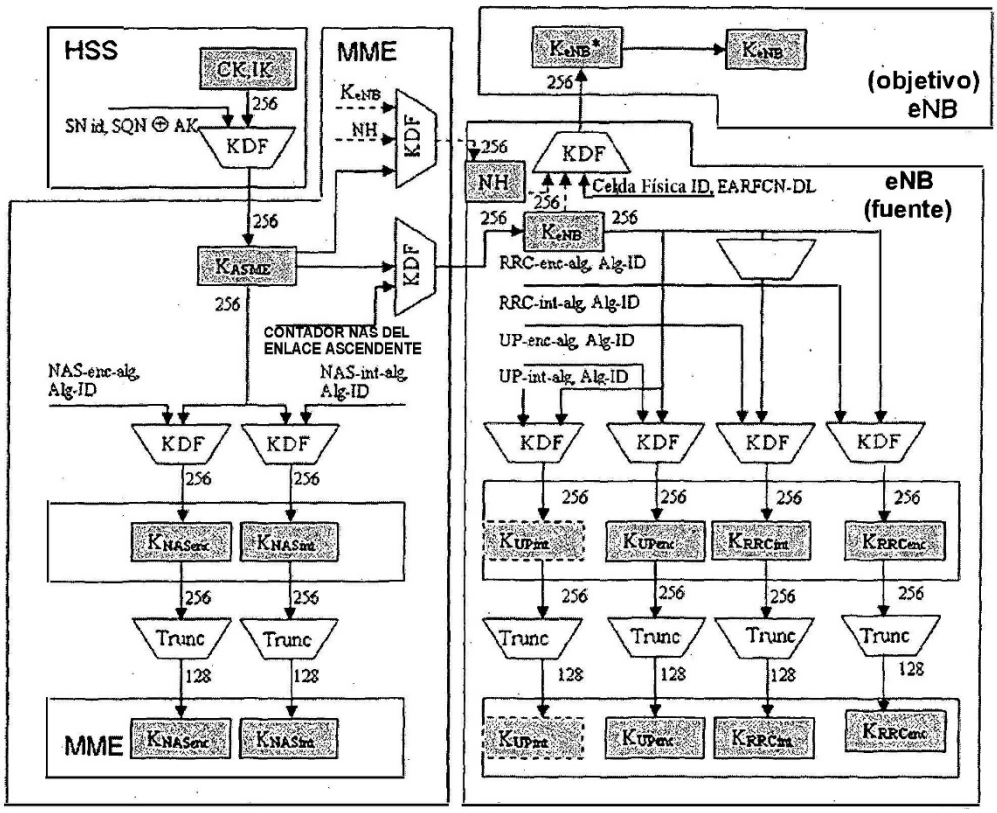
HSS
MME
CK, IK
256
SN id, SQN ⊕ AK
KDF
KeNB
NH
KDF
256
KASME
KDF
256
CONTADOR NAS DEL ENLACE ASCENDENTE
NAS-enc-alg, Alg-ID
NAS-int-alg, Alg-ID
KDF
KDF
256
256
KNASenc
KNASint
256
256
Trunc
Trunc
128
128
MME
KNASenc
KNASint
KeNB*
KeNB
256
(objetivo) eNB
KDF
256
NH
256
Celda Física ID, EARFCN-DL
eNB (fuente)
256
KeNB
256
RRC-enc-alg, Alg-ID
RRC-int-alg, Alg-ID
UP-enc-alg, Alg-ID
UP-int-alg, Alg-ID
KDF
KDF
KDF
KDF
256
256
256
256
KUPint
KUPenc
KRRCint
KRRCenc
256
256
256
256
Trunc
Trunc
Trunc
Trunc
128
128
128
128
KUPint
KUPenc
KRRCint
KRRCenc

Figura 3

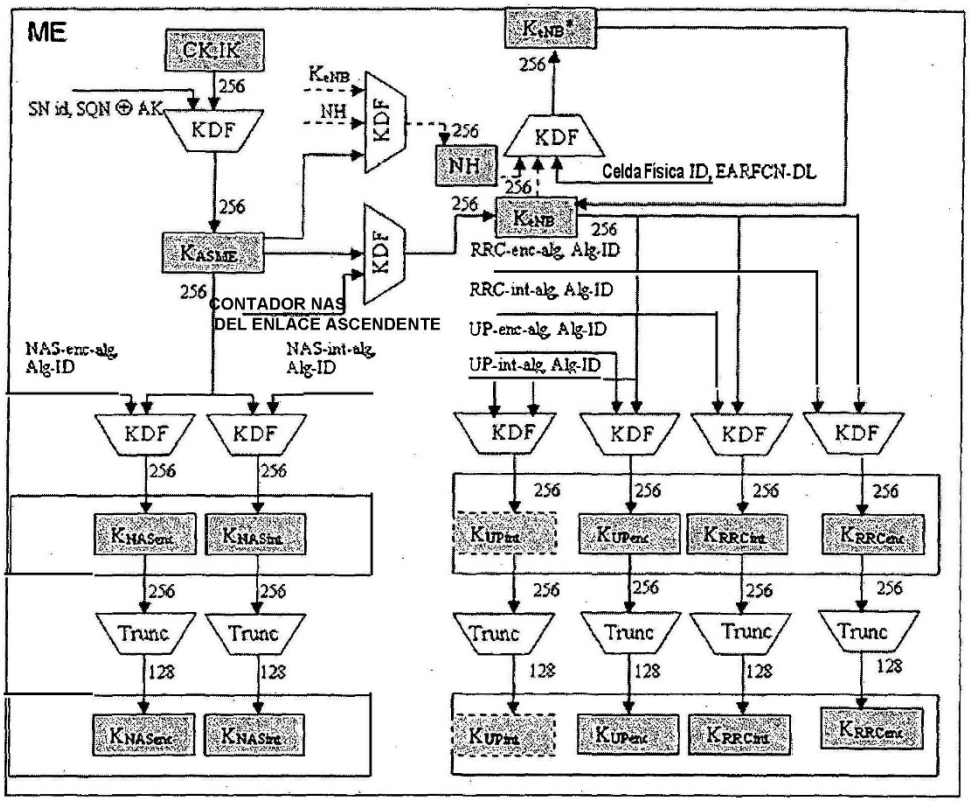
ME
CK IK
256
SN id, SQN ⊕ AK
KDF
256
KASME
256
CONTADOR NAS DEL ENLACE ASCENDENTE
NAS-enc-alg, Alg-ID
NAS-int-alg, Alg-ID
KeNB
NH
KDF
256
NH
Celda Física ID, EARFCN-DL
RRC-enc-alg, Alg-ID
RRC-int-alg, Alg-ID
UP-enc-alg, Alg-ID
UP-int-alg, Alg-ID
KNASenc
KNASint
KUPint
KUPenc
KRRCint
KRRCenc
Trunc
128

Figura 4

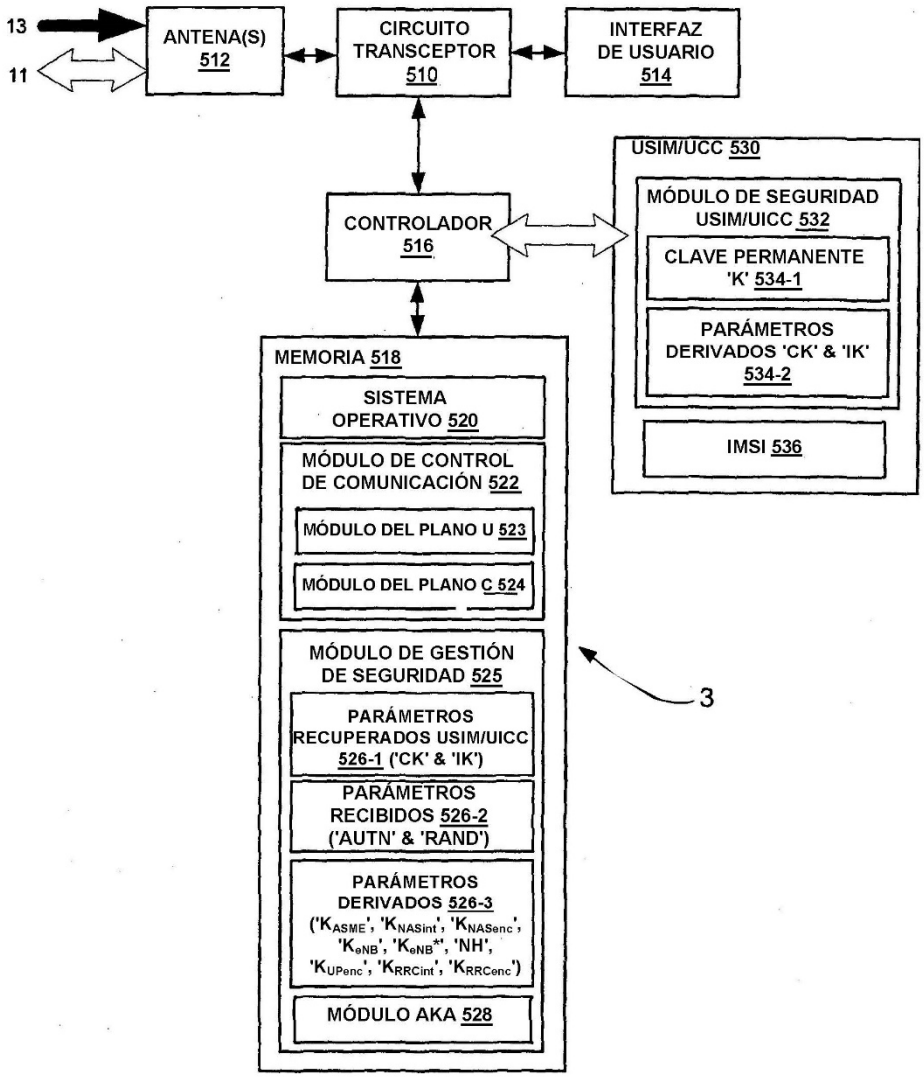
13
11
ANTENA(S) 512
CIRCUITO TRANSCEPTOR 510
INTERFAZ DE USUARIO 514
USIM/UCC 530
MÓDULO DE SEGURIDAD USIM/UICC 532
CLAVE PERMANENTE 'K' 534-1
PARÁMETROS DERIVADOS 'CK' & 'IK' 534-2
IMSI 536
CONTROLADOR 516
MEMORIA 518
SISTEMA OPERATIVO 520
MÓDULO DE CONTROL DE COMUNICACIÓN 522
MÓDULO DEL PLANO U 523
MÓDULO DEL PLANO C 524
MÓDULO DE GESTIÓN DE SEGURIDAD 525
PARÁMETROS RECUPERADOS USIM/UICC 526-1 ('CK' & 'IK')
PARÁMETROS RECIBIDOS 526-2 ('AUTN' & 'RAND')
PARÁMETROS DERIVADOS 526-3 ('KASME', 'KNASint', 'KNASenc', 'KeNB', 'KeNB*', 'NH', 'KUPenc', 'KRRCint', 'KRRCenc')
MÓDULO AKA 528
3

Figura 5

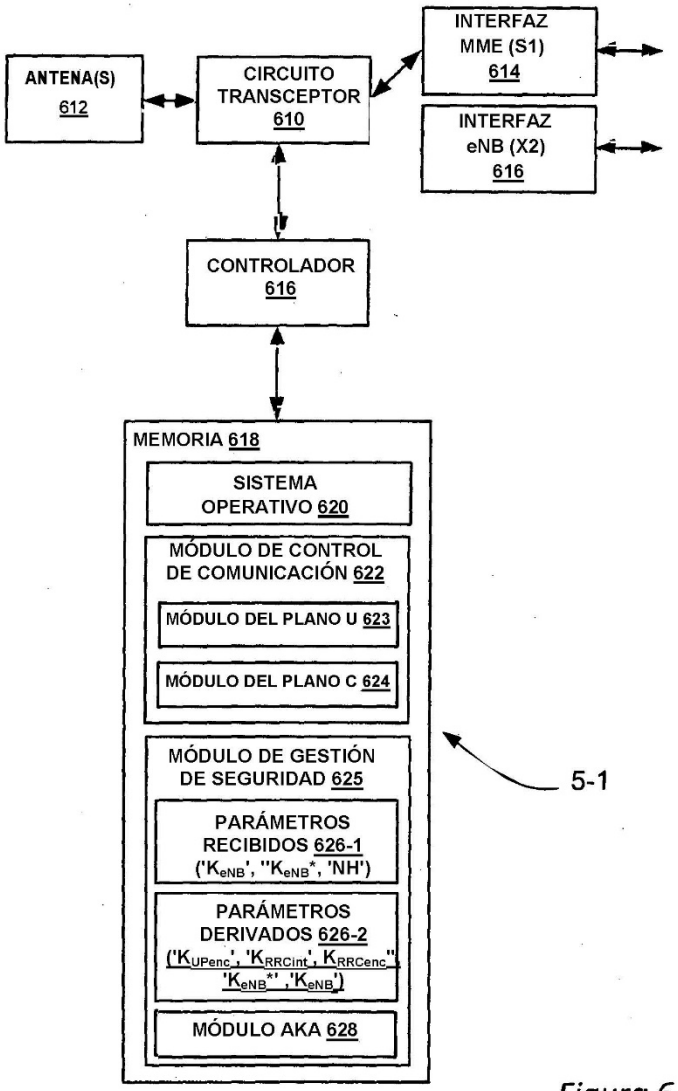
ANTENA(S)
612
CIRCUITO TRANSCEPTOR
610
INTERFAZ MME (S1)
614
INTERFAZ eNB (X2)
616
CONTROLADOR
616
MEMORIA 618
SISTEMA OPERATIVO 620
MÓDULO DE CONTROL DE COMUNICACIÓN 622
MÓDULO DEL PLANO U 623
MÓDULO DEL PLANO C 624
MÓDULO DE GESTIÓN DE SEGURIDAD 625
PARÁMETROS RECIBIDOS 626-1
('K_eNB', 'K_eNB*', 'NH')
PARÁMETROS DERIVADOS 626-2
('K_UPenc', 'K_RRCint', K_RRCenc', 'K_eNB*', 'K_eNB')
MÓDULO AKA 628
5-1

Figura 6

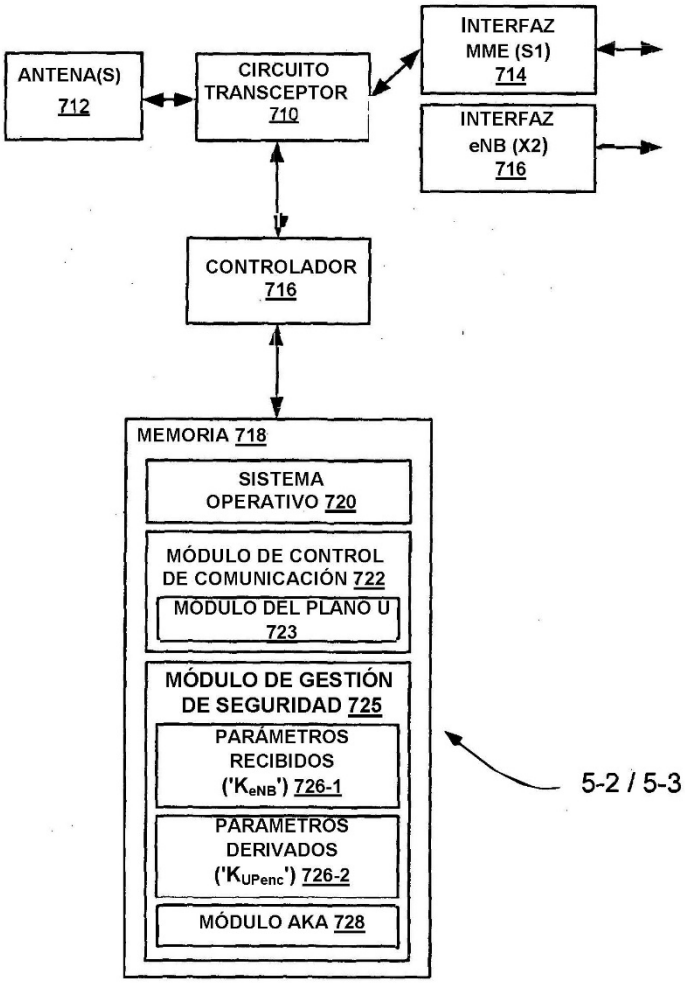
ANTENA(S)
712
CIRCUITO TRANSCEPTOR
710
INTERFAZ MME (S1)
714
INTERFAZ eNB (X2)
716
CONTROLADOR
716
MEMORIA 718
SISTEMA OPERATIVO 720
MÓDULO DE CONTROL DE COMUNICACIÓN 722
MÓDULO DEL PLANO U
723
MÓDULO DE GESTIÓN DE SEGURIDAD 725
PARÁMETROS RECIBIDOS ('K$_{eNB}$') 726-1
PARÁMETROS DERIVADOS ('K$_{UPenc}$') 726-2
MÓDULO AKA 728
5-2 / 5-3

Figura 7

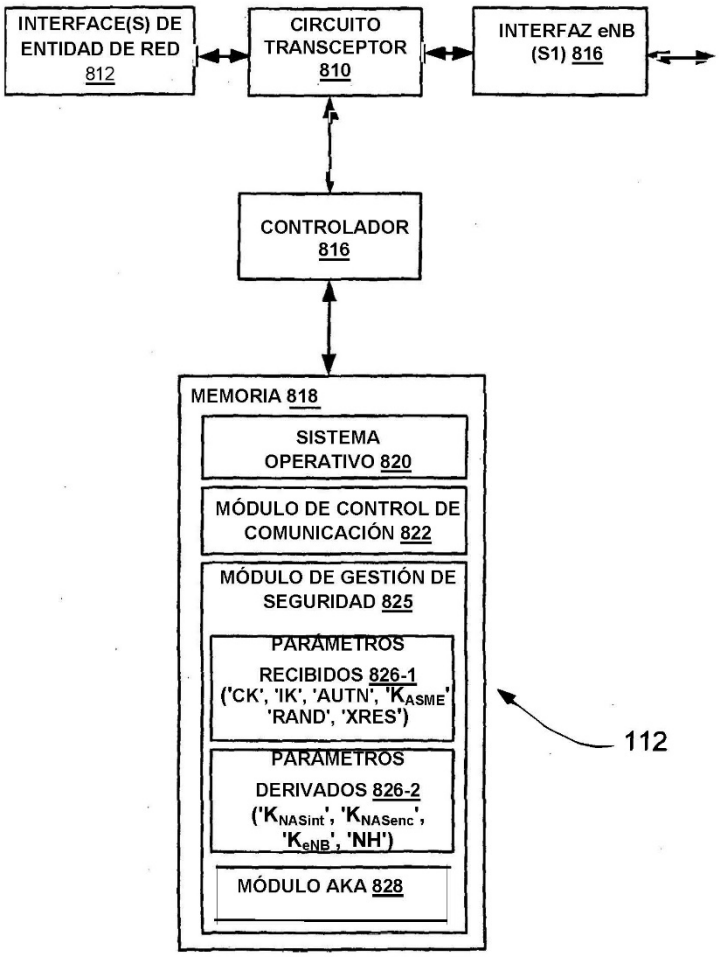
INTERFACE(S) DE ENTIDAD DE RED 812
CIRCUITO TRANSCEPTOR 810
INTERFAZ eNB (S1) 816
CONTROLADOR 816
MEMORIA 818
SISTEMA OPERATIVO 820
MÓDULO DE CONTROL DE COMUNICACIÓN 822
MÓDULO DE GESTIÓN DE SEGURIDAD 825
PARÁMETROS RECIBIDOS 826-1 ('CK', 'IK', 'AUTN', 'K_ASME' 'RAND', 'XRES')
PARÁMETROS DERIVADOS 826-2 ('K_NASint', 'K_NASenc', 'K_eNB', 'NH')
MÓDULO AKA 828
112

Figura 8

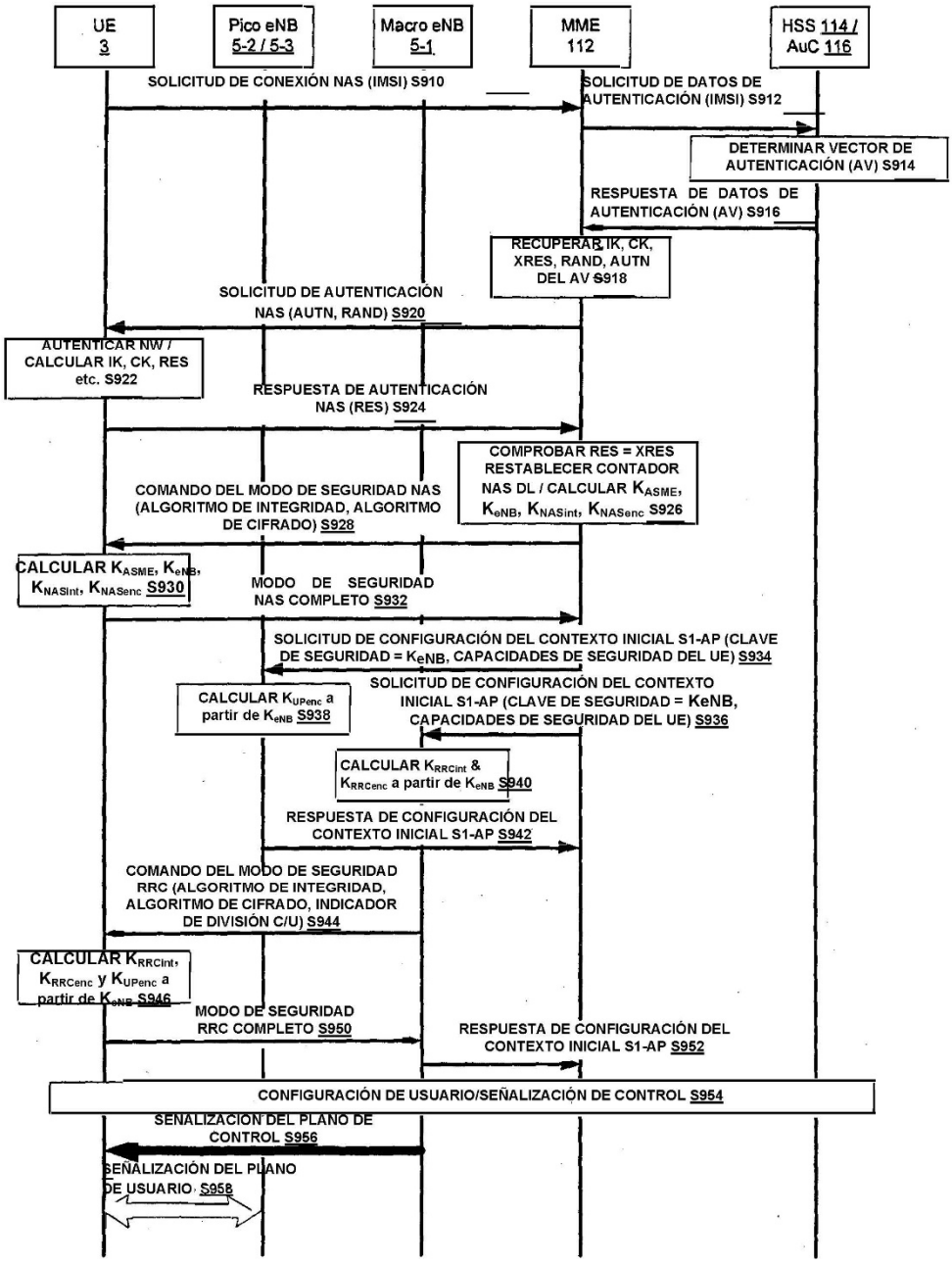
UE 3
Pico eNB 5-2 / 5-3
Macro eNB 5-1
MME 112
HSS 114 / AuC 116
SOLICITUD DE CONEXIÓN NAS (IMSI) S910
SOLICITUD DE DATOS DE AUTENTICACIÓN (IMSI) S912
DETERMINAR VECTOR DE AUTENTICACIÓN (AV) S914
RESPUESTA DE DATOS DE AUTENTICACIÓN (AV) S916
RECUPERAR IK, CK, XRES, RAND, AUTN DEL AV S918
SOLICITUD DE AUTENTICACIÓN NAS (AUTN, RAND) S920
AUTENTICAR NW / CALCULAR IK, CK, RES etc. S922
RESPUESTA DE AUTENTICACIÓN NAS (RES) S924
COMPROBAR RES = XRES RESTABLECER CONTADOR NAS DL / CALCULAR KASME, KeNB, KNASint, KNASenc S926
COMANDO DEL MODO DE SEGURIDAD NAS (ALGORITMO DE INTEGRIDAD, ALGORITMO DE CIFRADO) S928
CALCULAR KASME, KeNB, KNASint, KNASenc S930
MODO DE SEGURIDAD NAS COMPLETO S932
SOLICITUD DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP (CLAVE DE SEGURIDAD = KeNB, CAPACIDADES DE SEGURIDAD DEL UE) S934
CALCULAR KUPenc a partir de KeNB S938
SOLICITUD DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP (CLAVE DE SEGURIDAD = KeNB, CAPACIDADES DE SEGURIDAD DEL UE) S936
CALCULAR KRRCint & KRRCenc a partir de KeNB S940
RESPUESTA DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP S942
COMANDO DEL MODO DE SEGURIDAD RRC (ALGORITMO DE INTEGRIDAD, ALGORITMO DE CIFRADO, INDICADOR DE DIVISIÓN C/U) S944
CALCULAR KRRCint, KRRCenc y KUPenc a partir de KeNB S946
MODO DE SEGURIDAD RRC COMPLETO S950
RESPUESTA DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP S952
CONFIGURACIÓN DE USUARIO/SEÑALIZACIÓN DE CONTROL S954
SEÑALIZACIÓN DEL PLANO DE CONTROL S956
SEÑALIZACIÓN DEL PLANO DE USUARIO S958

Figura 9

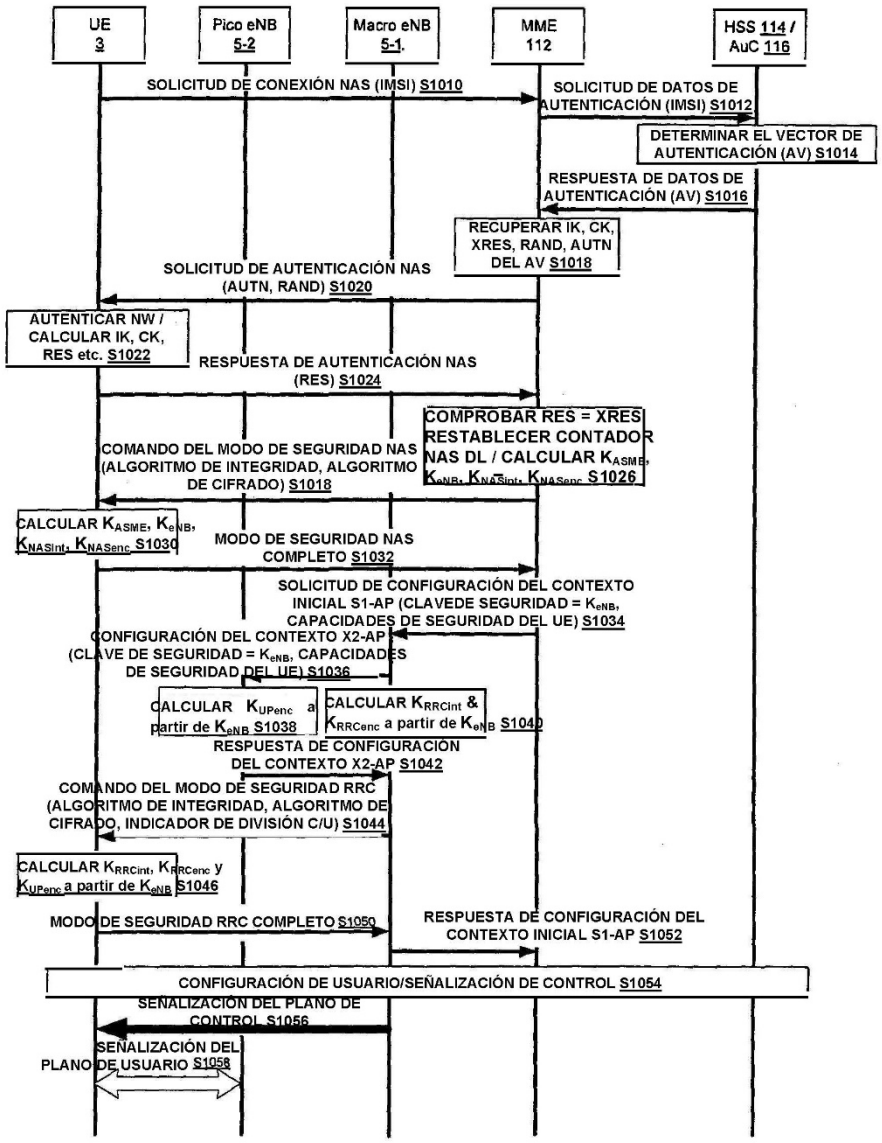
UE 3
Pico eNB 5-2
Macro eNB 5-1
MME 112
HSS 114 / AuC 116
SOLICITUD DE CONEXIÓN NAS (IMSI) S1010
SOLICITUD DE DATOS DE AUTENTICACIÓN (IMSI) S1012
DETERMINAR EL VECTOR DE AUTENTICACIÓN (AV) S1014
RESPUESTA DE DATOS DE AUTENTICACIÓN (AV) S1016
RECUPERAR IK, CK, XRES, RAND, AUTN DEL AV S1018
SOLICITUD DE AUTENTICACIÓN NAS (AUTN, RAND) S1020
AUTENTICAR NW / CALCULAR IK, CK, RES etc. S1022
RESPUESTA DE AUTENTICACIÓN NAS (RES) S1024
COMPROBAR RES = XRES RESTABLECER CONTADOR NAS DL / CALCULAR K_{ASME}, K_{eNB}, K_{NASint}, K_{NASenc} S1026
COMANDO DEL MODO DE SEGURIDAD NAS (ALGORITMO DE INTEGRIDAD, ALGORITMO DE CIFRADO) S1018
CALCULAR K_{ASME}, K_{eNB}, K_{NASint}, K_{NASenc} S1030
MODO DE SEGURIDAD NAS COMPLETO S1032
SOLICITUD DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP (CLAVEDE SEGURIDAD = K_{eNB}, CAPACIDADES DE SEGURIDAD DEL UE) S1034
CONFIGURACIÓN DEL CONTEXTO X2-AP (CLAVE DE SEGURIDAD = K_{eNB}, CAPACIDADES DE SEGURIDAD DEL UE) S1036
CALCULAR K_{UPenc} a partir de K_{eNB} S1038
CALCULAR K_{RRCint} & K_{RRCenc} a partir de K_{eNB} S1040
RESPUESTA DE CONFIGURACIÓN DEL CONTEXTO X2-AP S1042
COMANDO DEL MODO DE SEGURIDAD RRC (ALGORITMO DE INTEGRIDAD, ALGORITMO DE CIFRADO, INDICADOR DE DIVISIÓN C/U) S1044
CALCULAR K_{RRCint}, K_{RRCenc} y K_{UPenc} a partir de K_{eNB} S1046
MODO DE SEGURIDAD RRC COMPLETO S1050
RESPUESTA DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP S1052
CONFIGURACIÓN DE USUARIO/SEÑALIZACIÓN DE CONTROL S1054
SEÑALIZACIÓN DEL PLANO DE CONTROL S1056
SEÑALIZACIÓN DEL PLANO DE USUARIO S1058

Figura 10

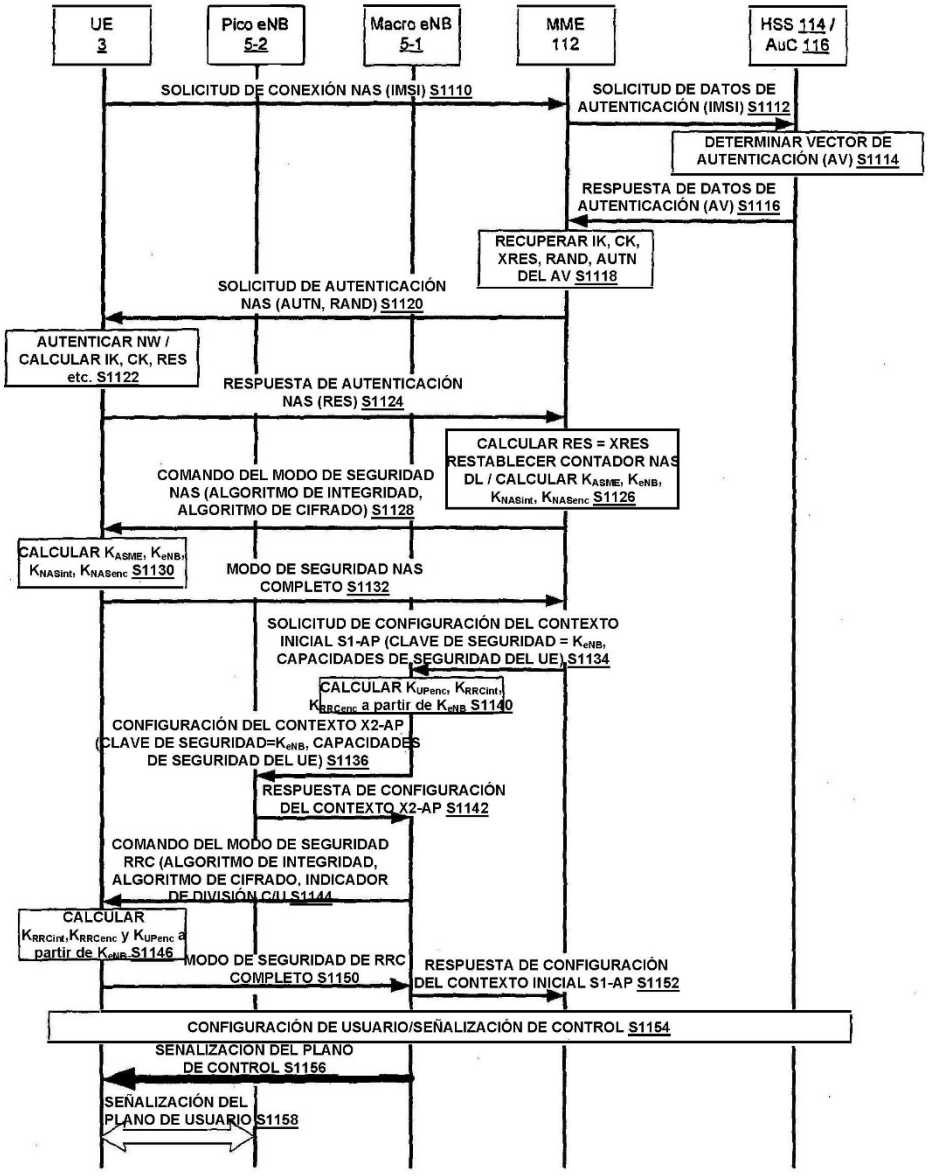
UE 3
Pico eNB 5-2
Macro eNB 5-1
MME 112
HSS 114 / AuC 116
SOLICITUD DE CONEXIÓN NAS (IMSI) S1110
SOLICITUD DE DATOS DE AUTENTICACIÓN (IMSI) S1112
DETERMINAR VECTOR DE AUTENTICACIÓN (AV) S1114
RESPUESTA DE DATOS DE AUTENTICACIÓN (AV) S1116
RECUPERAR IK, CK, XRES, RAND, AUTN DEL AV S1118
SOLICITUD DE AUTENTICACIÓN NAS (AUTN, RAND) S1120
AUTENTICAR NW / CALCULAR IK, CK, RES etc. S1122
RESPUESTA DE AUTENTICACIÓN NAS (RES) S1124
CALCULAR RES = XRES RESTABLECER CONTADOR NAS DL / CALCULAR KASME, KeNB, KNASint, KNASenc S1126
COMANDO DEL MODO DE SEGURIDAD NAS (ALGORITMO DE INTEGRIDAD, ALGORITMO DE CIFRADO) S1128
CALCULAR KASME, KeNB, KNASint, KNASenc S1130
MODO DE SEGURIDAD NAS COMPLETO S1132
SOLICITUD DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP (CLAVE DE SEGURIDAD = KeNB, CAPACIDADES DE SEGURIDAD DEL UE) S1134
CALCULAR KUPenc, KRRCint, KRRCenc a partir de KeNB S1140
CONFIGURACIÓN DEL CONTEXTO X2-AP (CLAVE DE SEGURIDAD=KeNB, CAPACIDADES DE SEGURIDAD DEL UE) S1136
RESPUESTA DE CONFIGURACIÓN DEL CONTEXTO X2-AP S1142
COMANDO DEL MODO DE SEGURIDAD RRC (ALGORITMO DE INTEGRIDAD, ALGORITMO DE CIFRADO, INDICADOR DE DIVISIÓN C/U S1144
CALCULAR KRRCint, KRRCenc y KUPenc a partir de KeNB S1146
MODO DE SEGURIDAD DE RRC COMPLETO S1150
RESPUESTA DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP S1152
CONFIGURACIÓN DE USUARIO/SEÑALIZACIÓN DE CONTROL S1154
SEÑALIZACIÓN DEL PLANO DE CONTROL S1156
SEÑALIZACIÓN DEL PLANO DE USUARIO S1158

Figura 11

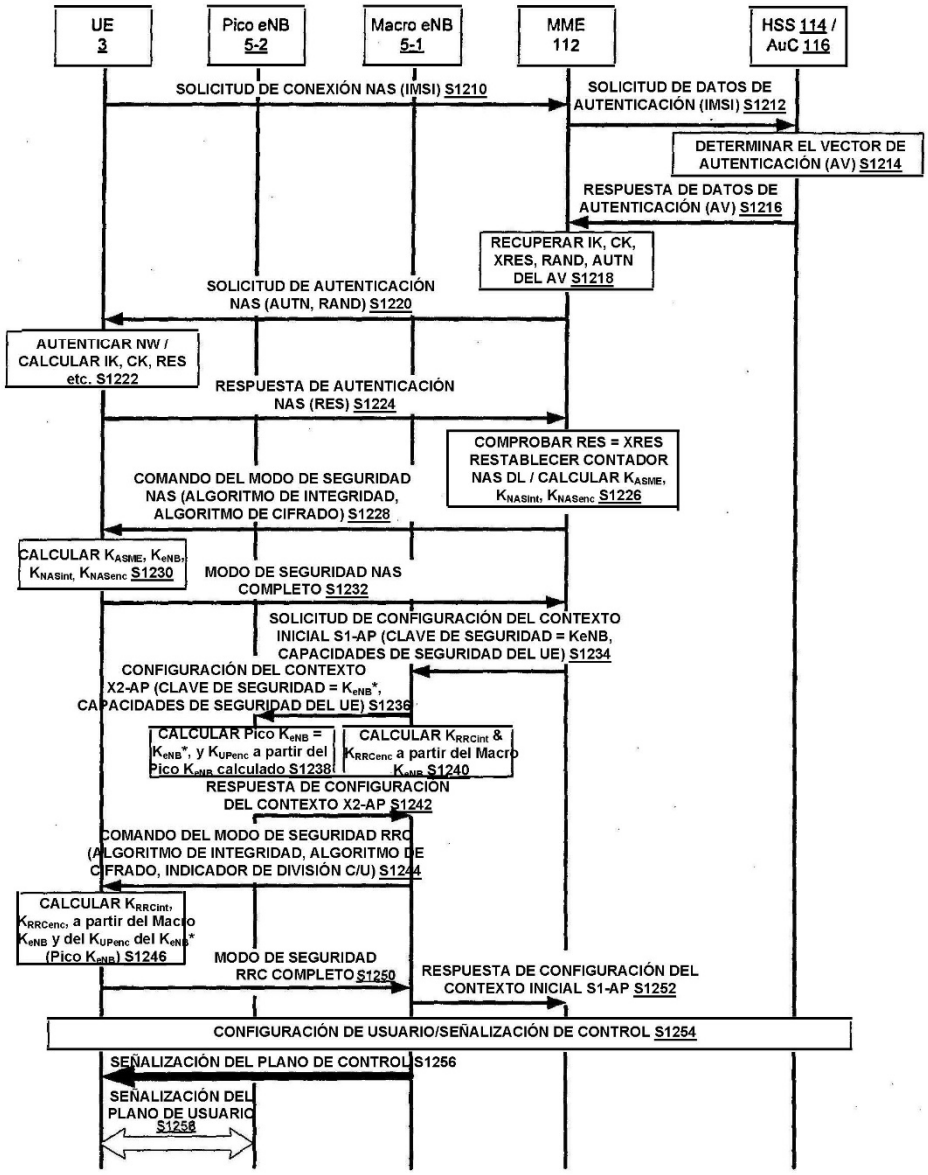
UE 3
Pico eNB 5-2
Macro eNB 5-1
MME 112
HSS 114 / AuC 116
SOLICITUD DE CONEXIÓN NAS (IMSI) S1210
SOLICITUD DE DATOS DE AUTENTICACIÓN (IMSI) S1212
DETERMINAR EL VECTOR DE AUTENTICACIÓN (AV) S1214
RESPUESTA DE DATOS DE AUTENTICACIÓN (AV) S1216
RECUPERAR IK, CK, XRES, RAND, AUTN DEL AV S1218
SOLICITUD DE AUTENTICACIÓN NAS (AUTN, RAND) S1220
AUTENTICAR NW / CALCULAR IK, CK, RES etc. S1222
RESPUESTA DE AUTENTICACIÓN NAS (RES) S1224
COMPROBAR RES = XRES RESTABLECER CONTADOR NAS DL / CALCULAR KASME, KNASint, KNASenc S1226
COMANDO DEL MODO DE SEGURIDAD NAS (ALGORITMO DE INTEGRIDAD, ALGORITMO DE CIFRADO) S1228
CALCULAR KASME, KeNB, KNASint, KNASenc S1230
MODO DE SEGURIDAD NAS COMPLETO S1232
SOLICITUD DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP (CLAVE DE SEGURIDAD = KeNB, CAPACIDADES DE SEGURIDAD DEL UE) S1234
CONFIGURACIÓN DEL CONTEXTO X2-AP (CLAVE DE SEGURIDAD = KeNB*, CAPACIDADES DE SEGURIDAD DEL UE) S1236
CALCULAR Pico KeNB = KeNB*, y KUPenc a partir del Pico KeNB calculado S1238
CALCULAR KRRCint & KRRCenc a partir del Macro KeNB S1240
RESPUESTA DE CONFIGURACIÓN DEL CONTEXTO X2-AP S1242
COMANDO DEL MODO DE SEGURIDAD RRC (ALGORITMO DE INTEGRIDAD, ALGORITMO DE CIFRADO, INDICADOR DE DIVISIÓN C/U) S1244
CALCULAR KRRCint, KRRCenc, a partir del Macro KeNB y del KUPenc del KeNB* (Pico KeNB) S1246
MODO DE SEGURIDAD RRC COMPLETO S1250
RESPUESTA DE CONFIGURACIÓN DEL CONTEXTO INICIAL S1-AP S1252
CONFIGURACIÓN DE USUARIO/SEÑALIZACIÓN DE CONTROL S1254
SEÑALIZACIÓN DEL PLANO DE CONTROL S1256
SEÑALIZACIÓN DEL PLANO DE USUARIO S1258

Figura 12

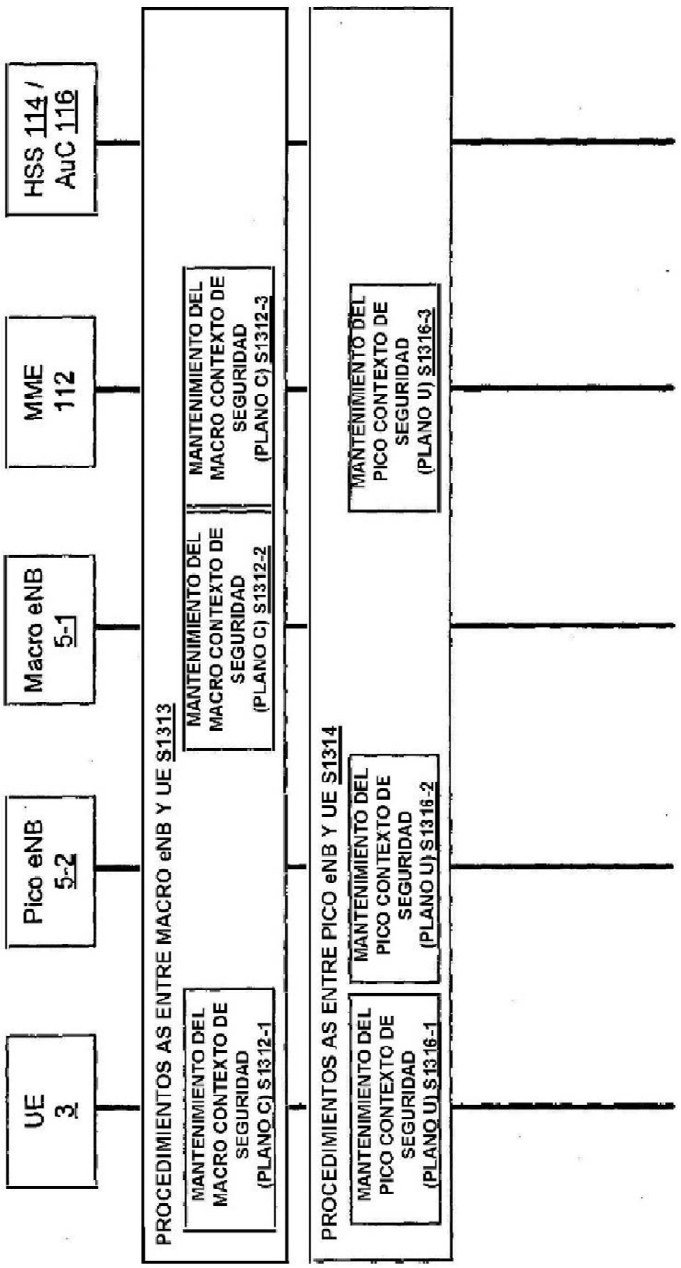
UE 3
Pico eNB 5-2
Macro eNB 5-1
MME 112
HSS 114 / AuC 116
PROCEDIMIENTOS AS ENTRE MACRO eNB Y UE S1313
MANTENIMIENTO DEL MACRO CONTEXTO DE SEGURIDAD (PLANO C) S1312-1
MANTENIMIENTO DEL MACRO CONTEXTO DE SEGURIDAD (PLANO C) S1312-2
MANTENIMIENTO DEL MACRO CONTEXTO DE SEGURIDAD (PLANO C) S1312-3
PROCEDIMIENTOS AS ENTRE PICO eNB Y UE S1314
MANTENIMIENTO DEL PICO CONTEXTO DE SEGURIDAD (PLANO U) S1316-1
MANTENIMIENTO DEL PICO CONTEXTO DE SEGURIDAD (PLANO U) S1316-2
MANTENIMIENTO DEL PICO CONTEXTO DE SEGURIDAD (PLANO U) S1316-3

Figura 13