(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 568 237**

(51) Int. CI.:

H04B 7/155 (2006.01)
H04W 24/02 (2009.01)
H04W 84/04 (2009.01)
H04W 12/06 (2009.01)
H04L 12/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.06.2011 E 11728147 (7)**

(97) Fecha y número de publicación de la concesión europea: **13.01.2016 EP 2583481**

(54) Título: **Método y aparato para la gestión y autorización de nodo repetidor**

(30) Prioridad:

16.06.2011 US 201113162332
18.06.2010 US 356409 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.04.2016

(73) Titular/es:

QUALCOMM INCORPORATED (100.0%)
5775 Morehouse Drive
San Diego, CA 92121-1714, US

(72) Inventor/es:

PALANIGOUNDER, ANAND y
ESCOTT, ADRIAN EDWARD

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Método y aparato para la gestión y autorización de nodo repetidor

ANTECEDENTES

Campo

Diversas características se refieren a sistemas de comunicaciones inalámbricas y, más particularmente, a nodos repetidores empleados en un sistema de comunicaciones inalámbricas.

Antecedentes

Según ha evolucionado la tecnología de las telecomunicaciones, se ha establecido equipo de acceso a red más avanzado que puede proporcionar servicios que no eran posibles previamente. Este equipo de acceso de red puede incluir sistemas y dispositivos que son mejoras del equipo equivalente en un sistema de telecomunicaciones inalámbricas tradicional. Dicho equipo avanzado o de próxima generación puede incluirse en estándares de comunicaciones inalámbricas de evolución, tal como evolución a largo plazo (LTE). Por ejemplo, un sistema LTE puede incluir un nodo B mejorado (eNB), un punto de acceso inalámbrico, o un componente similar en lugar de un nodo de acceso tradicional (o una estación base).

En algunas implementaciones, una red puede incluir tanto nodos de acceso como nodos repetidores, que también puede denominarse en el presente documento como dispositivo repetidor. Un nodo repetidor es un componente de red relativamente nuevo en una red inalámbrica que está configurado para extender o mejorar la cobertura creada por un nodo de acceso u otro nodo repetidor. El nodo de acceso y el nodo repetidor son ambos componentes de radio que pueden estar presentes en una red de comunicaciones inalámbrica. Un nodo repetidor requiere típicamente la cobertura inalámbrica de un nodo de acceso u otro nodo repetidor para acceder a otros componentes en un sistema de comunicaciones inalámbricas. Adicionalmente, pueden usarse en serie dos o más nodos repetidores para extender o mejorar la cobertura creada por un nodo de acceso.

Un nodo repetidor típicamente incorpora tanto funciones de terminal de acceso como funciones de nodo de acceso. Por ejemplo, El nodo repetidor recibe datos de la red como si fuese un terminal de acceso, y transmite los datos recibidas a un terminal de acceso como si fuese un nodo de acceso. Para que un nodo repetidor funciona apropiadamente, el nodo repetidor debe proveerse/configurarse apropiadamente con las credenciales operativas y de seguridad necesarias antes de que el nodo repetidor se ponga en funcionamiento. Dado que los nodos repetidores recién desplegados pueden no tener enlaces de comunicación existentes a un sistema de gestión de operador (por ejemplo, un sistema de Operación, Administración, Mantenimiento y Aprovisionamiento (OAM&P) de un operador), los nodos repetidores requieren convencionalmente personal operador que esté en el emplazamiento para configurar inicialmente el nodo repetidor. Sin embargo, requerir personal de operador en el emplazamiento de despliegue del repetidor es costoso, propenso a errores y no es seguro. La otra alternativa convencional es usar los métodos de comunicación preexistentes del operador, tal como enlaces IP arrendados o enlaces por microondas inalámbricos, para comunicar con el sistema de gestión del operador. Sin embargo, proporcionar conexión al nodo repetidor a través de estas otras formas de comunicación también es costoso.

El documento XP050422555 se refiere a la configuración y activación inicial de un RN. El nodo repetidor se autentica únicamente una vez (sin reautenticación). Después de proporcionar los datos de configuración de un servidor OAM, se realiza la reconfiguración de conexión RRC.

Por lo tanto, es deseable permitir que un nodo repetidor conecte de forma segura a un sistema de gestión para la configuración y autorización inicial antes del despliegue como un dispositivo repetidor plenamente operativo en una red de comunicaciones para transmitir el tráfico entre las terminales de acceso y otras entidades de red.

RESUMEN

Diversas características facilitan la configuración inalámbrica y la autorización de los nodos repetidores antes del despliegue como dispositivo repetidor en una red de comunicaciones. Una característica proporciona nodos repetidores que incluyen una interfaz de comunicación inalámbrica acoplada con un circuito de procesamiento. El circuito de procesamiento está adaptado para autenticar el nodo repetidor con una entidad de red usando las credenciales de seguridad iniciales para la autenticación. En respuesta a la autenticación inalámbrica usando las credenciales de seguridad iniciales, el circuito de procesamiento recibe autorización para comunicar inalámbricamente con una red de comunicación para un fin limitado de configuración del nodo repetidor. Como parte de las comunicaciones limitadas, el circuito de procesamiento recibe nuevas credenciales de seguridad a través de la interfaz de comunicación inalámbrica. Después, el circuito de procesamiento reautentica a la entidad de red usando las nuevas credenciales de seguridad antes de operar como un dispositivo repetidor en la red de comunicación.

También se proporcionan métodos operativos en un nodo repetidor de acuerdo con una característica para facilitar la configuración y la autorización inalámbrica del nodo repetidor antes del despliegue como un dispositivo repetidor en una red de comunicación. En al menos una implementación de dichos métodos, por ejemplo, el nodo repetidor se autentica por vía inalámbrica con una entidad de red usando las credenciales de seguridad iniciales. Se recibe la autorización para comunicar por vía inalámbrica con una red de comunicación para un fin limitado de configuración del nodo repetidor en la autenticación, donde la autorización se recibe en respuesta a la autenticación inalámbrica usando las credenciales de seguridad iniciales. Como parte de las comunicaciones limitadas, se reciben nuevas credenciales de seguridad. Después, el nodo repetidor se reautentica con respecto a la entidad de red usando las nuevas credenciales de seguridad antes de habilitarse para operar como un dispositivo repetidor en la red de comunicación.

Otra característica proporciona una o más entidades de red adaptadas para facilitar una configuración y autorización inalámbrica de los nodos repetidores antes del despliegue como un dispositivo repetidor en una red de comunicación. Tal entidad de red puede comprender una interfaz de comunicaciones acoplada con un circuito de procesamiento. El circuito de procesamiento está adaptado para autenticar un nodo repetidor usando las credenciales de seguridad iniciales asociadas al nodo repetidor. El circuito de procesamiento autorizar al nodo repetidor para comunicar inalámbrica con una red de comunicación para un fin limitado de configuración del nodo repetidor después de una autenticación satisfactoria del nodo repetidor usando las credenciales de seguridad iniciales. El circuito de procesamiento también reautentica el nodo repetidor usando nuevas credenciales de seguridad asociadas al nodo repetidor, y autoriza al nodo repetidor a operar como un dispositivo repetidor en la red de comunicación después de reautenticar satisfactoriamente el nodo repetidor.

También se proporcionan métodos operativos en una entidad de red de acuerdo con una característica para facilitar la configuración y autorización inalámbrica de un nodo repetidor antes del despliegue como dispositivo repetidor en una red de comunicación. En al menos una implementación de dichos métodos, la entidad de red autentica un nodo repetidor usando las credenciales de seguridad iniciales asociadas al nodo repetidor. El nodo repetidor se autoriza para comunicar inalámbricamente con una red de comunicación para un fin limitado de configuración del nodo repetidor después de autenticar satisfactoriamente el nodo repetidor usando las credenciales de seguridad iniciales. El nodo repetidor se reautentica usando nuevas credenciales de seguridad, y el nodo repetidor se autoriza para operar como un dispositivo repetidor en la red de comunicación después de reautenticar satisfactoriamente el nodo repetidor con las nuevas credenciales de seguridad.

La recepción de las nuevas credenciales de seguridad puede comprender recibir una nueva identidad del nodo repetidor y un nuevo secreto compartido asociado a la nueva identidad del nodo repetidor, y la reautenticación con la entidad de red usando las nuevas credenciales de seguridad comprende la reautenticación con la entidad de red usando la nueva identidad del nodo repetidor y el nuevo secreto compartido asociado a la nueva identidad del nodo repetidor. En este caso, la nueva identidad del nodo repetidor se asocia a un perfil de suscripción que autoriza acceso de red al nodo repetidor para operar como un dispositivo repetidor que transmite el tráfico entre uno o más terminales de acceso y la red de comunicación.

La reautenticación con la entidad de red usando las nuevas credenciales de seguridad puede comprender adicionalmente la reautenticación con la entidad de red usando las nuevas credenciales de seguridad y las credenciales de seguridad iniciales. En este caso, la autenticación por vía inalámbrica con la entidad de red usando una identidad del nodo repetidor inicial y un secreto compartido inicial asociado a la identidad del nodo repetidor inicial, donde la identidad del nodo repetidor inicial se asocia a un perfil de suscripción que autoriza acceso de red al nodo repetidor para un fin limitado de configuración del nodo repetidor en el momento de la autenticación inalámbrica con la entidad de red, y la reautenticación con la entidad de red usando la identidad del nodo repetidor inicial y el secreto compartido inicial asociado a la identidad del nodo repetidor inicial, donde, en el momento de la reautenticación con la entidad de red, la identidad del nodo repetidor inicial se asocia a un nuevo perfil de suscripción que autoriza acceso de red al nodo repetidor para operar como un dispositivo repetidor que transmite el tráfico de red entre una o más terminales de acceso y la red de comunicación.

La recepción de las nuevas credenciales de seguridad puede comprender recibir al menos una de las credenciales de operador o una clave compartida.

El método puede comprender adicionalmente aparecer como un dispositivo de usuario para la entidad de red al autenticarse por vía inalámbrica con la entidad de red usando las credenciales de seguridad iniciales, y aparecer como un dispositivo repetidor para la entidad de red al reautenticarse con la entidad de red usando las nuevas credenciales de seguridad.

El método puede comprender adicionalmente recibir datos de configuración para configurar el nodo repetidor como un dispositivo repetidor en la red de comunicación, recibiéndose los datos de configuración antes de la reautenticación con la entidad de red.

De acuerdo con un aspecto de la presente invención, se proporciona un nodo repetidor, que comprende:

medios para autenticar por vía inalámbrica con una entidad de red usando las credenciales de seguridad iniciales;

medios para recibir autorización para comunicar por vía inalámbrica con una red de comunicación para un fin limitado de configuración del nodo repetidor en respuesta a la autenticación inalámbrica usando las credenciales de seguridad iniciales;

medios para recibir nuevas credenciales de seguridad; y medios para reautenticar con la entidad de red usando las nuevas credenciales de seguridad antes de habilitarse para operar como un dispositivo repetidor en la red de comunicación.

De acuerdo con otro aspecto de la presente invención, se proporciona un medio legible por procesador que comprende instrucciones operativas en un nodo repetidor o en una entidad de red, que al ejecutarse por un procesador, hace que el procesador:

autentica inalámbricamente un o el nodo repetidor con una o la entidad de red usando las credenciales de seguridad iniciales; reciba autorización para comunicar inalámbricamente con una red de comunicación para un fin limitado de configuración del nodo repetidor en respuesta a la autenticación inalámbrica usando las credenciales de seguridad iniciales; reciba nuevas credenciales de seguridad; y
reautentique el nodo repetidor con respecto a la entidad de red usando las nuevas credenciales de seguridad antes de habilitarse para operar como un dispositivo repetidor en la red de comunicación

De acuerdo con otro aspecto de la presente invención, se proporciona un método operativo en una entidad de red, comprendiendo el método:

autenticar un nodo repetidor usando las credenciales de seguridad iniciales asociadas al nodo repetidor;

autorizar al nodo repetidor a comunicar inalámbricamente con una red de comunicación para un fin limitado de configuración del nodo repetidor después de una autenticación satisfactoria del nodo repetidor usando las credenciales de seguridad iniciales;

reautenticar el nodo repetidor usando nuevas credenciales de seguridad; y autorizar al nodo repetidor a operar como un dispositivo repetidor en la red de comunicación después de reautenticar satisfactoriamente el nodo repetidor.

La autorización del nodo repetidor para comunicar inalámbricamente con una red de comunicación para un fin limitado de configuración del nodo repetidor, puede comprender autorizar al nodo repetidor para comunicar inalámbricamente con una red de comunicación para un fin limitado de obtener nuevas credenciales de seguridad y datos de configuración.

La reautenticación del nodo repetidor usando las nuevas credenciales de seguridad, puede incluir reautenticar el nodo repetidor usando una nueva identidad del nodo repetidor y un nuevo secreto compartido asociado a la nueva identidad del nodo repetidor. En este caso, la reautenticación del nodo repetidor puede usar la nueva identidad del nodo repetidor y el nuevo secreto compartido asociado a la nueva identidad del nodo repetidor puede comprender obtener un perfil de suscripción asociado a la nueva identidad del nodo repetidor, donde el perfil de suscripción autoriza un acceso de red al nodo repetidor para operar como un dispositivo repetidor que transmite el tráfico entre uno o más terminales de acceso, y la red de comunicación.

Las nuevas credenciales de seguridad pueden incluir al menos una de las credenciales de operador o una clave compartida.

La reautenticación del nodo repetidor puede comprender reautenticar el nodo repetidor usando las nuevas credenciales de seguridad y las credenciales de seguridad iniciales. En este caso, las credenciales de seguridad iniciales pueden incluir una identidad del nodo repetidor inicial y un secreto compartido inicial asociado a la identidad del nodo repetidor inicial. En este caso, la autenticación del nodo repetidor usando las credenciales de seguridad iniciales puede comprender obtener un perfil de suscripción asociado a la identidad del nodo repetidor inicial, donde el perfil de suscripción autoriza la red de acceso para el nodo repetidor para un fin limitado de configuración del nodo repetidor, y la reautenticación del nodo repetidor usando las nuevas credenciales de seguridad comprende obtener un nuevo perfil de suscripción asociado a la identidad del nodo repetidor inicial, donde el nuevo perfil de suscripción autoriza suficiente acceso de red para el nodo repetidor para permitir que el nodo repetidor opere como un dispositivo repetidor que transmite el tráfico entre uno o más terminales de acceso y la red de comunicación.

La autenticación del nodo repetidor usando las credenciales de seguridad iniciales puede comprender autenticar el nodo repetidor apareciendo con respecto a la entidad de red como un dispositivo de usuario, y la reautenticación del nodo repetidor usando las nuevas credenciales de seguridad comprende reautenticar el nodo repetidor apareciendo con respecto a la entidad de red como un dispositivo repetidor.

De acuerdo con otro aspecto de la presente invención, se proporciona una entidad de red, que comprende:

medios para autenticar un nodo repetidor usando las credenciales de seguridad iniciales asociadas al nodo repetidor; medios para autorizar al nodo repetidor a comunicar por vía inalámbrica con una red de comunicación para un fin limitado de configuración del nodo repetidor después de una autenticación satisfactoria del nodo repetidor usando las credenciales de seguridad iniciales;
medios para reautenticar el nodo repetidor usando nuevas credenciales de seguridad; y
medios para autorizar al nodo repetidor para operar como un dispositivo repetidor en la red de comunicación después de reautenticar satisfactoriamente el nodo repetidor.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La FIG. 1 es un diagrama de bloques que ilustra un sistema de comunicación inalámbrica que emplea uno o más nodos repetidores y adaptado para facilitar la configuración y autorización inalámbrica de un nodo repetidor al desplegarse inicialmente.

La FIG. 2 es un diagrama de flujo que ilustra un ejemplo de al menos una implementación para configurar y autorizar inicialmente un nodo repetidor.

La FIG. 3 (que comprende la FIG. 3A y la FIG. 3B) es un diagrama de flujo que ilustra al menos un ejemplo de configuración y autorización inicial de un nodo repetidor usando las nuevas credenciales de seguridad para la reautenticación.

La FIG. 4 (que comprende la FIG. 4A y la FIG. 4B) es un diagrama de flujo que ilustra al menos un ejemplo de configuración y autorización inicial de un nodo repetidor usando las nuevas credenciales de seguridad para la reautenticación.

La FIG. 5 (que comprende la FIG. 5A y la FIG. 5B) es un diagrama de flujo que ilustra al menos un ejemplo de configuración y autorización inicial de un nodo repetidor usando las credenciales de seguridad iniciales junto con las nuevas credenciales de seguridad para la reautenticación.

La FIG. 6 es un diagrama de bloques que ilustra componentes seleccionados de un nodo repetidor de acuerdo con al menos una realización.

La FIG. 7 es un diagrama de flujo que ilustra un ejemplo de al menos una implementación de un método operativo en un nodo repetidor.

La FIG. 8 es un diagrama de bloques que ilustra componentes seleccionados de una entidad de red 800 de acuerdo con al menos una realización.

La FIG. 9 es un diagrama de flujo que ilustra un ejemplo de al menos una implementación de un método operativo en una entidad de red.

La FIG. 10 ilustra un ejemplo de cómo pueden usarse las credenciales de seguridad iniciales para generar una jerarquía de claves que puede implementarse en una red de comunicación inalámbrica típica.

DESCRIPCIÓN DETALLADA

En la siguiente descripción, se dan detalles específicos para proporcionar una comprensión profunda de las implementaciones descritas. Sin embargo, se entenderá por un experto en la técnica que pueden llevarse a la práctica diversas implementaciones sin estos detalles específicos. Por ejemplo, pueden mostrarse circuitos en diagramas de bloques para no complicar las implementaciones con detalles innecesarios. En otros casos, pueden mostrarse en detalle circuitos ya conocidos, estructuras y técnicas para no complicar las implementaciones descritas.

La expresión "ejemplar" se usa en el presente documento en el sentido de "que sirve como ejemplo, instancia o ilustración". Cualquier implementación o realización descrita en el presente documento como "ejemplar" no debe considerarse necesariamente como preferida o ventajosa con respecto a otras realizaciones o implementaciones. Asimismo, el término "realizaciones" no requiere que todas las realizaciones incluyan la característica, ventaja o modo de funcionamiento analizados.

Resumen

Una característica facilita el despliegue inicial de los nodos repetidores en una red de comunicación. Un nodo repetidor se une inicialmente inalámbricamente a la red de comunicación y se autentica usando unos parámetros de

seguridad iniciales proporcionados previamente en el nodo repetidor. Tras la autenticación, el nodo repetidor se autoriza para comunicar inalámbrica con la red de comunicación para el alcance limitado de obtener nuevas credenciales de seguridad y datos de configuración. Después de configurar el nodo repetidor para el funcionamiento como un dispositivo repetidor en la red, el nodo repetidor se une de nuevo a la red de comunicación y se reautentica. La reautenticación se basa en las nuevas credenciales de seguridad recibidas durante el periodo de acceso limitado para el nodo repetidor. Después de reautenticar el nodo repetidor, el nodo repetidor se autoriza para operar en la red de comunicación como un dispositivo repetidor que transmite el tráfico entre uno o más terminales de acceso y la red de comunicación.

Entorno de Red Ejemplar

La FIG. 1 es un diagrama de bloques que ilustra un sistema de comunicación inalámbrica que emplea uno o más nodos repetidores y adaptado para facilitar la configuración y autorización inalámbrica de un nodo repetidor al desplegarse inicialmente. En al menos algunas implementaciones, se emplean nodos repetidores 102 en redes de comunicaciones inalámbricas, tales como redes LTE o LTE-avanzada (LTE-A). El nodo repetidor 102 puede amplificar o repetir una señal recibida de un terminal de acceso 104 y hacer que la señal modificada se reciba en un nodo de acceso 106. En general, el nodo repetidor 102 puede aparecer para el terminal de acceso 104 como nodo de acceso (AN) y puede aparecer para el nodo de acceso como un terminal de acceso (AT), como se muestra en la FIG. 1. En algunas implementaciones, el nodo repetidor 102 recibe una señal con datos del terminal de acceso 104 y después genera una señal para transmitir los datos al nodo de acceso 106. El nodo repetidor 102 también puede recibir datos del nodo de acceso 106 y entregar los datos al terminal de acceso 104. El nodo repetidor 102 puede situarse cerca de los bordes de una célula de manera que el terminal de acceso 104 pueda comunicar con el nodo repetidor 102 en lugar de comunicar directamente con el nodo de acceso 106 para esa célula.

En sistemas de radio, una célula es un área geográfica de cobertura de recepción y transmisión. Las células pueden solaparse entre sí. En el ejemplo típico, hay un nodo de acceso asociado a cada célula. El tamaño de una célula se determina por factores tales como la banda de frecuencia, el nivel de potencia y las condiciones del canal. Pueden usarse nodos repetidores, tal como el nodo repetidor 102, para mejorar la cobertura dentro o cerca de una célula, o para extender el tamaño de cobertura de una célula. Adicionalmente, el uso de un nodo repetidor 102 puede mejorar el rendimiento de una señal dentro de una célula porque el terminal de acceso 104 puede acceder al nodo repetidor 102 a una mayor velocidad de datos o una transmisión de potencia inferior de la que el terminal de acceso 104 puede usar al comunicar directamente con el nodo de acceso 106 para esa célula. La transmisión a una mayor velocidad de datos crea una mayor eficiencia del espectro, y una potencia inferior beneficia al terminal de acceso 104 consumiendo menos potencia de la batería.

Un nodo repetidor 102 puede implementarse como uno de tres tipos: un nodo repetidor monocapa, un nodo repetidor bicapa, y un nodo repetidor tricapa. Un nodo repetidor monocapa es básicamente un repetidor que puede retransmitir una transmisión sin ninguna modificación distinta de la amplificación y un ligero retardo. Un nodo repetidor bicapa puede decodificar una transmisión que recibe, recodificar el resultado de la decodificación, y después transmitir los datos recodificados. Un nodo repetidor tricapa puede tener capacidades de control de recursos de radio completos y, por lo tanto, puede funcionar de forma análoga a un nodo de acceso. Los protocolos de control de recursos de radio usados por un nodo repetidor pueden ser los mismos que los usados por un nodo de acceso, y el nodo repetidor puede tener una única identidad de célula usada típicamente por un nodo de acceso.

Para el fin de esta divulgación, se distingue un nodo repetidor 102 de un nodo de acceso 106 por el hecho de que el nodo repetidor 102 puede basarse en la presencia de al menos un nodo de acceso 106 (y la célula asociada a ese nodo de acceso) u otro nodo repetidor para acceder a otros componentes en un sistema de telecomunicaciones (por ejemplo, la red 108). Es decir, el nodo repetidor 102 puede aparecer como un dispositivo de abonado, un dispositivo de cliente, o un terminal de acceso a la red, por lo tanto, conecta a un nodo de acceso para comunicar por la red. Sin embargo, otros dispositivos de abonado, dispositivos de usuario y/o terminales de acceso del nodo repetidor 102 pueden aparecer como un dispositivo de red (por ejemplo, un nodo de acceso). En consecuencia, el nodo repetidor 102 puede implementar una o más interfaces de comunicación para comunicar con un nodo de acceso y/o uno o más terminales de acceso/abonado/usuario. En un ejemplo, el mismo transmisor/receptor (por ejemplo, en uno o más canales inalámbricos) puede usarse por el nodo repetidor 102 para comunicar con su nodo de acceso y/o uno o más terminales de acceso. En otro ejemplo, el nodo repetidor 102 puede utilizar dos o más transmisores/receptores diferentes para comunicar con el nodo de acceso y/o el uno o más terminales de acceso.

El nodo de acceso 106 puede acoplarse con la red 108 (por ejemplo, una red central) a través de un enlace backhaul. La red 108 puede incluir una o más entidades de gestión de movilidad (MME) 110, un sistema de operaciones, administración, mantenimiento y aprovisionamiento (OAM&P) 112, y pasarelas de servicios y PDN (SGW/PGW) 114.

Cuando el nodo repetidor 102 se instala inicialmente y se configura, el nodo repetidor 102 se adapta para conectar de forma segura con la red 108 para configurarse y autorizarse para funcionar como un nodo repetidor. En particular, el nodo repetidor 102 incluye credenciales de seguridad iniciales, que permiten al nodo repetidor 102 unirse a la red 108 a través de un nodo de acceso 106 usando la red de comunicación, tal como una red LTE o LTE-A, como el

backhaul. Puede permitirse al nodo repetidor 102 acceder únicamente a los elementos de red de gestión necesarios para la configuración y autorización, tal como una entidad de gestión de movilidad (MME) 110 y un sistema de operaciones, administración, mantenimiento y aprovisionamiento (OAM&P) 112.

Después, los elementos de red de gestión pueden configurar el nodo repetidor 102 con la información operativa necesaria, incluyendo nuevas credenciales de seguridad. Después de configurar el nodo repetidor 102 y dotarlo de cualquier nueva credencial de seguridad, el nodo repetidor 102 puede reautenticar a la red 108 usando las nuevas credenciales de seguridad y la información operativa proporcionada que permite al nodo repetidor 102 funcionar como un dispositivo repetidor plenamente operativo.

Las credenciales de seguridad iniciales pueden incluir una o más claves, certificados y/o información de abonados/cuentas usados, por ejemplo, para conectar con una red, obtener servicio de una red, iniciar una sesión de comunicación, y/o asegurar un enlace de comunicación. A modo de ejemplo y sin limitación, las credenciales de seguridad iniciales y nuevas pueden referirse a una clave maestra y/o algoritmos empleados con una clave maestra para generar una pluralidad de claves de cifrado y/o integridad diferentes.

La FIG. 10 ilustra un ejemplo de cómo pueden usarse las credenciales de seguridad iniciales para generar una jerarquía de claves 1000 que puede implementarse en una red de comunicación inalámbrica típica para establecer claves de encriptación o seguridad para su uso en la encriptación de comunicaciones entre un nodo repetidor 102 y la red 108. El nodo repetidor 102 (por ejemplo, en una tarjeta de circuito integrado universal (UICC) y/o un entorno de confianza (TrE)) y la red 108 puede usar una clave maestra K 1002 para generar una clave de cifrado (CK) 1004 y una clave de integridad (IK) 1006. Después, la clave de cifrado (CK) 1004 y la clave de integridad (IK) 1006 pueden usarse por el nodo repetidor 102 y la red 108 para generar una clave de entidad de gestión de seguridad de acceso K_ASME 1008. La activación de la seguridad de un nodo repetidor 102 puede realizarse a través de un procedimiento de acuerdo de autenticación y clave (AKA), un procedimiento de configuración de modo seguro de estrato sin acceso (NAS) (NAS SMC) y/o un procedimiento de configuración de modo seguro de estrato de acceso (AS) (AS SMC). Se usa AKA para obtener la clave K_ASME 1008, que puede usarse como una clave base para el cálculo de las claves NAS (estrato sin acceso) 1010 y 1012 y las claves AS (estrato de acceso) 1014, 1016, 1018 y 1020. Después, el nodo repetidor 102 y la red 108 pueden usar la K_ASME 1008 para generar una o más de estas claves de seguridad.

Configuración y Autorización Inicial Ejemplar de un Nodo Repetidor

La FIG. 2 es un diagrama de flujo que ilustra un ejemplo de al menos una implementación para configurar y autorizar inicialmente un nodo repetidor. El nodo repetidor 102, el nodo de acceso 106, la entidad de gestión de movilidad 110 y el sistema de operaciones, administración, mantenimiento y aprovisionamiento (OAM&P) 112 de la FIG. 1 se muestran con fines ilustrativos. El nodo de acceso 106 se incluye para ilustrar que las comunicaciones entre el nodo repetidor 102 y las diversas entidades de red se facilitan a través del nodo de acceso 106.

Inicialmente, el nodo repetidor 102 está dotado de credenciales de seguridad 202 que permitirán al nodo repetidor 102 unirse a la red usando la red de comunicación inalámbrica con el backhaul y permitiendo un acceso limitado a los elementos de red de gestión. Las credenciales de seguridad iniciales pueden incluir una identidad del nodo repetidor 102 (por ejemplo, una identidad internacional de abonado móvil (IMSI)), así como una o más claves secretas compartidas previamente y/o certificados.

El nodo repetidor 102 puede comunicar con la entidad de gestión de movilidad (MME) 110 a través del nodo de acceso 106 para unirse inicialmente a la red y autenticarse 204. El nodo repetidor 102 puede unirse inicialmente a la red como un dispositivo de usuario (por ejemplo, como un terminal de acceso). Es decir, desde la perspectiva del nodo de acceso 106 y la red, el nodo repetidor 102 puede aparecer como un dispositivo de usuario cuando el nodo repetidor 102 se une inicialmente a la red. El nodo repetidor 102 puede autenticarse en la red usando las credenciales de seguridad iniciales. Por ejemplo, la entidad de gestión de movilidad (MME) 110 puede realizar un procedimiento pregunta-respuesta u otro procedimiento de autenticación convencional o algoritmo usando los parámetros de seguridad iniciales asociados al nodo repetidor 102.

Si el nodo repetidor 102 se autentica, la entidad de gestión de movilidad (MME) 110 puede autorizar al nodo repetidor 102 para un acceso limitado a la red 206. Por ejemplo, la entidad de gestión de movilidad (MME) 110 puede restringir los destinos que el nodo repetidor 102 puede alcanzar en la red. En algunas implementaciones, el nodo repetidor 102 puede restringirse a acceder a aquellas entidades en la red que se emplean para la gestión y configuración del nodo repetidor, tal como el sistema de operaciones, administración, mantenimiento y aprovisionamiento del operador de red (OAM&P) 112. Tal restricción puede realizarse, en al menos algunas implementaciones, restringiendo los nombres de puntos de acceso a los que el nodo repetidor 102 tiene permitido acceder. Estas restricciones pueden definirse por un perfil de suscripción asociado a la identidad del nodo repetidor (por ejemplo, IMSI) incluida con las credenciales de seguridad iniciales.

El nodo repetidor 102 puede comunicar con una o más entidades de red de gestión y configuración (por ejemplo, el sistema de operaciones, administración, mantenimiento y aprovisionamiento (OAM&P) 112) para obtener nuevas

credenciales de seguridad 208. En al menos algunas implementaciones, las nuevas credenciales de seguridad pueden incluir un certificado de operador y/o una nueva clave compartida expedida al nodo repetidor 102 desde una autoridad de certificación. En al menos algunas implementaciones, las nuevas credenciales de seguridad pueden incluir nuevas credenciales de acuerdo de autenticación y clave (AKA). Dichas nuevas credenciales de acuerdo de autenticación y clave (AKA) pueden incluir una nueva identidad del nodo repetidor (por ejemplo, IMSI) y/o una nueva clave compartida.

El nodo repetidor 102 también puede obtener datos de gestión y configuración adicionales 210 de la entidad de red de gestión y configuración (por ejemplo, del sistema de operación, administración, mantenimiento y aprovisionamiento (OAM&P) 112). Los datos de gestión y configuración obtenidos de la entidad de red (por ejemplo, OAM&P 112) pueden incluir información de configuración para permitir al nodo repetidor 102 operar como un dispositivo repetidor en la red de comunicación. Es decir, el nodo repetidor 102 puede obtener la información de configuración apropiada para permitir al nodo repetidor 102 transmitir el tráfico de red entre las terminales de acceso y las entidades de red (por ejemplo, nodos de acceso y/o otros nodos repetidores).

Habiendo recibido las nuevas credenciales de seguridad (es decir, las credenciales de operador, las nuevas credenciales AKA, o ambas), el nodo repetidor 102 se reautentica con la red usando las nuevas credenciales de seguridad 212. Por ejemplo, el nodo repetidor 102 puede unirse de nuevo con la entidad de gestión de movilidad (MME) 110 y reautenticarse por la entidad de gestión de movilidad (MME) 110 usando al menos las nuevas credenciales de seguridad.

Si el nodo repetidor 102 se reautentica con las nuevas credenciales de seguridad, la entidad de gestión de movilidad (MME) 110 puede autorizar al nodo repetidor 102 a funcionar como un dispositivo repetidor plenamente operativo. Es decir, el nodo repetidor 102 puede ser autorizado a acceder a cualquier entidad de red necesaria para cumplir su función como dispositivo repetidor que transmite el tráfico de red entre las terminales de acceso y las entidades de red. En al menos algunas implementaciones, esto puede incluir la entidad de gestión de movilidad (MME) 110 que autoriza al nodo repetidor 102 a acceder a cualquier nombre o nombres de punto de acceso (APN) necesarios para transmitir el a y/o desde una o más terminales de acceso. Dicho acceso puede definirse por un perfil de suscripción asociado a la identidad del nodo repetidor (por ejemplo, nueva IMSI o IMSI inicial) incluido con las credenciales de seguridad empleadas para el procedimiento de reautenticación.

Primera Configuración y Autorización Inicial Ejemplar de Nodos Repetidores Usando Nuevas Credenciales AKA para la Reautenticación

La FIG. 3 (que comprende la FIG. 3A y la FIG. 3B) es un diagrama de flujo que ilustra al menos un ejemplo de configuración y autorización inicial de un nodo repetidor usando las nuevas credenciales de seguridad para la reautenticación. En el ejemplo de la FIG. 3, el nodo repetidor 102, el nodo de acceso 106, la entidad de gestión de movilidad 110 y el sistema de operación, administración, mantenimiento y aprovisionamiento (OAM&P) 112 se muestran con fines ilustrativos. El nodo de acceso 106 se incluye para ilustrar que las comunicaciones entre el nodo repetidor 102 y las diversas entidades de red se facilitan a través del nodo de acceso 106.

En el ejemplo de la FIG. 3, el nodo repetidor 102 emplea tanto una tarjeta de circuitos integrados universal (UICC) 302 como un entorno de confianza (TrE) 304 (también conocido como un entorno de ejecución de confianza o TEE). La UICC 302 puede ser parte de un módulo extraíble, mientras que el TrE 304 puede implementarse en un procesador (por ejemplo, distinto de la UICC) del nodo repetidor 102. Haciendo referencia inicialmente a la FIG. 3A, la UICC 302 puede incluir una aplicación de módulo de identidad del abonado universal (USIM), y puede comprender credenciales de seguridad iniciales proporcionadas de forma segura en la misma. Por ejemplo, la UICC 302 puede incluir credenciales de seguridad iniciales que comprenden credenciales de acuerdo de autenticación y clave (AKA) iniciales que se proporcionan de forma segura 306 en la misma. Además, el nodo repetidor 102 puede incluir credenciales de proveedor proporcionadas de forma segura y contenidas en el entorno de confianza (TrE) 304 del nodo repetidor 102. Un entorno de confianza (TrE) 304 de un nodo se especifica en el Detalle de Especificaciones 3GPP en TS 33.320.

El nodo repetidor 102 puede unirse (o conectar inalámbricamente) a la entidad de gestión de movilidad (MME) 110 y autenticarse 310 usando las credenciales de acuerdo de autenticación y clave iniciales almacenadas en la UICC 302. Para autenticar el nodo repetidor 102, la entidad de gestión de movilidad (MME) 110 puede obtener la información de suscripción y autenticación del nodo repetidor 312 de un servidor local de abonado (HSS) 314. Usando la información de suscripción y autenticación obtenida del servidor local de abonado (HSS) 314, la entidad de gestión de movilidad (MME) 110 y el nodo repetidor 102 pueden comunicarse para autenticar el nodo repetidor 102. Por ejemplo, la entidad de gestión de movilidad (MME) 110 puede obtener un secreto compartido asociado a una identidad (por ejemplo, IMSI) del nodo repetidor 102, y puede emplear un algoritmo de autenticación para verificar el nodo repetidor 102. Después de que la entidad de gestión de movilidad (MME) 110 autentica el nodo repetidor 102, la entidad de gestión de movilidad (MME) 110 puede autorizar al nodo repetidor 102 acceso limitado a la red en la etapa 316. Por ejemplo, la entidad de gestión de movilidad (MME) 110 puede autorizar el acceso para el nodo repetidor 102 a nombres de punto de acceso limitados (APN), tal como al sistema OAM&P del operador 112.

En al menos algunas implementaciones, el sistema OAM&P del operador 112 puede expedir 318 credenciales de operador (por ejemplo, un certificado de operador) al nodo repetidor 102. Las credenciales de operador pueden expedirse por una autoridad de certificación (CA) 320 del sistema OAM&P del operador 112. En la implementación ilustrada, las credenciales de operador pueden almacenarse en el entorno de confianza (TrE) 304 del nodo repetidor 102. Las credenciales de operador pueden expedirse de forma segura al nodo repetidor 102 usando las credenciales de proveedor (por ejemplo, par de claves privada y pública) contenidas en el entorno de confianza (TrE) 304 del nodo repetidor 102.

El nodo repetidor 102 puede recibir 322 nuevas credenciales de acuerdo de autenticación y clave (AKA) expedidas desde el sistema OAM&P del operador 112. Por ejemplo, las nuevas credenciales de acuerdo de autenticación y clave (AKA) pueden expedirse desde el sistema OAM&P del operador 112 y almacenarse en el entorno de confianza (TrE) 304 del nodo repetidor 102 para su uso en comunicaciones de acuerdo de autenticación y clave (AKA) posteriores del nodo repetidor 102. Las nuevas credenciales de acuerdo de autenticación y clave (AKA) pueden expedirse de forma segura por un servidor de gestión del nodo repetidor (RN-MS) 324 del sistema OAM&P del operador 112 usando un par de claves privada/pública asociado a las credenciales de proveedor o las credenciales de operador (si se emiten) en el entorno de confianza (TrE) 304. A modo de ejemplo y sin limitación, las nuevas credenciales de acuerdo de autenticación y clave (AKA) pueden incluir una nueva identidad internacional de abonado móvil (IMSI) y/o una clave de encriptación y parámetros de personalización del algoritmo del acuerdo de autenticación y clave (AKA). Por ejemplo, la clave de encriptación y los parámetros del algoritmo AKA pueden cumplir el algoritmo MILENAGE, comprendiendo los parámetros de personalización de AKA un campo de configuración de algoritmo específico del operador (por ejemplo, campo OP), y obteniéndose la clave de encriptación (por ejemplo, OPc) a partir del campo de configuración del algoritmo específico del operador. El sistema OAM&P del operador 112 también actualizar 326 el servidor local de abonado (HSS) 314 con la nueva información de autenticación y suscripción asociada al nodo repetidor 102.

Haciendo referencia ahora a la FIG. 3B, el sistema OAM&P del operador 112 también puede gestionar 328 el nodo repetidor 102 para configurar el nodo repetidor 102 para su uso en la red de comunicación como un dispositivo repetidor que transmite el tráfico entre las terminales de acceso y las entidades de red (por ejemplo, nodos de acceso, otros nodos repetidores). Puede usarse cualquier protocolo de gestión convencional para configurar el nodo repetidor 102, tal como, por ejemplo, TR-069 o protocolos OAM&P existentes.

Después de que el nodo repetidor 102 haya recibido las nuevas credenciales de acuerdo de autenticación y clave (AKA), y antes de operar en la red como un dispositivo repetidor plenamente operativo, el nodo repetidor 102 se une de nuevo a la red y se reautentica 330 usando las nuevas credenciales de acuerdo de autenticación y clave (AKA) almacenadas en el entorno de confianza (TrE) 304 del nodo repetidor 102. Por ejemplo, la entidad de gestión de movilidad (MME) 110 puede obtener 332 la nueva información de suscripción y autenticación del nodo repetidor del servidor local de abonado (HSS) 314. Usando la información de suscripción y autenticación obtenida del servidor local de abonado (HSS) 314, la entidad de gestión de movilidad (MME) 110 y el nodo repetidor 102 pueden comunicarse para autenticar el nodo repetidor 102. Por ejemplo, la entidad de gestión de movilidad (MME) 110 puede obtener el nuevo secreto compartido asociado a una nueva identidad (por ejemplo, IMSI) del nodo repetidor 102, y puede emplear un algoritmo de autenticación para verificar el nodo repetidor 102.

Después de que el nodo repetidor 102 se autentica usando las nuevas credenciales de acuerdo de autenticación y clave (AKA), la entidad de gestión de movilidad (MME) 110 puede autorizar 334 al nodo repetidor 102 como un dispositivo repetidor plenamente operativo. Es decir, el nodo repetidor 102 puede autorizarse para acceder a cualquier nombre de punto de acceso (APN) necesario para transmitir el tráfico a y/o desde una o más terminales de acceso. El nodo repetidor 102 puede aparecer como un dispositivo de red para terminales de abonado o cliente que usan el nodo repetidor para transmitir comunicaciones a la red de comunicación.

La FIG. 4 (que comprende la FIG. 4A y la FIG. 4B) es un diagrama de flujo que ilustra al menos un ejemplo de configuración y autorización inicial de un nodo repetidor usando las nuevas credenciales de seguridad para la reautenticación. En el ejemplo de la FIG. 4, el nodo repetidor 102, el nodo de acceso 106, la entidad de gestión de movilidad 110 y el sistema de operación, administración, mantenimiento y aprovisionamiento (OAM&P) 112 se muestran con fines ilustrativos. El nodo de acceso 106 se incluye para ilustrar que las comunicaciones entre el nodo repetidor 102 y las diversas entidades de red se facilitan a través del nodo de acceso 106.

En el ejemplo de la FIG. 4, el nodo repetidor 102 emplea un entorno de confianza (TrE) 401. Haciendo referencia inicialmente a la FIG. 4A, el entorno de confianza (TrE) 401 comprende las credenciales de seguridad iniciales proporcionadas de forma segura en el mismo. Por ejemplo, el entorno de confianza (TrE) 401 puede incluir las credenciales de seguridad iniciales que comprenden las credenciales de acuerdo de autenticación y clave (AKA) iniciales (por ejemplo, una identidad del nodo repetidor (IMSI) y/o una clave compartida) y las credenciales de proveedor 402 que se proporcionan de forma segura en el mismo.

El nodo repetidor 102 puede unirse (o conectarse inalámbricamente) a la entidad de gestión de movilidad (MME) 110 y autenticarse usando las credenciales de acuerdo de autenticación y clave iniciales 404 almacenadas en el entorno de confianza (TrE) 401. Para autenticar el nodo repetidor 102, la entidad de gestión de movilidad (MME) 110 puede

obtener la información de suscripción y autenticación del nodo repetidor 406 de un servidor local de abonado (HSS) 407. Usando la información de suscripción y autenticación obtenida del servidor local de abonado (HSS) 407, la entidad de gestión de movilidad (MME) 110 y el nodo repetidor 102 pueden comunicarse para autenticar el nodo repetidor 102. Por ejemplo, la entidad de gestión de movilidad (MME) 110 puede obtener un secreto compartido asociado a una identidad (por ejemplo, IMSI) del nodo repetidor 102, y puede emplear un algoritmo de autenticación para verificar el nodo repetidor 102.

Después de que la entidad de gestión de movilidad (MME) 110 autentica el nodo repetidor 102, la entidad de gestión de movilidad (MME) 110 puede autorizar al nodo repetidor 102 acceso limitado a la red en la etapa 408. Por ejemplo, la entidad de gestión de movilidad (MME) 110 puede autorizar el acceso para el nodo repetidor 102 a nombres de punto de acceso limitados (APN), tal como al sistema OAM&P del operador 112.

En al menos algunas implementaciones, el sistema OAM&P del operador 112 puede expedir 410 credenciales de operador (por ejemplo, un certificado de operador) al nodo repetidor 102. Las credenciales de operador pueden expedirse por una autoridad de certificación (CA) 411 del sistema OAM&P del operador 112. En la implementación ilustrada, las credenciales de operador se almacenan en el entorno de confianza (TrE) 401 del nodo repetidor 102. Las credenciales de operador pueden expedirse de forma segura al nodo repetidor 102 usando las credenciales de proveedor (por ejemplo, par de claves privada y pública) contenidas en el entorno de confianza (TrE) 401 del nodo repetidor 102.

El nodo repetidor 102 puede recibir nuevas credenciales de acuerdo de autenticación y clave (AKA) 412 expedidas desde el sistema OAM&P del operador 112. Por ejemplo, las nuevas credenciales de acuerdo de autenticación y clave (AKA) pueden expedirse desde el sistema OAM&P del operador 112 y almacenarse en el entorno de confianza (TrE) 401 del nodo repetidor 102 para su uso en comunicaciones de acuerdo de autenticación y clave (AKA) posteriores del nodo repetidor 102. Las nuevas credenciales de acuerdo de autenticación y clave (AKA) pueden expedirse de forma segura por un servidor de gestión del nodo repetidor (RN-MS) 413 del sistema OAM&P del operador 112 usando un par de claves privada/pública asociado a las credenciales de proveedor o las credenciales de operador (si se emiten) almacenadas en el entorno de confianza (TrE) 401. A modo de ejemplo y sin limitación, las nuevas credenciales de acuerdo de autenticación y clave (AKA) pueden incluir una nueva identidad internacional de abonado móvil (IMSI) y/o una clave de encriptación y parámetros de personalización del algoritmo del acuerdo de autenticación y clave (AKA). Por ejemplo, la clave de encriptación y los parámetros del algoritmo AKA pueden cumplir el algoritmo MILENAGE, comprendiendo los parámetros de personalización de AKA un campo de configuración de algoritmo específico del operador (por ejemplo, campo OP), y obteniéndose la clave de encriptación (por ejemplo, OPc) a partir del campo de configuración del algoritmo específico del operador. El sistema OAM&P del operador 112 también actualiza 414 el servidor local de abonado (HSS) 407 con la nueva información de autenticación y suscripción asociada al nodo repetidor 102.

Haciendo referencia ahora a la FIG. 4B, el sistema OAM&P del operador 112 también puede gestionar 416 el nodo repetidor 102 para configurar el nodo repetidor 102 para su uso en la red de comunicación como un dispositivo repetidor que transmite el tráfico entre las terminales de acceso y las entidades de red (por ejemplo, nodos de acceso, otros nodos repetidores). Puede usarse cualquier protocolo de gestión convencional para configurar el nodo repetidor 102, tal como, por ejemplo, TR-069 o protocolos OAM&P existentes.

Después de que el nodo repetidor 102 haya recibido las nuevas credenciales de acuerdo de autenticación y clave (AKA), y antes de operar en la red como un dispositivo repetidor plenamente operativo, el nodo repetidor 102 se une de nuevo a la red y se reautentica 418 usando las nuevas credenciales de acuerdo de autenticación y clave (AKA) almacenadas en el entorno de confianza (TrE) 401 del nodo repetidor 102. Por ejemplo, la entidad de gestión de movilidad (MME) 110 puede obtener 420 la nueva información de suscripción y autenticación del nodo repetidor del servidor local de abonado (HSS) 407. Usando la información de suscripción y autenticación obtenida del servidor local de abonado (HSS) 407, la entidad de gestión de movilidad (MME) 110 y el nodo repetidor 102 pueden comunicarse para autenticar el nodo repetidor 102. Por ejemplo, la entidad de gestión de movilidad (MME) 110 puede obtener el nuevo secreto compartido asociado a una nueva identidad (por ejemplo, IMSI) del nodo repetidor 102, y puede emplear un algoritmo de autenticación para verificar el nodo repetidor 102.

Después de que el nodo repetidor 102 se autentica usando las nuevas credenciales de acuerdo de autenticación y clave (AKA), la entidad de gestión de movilidad (MME) 110 puede autorizar 422 al nodo repetidor 102 como un dispositivo repetidor plenamente operativo. Es decir, el nodo repetidor 102 puede autorizarse para acceder a cualquier nombre de punto de acceso (APN) necesario para transmitir el tráfico a y/o desde una o más terminales de acceso.

Segunda Configuración y Autorización Inicial Ejemplar de Nodos Repetidores Usando Nuevas Credenciales AKA para la Reautenticación

La FIG. 5 (que comprende la FIG. 5A y la FIG. 5B) es un diagrama de flujo que ilustra al menos un ejemplo de configuración y autorización inicial de un nodo repetidor usando las credenciales de seguridad iniciales junto con las nuevas credenciales de seguridad para la reautenticación. En el ejemplo de la FIG. 5, el nodo repetidor 102, el nodo

de acceso 106, la entidad de gestión de movilidad 110 y el sistema de operación, administración, mantenimiento y aprovisionamiento (OAM&P) 112 se muestran con fines ilustrativos. El nodo de acceso 106 se incluye para ilustrar que las comunicaciones entre el nodo repetidor 102 y las diversas entidades de red se facilitan a través del nodo de acceso 106.

En el ejemplo de la FIG. 5, el nodo repetidor 102 emplea tanto una tarjeta de circuitos integrados universal (UICC) 502 como un entorno de confianza (TrE) 504. Haciendo referencia inicialmente a la FIG. 5A, la UICC 502 puede incluir una aplicación de módulo de identidad del abonado universal (USIM), y puede comprender credenciales de seguridad iniciales proporcionadas de forma segura en la misma. Por ejemplo, la UICC 502 puede incluir credenciales de seguridad iniciales que comprenden credenciales de acuerdo de autenticación y clave (AKA) iniciales que se proporcionan de forma segura 506 en la misma. Además, el nodo repetidor 102 puede incluir credenciales de proveedor proporcionadas de forma segura y contenidas en el entorno de confianza (TrE) 504 del nodo repetidor 102.

El nodo repetidor 102 puede unirse (o conectar inalámbricamente) a la entidad de gestión de movilidad (MME) 110 y autenticarse 510 usando las credenciales de acuerdo de autenticación y clave iniciales almacenadas en la UICC 502. Para autenticar el nodo repetidor 102, la entidad de gestión de movilidad (MME) 110 puede obtener la información de suscripción y autenticación del nodo repetidor 512 de un servidor local de abonado (HSS) 514. Usando la información de suscripción y autenticación obtenida del servidor local de abonado (HSS) 514, la entidad de gestión de movilidad (MME) 110 y el nodo repetidor 102 pueden comunicarse para autenticar el nodo repetidor 102. Por ejemplo, la entidad de gestión de movilidad (MME) 110 puede obtener un secreto compartido asociado a una identidad (por ejemplo, IMSI) del nodo repetidor 102, y puede emplear un algoritmo de autenticación para verificar el nodo repetidor 102.

Después de que la entidad de gestión de movilidad (MME) 110 autentica el nodo repetidor 102, la entidad de gestión de movilidad (MME) 110 puede autorizar al nodo repetidor 102 acceso limitado a la red en la etapa 516. Por ejemplo, la entidad de gestión de movilidad (MME) 110 puede autorizar el acceso para el nodo repetidor 102 a nombres de punto de acceso limitados (APN), tal como al sistema OAM&P del operador 112. En al menos algunas implementaciones, el acceso limitado puede definirse por el perfil de suscripción obtenido del servidor local de abonado (HSS) 514. Es decir, el servidor local de abonado (HSS) 514 puede proporcionar el perfil de suscripción asociado a la identidad del nodo repetidor (por ejemplo, IMSI), donde el perfil de suscripción indica que el nodo repetidor 102 está autorizado a acceder a un número limitado de entidades (por ejemplo, un número limitado de nombres de punto de acceso (APN)).

El sistema OAM&P del operador 112 puede expedir credenciales de operador 518 (por ejemplo, un certificado de operador, una clave compartida) al nodo repetidor 102. Las credenciales de operador pueden expedirse por una autoridad de certificación (CA) 520 del sistema OAM&P del operador 112. En la implementación ilustrada, las credenciales de operador pueden almacenarse en el entorno de confianza (TrE) 504 del nodo repetidor 102. Las credenciales de operador pueden expedirse de forma segura al nodo repetidor 102 usando las credenciales de proveedor (por ejemplo, par de claves privada y pública) contenidas en el entorno de confianza (TrE) 504 del nodo repetidor 102.

En la implementación de la FIG. 5, no hay nuevas credenciales de acuerdo de autenticación y clave (AKA) enviadas al nodo repetidor 102. En su lugar, el sistema OAM&P del operador 112 puede comunicar con el servidor local de abonado (HSS) 514 para actualizar 522 el perfil de suscripción del nodo repetidor. La actualización del perfil de suscripción del nodo repetidor 102 puede incluir definir entidades de red adicionales (por ejemplo, nombres de punto de acceso (APN)) a las que el nodo repetidor 102 tiene autorizado acceder. Dichas entidades de red pueden comprender aquellas entidades necesarias para realizar las funciones de un dispositivo repetidor que transmite el tráfico a y/o desde una o más terminales de acceso. En el ejemplo mostrado, el servidor de gestión del nodo repetidor (RN-MS) 524 del sistema OAM&P del operador 112 puede comprender la entidad para comunicar con el servidor local de abonado (HSS) 514 para actualizar el perfil de suscripción del nodo repetidor 102.

Haciendo referencia ahora a la FIG. 5B, el sistema OAM&P del operador 112 también puede gestionar 526 el nodo repetidor 102 para configurar el nodo repetidor 102 para su uso en la red de comunicación como un dispositivo repetidor que transmite el tráfico entre las terminales de acceso y las entidades de red (por ejemplo, nodos de acceso, otros nodos repetidores). Puede usarse cualquier protocolo de gestión convencional para configurar el nodo repetidor 102, tal como, por ejemplo, TR-069 o protocolos OAM&P existentes.

Después de que el nodo repetidor 102 haya recibido las credenciales de operador, y antes de operar en la red como un dispositivo repetidor plenamente operativo, el nodo repetidor 102 se une de nuevo a la red y se reautentica 528 usando las credenciales de acuerdo de autenticación y clave (AKA) iniciales almacenadas en la UICC 502 del nodo repetidor 102 junto con las credenciales del dispositivo (por ejemplo, las credenciales de operador) almacenadas en el entorno de confianza (TrE) 504. Para autenticar el nodo repetidor 102, la entidad de gestión de movilidad (MME) 110 puede obtener 530 la nueva información de suscripción y autenticación del nodo repetidor desde el servidor local de abonado (HSS) 514. Como se ha señalado previamente, la nueva información de suscripción y autenticación puede indicar a qué entidades de red tiene permitido el acceso la identidad del nodo repetidor inicial

(por ejemplo, IMSI). Usando la nueva información de suscripción y autenticación obtenida del servidor local de abonado (HSS) 514, la entidad de gestión de movilidad (MME) 110 y el nodo repetidor 102 pueden comunicar para autenticar el nodo repetidor 102. Por ejemplo, la entidad de gestión de movilidad (MME) 110 puede obtener un secreto compartido asociado a la identidad (por ejemplo, IMSI) del nodo repetidor 102, y puede emplear un algoritmo de autenticación para verificar el nodo repetidor 102.

Después de que el nodo repetidor 102 se autentica usando la nueva información de suscripción y autenticación asociada a la identidad del nodo repetidor, la entidad de gestión de movilidad (MME) 110 puede autorizar 532 al nodo repetidor 102 como un dispositivo repetidor plenamente operativo. Es decir, el nodo repetidor 102 puede autorizarse para acceder a cualquier nombre de punto de acceso (APN) necesario para transmitir el tráfico a y/o desde una o más terminales de acceso.

Nodo Repetidor Ejemplar

La FIG. 6 es un diagrama de bloques que ilustra componentes seleccionados de un nodo repetidor 600 de acuerdo con al menos una realización. El nodo repetidor 600 incluye generalmente un circuito de procesamiento 602 acoplado a una interfaz de comunicación inalámbrica 604.

El circuito de procesamiento 602 se dispone para obtener, procesar y/o enviar datos, controlar el acceso y almacenamiento de datos, emitir comandos, y controlar otras operaciones deseadas. El circuito de procesamiento 602 puede comprender circuitería configurada para implementar una programación deseada proporcionada por medios apropiados en al menos una realización. Por ejemplo, el circuito de procesamiento 602 puede implementarse como uno o más de un procesador, un controlador, una pluralidad de procesadores y/u otra estructura configurada para ejecutar instrucciones ejecutables incluyendo, por ejemplo, instrucciones de software y/o firmware, y/o circuitería de hardware. Las realizaciones del circuito de procesamiento 602 pueden incluir un procesador de propósito general, un procesador de señales digitales (DSP), un circuito integrado de aplicación específica (ASIC), una matriz de puertas de campo programable (FPGA) u otro componente de lógica programable, lógica de transistor o de puertas discretas, componentes de hardware discretos, o cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de propósito general puede ser un microprocesador, pero, como alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estado convencional. Un procesador también puede implementarse como una combinación de componentes informáticos, tal como una combinación de un DSP y un microprocesador, varios microprocesadores, uno o más microprocesadores junto con un núcleo de DSP o cualquier otra configuración de este tipo. Estos ejemplos del circuito de procesamiento 602 son con fines de ilustración y también se contemplan otras configuraciones adecuadas dentro del alcance de la presente divulgación.

El circuito de procesamiento 602 incluye un módulo de autenticación y reautenticación 603. El módulo de autenticación y reautenticación 603 puede comprender circuitería y/o programación adaptada para realizar procedimientos de autenticación usando las credenciales de seguridad iniciales, y adaptada para realizar procedimientos de reautenticación usando nuevas credenciales de seguridad.

La interfaz de comunicaciones 604 se configura para facilitar las comunicaciones inalámbricas del nodo repetidor 600. Por ejemplo, la interfaz de comunicaciones 604 puede configurarse para comunicar información bidireccionalmente con respecto a otros dispositivos inalámbricos, tales como terminales de acceso, nodos de acceso, otros nodos repetidores, etc. La interfaz de comunicaciones 604 puede acoplarse a una antena (no mostrada) y puede incluir circuitería de transceptor inalámbrica, incluyendo, al menos, un transmisor y/o, al menos, un receptor (por ejemplo, una o más cadenas de transmisor/receptor) para comunicaciones inalámbricas.

En algunas realizaciones, el nodo repetidor 600 puede incluir un entorno de confianza (TrE) 606. El entorno de confianza 606 puede adaptarse para cumplir las especificaciones para un entorno de confianza en el Detalle de las Especificaciones 3GPP en TS 33.320. El entorno de confianza 606 puede proporcionarse previamente (o integrarse de forma segura) con al menos algunas de las credenciales de seguridad iniciales. Por ejemplo, el entorno de confianza 606 puede tener credenciales de proveedor y/o credenciales de acuerdo de autenticación y clave (AKA) iniciales almacenadas en el mismo.

En algunas realizaciones, el nodo repetidor 600 puede incluir un procesador seguro 608 que se proporciona previamente con credenciales de seguridad iniciales, tales como credenciales de acuerdo de autenticación y clave (AKA) iniciales. El procesador seguro 608 puede comprender una tarjeta inteligente, tal como una tarjeta de circuitos integrados universal (UICC), y/o puede incluir una aplicación de módulo de identidad de abonado universal (USIM).

De acuerdo con una o más características del nodo repetidor 600, el circuito de procesamiento 602 puede adaptarse para realizar cualquiera o cada uno de los procesos, funciones, etapas y/o rutinas relacionadas con los diversos nodos repetidores que se han descrito en el presente documento anteriormente con referencia a las FIGS. 1-5 (por ejemplo, nodo repetidor 102). Como se usa en el presente documento, el término "adaptado" en relación con el circuito de procesamiento 602 puede referirse al circuito de procesamiento 602 que está uno o más de configurado, empleado, implementado o programado para realizar un proceso, función, etapa y/o rutina particular de acuerdo con

diversas características descritas en el presente documento.

La FIG. 7 es un diagrama de flujo que ilustra un ejemplo de al menos una implementación de un método operativo en un nodo repetidor, tal como el nodo repetidor 600. Con referencia a ambas de las FIGS. 6 y 7, un nodo repetidor 600 puede iniciar la comunicación con una entidad de red en la etapa 702. Por ejemplo, el circuito de procesamiento 602 puede unirse inalámbricamente a una entidad de red (por ejemplo, una entidad de gestión de movilidad (MME)) usando la interfaz de comunicaciones 604. En el momento en que el nodo repetidor 600 se une inicialmente a la entidad de red, el nodo repetidor 600 puede aparecer como un dispositivo de usuario (por ejemplo, un terminal de acceso o dispositivo de cliente) para la entidad de red.

En la etapa 704, el nodo repetidor puede autenticarse inalámbricamente con la entidad de red usando sus credenciales de seguridad iniciales. Por ejemplo, el circuito de procesamiento 602 puede autenticar el nodo repetidor para la entidad de red a través de la interfaz de comunicaciones 604. En al menos una implementación, el módulo de autenticación y reautenticación 603 puede usar las credenciales de seguridad iniciales almacenadas en el nodo repetidor 600 para realizar el procedimientos de autenticación. El módulo de autenticación y reautenticación 603 puede emplear cualquier esquema de autenticación convencional, tal como una autenticación de pregunta-respuesta. En algunas implementaciones, las credenciales de seguridad iniciales empleadas por el módulo de autenticación y reautenticación 603 pueden incluir las credenciales de acuerdo de autenticación y clave (AKA) iniciales y/o credenciales de proveedor (por ejemplo, un certificado de proveedor). Las credenciales de acuerdo de autenticación y clave (AKA) iniciales pueden almacenarse en el entorno de confianza (TrE) 606 o el procesador seguro 608 del nodo repetidor 600. Las credenciales de proveedor pueden almacenarse en el entorno de confianza (TrE) 606.

Las credenciales de acuerdo de autenticación y clave (AKA) iniciales pueden incluir una identidad del nodo repetidor inicial (por ejemplo, IMSI) y un secreto compartido inicial asociado a la identidad del nodo repetidor inicial. En el momento de la autenticación inalámbrica, la identidad del nodo repetidor inicial puede asociarse a un perfil de suscripción en la red de comunicación que autoriza un acceso de red para el nodo repetidor 600 para el fin limitado de configuración inicial.

En la etapa 706, el nodo repetidor 600 recibe autorización para comunicar inalámbricamente con la red de comunicación para un fin limitado de configuración. Por ejemplo, el circuito de procesamiento 602 puede recibir, a través de la interfaz de comunicaciones 604, autorización para comunicar inalámbricamente con una porción limitada de la red de comunicación para obtener nuevas credenciales de seguridad y, en algunas implementaciones, datos de configuración. La autorización puede limitar el nodo repetidor 600 para acceder únicamente a entidades de red que están implicadas en la configuración y gestión de los dispositivos repetidores. En algunas implementaciones, el acceso de red para el nodo repetidor 600 puede restringirse limitando los nombres del punto de acceso (APN) con los que el nodo repetidor 600 tiene permitido comunicar.

Tras la autorización para acceder a la red de comunicación, el nodo repetidor 600 recibe nuevas credenciales de seguridad en la etapa 708. Por ejemplo, el circuito de procesamiento 602 puede recibir, a través de la interfaz de comunicaciones 604, nuevas credenciales de seguridad de una entidad de gestión y configuración de la red, tal como el sistema OAM&P del operador. En algunas implementaciones, el circuito de procesamiento 602 puede recibir nuevas credenciales de acuerdo de autenticación y clave (AKA), tales como una nueva identidad del nodo repetidor (por ejemplo, una nueva IMSI) y un nuevo secreto compartido asociado a la nueva identidad del nodo repetidor. En algunas implementaciones, el circuito de procesamiento 602 puede recibir credenciales de operador, gal como un certificado de operador y/o una nueva clave compartida. Las nuevas credenciales de seguridad pueden almacenarse por el circuito de procesamiento 602 en el entorno de confianza (TrE) 606. En algunas implementaciones, el nodo repetidor 600 puede conservar la misma identidad del nodo repetidor inicial (IMSI), pero la identidad del nodo repetidor inicial puede asociarse a un nuevo perfil de suscripción autorizando cualquier acceso de red necesario para el nodo repetidor 600 para operar como un dispositivo repetidor para transmitir el tráfico de red entre una o más terminales de acceso y la red de comunicación.

De acuerdo con al menos algunas implementaciones, el nodo repetidor 600 también puede recibir datos de configuración además de las nuevas credenciales de seguridad. Por ejemplo, el circuito de procesamiento 602 puede recibir información de configuración adaptada para permitir que el nodo repetidor 600 opere como un dispositivo repetidor en la red de comunicación. Es decir, el nodo repetidor 600 puede obtener la información de configuración apropiada para permitirle transmitir tráfico de red entre las terminales de acceso y las entidades de red (por ejemplo, nodos de acceso y/o otros nodos repetidores) en la red de comunicación.

Después de que el nodo repetidor 600 recibe e implementa las nuevas credenciales de seguridad y cualquier dato de configuración (si se reciben), el nodo repetidor 600 puede reautenticar con la entidad de red usando las nuevas credenciales de seguridad en la etapa 710, antes de operar como un dispositivo repetidor en la red de comunicación. Por ejemplo, el circuito de procesamiento 602 puede conectar de nuevo con la entidad de red a través de la interfaz de comunicaciones 604, y puede reautenticar con la entidad de red usando las nuevas credenciales de seguridad. En al menos algunas implementaciones, el módulo de autenticación y reautenticación 603 puede obtener las nuevas credenciales de seguridad del entorno de confianza (TrE) 606, y puede emplear cualquier esquema de autenticación

convencional, tal como un algoritmo de autenticación de pregunta-respuesta, usando las nuevas credenciales de seguridad. En el momento en que el nodo repetidor 600 se une de nuevo a la entidad de red para la reautenticación, el nodo repetidor 600 puede aparecer como un dispositivo repetidor para la entidad de red.

Entidad de Red Ejemplar

La FIG. 8 es un diagrama de bloques que ilustra componentes seleccionados de una entidad de red 800 de acuerdo con al menos una realización. La entidad de red 800 puede incluir un circuito de procesamiento 802 acoplado a una interfaz de comunicaciones 804.

El circuito de procesamiento 802 se dispone para obtener, procesar y/o enviar datos, controlar el acceso y almacenamiento de datos, emitir comandos, y controlar otras operaciones deseadas. El circuito de procesamiento 802 puede comprender circuitería configurada para implementar una programación deseada proporcionada por medios apropiados en al menos una realización. Por ejemplo, el circuito de procesamiento 802 puede implementarse como uno o más de un procesador, un controlador, una pluralidad de procesadores y/u otra estructura configurada para ejecutar instrucciones ejecutables incluyendo, por ejemplo, instrucciones de software y/o firmware, y/o circuitería de hardware. Las realizaciones del circuito de procesamiento 802 pueden incluir un procesador de propósito general, un procesador de señales digitales (DSP), un circuito integrado de aplicación específica (ASIC), una matriz de puertas de campo programable (FPGA) u otro componente de lógica programable, lógica de transistor o de puertas discretas, componentes de hardware discretos, o cualquier combinación de los mismos diseñada para realizar las funciones descritas en el presente documento. Un procesador de propósito general puede ser un microprocesador, pero, como alternativa, el procesador puede ser cualquier procesador, controlador, microcontrolador o máquina de estado convencional. Un procesador también puede implementarse como una combinación de componentes informáticos, tal como una combinación de un DSP y un microprocesador, varios microprocesadores, uno o más microprocesadores junto con un núcleo de DSP o cualquier otra configuración de este tipo. Estos ejemplos del circuito de procesamiento 802 son con fines de ilustración y también se contemplan otras configuraciones adecuadas dentro del alcance de la presente divulgación.

El circuito de procesamiento 802 incluye un módulo de autenticación y reautenticación 806. El módulo de autenticación y reautenticación 806 puede comprender circuitería y/o programación adaptada para realizar procedimientos de autenticación para autenticar nodos repetidores usando las credenciales de seguridad iniciales, y adaptada para realizar procedimientos de reautenticación para la autenticación posteriormente de nodos repetidores usando nuevas credenciales de seguridad.

La interfaz de comunicaciones 804 se configura para facilitar las comunicaciones de la entidad de red 800 para comunicar, directa o indirectamente (por ejemplo, a través de una o más entidades de red distintas), con un nodo repetidor.

De acuerdo con una o más características de la entidad de red 800, el circuito de procesamiento 802 puede adaptarse para realizar cualquier o cada uno de los procesos, funciones, etapas y/o rutinas relacionadas con las diversas entidades de red que se han descrito en el presente documento anteriormente con referencia a las FIGS. 1-5 (por ejemplo, entidad de gestión de movilidad (MME) 110, OAM&P 112). Además, la entidad de red 800 puede comprender una única entidad, o una combinación de dos o más entidades de la red. A modo de ejemplo y sin limitación, la entidad de red 800 puede comprender una entidad de gestión de movilidad (MME), un sistema de operaciones, administración, mantenimiento y aprovisionamiento del operador (OAM&P) (por ejemplo, un sistema de gestión de nodo repetidor (RN-MS) y/o una autoridad de certificación (CA)), y/o un servidor local de abonado (HSS). Como se usa en el presente documento, el término "adaptado" en relación con el circuito de procesamiento 802 puede referirse al circuito de procesamiento 802 que está uno o más de configurado, empleado, implementado o programado para realizar un proceso, función, etapa y/o rutina particular de acuerdo con diversas características descritas en el presente documento.

La FIG. 9 es un diagrama de flujo que ilustra un ejemplo de al menos una implementación de un método operativo en una entidad de red, tal como la entidad de red 800. Con referencia a ambas de las FIGS. 8 y 9, una entidad de red puede autenticar un nodo repetidor usando credenciales de seguridad iniciales asociadas al nodo repetidor, en la etapa 902. Por ejemplo, el circuito de procesamiento 802 puede comunicar con un nodo repetidor a través de la interfaz de comunicaciones 804 para autenticar el nodo repetidor. De acuerdo con al menos algunas implementaciones, el módulo de autenticación y reautenticación 806 puede emplear cualquier esquema de autenticación convencional, tal como un algoritmo de autenticación de pregunta-respuesta, para autenticar un nodo repetidor usando las credenciales de seguridad iniciales del nodo repetidor. En el momento en que el nodo repetidor se autentica por la entidad de red 800, el nodo repetidor puede aparecer para la entidad de red 800 como un dispositivo de usuario (por ejemplo, un terminal de acceso).

En algunas implementaciones, las credenciales de seguridad iniciales pueden incluir credenciales de acuerdo de autenticación y clave (AKA) iniciales y/o credenciales de proveedor (por ejemplo, un certificado de proveedor). Las credenciales de acuerdo de autenticación y clave (AKA) iniciales pueden incluir una identidad del nodo repetidor inicial y un secreto compartido inicial asociado a la identidad del nodo repetidor inicial.

En la etapa 904, la entidad de red 800 puede autorizar al nodo repetidor para comunicar inalámbricamente con la red de comunicación para el fin limitado de configurar el nodo repetidor. Por ejemplo, el circuito de procesamiento 802 puede determinar, basándose en la identidad del nodo repetidor inicial, que el nodo repetidor se autoriza para un acceso de red limitado. En algunas implementaciones, el módulo de autenticación y reautenticación 806 puede obtener un perfil de suscripción asociado a la identidad del nodo repetidor inicial durante la autenticación, donde el perfil de suscripción indica que el nodo repetidor se autoriza para acceder a la red de comunicación para un fin limitado de configuración del nodo repetidor. El circuito de procesamiento 802 puede adaptarse para limitar el acceso de red para el nodo repetidor restringiendo los nombres del punto de acceso (APN) con los que el nodo repetidor tiene permitido comunicar.

De acuerdo con al menos algunas implementaciones, la entidad de red 800 puede autorizar al nodo repetidor a comunicar para el fin limitado de obtener nuevas credenciales de seguridad y datos de configuración. Es decir, el circuito de procesamiento 802 puede adaptarse para autorizar al nodo repetidor a comunicar con la red de comunicación para que el nodo repetidor obtenga nuevas credenciales de seguridad y datos de configuración, mientras que restringe la comunicación inalámbrica del nodo repetidor para otros fines.

Tras la autenticación y autorización del nodo repetidor, y después de que el nodo repetidor ha obtenido nuevas credenciales de seguridad y datos de configuración de la red de comunicación, la entidad de red 800 reautentica el nodo repetidor usando las nuevas credenciales de seguridad asociadas al nodo repetidor, en la etapa 906. Por ejemplo, el circuito de procesamiento 802 puede reautenticar el nodo repetidor usando las nuevas credenciales de seguridad. En al menos algunas implementaciones, el módulo de autenticación y reautenticación 806 puede emplear un esquema de autenticación convencional, tal como un algoritmo de autenticación de pregunta-respuesta, usando las nuevas credenciales de seguridad para autenticar el nodo repetidor usando sus nuevas credenciales de seguridad. En el momento en que la entidad de red 800 reautentica el nodo repetidor, el nodo repetidor puede aparecer para la entidad de red 800 como un dispositivo repetidor. El nodo repetidor puede aparecer como un dispositivo de red para terminales de abonado o cliente que usan el nodo repetidor para transmitir comunicaciones a la red de comunicación.

En al menos algunas implementaciones, las nuevas credenciales de seguridad pueden incluir nuevas credenciales de acuerdo de autenticación y clave (AKA), tal como una nueva identidad del nodo repetidor (por ejemplo, una nueva IMSI) y un nuevo secreto compartido asociado a la nueva identidad del nodo repetidor. En dichas implementaciones, el módulo de autenticación y reautenticación 806 puede obtener un perfil de suscripción asociado a la nueva identidad del nodo repetidor durante los procedimientos de reautenticación, donde el perfil de suscripción autoriza una red de acceso al nodo repetidor para operar como un dispositivo repetidor que transmite el tráfico entre uno o más terminales de acceso y la red de comunicación.

En al menos algunas implementaciones, el módulo de autenticación y reautenticación 806 puede reautenticar el nodo repetidor usando tanto las nuevas credenciales de seguridad como las credenciales de seguridad iniciales. En dichas implementaciones, las nuevas credenciales de seguridad pueden incluir credenciales de operador, tal como un certificado de operador, y/o una nueva clave compartida. Las credenciales de seguridad iniciales empleadas junto con las nuevas credenciales de seguridad pueden incluir la identidad del nodo repetidor inicial (IMSI), pero la identidad del nodo repetidor inicial puede asociarse a un nuevo perfil de suscripción que autoriza cualquier acceso de red necesario para el nodo repetidor para operar como un dispositivo repetidor para transmitir el tráfico de red entre una o más terminales de acceso y la red de comunicación. En dichas implementaciones, el módulo de autenticación y reautenticación 806 puede obtener el nuevo perfil de suscripción asociado a la identidad del nodo repetidor inicial durante el procedimiento de reautenticación.

En respuesta a una reautenticación satisfactoria del nodo repetidor, la entidad de red 800 puede autorizar, en la etapa 908, al nodo repetidor para operar como un dispositivo repetidor en la red de comunicación. Por ejemplo, el circuito de procesamiento 802 puede autorizar al nodo repetidor, basándose en una reautenticación satisfactoria, para operar como un dispositivo repetidor que transmite el tráfico entre uno o más terminales de acceso y la red de comunicación.

Uno o mas de los componentes, etapas, características y/o funciones que se ilustran en las FIGS. 1, 2, 3, 4, 5, 6, 7, 8, 9 y/o 10 pueden reorganizarse y/o combinarse en un único componente, etapa, característica o función o constituirse en varios componentes, etapas o funciones. También pueden añadirse elementos, componentes, etapas y/o funciones adicionales sin apartarse de la presente divulgación. El aparato, dispositivos y/o componentes que se ilustran en las FIGS. 1, 6 y/o 8 pueden configurarse para realizar uno o más de los métodos, características o etapas que se describen en las FIGS. 2, 3, 4, 5, 7 y/o 9. Los nuevos algoritmos descritos en el presente documento también pueden implementarse eficientemente en software y/o integrarse en hardware.

Además, se aprecia que se han descrito al menos algunas implementaciones como un proceso que se representa como un organigrama, un diagrama de flujo, un diagrama estructural, o un diagrama de bloques. Aunque un diagrama de flujo puede describir las operaciones como un proceso secuencial, muchas de las operaciones pueden realizarse en paralelo o simultáneamente. Además, el orden de las operaciones puede reorganizarse. Un proceso se

termina cuando sus operaciones se completan. Un proceso puede corresponder a un método, una función, un procedimiento, una sub-rutina, un sub-programa, etc. Cuando un proceso se corresponde a una función, su terminación corresponde al retorno de la función a la función de llamada o la función principal.

Además, las realizaciones pueden implementarse en hardware, software, firmware, middleware, microcódigo, o cualquier combinación de los mismos. Al implementarse en software, firmware, middleware o microcódigo, el código de programa o segmentos de código para realizar las tareas necesarias pueden almacenarse en un medio legible por máquina, tal como un medio de almacenamiento u otro almacenamiento o almacenamientos. Un procesador puede realizar las tareas necesarias. Un segmento de código puede representar un procedimiento, una función, un subprograma, un programa, una rutina, una subrutina, un módulo, un paquete de software, una clase o cualquier combinación de instrucciones, estructuras de datos o sentencias de programa. Un segmento de código puede acoplarse a otro segmento de código o a un circuito de hardware pasando y/o recibiendo información, datos, argumentos, parámetros o contenidos de memoria. La información, argumentos, parámetros, datos, etc. se puede pasar, enviar o transmitir a través de un medio adecuado que incluye compartir la memoria, el paso de mensajes, el paso de testigos, transmisión por red, etc.

Las expresiones "medio legible a máquina", "medio legible por ordenador", y/o "medio legible por procesador" pueden incluir, pero sin limitación, dispositivos de almacenamiento fijos y extraíbles, dispositivos de almacenamiento ópticos, y diversos medios no transitorios diferentes capaces de almacenar, contener o portar instrucciones y/o datos. Por lo tanto, los diversos métodos descritos en el presente documento pueden implementarse parcial o completamente por instrucciones y/o datos que pueden almacenarse en un "medio legible por máquina", "medio legible por ordenador", y/o un "medio legible por procesador" y ejecutarse por uno o más procesadores, máquinas y/o dispositivos.

Los métodos o algoritmos descritos en relación con los ejemplos desvelados en el presente documento pueden incorporarse directamente en hardware, en un módulo de software ejecutable por un procesador, o en una combinación de ambos, en forma de unidad de procesamiento, instrucciones de programación, u otras direcciones, y pueden contenerse en un único dispositivo o distribuirse a través de múltiples dispositivos. Un módulo de software puede residir en memoria RAM, memoria flash, memoria ROM, memoria EPROM, memoria EEPROM, registros, un disco duro, un disco extraíble, un CD-ROM o en cualquier otra forma de medio de almacenamiento no transitorio conocida en la técnica. Un medio de almacenamiento puede estar acoplado al procesador de manera que el procesador pueda leer información de, y escribir información en, el medio de almacenamiento. Como alternativa, el medio de almacenamiento puede ser una parte integrante del procesador.

Los expertos en la técnica apreciarán además que los diversos bloques lógicos, módulos, circuitos y etapas de algoritmo ilustrativos descritos en relación con las realizaciones desveladas en el presente documento pueden implementarse como hardware electrónico, software informático o combinaciones de ambos. Para ilustrar claramente esta intercambiabilidad de hardware y software, anteriormente se han descrito diversos componentes, bloques, módulos, circuitos y etapas ilustrativos, generalmente, en lo que respecta a su funcionalidad. Si tal funcionalidad se implementa como hardware o software, dependerá de la aplicación particular y de las limitaciones de diseño impuestas sobre todo el sistema.

Las diversas características de la invención descritas en el presente documento pueden implementarse en diferentes sistemas sin apartarse de la invención. Cabe apreciarse que las realizaciones anteriores son simplemente ejemplos y no han de interpretarse como limitantes de la invención. La descripción de las realizaciones pretende ser ilustrativa, y no limitar el alcance de la divulgación.

REIVINDICACIONES

1. Un nodo repetidor (102, 600), que comprende:

medios para autenticar inalámbricamente (310) con una entidad de red (800) usando credenciales de seguridad iniciales (202); y, medios para recibir autorización para comunicar inalámbricamente con una red de comunicación(108) para un fin limitado de configuración del nodo repetidor (102, 600) en respuesta a la autenticación inalámbrica usando las credenciales de seguridad iniciales (202),

caracterizado por que el nodo repetidor (102, 600) comprende adicionalmente:

medios para recibir nuevas credenciales de seguridad (208); y
medios para reautenticar con la entidad de red (800) usando las nuevas credenciales de seguridad (208) antes de habilitarse para operar como un dispositivo repetidor en la red de comunicación (108).

2. El nodo repetidor (102, 600) de la reivindicación 1, en el que las nuevas credenciales de seguridad (208) incluyen una nueva identidad del nodo repetidor y un nuevo secreto compartido asociado a la nueva identidad del nodo repetidor; en el que el nodo repetidor (102, 600) está adaptado adicionalmente para:

reautenticar el nodo repetidor (102, 600) con respecto a la entidad de red (800) usando la nueva identidad del nodo repetidor y el nuevo secreto compartido asociado a la nueva identidad del nodo repetidor antes de operar como un dispositivo repetidor en la red de comunicación (108).

3. El nodo repetidor (102, 600) de la reivindicación 2, en el que la nueva identidad del nodo repetidor se asocia a un perfil de suscripción que autoriza acceso de red al nodo repetidor (102, 600) para operar como un dispositivo repetidor que transmite el tráfico entre uno o más terminales de acceso (104) y la red de comunicación (108).

4. El nodo repetidor (102, 600) de la reivindicación 1, que comprende adicionalmente un entorno de confianza acoplado al circuito de procesamiento (602), en el que el circuito de procesamiento (602) está adaptado adicionalmente para almacenar las nuevas credenciales de seguridad (208) en el entorno de confianza.

5. El nodo repetidor (102, 600) de la reivindicación 4, en el que al menos algunas de las credenciales de seguridad iniciales (202) se almacenan en el entorno de confianza.

6. El nodo repetidor (102, 600) de la reivindicación 1, que comprende adicionalmente un procesador seguro (608) acoplado al circuito de procesamiento (602), en el que al menos algunas de las credenciales de seguridad iniciales (202) se almacenan en el procesador seguro (608).

7. El nodo repetidor (102, 600) de la reivindicación 1, en el que el circuito de procesamiento (602) está adaptado adicionalmente para:

recibir datos de configuración a través de la interfaz de comunicaciones inalámbrica para configurar el nodo repetidor (102, 600) como un dispositivo repetidor en la red de comunicación (108), recibiéndose los datos de configuración antes de la reautenticación con la entidad de red (800).

8. El nodo repetidor (102, 600) de la reivindicación 1, en el que:

el nodo repetidor (102, 600) aparece como un dispositivo de usuario para la entidad de red (800) al autenticarse con la entidad de red (800) con los parámetros de seguridad iniciales; y el nodo repetidor (102, 600) aparece como un dispositivo repetidor al reautenticarse con la entidad de red (800) con los nuevos parámetros de seguridad.

9. Una entidad de red (800), que comprende:

medios para autenticar un nodo repetidor (102, 600) usando credenciales de seguridad iniciales (202) asociadas al nodo repetidor (102, 600); y medios para autorizar al nodo repetidor (102, 600) a comunicar inalámbricamente con una red de comunicación (108) para un fin limitado de configuración del nodo repetidor (102, 600) después de una autenticación satisfactoria del nodo repetidor (102, 600) usando las credenciales de seguridad iniciales (202), **caracterizada por que** la entidad de red (800) comprende adicionalmente:

medios para reautenticar el nodo repetidor (102, 600) usando nuevas credenciales de seguridad (208); y medios para autorizar al nodo repetidor (102, 600) para operar como un dispositivo repetidor en la red de comunicación (108) después de reautenticar satisfactoriamente el nodo repetidor (102, 600).

10. La entidad de red (800) de la reivindicación 9, en la que el circuito de procesamiento (602) está adaptado para autorizar al nodo repetidor (102, 600) a comunicar por vía inalámbrica con la red de comunicación (108) para un fin limitado de obtener nuevas credenciales de seguridad (208) y datos de configuración.

11. La entidad de red (800) de la reivindicación 9, en la que las nuevas credenciales de seguridad (208) incluyen una nueva identidad del nodo repetidor y un nuevo secreto compartido asociado a la nueva identidad del nodo repetidor.

12. La entidad de red (800) de la reivindicación 11, en la que el circuito de procesamiento (602) está adaptado adicionalmente para obtener un perfil de suscripción asociado a la nueva identidad del nodo repetidor al reautenticar el nodo repetidor (102, 600), en la que el perfil de suscripción autoriza un acceso de red al nodo repetidor (102, 600) para operar como un dispositivo repetidor que transmite el tráfico entre uno o más terminales de acceso y la red de comunicación (108).

13. La entidad de red (800) de la reivindicación 9, en la que el nodo repetidor (102, 600) aparece como un dispositivo de usuario al autenticarse usando las credenciales de seguridad iniciales (202), y el nodo repetidor (102, 600) aparece como un dispositivo repetidor al reautenticarse usando las nuevas credenciales de seguridad (208).

14. La entidad de red (800) de la reivindicación 9, en la que la entidad de red (800) comprende una entidad de gestión de movilidad, MME (110).

15. El nodo repetidor de la reivindicación 1, o la entidad de red (800) de la reivindicación 9, en el que las nuevas credenciales de seguridad (208) incluyen al menos una de las credenciales de operador o una clave compartida.

16. La entidad de red (800) de la reivindicación 9, adaptada para reautenticar el nodo repetidor (102, 600) usando las nuevas credenciales de seguridad (208) y las credenciales de seguridad iniciales (202), en la que las credenciales de seguridad iniciales (202) incluyen preferiblemente una identidad del nodo repetidor inicial y un secreto compartido inicial asociado a la identidad del nodo repetidor inicial.

17. La entidad de red (800) de la reivindicación 16, adaptada adicionalmente para obtener un perfil de suscripción asociado a la identidad del nodo repetidor inicial para autenticar el nodo repetidor (102, 600) usando las credenciales de seguridad iniciales (202), en la que el perfil de suscripción autoriza la red de acceso para el nodo repetidor (102, 600) para un fin limitado de configuración del nodo repetidor (102, 600);

obtener un nuevo perfil de suscripción asociado a la identidad del nodo repetidor inicial para reautenticar el nodo repetidor (102, 600) usando las nuevas credenciales de seguridad (208), donde el nuevo perfil de suscripción autoriza un acceso de red suficiente para el nodo repetidor (102, 600) para permitir que el nodo repetidor (102, 600) opere como un dispositivo repetidor que transmite el tráfico entre uno o más terminales de acceso y la red de comunicación (108).

18. Un método operativo en un nodo repetidor (102, 600), que comprende:

autenticar por vía inalámbrica el nodo repetidor (102, 600) a una entidad de red (800) usando credenciales de seguridad iniciales (202); y, recibir autorización (204) para comunicar por vía inalámbrica con una red de comunicación (108) para un fin limitado de configuración del nodo repetidor (102, 600) en respuesta a la autenticación inalámbrica usando las credenciales de seguridad iniciales (202),
caracterizado por:

recibir nuevas credenciales de seguridad (208); y reautenticar el nodo repetidor (102, 600) para la entidad de red (800) usando las nuevas credenciales de seguridad (208) antes de habilitarse para operar como un dispositivo repetidor en la red de comunicación (108).

19. Un método operativo en una entidad de red (800), que comprende:

autenticar (204) un nodo repetidor (102, 600) usando credenciales de seguridad iniciales (202) asociadas al nodo repetidor (102, 600); y, autorizar el nodo repetidor (102, 600) para comunicar por vía inalámbrica con una red de comunicación (108) para un fin limitado de configuración del nodo repetidor (102, 600) después de una autenticación satisfactoria del nodo repetidor (102, 600) usando las credenciales de seguridad iniciales (202),
caracterizado por:

reautenticar el nodo repetidor (102, 600) usando nuevas credenciales de seguridad (208); y autorizar el nodo repetidor (102, 600) para operar como un dispositivo repetidor en la red de comunicación (108) después de reautenticar satisfactoriamente el nodo repetidor (102, 600).

20. Un medio legible por procesador que comprende instrucciones operativas sobre un repetidor o sobre una entidad de red (800), que al ejecutarse por un procesador hace que el procesador realice el método de acuerdo con la reivindicación 18 o la reivindicación 19.

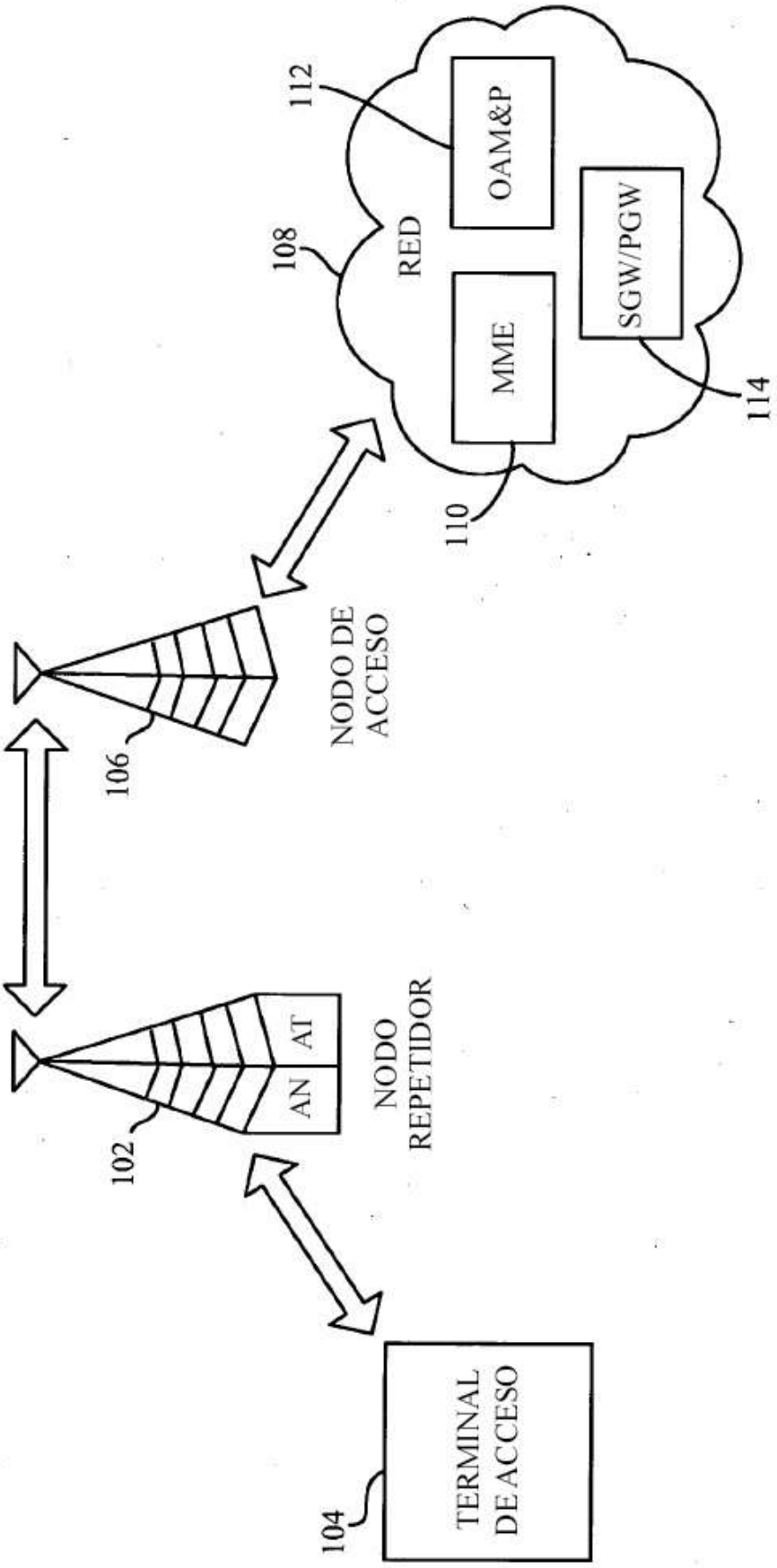
112
OAM&P
108
RED
SGW/PGW
MME
114
110
NODO DE ACCESO
106
AT
AN
NODO REPETIDOR
102
TERMINAL DE ACCESO
104

FIG. 1

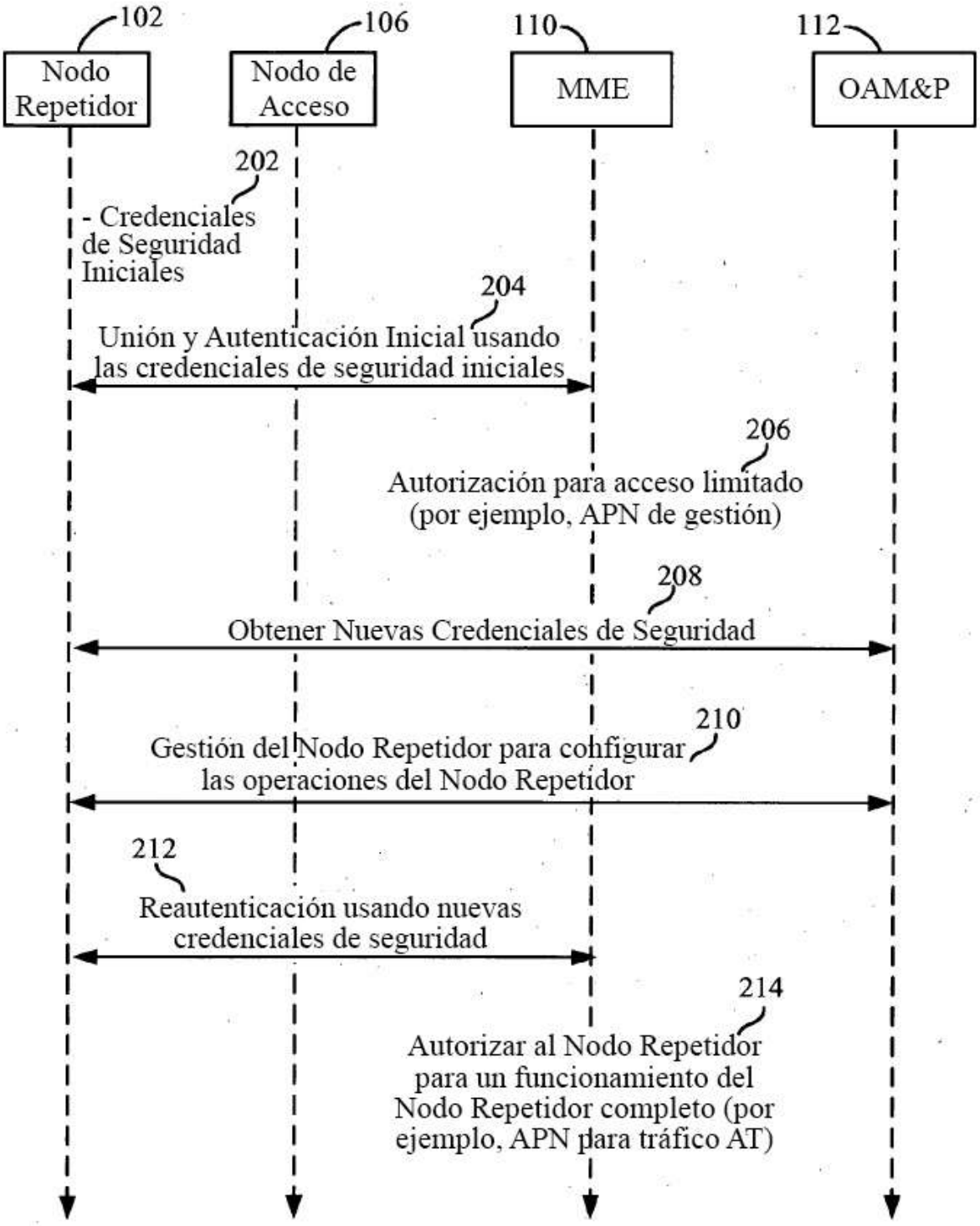
102
Nodo Repetidor
106
Nodo de Acceso
110
MME
112
OAM&P
202
- Credenciales de Seguridad Iniciales
204
Unión y Autenticación Inicial usando las credenciales de seguridad iniciales
206
Autorización para acceso limitado (por ejemplo, APN de gestión)
208
Obtener Nuevas Credenciales de Seguridad
210
Gestión del Nodo Repetidor para configurar las operaciones del Nodo Repetidor
212
Reautenticación usando nuevas credenciales de seguridad
214
Autorizar al Nodo Repetidor para un funcionamiento del Nodo Repetidor completo (por ejemplo, APN para tráfico AT)

FIG. 2

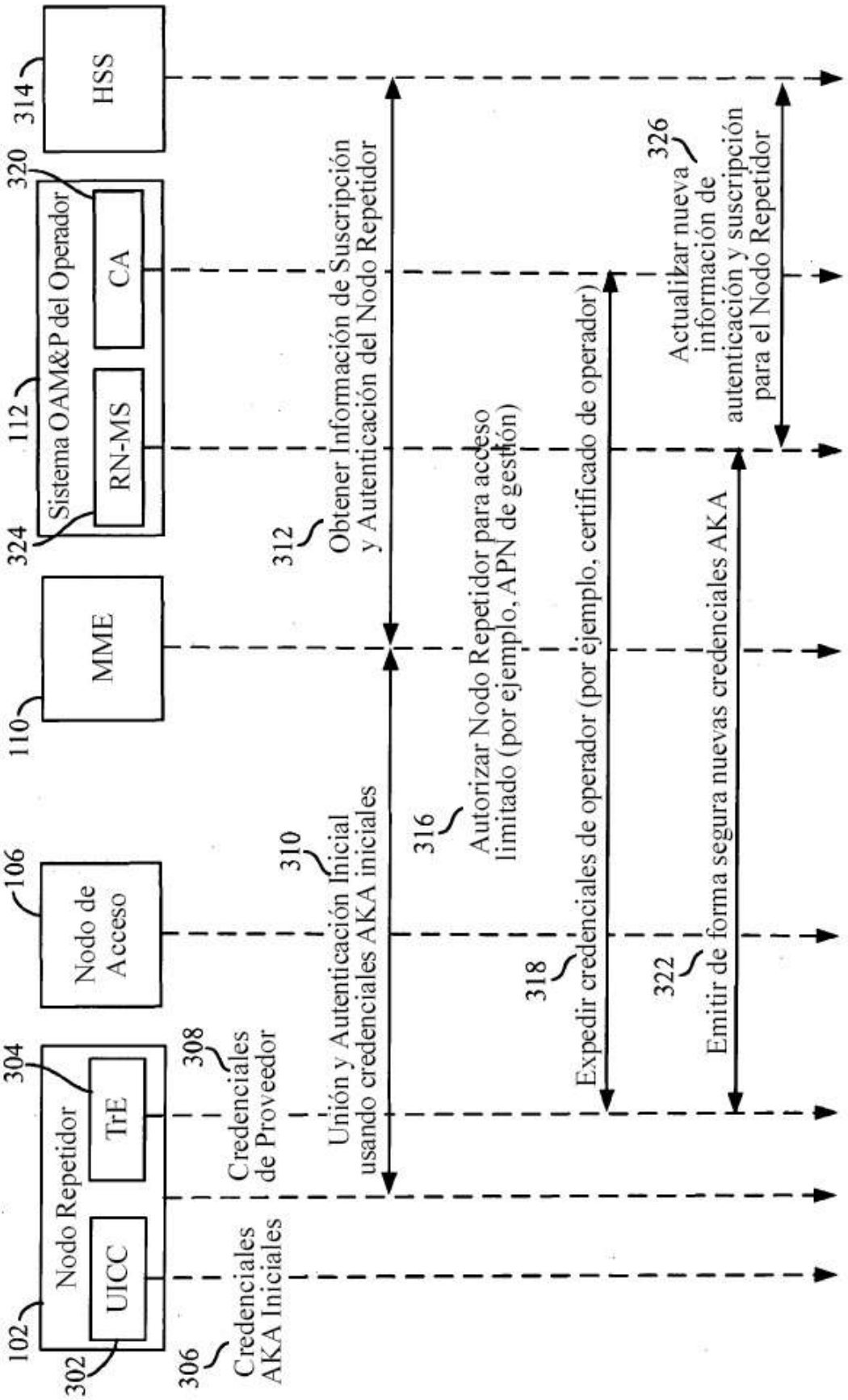
102
Nodo Repetidor
UICC
TrE
302
304
106
Nodo de Acceso
110
MME
112
Sistema OAM&P del Operador
RN-MS
CA
320
324
314
HSS
306
Credenciales AKA Iniciales
308
Credenciales de Proveedor
310
Unión y Autenticación Inicial usando credenciales AKA iniciales
312
Obtener Información de Suscripción y Autenticación del Nodo Repetidor
316
Autorizar Nodo Repetidor para acceso limitado (por ejemplo, APN de gestión)
318
Expedir credenciales de operador (por ejemplo, certificado de operador)
322
Emitir de forma segura nuevas credenciales AKA
326
Actualizar nueva información de autenticación y suscripción para el Nodo Repetidor

FIG. 3A

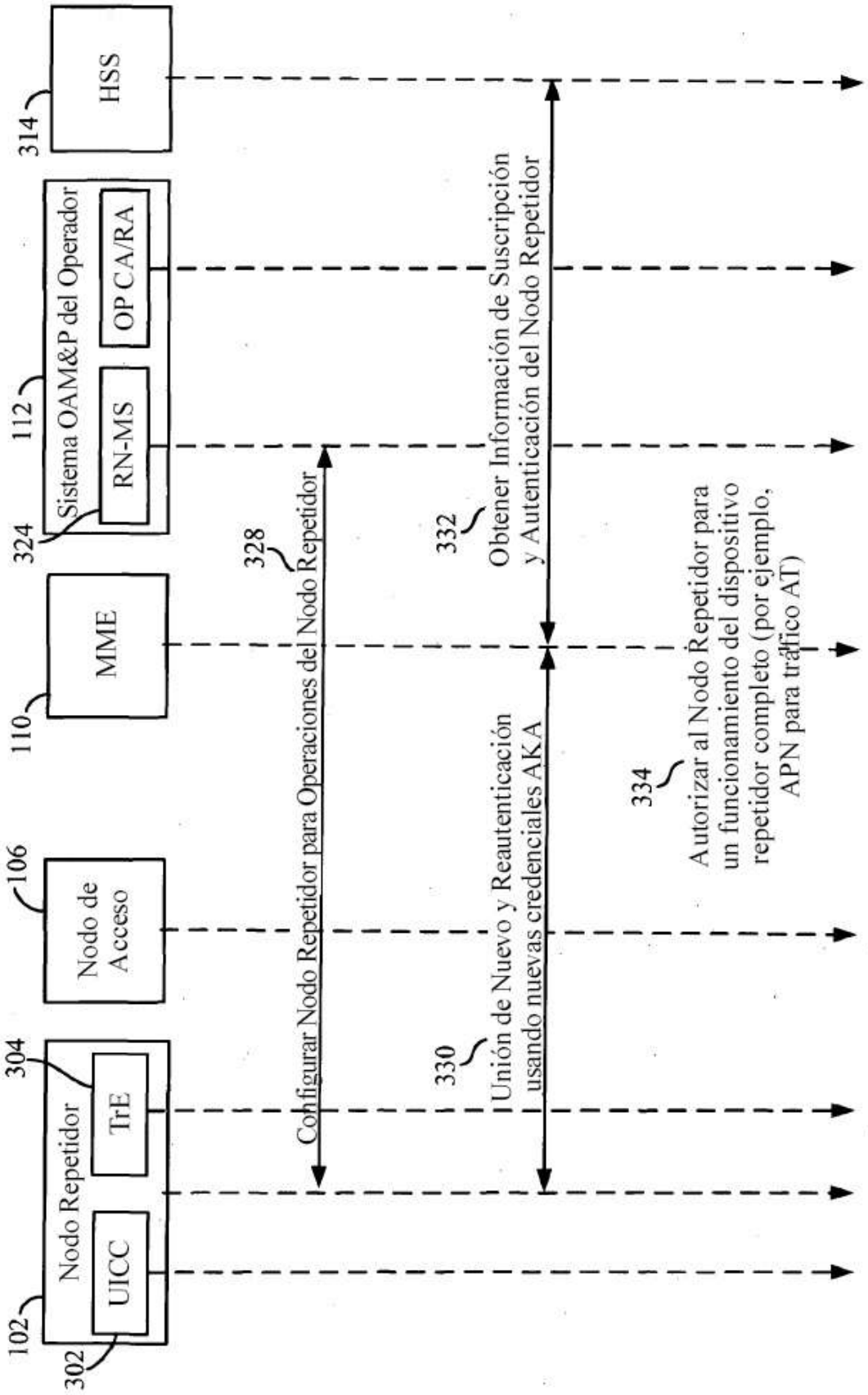
102
Nodo Repetidor
UICC
302
304
TrE
106
Nodo de Acceso
110
MME
112
Sistema OAM&P del Operador
RN-MS
OP CA/RA
324
314
HSS
328
Configurar Nodo Repetidor para Operaciones del Nodo Repetidor
330
Unión de Nuevo y Reautenticación usando nuevas credenciales AKA
332
Obtener Información de Suscripción y Autenticación del Nodo Repetidor
334
Autorizar al Nodo Repetidor para un funcionamiento del dispositivo repetidor completo (por ejemplo, APN para tráfico AT)

FIG. 3B

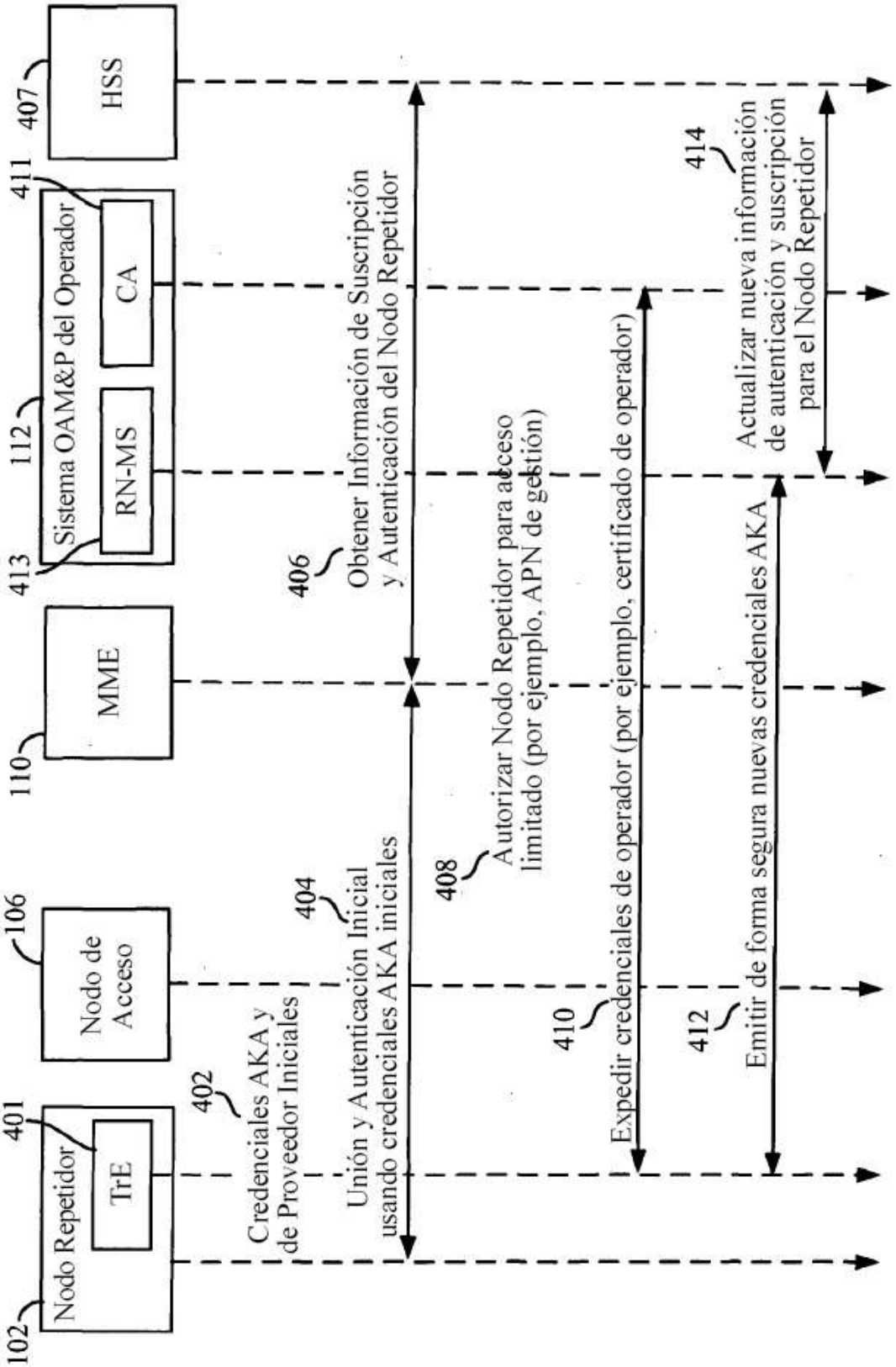
Nodo Repetidor
TrE
Nodo de Acceso
MME
Sistema OAM&P del Operador
RN-MS
CA
HSS
102
401
106
110
411
112
413
407
402
Credenciales AKA y de Proveedor Iniciales
404
Unión y Autenticación Inicial usando credenciales AKA iniciales
406
Obtener Información de Suscripción y Autenticación del Nodo Repetidor
408
Autorizar Nodo Repetidor para acceso limitado (por ejemplo, APN de gestión)
410
Expedir credenciales de operador (por ejemplo, certificado de operador)
412
Emitir de forma segura nuevas credenciales AKA
414
Actualizar nueva información de autenticación y suscripción para el Nodo Repetidor

FIG. 4A

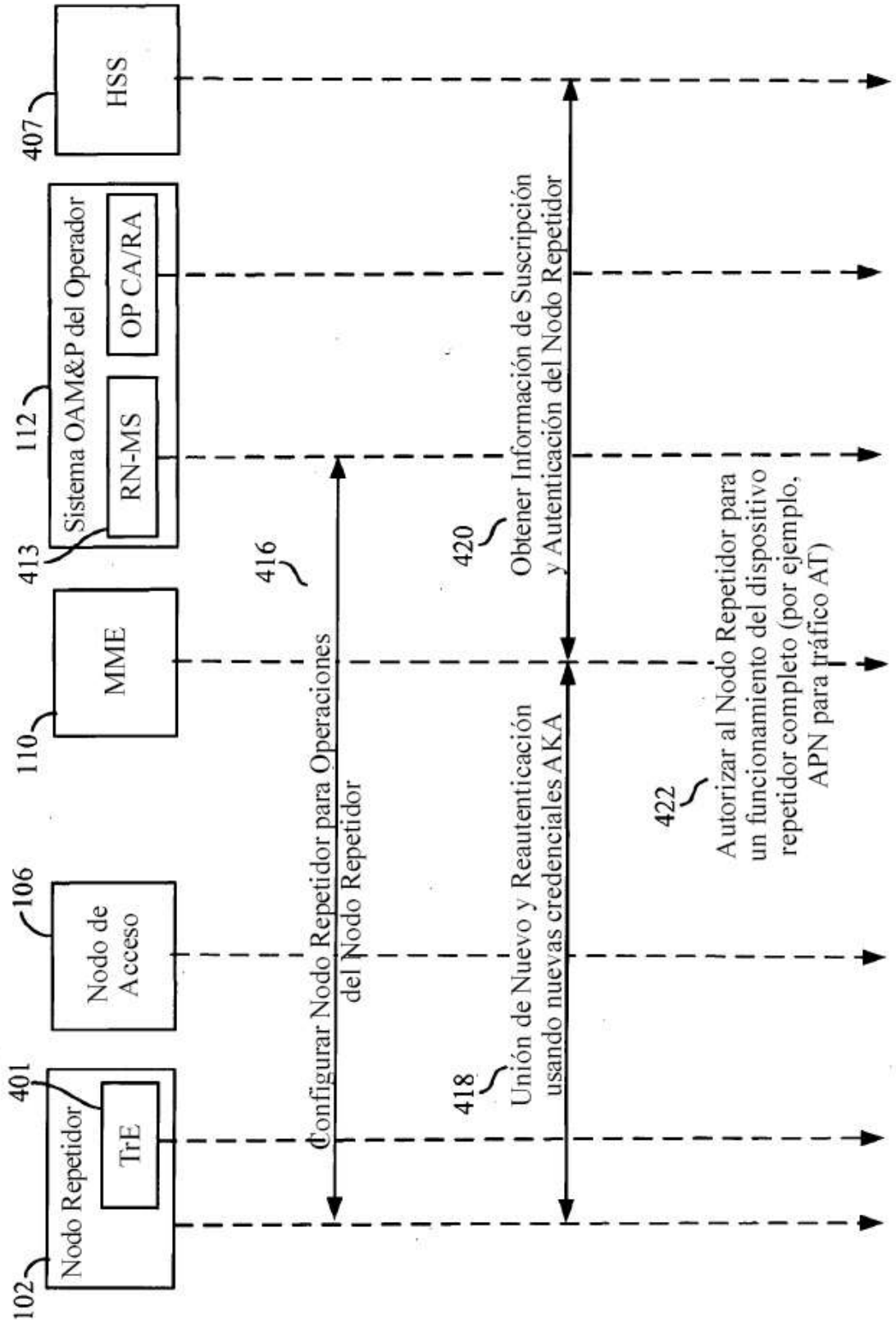
HSS
407
Sistema OAM&P del Operador
112
RN-MS
OP CA/RA
413
MME
110
Nodo de Acceso
106
Nodo Repetidor
TrE
401
102
416
Configurar Nodo Repetidor para Operaciones del Nodo Repetidor
420
Obtener Información de Suscripción y Autenticación del Nodo Repetidor
418
Unión de Nuevo y Reautenticación usando nuevas credenciales AKA
422
Autorizar al Nodo Repetidor para un funcionamiento del dispositivo repetidor completo (por ejemplo, APN para tráfico AT)

FIG. 4B

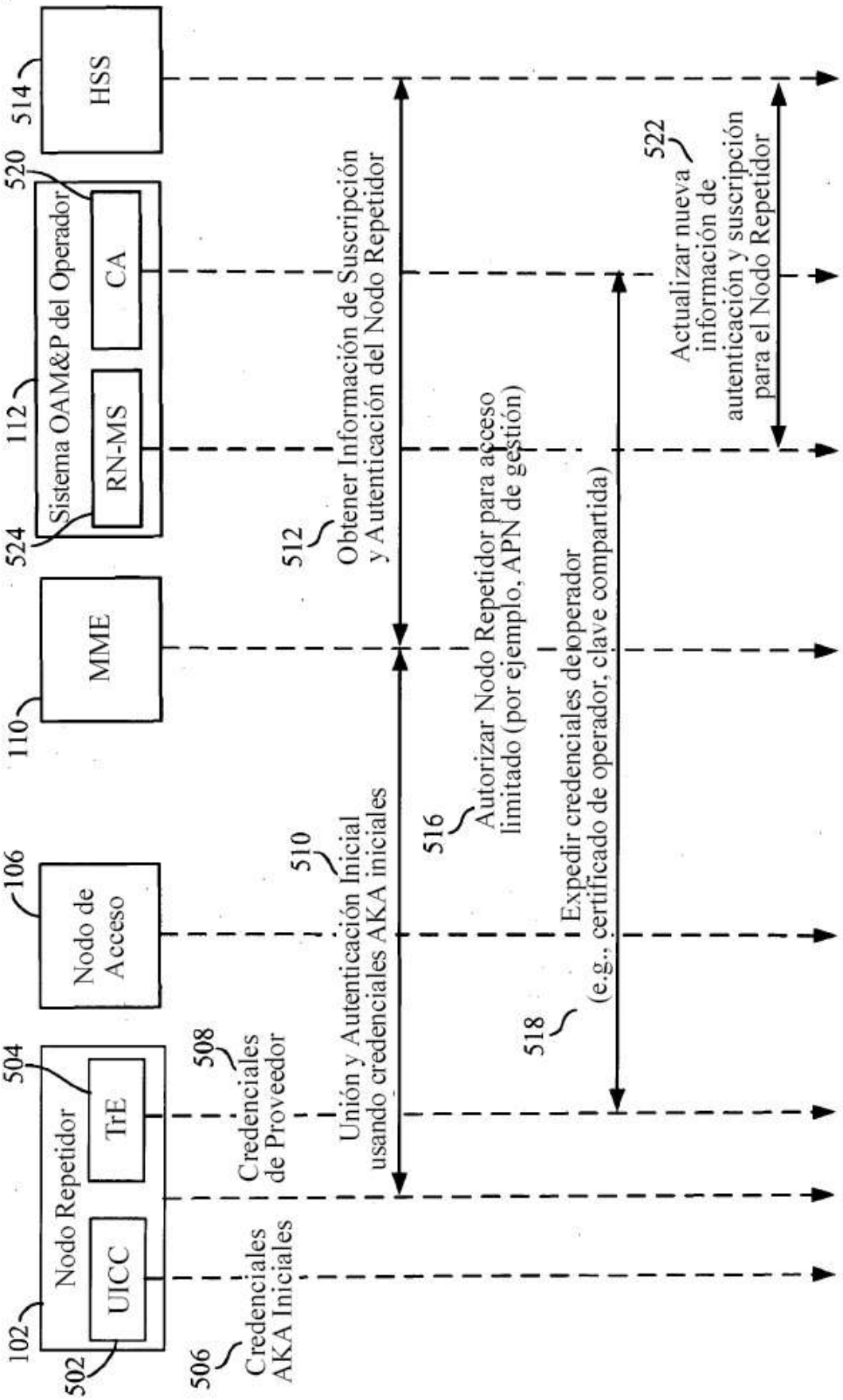
102
Nodo Repetidor
UICC
502
TrE
504
Nodo de Acceso
106
MME
110
Sistema OAM&P del Operador
112
RN-MS
524
CA
520
HSS
514
506
Credenciales AKA Iniciales
508
Credenciales de Proveedor
510
Unión y Autenticación Inicial usando credenciales AKA iniciales
512
Obtener Información de Suscripción y Autenticación del Nodo Repetidor
516
Autorizar Nodo Repetidor para acceso limitado (por ejemplo, APN de gestión)
518
Expedir credenciales de operador (e.g., certificado de operador, clave compartida)
522
Actualizar nueva información de autenticación y suscripción para el Nodo Repetidor

FIG. 5A

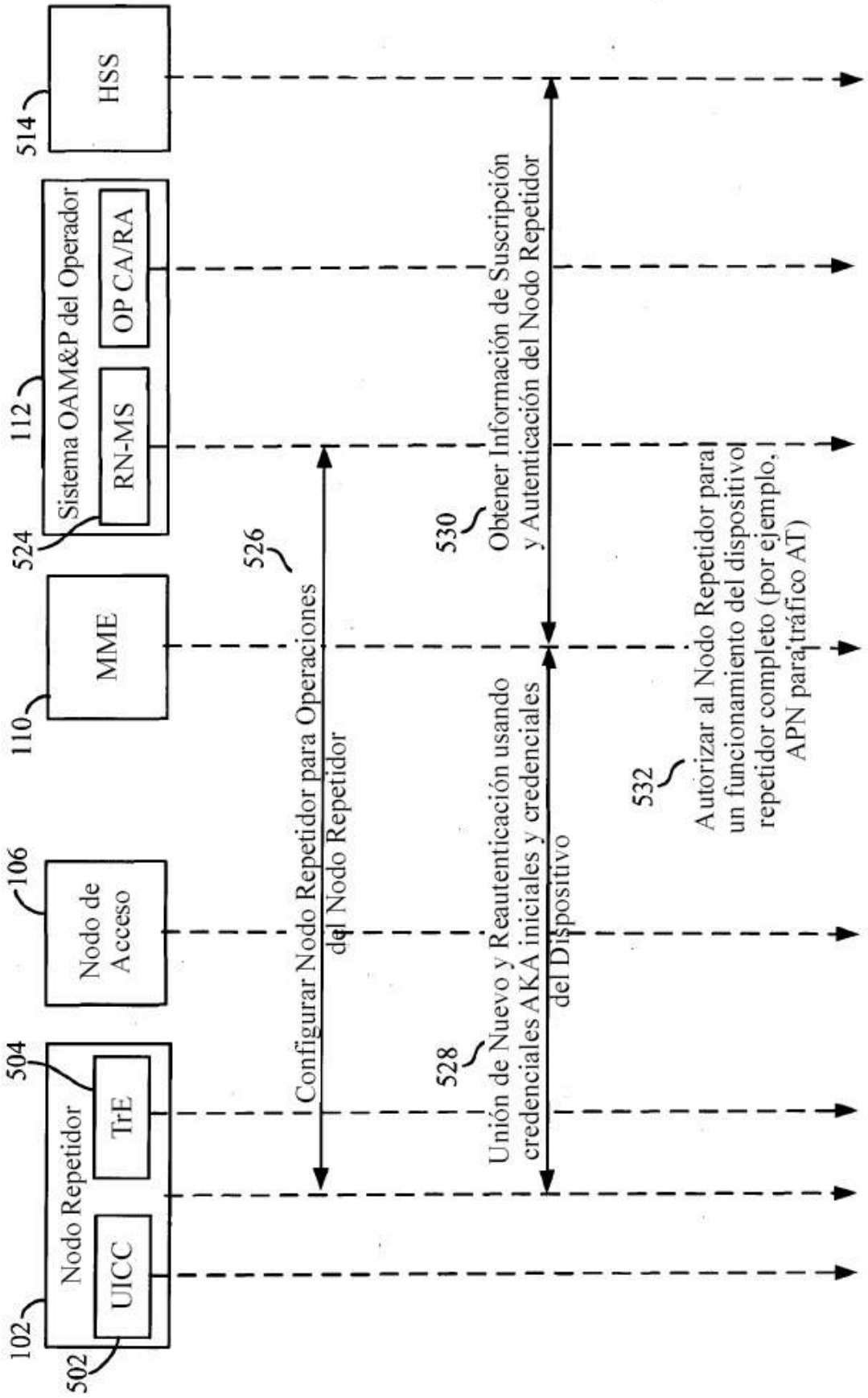
102
Nodo Repetidor
UICC
502
504
TrE
106
Nodo de Acceso
110
MME
112
Sistema OAM&P del Operador
RN-MS
OP CA/RA
514
HSS
524
526
Configurar Nodo Repetidor para Operaciones del Nodo Repetidor
528
Unión de Nuevo y Reautenticación usando credenciales AKA iniciales y credenciales del Dispositivo
530
Obtener Información de Suscripción y Autenticación del Nodo Repetidor
532
Autorizar al Nodo Repetidor para un funcionamiento del dispositivo repetidor completo (por ejemplo, APN para tráfico AT)

FIG. 5B

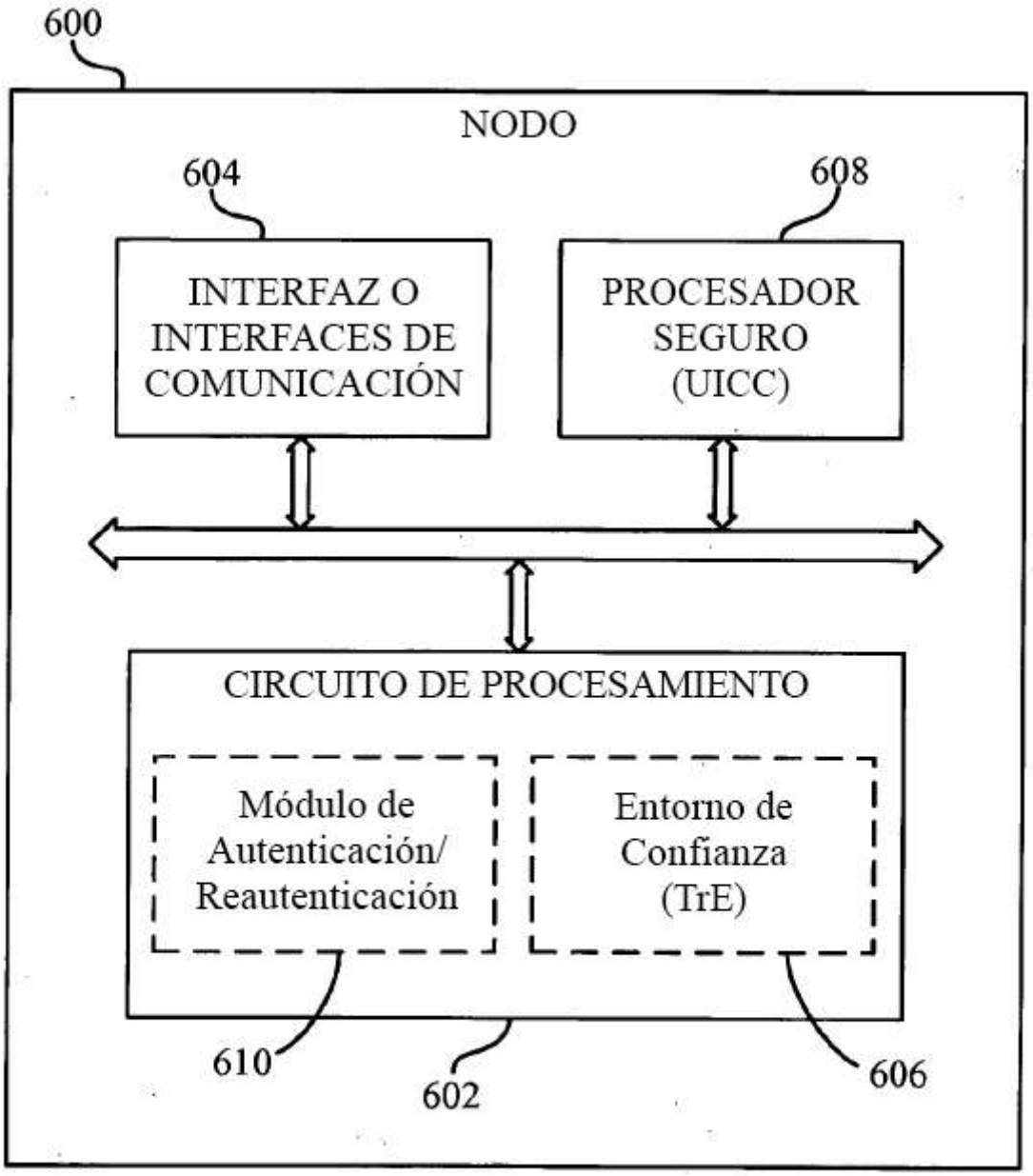
600
NODO
604
608
INTERFAZ O INTERFACES DE COMUNICACIÓN
PROCESADOR SEGURO (UICC)
CIRCUITO DE PROCESAMIENTO
Módulo de Autenticación/ Reautenticación
Entorno de Confianza (TrE)
610
602
606

FIG. 6

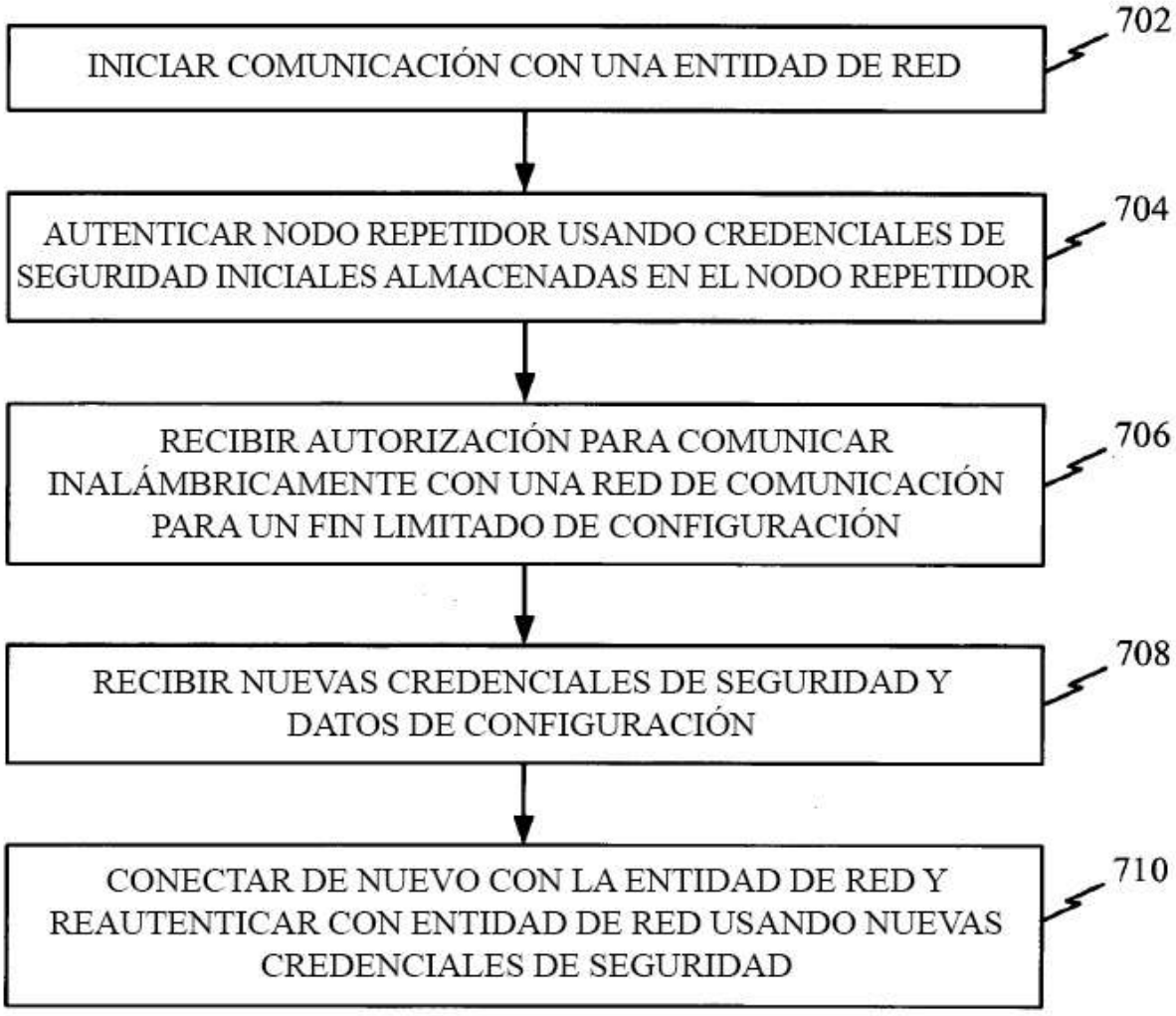
INICIAR COMUNICACIÓN CON UNA ENTIDAD DE RED
702
AUTENTICAR NODO REPETIDOR USANDO CREDENCIALES DE SEGURIDAD INICIALES ALMACENADAS EN EL NODO REPETIDOR
704
RECIBIR AUTORIZACIÓN PARA COMUNICAR INALÁMBRICAMENTE CON UNA RED DE COMUNICACIÓN PARA UN FIN LIMITADO DE CONFIGURACIÓN
706
RECIBIR NUEVAS CREDENCIALES DE SEGURIDAD Y DATOS DE CONFIGURACIÓN
708
CONECTAR DE NUEVO CON LA ENTIDAD DE RED Y REAUTENTICAR CON ENTIDAD DE RED USANDO NUEVAS CREDENCIALES DE SEGURIDAD
710

FIG. 7

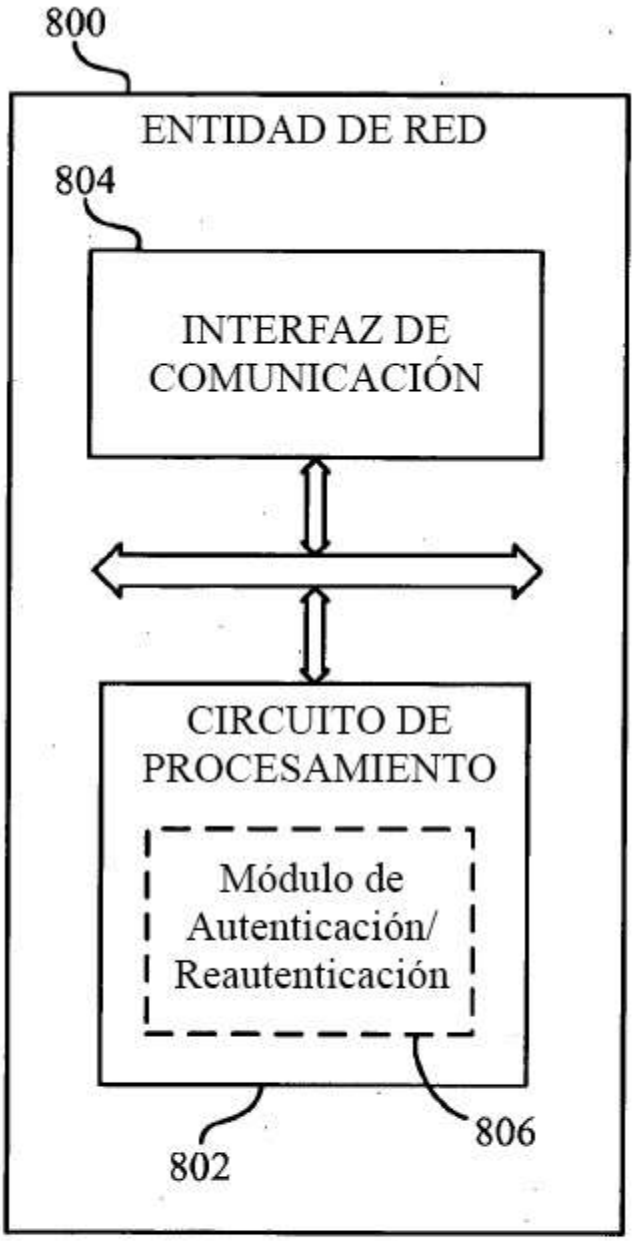
800
ENTIDAD DE RED
804
INTERFAZ DE COMUNICACIÓN
CIRCUITO DE PROCESAMIENTO
Módulo de Autenticación/ Reautenticación
802
806

FIG. 8

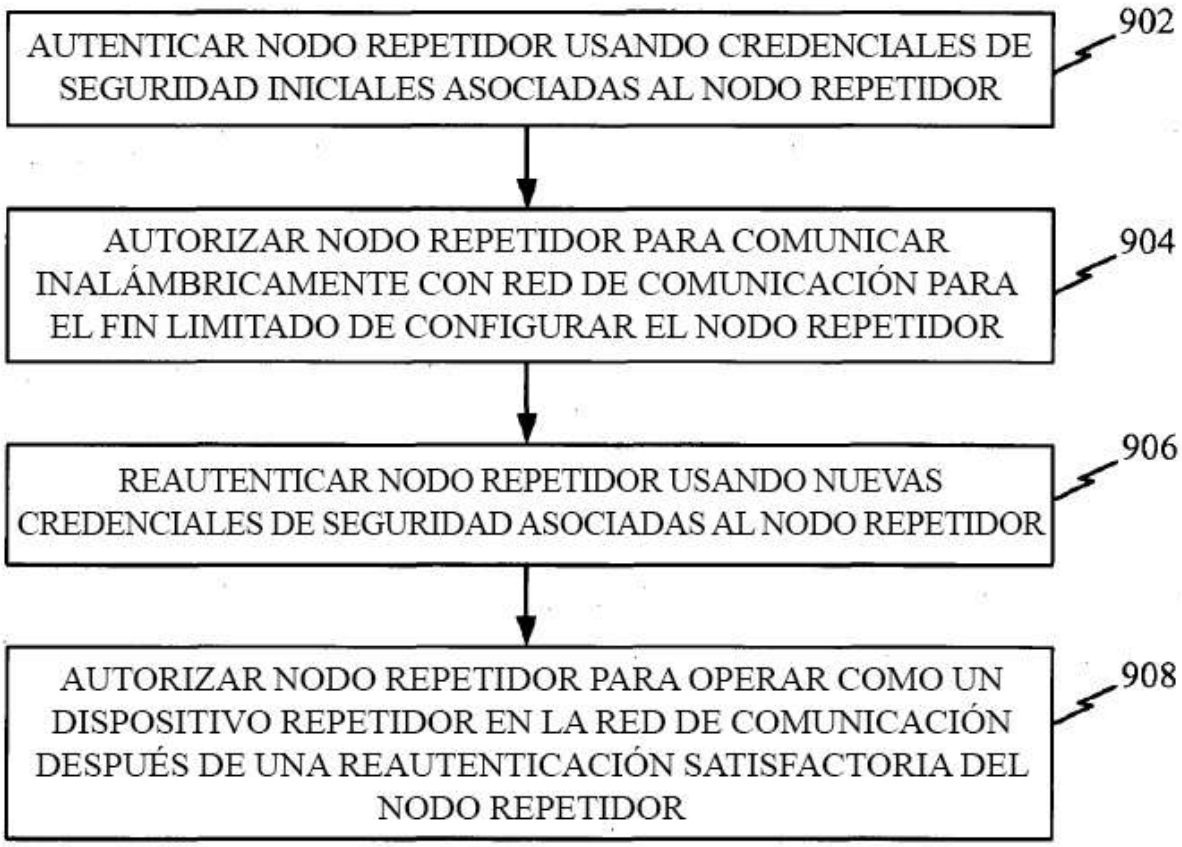
AUTENTICAR NODO REPETIDOR USANDO CREDENCIALES DE SEGURIDAD INICIALES ASOCIADAS AL NODO REPETIDOR
902
AUTORIZAR NODO REPETIDOR PARA COMUNICAR INALÁMBRICAMENTE CON RED DE COMUNICACIÓN PARA EL FIN LIMITADO DE CONFIGURAR EL NODO REPETIDOR
904
REAUTENTICAR NODO REPETIDOR USANDO NUEVAS CREDENCIALES DE SEGURIDAD ASOCIADAS AL NODO REPETIDOR
906
AUTORIZAR NODO REPETIDOR PARA OPERAR COMO UN DISPOSITIVO REPETIDOR EN LA RED DE COMUNICACIÓN DESPUÉS DE UNA REAUTENTICACIÓN SATISFACTORIA DEL NODO REPETIDOR
908

FIG. 9

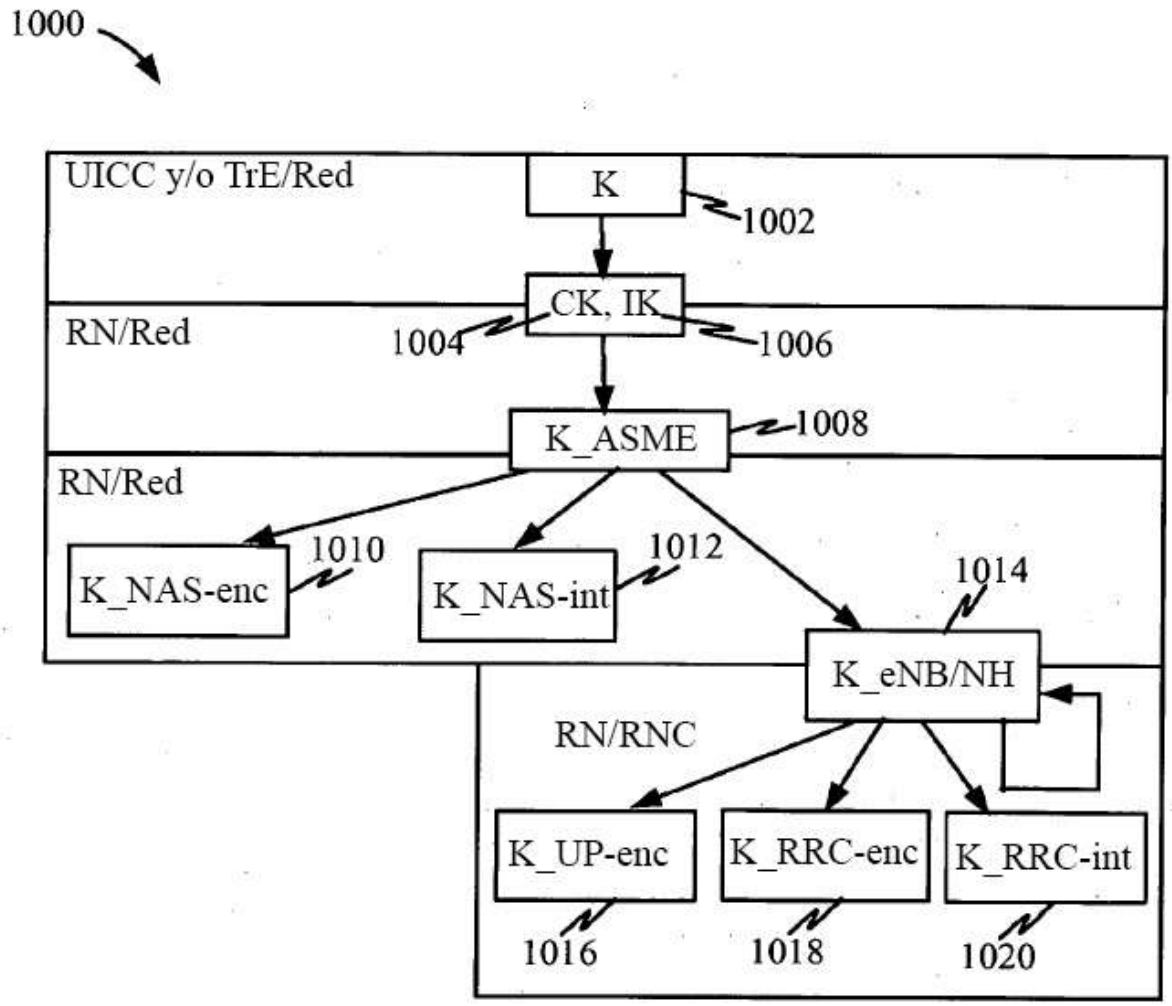
1000
UICC y/o TrE/Red
K
1002
CK, IK
RN/Red
1004
1006
K_ASME
1008
RN/Red
K_NAS-enc
1010
K_NAS-int
1012
1014
K_eNB/NH
RN/RNC
K_UP-enc
K_RRC-enc
K_RRC-int
1016
1018
1020

FIG. 10