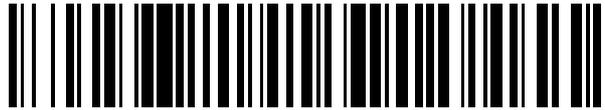


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 815 541**

51 Int. Cl.:

H04W 48/02 (2009.01)

H04W 4/70 (2008.01)

H04W 24/10 (2009.01)

H04W 48/08 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **26.09.2016 PCT/FI2016/050669**

87 Fecha y número de publicación internacional: **11.05.2017 WO17077175**

96 Fecha de presentación y número de la solicitud europea: **26.09.2016 E 16861667 (0)**

97 Fecha y número de publicación de la concesión europea: **15.07.2020 EP 3371985**

54 Título: **Métodos, aparatos y productos de programa informático para implementar control de acceso**

30 Prioridad:

06.11.2015 US 201514935099

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

30.03.2021

73 Titular/es:

**NOKIA SOLUTIONS AND NETWORKS OY
(100.0%)**

**Karakaari 7
02610 Espoo, FI**

72 Inventor/es:

**KOSKINEN, JUSSI-PEKKA y
KOSKELA, JARKKO**

74 Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

ES 2 815 541 T3

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

Métodos, aparatos y productos de programa informático para implementar control de acceso

5 Antecedentes:**Campo:**

La presente invención se refiere a implementar control de acceso.

10

Descripción de la técnica relacionada:

La tecnología de Internet de la Cosas (IOT) se refiere a redes de objetos físicos que se embeben con electrónica, software, sensores y/o conectividad de red. La tecnología de IOT habilita que estos objetos recopilen e intercambien datos. Desde su comienzo, la tecnología de IOT ha visto un despliegue extensivo en una amplia variedad de contextos que implican la comunicación de datos. Los siguientes documentos analizan problemas relacionados con la prohibición de acceso: "Access class barring design for MTC" de Samsung (R2-104890), "Coverage Enhancement Targets" de Alcatel-Lucent (R1-144695), "NB M2M Access Class Barring for Cellular IoT" de Huawei Technologies, el documento US 2011/302310 y "Principles for NB-IoT: GERAN agreed Operator requirements on network sharing, cell barring and access control" de Deutsche Telekom.

15

20

Sumario:

La invención se define mediante las reivindicaciones independientes. Se definen algunas realizaciones en las reivindicaciones dependientes.

25

Breve descripción de los dibujos:

Para un entendimiento apropiado de la invención, debería hacerse referencia a los dibujos adjuntos, en los que:

30

La Figura 1 ilustra una Notación de Sintaxis Abstracta Uno (ASN.1) de ejemplo, de acuerdo con ciertas realizaciones.

La Figura 2 ilustra un diagrama de flujo de un método de acuerdo con ciertas realizaciones de la invención.

La Figura 3 ilustra un diagrama de flujo de un método de acuerdo con ciertas realizaciones de la invención.

35

La Figura 4 ilustra un aparato de acuerdo con ciertas realizaciones de la invención.

La Figura 5 ilustra un aparato de acuerdo con ciertas realizaciones de la invención.

La Figura 6 ilustra un aparato de acuerdo con ciertas realizaciones de la invención.

Descripción detallada:

40

Ciertas realizaciones de la presente invención se refieren a implementar control de acceso para, al menos, dispositivos de comunicación que usan tecnología de Internet de la Cosas de banda estrecha (NB-IOT). Aunque la descripción se escribe usando la NB-IOT como la tecnología de acceso, las realizaciones con aplicables también para implementar control de acceso para dispositivos de comunicación que también usan otras tecnologías, tales como Sistema Global para Comunicaciones Móviles (GSM, 2G), red de acceso de radio GSM EDGE (GERAN), Servicio General de Paquetes de Radio (GRPS), Sistema de Telecomunicaciones Móviles Universales (UMTS, 3G) basado en acceso múltiple por división de código de banda ancha básica (W-CDMA), acceso de paquetes de alta velocidad (HSPA), Evolución a Largo Plazo (LTE), LTE Avanzada y/o sistema 5G. El concepto de NB-IOT incluye, por ejemplo, LTE de banda estrecha, M2M de banda estrecha y técnicas de OFDMA de banda estrecha.

45

50

Ciertas realizaciones de la presente invención pueden referirse a un artículo de trabajo de 3GPP titulado "Narrowband IOT". Este artículo de trabajo de 3GPP indica "el objetivo del artículo de trabajo es especificar un acceso de radio para Internet de las Cosas celular, basándose en gran medida en una variante no compatible hacia atrás de E-UTRA, que aborda cobertura en interiores mejorada, soporte para un número masivo de dispositivos de caudal bajo, sensibilidad de retado baja, coste de dispositivo ultra bajo, consumo de potencia de dispositivo bajo y arquitectura de red (optimizada)".

55

Los métodos/esquemas de control de acceso actuales no son generalmente adecuados/suficientes para su uso con la tecnología de Internet de la Cosas de banda estrecha (NB-IOT). NB-IOT soporta niveles de Mejora de Cobertura (CE) Múltiple. También, con NB-IOT, equipo de usuario (UE) que está en cobertura mejorada profunda puede provocar más carga e interferencia, en comparación con UE en cobertura normal. Esta mayor cantidad de carga e interferencia puede resultar a partir de una alta cantidad de repeticiones de transmisión realizadas por los UE. La mayor carga/interferencia también puede resultar a partir de una alta potencia de transmisión usada por las UE. Con NB-IOT, la necesidad de soportar múltiples niveles de CE, junto con la mayor cantidad de carga/interferencia potencial, puede provocar que los métodos/esquemas de control de acceso actuales no sean adecuados/suficientes para su uso.

60

65

Con respecto a algunos ejemplos de control de acceso, 3GPP define dos mecanismos de control de acceso como se indica a continuación:

- 5 - Prohibición de Clase de Acceso (ACB), en la que la prohibición de acceso se realiza por clase de acceso almacenada en el Módulo de Identidad de Abonado Universal (USIM) de los UE.
- 10 - Prohibición de Clase de Acceso Extendida (EAB) se realiza por UE, que están sujetos a EAB. Por ejemplo, EAB puede realizarse únicamente por dispositivos que se configuran (a través de fabricación, programación, USIM, etc.) para ser UE de EAB. La prohibición se realiza por cada categoría de UE para los que se aplica EAB. Por ejemplo, el valor a corresponde a todos los UE, valor b corresponde a los UE que no están ni en su Red Móvil Pública Terrestre Doméstica (HPLMN), ni en una PLMN que es equivalente a la misma, y el valor c corresponde a los UE que no están ni en la PLMN listada como la PLMN más preferida del país donde los UE están realizando itinerancia en la lista de selectores de PLMN definida por el operador, no están en su HPLMN, ni en una PLMN que es equivalente a su HPLMN.
- 15 Ciertas realizaciones de la presente invención se dirigen a mecanismos de control de acceso para NB-IOT, en los que la red (NW) proporciona parámetros de prohibición a UE para la consideración del UE. El UE considera que los parámetros de prohibición recibidos determinan si el UE puede acceder a la NW. La NW puede proporcionar parámetros de prohibición al UE a través de señalización de difusión. Ciertas realizaciones de la presente invención pueden considerar los siguientes parámetros/criterios cuando se determina un estado de prohibición para el UE, en el que el estado de prohibición determina si se concede o deniega al UE un acceso a la NW. Como se describe en más detalle a continuación, la NW (a través de un eNB, por ejemplo) puede transmitir los parámetros de prohibición/control de acceso al UE. Como se ha descrito anteriormente, con ciertas realizaciones, el UE puede considerar los parámetros/criterios recibidos para determinar si se permite que el UE acceda a la red.
- 20
- 25 Con ciertas realizaciones, el acceso a la NW puede concederse o denegarse basándose en si se está realizando la notificación normal y/o notificación de excepción por el UE. Con ciertas realizaciones, la NW puede transmitir un parámetro de prohibición de acceso al UE que indica que únicamente se permite acceso a la NW al UE que realiza notificación de excepción. La NW puede ser capaz de prohibir notificación normal o notificación de excepción. La NW también puede ser capaz de prohibir ambos tipos de notificación. La NW puede transmitir un parámetro de prohibición de acceso que prohíbe UE que realizan notificación normal y/o notificación de excepción.
- 30

Con respecto a la notificación de excepción, puede esperarse que muchas aplicaciones de tipo de sensor supervisen una condición física y desencadenen un informe de excepción cuando se detecta un evento. Se espera que tales eventos sean generalmente raros, produciéndose habitualmente cada pocos meses o incluso años. Ejemplos de tales aplicaciones incluyen detectores de alarma de humo, notificaciones de fallo de potencia desde contadores inteligentes y notificaciones contra manipulación. En una realización, la notificación de excepción comprende datos de prioridad alta.

Con respecto a la notificación normal, se espera que la notificación de enlace ascendente periódica normal sea común para aplicaciones de IoT celulares tales como aplicaciones relacionadas con informes de medición de servicios públicos (gas/agua/electricidad) inteligentes, agricultura inteligente y/o entorno inteligente, por ejemplo. En una realización, la notificación normal comprende datos de prioridad normal y/o baja.

Con ciertos ejemplos, útiles para el entendimiento de la invención, el acceso puede basarse en un nivel de mejora de cobertura. Por ejemplo, la NW puede transmitir un parámetro de prohibición de acceso que prohíbe UE que están en área o áreas de cobertura específicas. La NW puede transmitir un parámetro de prohibición de acceso que indica qué áreas de cobertura están prohibidas. Por ejemplo, la NW puede indicar un nivel de CE explícito que se prohíbe. La NW puede prohibir cualquiera o todos de una cobertura normal, una cobertura extendida, una cobertura extendida superficial y/o una cobertura extendida profunda. La NW puede señalar al UE la clase de área de cobertura en la que está el UE en la actualidad. En una realización, el UE puede determinar el nivel de área de cobertura basándose en las mediciones de radio. La NW puede proporcionar umbrales/criterios para cada área de cobertura al UE.

El acceso puede depender de al menos una clase de cobertura a la que se permite o no acceder a la red. Por lo tanto, únicamente dispositivos con una clase de cobertura permitida/autorizada pueden permitirse o pueden no permitirse que accedan a la red. "Clase de área de cobertura" habitualmente significa la capacidad del dispositivo para operar en cierta extensión o extensiones de cobertura, mientras que "Área de cobertura" habitualmente significa la ubicación en la que el dispositivo se ubica físicamente en la célula.

Con ciertas realizaciones, el acceso puede basarse en potencia de radio y/o umbrales de nivel de calidad. La NW puede transmitir un parámetro de prohibición de acceso que corresponde a umbrales de potencia de radio / nivel de calidad que tienen que cumplirse (por el UE) para acceder a la red. El UE puede medir el nivel de potencia recibida / calidad de señal basándose en mediciones de radio normales, tales como basándose en una potencia de recepción de señal de referencia (RSRP) o un indicador de intensidad de señal recibida (RSSI). Con ciertas realizaciones, si un UE no tiene suficiente potencia de radio, o un nivel de calidad suficiente, a continuación puede prohibirse que el UE acceda. En una realización, el UE puede usar la potencia de señal recibida/nivel de calidad, tal como RSRP y/o RSSI, para determinar la clase/nivel de área de cobertura en la que se ubica el UE en la actualidad.

La prohibición, o control de acceso en general, puede realizarse habitualmente en situaciones de carga, y dispositivos en mala cobertura provocarán más carga debido a malas condiciones de radio y repeticiones de transmisión recibidas. Por lo tanto, puede proporcionar beneficios si estos dispositivos pueden prohibirse en situación de carga. Por otra parte, podría haber diferentes clases de dispositivos con diferentes clases de servicios y puede ser bueno no prohibir ciertos dispositivos incluso en mala cobertura de NW. Debido a las realizaciones de la invención, estos aspectos pueden tenerse en cuenta y el mecanismo de prohibición se vuelve más flexible.

Con ciertos ejemplos, útiles para el entendimiento la invención, si acceder o no puede basarse en un momento en el que la notificación se realizó por última vez satisfactoriamente o no satisfactoriamente (cuando se realiza notificación normal o de excepción, por ejemplo). La NW puede prohibir los dispositivos que fueron capaces de realizar recientemente la notificación. La NW puede controlar con qué frecuencia pueden intentar los dispositivos realizar la notificación de nuevo. La NW puede transmitir parámetros de prohibición de acceso que reflejan las condiciones de prohibición anteriores.

Con ciertos ejemplos, útiles para el entendimiento la invención, la prohibición también puede determinarse basándose en una clase de suscripción. Por ejemplo, puede permitirse que un usuario oro acceda a la red, pero puede no permitirse que un usuario bronce acceda a la red.

Ciertos ejemplos, útiles para el entendimiento la invención, pueden definir que el acceso se permite con ciertos tipos de dispositivos. Por ejemplo, puede permitirse que dispositivos sensores envíen datos de sensor medidos, mientras que puede no permitirse que otro tipo de dispositivos accedan a la red.

Ciertas realizaciones pueden trabajar junto con mecanismos de prohibiciones típicos. Por ejemplo, el eNB podría aún prohibir, por ejemplo, un cierto porcentaje de UE (tal como, por ejemplo, un 30 % de UE) en un cierto nivel de cobertura.

Además, ciertos ejemplos, útiles para el entendimiento la invención, también pueden usar la siguiente información/criterios para determinar un estado de prohibición de una célula. La NW puede realizar prohibición de UE basándose en qué Red Móvil Pública Terrestre (PLMN) corresponde al UE. Por ejemplo, la NW puede prohibir UE que corresponden a cualquiera de 6 PLMN, por ejemplo. Ciertos ejemplos, útiles para el entendimiento la invención, pueden realizar prohibición de acuerdo con la clase de acceso (según se almacena el módulo de identidad de abonado universal (USIM) del UE). Las clases de acceso pueden oscilar de 0 a 15.

Además, ciertos ejemplos, útiles para el entendimiento la invención, pueden determinar si se permite que un UE acceda a la NW, basándose en si el UE está realizando itinerancia. Ciertos ejemplos, útiles para el entendimiento la invención, pueden diferenciar entre UE en itinerancia y no en itinerancia. La NW puede transmitir parámetros de prohibición de acceso que conceden o deniegan acceso a UE en itinerancia. Ciertos ejemplos, útiles para el entendimiento la invención, pueden diferenciar entre UE en itinerancia en la PLMN más preferida y otros UE en itinerancia. Por ejemplo, la NW puede conceder acceso a UE en la PLMN más preferida.

Ciertas realizaciones de la presente invención pueden usar cualquier combinación de las anteriores. Por ejemplo, ciertas realizaciones pueden prohibir UE en una PLMN específica, puede prohibir UE de una clase de acceso Y, o puede permitir que un usuario de itinerancia envíe únicamente datos de excepción en caso de que un nivel de CE es X, por ejemplo. Ciertas realizaciones pueden reducir interferencia en únicamente ciertas regiones. Por ejemplo, un Nodo B evolucionado (eNB) puede prohibir UE de cobertura normal en casos en los que el eNB quiere más recursos para UE de cobertura extendida.

La Figura 1 ilustra una Notación de Sintaxis Abstracta Uno (ASN.1) de ejemplo, de acuerdo con ciertas realizaciones. La ASN.1 puede describir reglas y estructuras para representar, codificar, transmitir y decodificar datos en telecomunicaciones y redes informáticas.

Ciertas realizaciones pueden proporcionar control de acceso flexible con uno o más mecanismos de control de acceso. Ciertas realizaciones pueden tener la capacidad de tratar UE en itinerancia. Ciertas realizaciones también pueden tener la capacidad de tratar diferentes suscripciones de forma diferente.

La Figura 2 ilustra un diagrama de flujo de un método de acuerdo con ciertas realizaciones de la invención. El método ilustrado en la Figura 2 incluye, en 210, determinar, por un nodo de red de una red, al menos un criterio de control de acceso para un dispositivo de comunicación. Cumplir el al menos un criterio de control de acceso depende de acciones del dispositivo de comunicación. El método puede incluir también, en 220, transmitir el al menos un criterio de control de acceso al dispositivo de comunicación. El al menos un criterio de control de acceso habilita que el dispositivo de comunicación determine si se permite que el dispositivo de comunicación acceda a una red.

Los criterios/parámetros de control de acceso pueden verse que comprenden o bien criterios/parámetros de concesión de acceso y/o criterios/parámetros de prohibición de acceso. Los criterios/parámetros pueden indicarse de una manera positiva (por ejemplo, indicando cuando se permite el acceso) y/o de una manera negativa (por ejemplo, indicando cuando no se permite el acceso, tal como, en mala cobertura, no se permite el acceso).

Los criterios propuestos pueden ser dinámicos en naturaleza de tal forma que si se permite que el dispositivo de comunicación acceda a la red o puede no depender de acciones recientes del dispositivo de comunicación. Por ejemplo, puede permitirse que el dispositivo acceda a la red si el UE no ha enviado ningún dato a la red en un periodo de tiempo predeterminado. Por ejemplo, puede prohibirse que el dispositivo acceda si el UE se ha movido a un área de cobertura o clase de cobertura no autorizada/no aceptada. Por ejemplo, si el dispositivo está a punto de iniciar el acceso a la red sobre la base de una necesidad de realizar notificación de excepción, tal como datos de prioridad alta (por ejemplo, el dispositivo ha detectado una excepción y necesita enviar una alarma), puede permitirse el acceso. Por lo tanto, en una realización, los criterios propuestos dependen de las acciones del dispositivo. Por lo tanto, pueden verse como dinámicos en naturaleza - en algún punto, el dispositivo puede acceder a la red mientras que, en otro punto, no puede, independientemente del hecho de que los propios criterios pueden haber permanecido los mismos. Por otra parte, los criterios también pueden ser dinámicos, ya que la NW puede configurar el dispositivo con criterios actualizados siempre que se necesitan.

En una realización, el al menos un criterio comprende un criterio/parámetro relacionado con comunicación de Internet de las Cosas de banda estrecha.

La Figura 3 ilustra un diagrama de flujo de un método de acuerdo con ciertas realizaciones de la invención. El método ilustrado en la Figura 3 incluye, en 310, recibir, por un dispositivo de comunicación, al menos un criterio de control de acceso desde un nodo de red de una red. El método puede incluir también, en 320, determinar una necesidad de acceder a la red. El método puede incluir también, en 330, determinar si se permite que el dispositivo de comunicación acceda a la red basándose en si se cumple o no el al menos un criterio de control de acceso recibido. Cumplir el al menos un criterio de control de acceso depende de acciones del dispositivo de comunicación.

La Figura 4 ilustra un aparato de acuerdo con ciertas realizaciones de la invención. En una realización, el aparato puede ser una estación base y/o un Nodo B evolucionado, por ejemplo. En otra realización, el aparato puede ser un UE, por ejemplo. El aparato puede configurarse para realizar, al menos, los métodos descritos en la Figura 2 y/o la Figura 3. El aparato 10 puede incluir un procesador 22 para procesar información y ejecutar instrucciones u operaciones. El procesador 22 puede ser cualquier tipo de procesador de fin general o específico. Mientras en la Figura 4 se muestra un único procesador 22, pueden utilizarse múltiples procesadores de acuerdo con otras realizaciones. El procesador 22 también puede incluir uno o más de ordenadores de fin general, ordenadores de fin especial, microprocesadores, procesadores de señales digitales (DSP), campos de matrices de puertas programables (FPGA), circuitos integrados específicos de la aplicación (ASIC) y procesadores basándose en una arquitectura de procesador multinúcleo, como ejemplos.

El aparato 10 puede incluir adicionalmente una memoria 14, acoplada al procesador 22, para almacenar información e instrucciones que pueden ejecutarse por el procesador 22. La memoria 14 puede ser una o más memorias y de cualquier tipo adecuado al entorno de aplicación local, y puede implementarse usando cualquier tecnología de almacenamiento de datos volátil o no volátil adecuada tal como un dispositivo de memoria basada en semiconductores, un dispositivo y sistema de memoria magnética, un dispositivo y sistema de memoria óptica, memoria fija y memoria extraíble. Por ejemplo, la memoria 14 incluye cualquier combinación de memoria de acceso aleatorio (RAM), memoria de sólo lectura (ROM), almacenamiento estático tal como un disco magnético u óptico, o cualquier otro tipo de medio legible por máquina u ordenador no transitorio. Las instrucciones almacenadas en la memoria 14 pueden incluir instrucciones de programa o código de programa informático que, cuando se ejecutan por el procesador 22, habilitan que el aparato 10 realice tareas como se describe en este documento.

El aparato 10 también puede incluir una o más antenas (no mostradas) para transmitir y recibir señales y/o datos a y desde el aparato 10. El aparato 10 puede incluir adicionalmente un transceptor 28 que modula información en una forma de onda portadora para transmisión por la antena o antenas y demodula información recibida a través de la antena o antenas para su procesamiento adicional por otros elementos de aparato 10. En otras realizaciones, el transceptor 28 puede ser capaz de transmitir y recibir señales o datos directamente.

El procesador 22 puede realizar funciones asociadas con la operación de aparato 10 incluyendo, sin limitación, precodificación parámetros de ganancia/fase de antena, codificación y decodificación de bits individuales que forman un mensaje de comunicación, formateo de información y control general del aparato 10, incluyendo procesos relacionados con gestión de recursos de comunicación.

En una realización, la memoria 14 puede almacenar módulos de software que proporcionan funcionalidad cuando se ejecutan por el procesador 22. Los módulos pueden incluir un sistema operativo 15 que proporciona funcionalidad de sistema operativo para el aparato 10. La memoria también puede almacenar uno o más módulos funcionales 18, tal como una aplicación o programa, para proporcionar funcionalidad adicional para el aparato 10. Los componentes de aparato 10 pueden implementarse en hardware, o como cualquier combinación adecuada de hardware y software.

La Figura 5 ilustra un aparato de acuerdo con ciertas realizaciones de la invención. El aparato 500 puede ser un nodo de red tal como una estación base y/o un eNB, por ejemplo. En una realización, el aparato 500 puede comprender una unidad de control remoto acoplada operativamente (por ejemplo, a través de una red inalámbrica o por cable) a un

cabezal de radio remoto (RRH) ubicado en la estación base. En una realización, al menos algunos de los procesos descritos pueden realizarse por la unidad de control remoto. En una realización, la ejecución de los procesos puede compartirse entre el RRH y el aparato 500 que ubican en la unidad de control remoto, que también puede denominarse como una unidad central o "nube".

5 El aparato 500 puede incluir una unidad de determinación 510 que determina al menos un criterio de control de acceso para un dispositivo de comunicación. Cumplir el al menos un criterio de control de acceso depende de acciones del dispositivo de comunicación. El aparato 500 también puede incluir una unidad de transmisión 520 que transmite el al
10 menos un criterio de control de acceso al dispositivo de comunicación. El al menos un criterio de control de acceso habilita que el dispositivo de comunicación determine si se permite que el dispositivo de comunicación acceda a una red.

La Figura 6 ilustra un aparato de acuerdo con ciertas realizaciones de la invención. El aparato 600 puede ser un equipo de usuario, por ejemplo. El aparato 600 puede comprender el dispositivo terminal de un sistema de comunicación
15 celular, por ejemplo un equipo de usuario (UE), un terminal de usuario (UT), un ordenador (PC), un portátil, un ordenador de tableta, un teléfono celular, un teléfono móvil, un comunicador, un teléfono inteligente, un ordenador de mano, o cualquier otro aparato de comunicación. Como alternativa, el aparato 600 se comprende en un dispositivo terminal de este tipo. Además, el aparato 600 puede ser o comprender un módulo (que hay que unir al UE) que proporciona conectividad, tal como una unidad de extensión, una "llave USB" o cualquier otra clase de unidad. La
20 unidad puede instalarse o bien dentro del UE o unido al UE con un conector o incluso inalámbricamente.

El aparato 600 puede incluir una unidad de recepción 610 que recibe al menos un criterio de control de acceso desde un nodo de red de una red. El aparato 600 también puede incluir una primera unidad de determinación 620 que
25 determina una necesidad de acceder a la red. El aparato 600 también puede incluir una segunda unidad de determinación 630 que determina si se permite que el dispositivo de comunicación acceda a la red basándose en si se cumple o no el al menos un criterio de control de acceso recibido. Cumplir el al menos un criterio de control de acceso depende de acciones del dispositivo de comunicación.

Las características descritas, ventajas y características de la invención pueden combinarse de cualquier manera adecuada en una o más realizaciones. Un experto en la técnica pertinente reconocerá que la invención puede
30 practicarse sin una o más de las características específicas o ventajas de una realización particular. En otros casos, pueden reconocerse características y ventajas adicionales en ciertas realizaciones que pueden no estar presentes en todas las realizaciones de la invención. Un experto en la materia entenderá fácilmente que la invención como se ha analizado anteriormente puede practicarse con etapas en un orden diferente, y/o con elementos de hardware en
35 configuraciones que son diferentes de las que se describen. Por lo tanto, aunque la invención se ha descrito basándose en estas realizaciones preferidas, sería evidente para los expertos en la materia que ciertas modificaciones, variaciones y construcciones alternativas serían evidentes, mientras se mantienen dentro del alcance de la invención.

REIVINDICACIONES

1. Un aparato (600) para su uso en un equipo de usuario, comprendiendo el aparato:
 - 5 medios para recibir (610), a través de señalización de difusión, al menos un criterio de control de acceso desde un nodo de red de una red, en el que el al menos un criterio de control de acceso indica un umbral de potencia recibida que tiene que cumplirse para acceder a la red;
 - medios para determinar (620) una necesidad de acceder a la red;
 - medios para determinar un estado de prohibición para el equipo de usuario basándose en si se cumple o no el al menos un criterio de control de acceso recibido; y
 - 10 medios para determinar (630) si se permite que el equipo de usuario acceda a la red basándose en el estado de prohibición determinado.
2. El aparato de acuerdo con la reivindicación 1, en el que el al menos un criterio de control de acceso indica un tipo de notificación que puede acceder a la red.
3. El aparato de acuerdo con la reivindicación 2, en el que el tipo de notificación que puede acceder a la red comprende únicamente notificación de excepción.
- 20 4. El aparato de acuerdo con la reivindicación 2, en el que el tipo de notificación que puede acceder a la red comprende notificación normal.
5. El aparato de acuerdo con cualquiera de las reivindicaciones 1 a 4, en el que el al menos un criterio de control de acceso indica al menos un área de cobertura en la que se requiere que se ubique el equipo de usuario para acceder a la red.
- 25 6. El aparato de acuerdo con cualquiera de las reivindicaciones 1 a 5, en el que el al menos un criterio de control de acceso indica al menos una clase de cobertura a la que se permite o no acceder a la red.
- 30 7. El aparato de acuerdo con cualquiera de las reivindicaciones 1 a 6, en el que el al menos un criterio de control de acceso indica un tiempo que se requiere que haya transcurrido desde la última notificación por el equipo de usuario para acceder a la red.
8. El aparato de acuerdo con cualquiera de las reivindicaciones 1 a 7, comprendiendo adicionalmente:
 - 35 medios para aplicar comunicación de Internet de la Cosas de banda estrecha para el acceso a la red.
9. Un aparato (500) para su uso en un nodo de red de una red, comprendiendo el aparato:
 - 40 medios para determinar (510) al menos un criterio de control de acceso para un equipo de usuario, en el que el al menos un criterio de control de acceso indica un umbral de potencia recibida que tiene que cumplirse para acceder a la red; y
 - medios para transmitir (520), a través de señalización de difusión, el al menos un criterio de control de acceso al equipo de usuario, en el que el al menos un criterio de control de acceso habilita que el equipo de usuario determine un estado de prohibición para el equipo de usuario basándose en si se cumple o no el al menos un criterio de control de acceso recibido y determine si se permite que el equipo de usuario acceda a una red basándose en el estado de prohibición.
 - 45
10. El aparato de acuerdo con la reivindicación 9, en el que el al menos un criterio de control de acceso indica al menos uno de: un tipo de notificación que puede acceder a la red, al menos un área de cobertura en la que se requiere que el aparato se ubique para acceder a la red, al menos una clase de cobertura a la que se permite o no acceder a la red, un nivel de calidad de señal recibida que tiene que cumplirse para acceder a la red, un tiempo que se requiere que haya transcurrido desde la última notificación por el aparato para acceder a la red, y una clase de suscripción que se requiere desde una suscripción de usuario para acceder a la red.
- 50
- 55 11. Un método realizado por un equipo de usuario, comprendiendo el método:
 - recibir (310), a través de señalización de difusión, al menos un criterio de control de acceso desde un nodo de red de una red, en el que el al menos un criterio de control de acceso indica un umbral de potencia recibida que tiene que cumplirse para acceder a la red;
 - 60 determinar (320) una necesidad de acceder a la red; determinar un estado de prohibición para el equipo de usuario basándose en si se cumple o no el al menos un criterio de control de acceso recibido; y
 - determinar (330) si se permite que el equipo de usuario acceda a la red basándose en el estado de prohibición determinado.
- 65 12. Un método realizado por un nodo de red de una red, comprendiendo el método:

- determinar (210) al menos un criterio de control de acceso para un equipo de usuario, en el que el al menos un criterio de control de acceso indica un umbral de potencia recibida que tiene que cumplirse para acceder a la red;
y
5 transmitir (220), a través de señalización de difusión, el al menos un criterio de control de acceso al equipo de usuario, en el que el al menos un criterio de control de acceso habilita que el equipo de usuario determine un estado de prohibición para el equipo de usuario basándose en si se cumple o no el al menos un criterio de control de acceso recibido y determine si se permite que el equipo de usuario acceda a una red basándose en el estado de prohibición.
- 10 13. Un producto de programa informático incorporado en un medio legible por ordenador no transitorio, comprendiendo el producto de programa informático medios de código que cuando se ejecutan por un procesador de un equipo de usuario realizan todas las etapas de un método de acuerdo con la reivindicación 11.
- 15 14. Un producto de programa informático incorporado en un medio legible por ordenador no transitorio, comprendiendo el producto de programa informático medios de código que cuando se ejecutan por un procesador de un nodo de red de una red realizan todas las etapas de un método de acuerdo con la reivindicación 12.

```

AC-BarringPerPLMN-List-r13 ::= SEQUENCE (SIZE (1..maxPLMN-r11))
OF AC-BarringPerPLMN-r13

AC-BarringPerPLMN-r13 ::= SEQUENCE {
    plmn-IdentityIndex-r13
        INTEGER(1..maxPLMN-r11),
    ac-BarringPerCE
        SEQUENCE (SIZE (1..
maxCEs-r13)) OF AC-BarringInfo
    }
NeedOP
    OPTIONAL, --
}

AC-BarringInfo ::= SEQUENCE {
    ac-BarringForNormal-r13
        AC-BarringConfig OPTIONAL, -- Need OP
    ac-BarringForExceptional-r13
        AC-BarringConfig OPTIONAL, -- Need OP
    }

```

Fig. 1

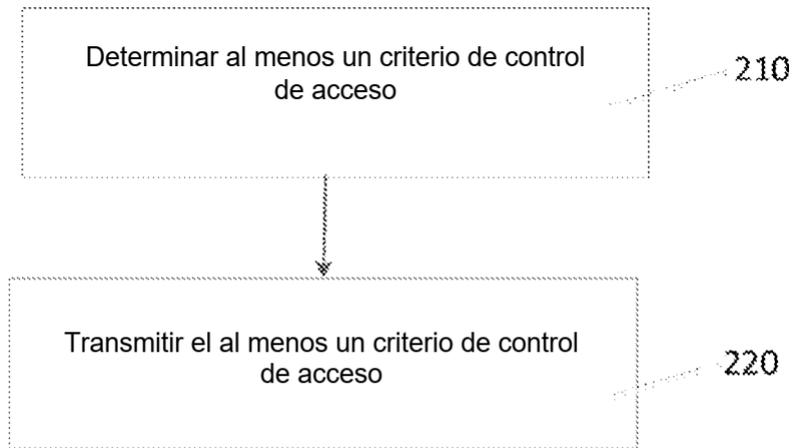


Fig. 2

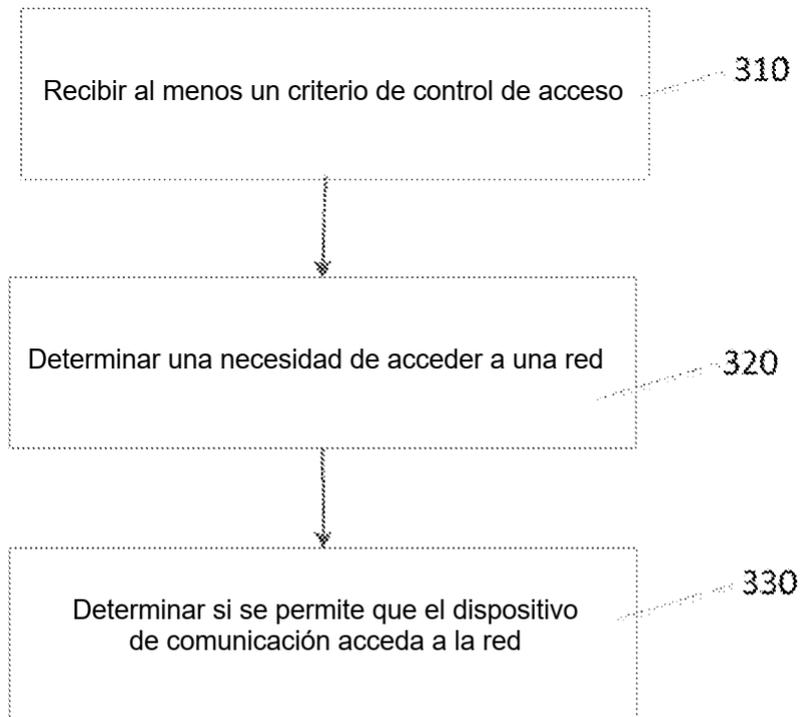


Fig. 3

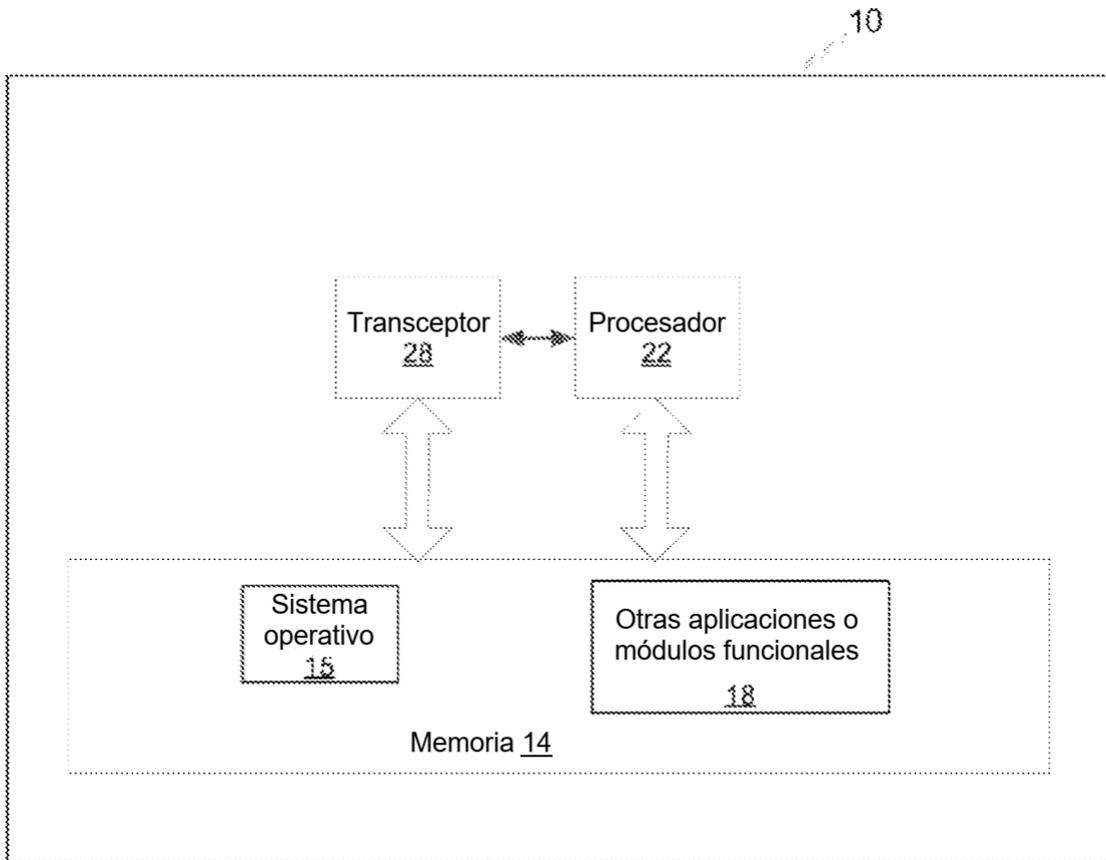


Fig. 4

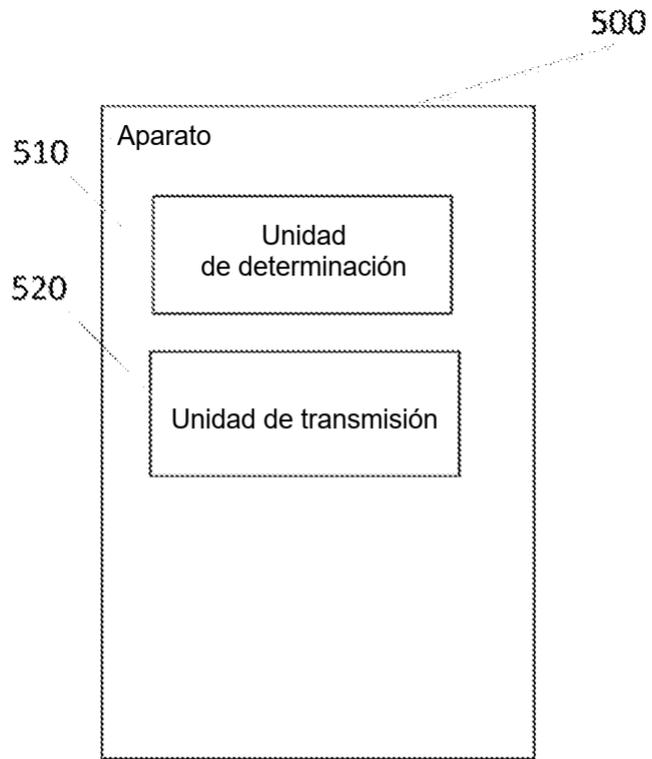


Fig. 5

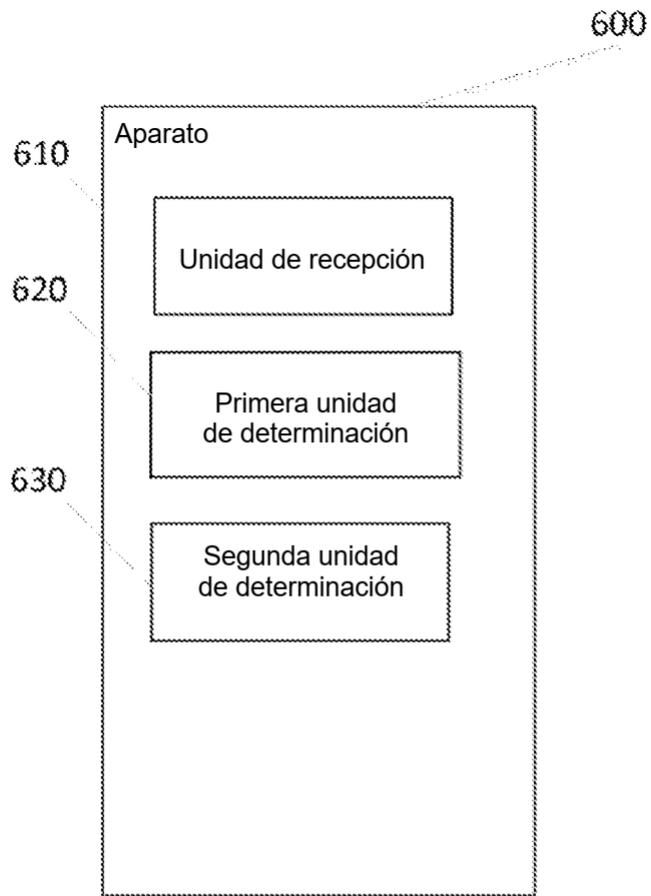


Fig. 6