

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 753 193**

51 Int. Cl.:

H04W 4/00 (2008.01)

H04L 29/06 (2006.01)

H04W 12/12 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **06.12.2016 PCT/FR2016/053216**

87 Fecha y número de publicación internacional: **15.06.2017 WO17098127**

96 Fecha de presentación y número de la solicitud europea: **06.12.2016 E 16819980 (0)**

97 Fecha y número de publicación de la concesión europea: **07.08.2019 EP 3387846**

54 Título: **Procedimiento de seguridad de un terminal móvil y terminal correspondiente**

30 Prioridad:

07.12.2015 FR 1561935

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

07.04.2020

73 Titular/es:

**ORANGE (100.0%)
78, rue Olivier de Serres
75015 Paris, FR**

72 Inventor/es:

ALLAL, IMED

74 Agente/Representante:

ISERN JARA, Jorge

ES 2 753 193 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

Procedimiento de seguridad de un terminal móvil y terminal correspondiente

5 Campo de la invención

La presente invención se refiere al campo de las telecomunicaciones. La invención se refiere a un procedimiento de seguridad de un terminal móvil adecuado para comunicarse con una red de telecomunicación.

10 La red de telecomunicación es una red estandarizada, por ejemplo, por 3GPP (LTE, LTE-Adv, etc.), GSM, etc.) que permite el establecimiento de comunicaciones entre terminales tanto móviles como fijos.

Desde el estándar GSM, los terminales móviles han evolucionado de manera muy significativa para convertirse en teléfonos inteligentes o *smartphones* del inglés. Están equipados con pantallas de muy buena calidad, procesadores rápidos y sistemas operativos que permiten usos variados con un consumo cada vez mayor de imágenes de vídeo.

15 Estos objetos portátiles se han convertido en objetos de gran valor y a menudo codiciados.

20 Técnica anterior

Para luchar contra el robo de teléfonos inteligentes, se conocen aplicaciones de software tales como los productos comerciales Lookout o Findmymobile que permiten geolocalizar el terminal perdido o robado. La aplicación indica en un mapa mostrado en una pantalla la ubicación que ha determinado como la ubicación donde debería ubicarse el terminal. Esta determinación se obtiene buscando en la red el identificador único, IMEI (Identidad Internacional de Equipo Móvil, *International Mobile Equipment Identity*, según la terminología inglesa) y su ubicación asociada. Este identificador es realmente necesario en los mecanismos de autenticación implementados en cada inicialización de una comunicación. La red realiza un seguimiento de este identificador cada vez que el terminal se comunica y tan pronto como su comunicación se cambia a una nueva estación base durante un desplazamiento del terminal móvil.

30 Sin embargo, estas aplicaciones constan de fallas ya que el identificador IMEI puede modificarse bajo la condición de manipulaciones particulares de la terminación o mediante el uso de aplicaciones disponibles en Internet. Al atribuir un nuevo identificador IMEI, el ladrón escapa de la geolocalización del terminal a través de aplicaciones tales como Lookout o Findmymobile. Los documentos US2011/087782, US2007/077912 y CN 100 362 884 se consideran como el estado de la técnica.

35 Descripción de la invención

La invención tiene como objeto un procedimiento de seguridad de un terminal móvil adecuado para comunicarse con una primera red de telecomunicación. El procedimiento comprende la transmisión periódica de un identificador único desde el terminal y hasta una red central de la primera red de telecomunicación a través de un canal de control basado en una segunda red de telecomunicación de tipo de bajo consumo energético. La invención tiene además como objeto un procedimiento de seguridad de un terminal móvil adecuado para comunicarse con una primera red de telecomunicación de tal manera que el procedimiento comprende la transmisión periódica de un identificador único desde una memoria dedicada no modificable del terminal y hasta a una red central de la primera red de telecomunicación a través de un canal de control basado en una segunda red de telecomunicación de tipo de bajo consumo energético.

La invención tiene además por objeto un terminal móvil que comprende una interfaz de radio a una primera red de telecomunicación. El terminal comprende, además:

- una interfaz inalámbrica adecuada para comunicarse con una segunda red de telecomunicación de tipo de bajo consumo energético,
- una memoria de un identificador único del teléfono,
- un componente adecuado para pilotar la interfaz inalámbrica para que el identificador memorizado en la memoria se emita de manera periódica a través de esta interfaz.

La invención tiene además por objeto un terminal móvil que comprende una interfaz de radio a una primera red de telecomunicación. El terminal comprende además formando un bloque inamovible:

- una interfaz inalámbrica adecuada para comunicarse con una segunda red de telecomunicación de tipo de bajo consumo energético,
- una memoria no modificable dedicada a la copia de seguridad de un identificador único del teléfono,
- un componente adecuado para pilotar la interfaz inalámbrica para que el identificador memorizado en la memoria se emita de manera periódica a través de esta interfaz,
- una alimentación autónoma del bloque.

La invención tiene, además, por objeto un sistema de telecomunicación que comprende una primera red de telecomunicación, una red central, un terminal móvil adecuado para comunicarse con la primera red. El sistema comprende, además, una segunda red de telecomunicación de tipo de bajo consumo energético para transmitir hasta la red central un identificador único emitido por el terminal. El sistema es tal que el terminal es según un objeto anterior.

5 Por lo tanto, la invención es una nueva solución para luchar contra el robo de terminales móviles. Su implementación necesita que se integre desde el diseño de los terminales para que el bloque sea consistente con el terminal y de ninguna manera se pueda extraer del terminal. Los elementos que forman este bloque pueden, por ejemplo, distribuirse en diferentes lugares del terminal y/o incrustarse en la carcasa del terminal. La alimentación de los elementos de bloque está totalmente separada de la alimentación del resto del terminal. Se puede basar en una microbatería que forma parte del bloque y cuya vida útil asegura una autonomía compatible con la vida útil promedio de un terminal. La separación física del resto de los componentes electrónicos del terminal garantiza la ausencia de fallas de seguridad de tipo software.

15 La memoria no modificable memoriza un identificador único del terminal, puede ser el IMEI atribuido originalmente al terminal. Este identificador puede ser fácilmente un identificador de un nuevo tipo con más caracteres. Es único en el sentido de que solo se atribuye una vez; permite distinguir cualquier terminal móvil de otro terminal móvil. El identificador se puede almacenar opcionalmente en forma cifrada. Esta memoria no es accesible desde los otros elementos del terminal fuera del bloque, tanto en lectura como en escritura. De este modo, incluso si se descarga una aplicación de software al terminal, nunca podrá modificar este identificador ya que la descarga se efectúa a través de la interfaz de radio a la primera red de telecomunicación y hacia una memoria modificable (RAM, por ejemplo) que no forma parte del bloque.

20 La interfaz inalámbrica es adecuada para comunicarse con una segunda red de telecomunicación de tipo de bajo consumo energético.

La segunda red de telecomunicación de tipo de bajo consumo energético se usa como canal de transporte del identificador. Esta transmisión está protegida por las características técnicas de esta red.

30 El procedimiento se aplica, por ejemplo, cuando la primera red de telecomunicación es dicha red móvil, tal como 3G, 4G, 5G, etc., y la segunda red es una red de sensores, tal como una red de tipo LoRa o Sigfox y, más generalmente, una red llamada IoT (Internet de las cosas, del inglés *Internet of Things*).

35 Según un modo de realización del terminal, el bloque constituye un objeto conectado a una red LoRa.

Según un modo de realización, la red central compara el identificador único con el identificador IMEI proporcionado por el terminal para autenticarse con la primera red, para autenticar este móvil de nuevo. Esto permite controlar de manera central la autenticidad de los terminales y establecer medidas de lucha centralizada.

40 Según un modo de realización, la red central compara el identificador único con un archivo de terminales móviles declarados como robados o perdidos. El procedimiento permite prohibir rápidamente el uso del terminal reconocido como robado o perdido por la red central.

Lista de las figuras

45 Otras características y ventajas de la invención surgirán más claramente tras la lectura de la siguiente descripción de modos de realización particulares de objetos de la invención, dados a título de simples ejemplos ilustrativos y no limitativos y de los dibujos adjuntos siguientes.

50 La figura 1 es un esquema de un sistema de telecomunicación según la invención.

La figura 2 es un esquema de un terminal según la invención.

Descripción de modos de realización de la invención

55 La arquitectura asociada con el procedimiento de seguridad se ilustra en la figura 1. El sistema SYS de telecomunicación ilustrado comprende:

- una red central (CN),
- 60 - una red de acceso de una primera red de telecomunicación,
- una estación base BS de la red de acceso,
- una segunda red de telecomunicación de tipo de bajo consumo energético,
- un terminal móvil UE equipado con un objeto conectado IoT_O.

65 La primera red de telecomunicación es, por ejemplo, una red móvil de tipo 2G, 3G, 4G, 5G, etc.

La segunda red es, por ejemplo, una red tal como se define por la alianza LoRa o propuesta por el operador Sigfox. Tal red a veces se designa mediante el acrónimo IoT (Internet de las cosas, del inglés *Internet of Things*). La red está constituida por nodos Nd_LPC (Nodo de bajo consumo energético), así como puertas de enlace hacia la red central. Los nodos Nd_LPC están equipados con una interfaz de radio con un alcance generalmente mayor que el alcance de las estaciones base de la red de acceso. Esta red puede cubrir así una gran zona geográfica con pocos dispositivos. Tal red está dedicada a las comunicaciones de baja velocidad.

Los enlaces entre los nodos de la segunda red y la red central son de tipo estandarizados conocidos y comúnmente llamados "*backhaul*" según la terminología anglosajona. Es lo mismo para los enlaces entre las estaciones base de la red de acceso y la red central.

El alcance de radio de los nodos Nd_LPC puede ser mayor que el de los de las estaciones base.

El terminal móvil UE ilustrado en la figura 2 comprende, de una manera conocida, una interfaz de radio I_NW_1 a la red de acceso de la primera red de telecomunicación, así como un microprocesador μ P y memoria modificable RAM. Por lo tanto, puede establecer comunicaciones a través de esta red de acceso. Este terminal además está equipado con un objeto conectado IoT_O. Este objeto forma un bloque inamovible con el cuerpo del terminal o con su placa base. Este objeto comprende:

- una interfaz inalámbrica I_NW_2 adecuada para comunicarse con la segunda red de telecomunicación de tipo de bajo consumo energético,
- una memoria no modificable ROM dedicada a la copia de seguridad de un identificador único del teléfono,
- un componente CT electrónico adecuado para pilotar la interfaz I_NW_2 para que el identificador memorizado en la memoria ROM se emita de manera periódica a través de esta interfaz,
- una alimentación BAT autónoma del objeto.

El identificador opcionalmente se puede encapsular en un paquete o mensaje antes de ser emitido. Los nodos Nd_LPC reciben el identificador, Id_UE y lo transmiten a la red central. Por otra parte, el terminal móvil se autentica con la primera red cada vez que establece una nueva comunicación. Esta autenticación se basa en el identificador IMEI asociado con el terminal y se desarrolla según mecanismos conocidos que generalmente se especifican en una memoria descriptiva técnica del estándar de telecomunicación. La red central puede recuperar de la primera red, ya sea el identificador IMEI, o bien una imagen de este identificador IMEI. De este modo, puede comparar estos datos con el identificador del terminal Id_UE y determinar si el identificador IMEI proporcionado es original, es decir, idéntico al identificador o si se ha modificado, es decir, diferente del identificador. Si el identificador IMEI proporcionado se ha modificado, existe una probabilidad muy significativa de que el terminal se use de manera fraudulenta, por ejemplo, después de un robo. La red central puede comparar el identificador del terminal Id_UE con un archivo de terminales declarados como robados o perdidos.

La red central puede recuperar una información de ubicación del terminal, a través de la primera red por mecanismos conocidos: GPS del teléfono, identificación de la estación base, etc. Según un modo de realización, la red central puede recuperar una información de ubicación del terminal, a través de la segunda red. Un primer mecanismo de ubicación de terminal puede basarse en una triangulación entre varios nodos Nd_LPC que reciben la emisión periódica del mismo terminal. Esto necesita un despliegue suficiente de nodos para implementar esta triangulación. Un segundo mecanismo de ubicación del terminal móvil puede basarse en la recuperación de la posición GPS de este terminal por el nodo a través de una interfaz del terminal, adaptada a la segunda red de telecomunicación. Esta interfaz es diferente de la que emite el identificador para conservar una separación total entre la memoria del identificador y el resto del terminal en caso de que el resto del terminal tenga acceso a la posición GPS.

De este modo, la red central puede ubicar en un mapa un terminal robado y transmitir tal información a un servicio de policía para encontrar esta terminal con su información.

Según un uso, la primera red de telecomunicación es una red denominada 5G que es objeto de trabajo de estandarización en el seno del 3GPP (LTE-A).

REIVINDICACIONES

- 5 1. Procedimiento (1) de seguridad de un terminal móvil (UE) adecuado para comunicarse con una primera red de telecomunicación (2G, 3G, 4G, 5G), caracterizado por que comprende la transmisión periódica de un identificador único del terminal desde el terminal y hasta una red central de la primera red de telecomunicación a través de un canal de control basado en una segunda red (LoRa, IoT) de telecomunicación de tipo de bajo consumo energético.
- 10 2. Procedimiento (1) según la reivindicación 1, que comprende, además, la comparación por la red central del identificador único con el identificador IMEI proporcionado por el terminal para autenticarse con la primera red, para autenticar este terminal de nuevo.
- 15 3. Procedimiento (I) según la reivindicación 1, en donde la red central compara el identificador único con un archivo de terminales móviles declarados como robados o perdidos.
- 20 4. Procedimiento según una de las reivindicaciones anteriores, según el cual, la transmisión del identificador único se hace desde una memoria dedicada no modificable del terminal.
- 25 5. Terminal móvil (UE) que comprende una interfaz de radio a una primera red de telecomunicación, caracterizado por que además comprende:
- una interfaz inalámbrica (I_NW_2) adecuada para comunicarse con una segunda red (LoRa, IoT) de telecomunicación de tipo de bajo consumo energético,
 - una memoria (ROM) para memorizar un identificador único del terminal,
 - un componente adecuado para pilotar la interfaz (I_NW_2) para que el identificador memorizado en la memoria (ROM) se emita de manera periódica a través de esta interfaz.
- 30 6. Terminal móvil (UE) según la reivindicación anterior que comprende además una alimentación (BAT) autónoma de un bloque formado por la interfaz inalámbrica adecuada para comunicarse con la segunda red, la memoria, el componente y la alimentación y tal que la memoria es no modificable y se dedica a la copia de seguridad del identificador.
- 35 7. Sistema (SYS) de telecomunicación que comprende una primera red de telecomunicación (3G, 4G, 5G), una red central (CN), un terminal móvil (UE) adecuado para comunicarse con la primera red, caracterizado por que el terminal comprende, además:
- una interfaz inalámbrica adecuada para comunicarse con una segunda red (LoRa, IoT) de telecomunicación de tipo de bajo consumo energético,
 - una memoria para memorizar un identificador único del terminal,
 - un componente adecuado para pilotar la interfaz (I_NW_2) para que el identificador memorizado en la memoria (ROM) se emita de manera periódica a través de esta interfaz y caracterizado por que el sistema comprende, además:
 - la segunda red de telecomunicación de tipo de bajo consumo energético para transmitir hasta la red central el identificador único emitido por el terminal.
- 40
- 45 8. Sistema (SYS) de telecomunicación según la reivindicación anterior, tal que el terminal comprende, además, una alimentación (BAT) autónoma de un bloque formado por la interfaz inalámbrica adecuada para comunicarse con la segunda red, la memoria, el componente y la alimentación y tal que la memoria es no modificable y se dedica a la copia de seguridad del identificador.

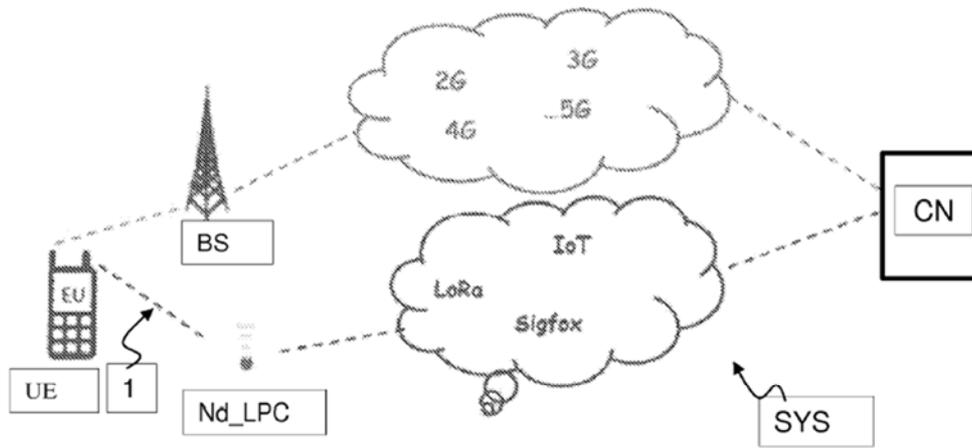


Fig.1

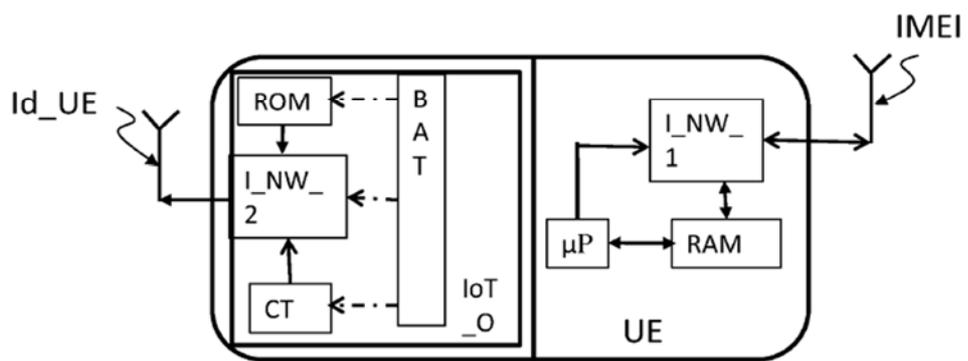


Fig.2