(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 957 492**

(51) Int. Cl.:

G06F 21/88	(2013.01)	***H04W 4/06***	(2009.01)
G06F 21/44	(2013.01)	***H04W 12/126***	(2011.01)
G01S 5/00	(2006.01)	***H04W 4/18***	(2009.01)
H04W 4/80	(2008.01)	***H04W 12/50***	(2011.01)
H04W 12/00	(2011.01)	***H04W 12/79***	(2011.01)
H04W 12/12	(2011.01)	***H04W 12/63***	(2011.01)
H04W 4/02	(2008.01)		
H04W 4/029	(2008.01)		
H04L 9/32	(2006.01)		
H04L 9/40	(2012.01)		

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **01.04.2020 E 20315093 (3)**

(97) Fecha y número de publicación de la concesión europea: **16.08.2023 EP 3889818**

(54) Título: **Método para localizar una baliza**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.01.2024

(73) Titular/es:

THALES DIS FRANCE SAS (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

DELSUC, JULIEN;
COURTIADE, FABIEN y
SIEPRAWSKI, NICOLAS

(74) Agente/Representante:

DEL VALLE VALIENTE, Sonia

DESCRIPCIÓN

Método para localizar una baliza

La presente invención se refiere a las telecomunicaciones y, en particular, a un método que permite a un usuario de un terminal de telecomunicación, como, por ejemplo, un teléfono móvil, un PDA, un teléfono inteligente, un reloj inteligente o una tableta, localizar una baliza activa o cualquier dispositivo RFID activo. En la actualidad, en el campo de la confidencialidad y la seguridad, muchos artículos confidenciales, incluidos CD, unidades flash USB, llaves de puerta, libros de notas, documentos, etc. confidenciales, carecen de un control antipérdida eficaz, y existe un riesgo potencial de pérdida. Por lo tanto, es especialmente importante evitar la pérdida de artículos confidenciales o personales.

En el actual campo técnico relacionado, el sistema antipérdida basado en tecnología RFID activa no está muy extendido, sino que adopta principalmente el sistema de tecnología Bluetooth o la tecnología RFID pasiva. Sin embargo, la tecnología Bluetooth tiene la desventaja de ser obstruida fácilmente, y la tecnología RFID pasiva causa un problema de batería en el extremo de detección.

Hoy en día podemos encontrar sistemas que permiten usar una flota de dispositivos para encontrar de manera remota un objeto gracias a una baliza emisora de radio (BLE) sujeta al dispositivo. Esos sistemas se basan en la colaboración de varios teléfonos a través de un servidor web. Esto se denomina localización colaborativa de objetos. Sin embargo, con esta solución existen varias cuestiones de privacidad:

1. El servidor está al tanto de qué objeto está perdido a partir de la posición de todos los objetos que gestiona;

2. La aplicación que se ejecuta en los teléfonos puede verse en peligro, y sus datos también pueden ser recogidos por hackers;

3. Las balizas normalmente difunden un identificador estático que permite rastrear fácilmente a su propietario.

Por lo tanto, las soluciones conocidas no son conformes al Reglamento General de Protección de Datos (RGPD).

Tales soluciones se describen, por ejemplo, en los documentos US 2020/0021945, US 2016/0105766 y US 2016/0373894 de Tile Inc.

El propósito de la presente invención es proponer un método que permita a un usuario de un terminal de telecomunicación localizar una baliza a la que está sujeto un objeto utilizando esta localización colaborativa de objetos sin que surjan cuestiones de privacidad.

Por lo tanto, la presente invención propone un método para localizar una baliza, habiéndose emparejado la baliza durante una etapa de emparejamiento para que se comparta una clave secreta entre la baliza y un primer terminal de telecomunicación, comprendiendo el método:

i- Enviar del primer terminal de telecomunicación a un servidor remoto:

- un alto cifrado mediante la clave secreta;

- una indicación de ubicación aproximada de la baliza que define una zona de búsqueda,

ii- Enviar el alto cifrado del servidor remoto a al menos un segundo terminal de telecomunicación presente en la zona de búsqueda;

iii- Una vez que haya recibido un mensaje dinámico procedente de la baliza, enviar el alto cifrado del al menos segundo terminal de telecomunicación a la baliza;

iv- Descifrar el alto cifrado en la baliza y enviar el alto a al menos el segundo terminal de telecomunicación;

v- Enviar del al menos segundo terminal de telecomunicación al primer terminal de telecomunicación, a través del servidor remoto, el alto y la ubicación del al menos segundo terminal de telecomunicación;

vi- Verificar el alto en el primer terminal de telecomunicación.

Preferiblemente, las etapas -iii- y -iv- se ejecutan en la UWB para calcular una distancia demostrada entre el segundo terminal y la baliza gracias a la medición del tiempo de vuelo. Ventajosamente, para cifrar el alto mediante la clave secreta se utiliza un algoritmo AES.

Preferiblemente, si en la etapa -vi- se indica que el alto es el que se envió en la etapa -i-:

- el primer terminal de telecomunicación envía a la baliza una orden de que emita un sonido o luz, o

- el primer terminal de telecomunicación envía al segundo terminal de telecomunicación un mensaje que pide al segundo terminal de telecomunicación que envíe a la baliza una orden de que emita un sonido o luz.

Ventajosamente, el alto va acompañado de una suma de verificación, como un MAC, por ejemplo. La presente invención se entenderá mejor leyendo la siguiente descripción de una realización preferida de la invención en vista de las figuras, que representan:

- La figura 1, el emparejamiento entre un terminal de telecomunicación y una baliza;

- la figura 2, una realización preferida del método de la invención.

La figura 1 representa el emparejamiento entre un terminal de telecomunicación y una baliza.

Un terminal de telecomunicación está constituido aquí por un teléfono móvil 10 denominado teléfono 1. Se denominará en lo sucesivo primer terminal de telecomunicación. También podría ser un PDA, un teléfono inteligente o un ordenador personal, por ejemplo.

El terminal 10 de telecomunicación es capaz de comunicarse inalámbricamente o no con una baliza 11 que tiene preferiblemente una interfaz BLE (Bluetooth Low Energy) o una interfaz UWB (banda ultraancha).

Después de haberse establecido una autenticación mutua (etapa 15) entre el terminal 10 de telecomunicación y la baliza 11 utilizando pares de claves y certificados, la baliza 11 es capaz de generar una clave secreta SK (etapa 16) y transmitírsela al terminal 10 de telecomunicación (etapa 17). De manera alternativa, el terminal 10 de telecomunicación también puede generar esta clave secreta SK y transmitírsela a la baliza 11, siendo el aspecto importante que tanto el terminal 10 de telecomunicación como la baliza 11 comparten la clave secreta SK al final del proceso de emparejamiento. Tal y como se verá más adelante, la clave SK se utilizará como clave de AES (Advanced Encryption Standard).

Por lo tanto, en esta primera etapa de emparejamiento se realiza un emparejamiento entre el terminal 10 de telecomunicación y la baliza 11, conteniendo ambos unos pares de claves asimétricas (PKI, que utilizan un certificado y claves privadas). Gracias a esas claves, se establece un canal seguro, y se comparte una clave secreta SK de emparejamiento.

La figura 2 representa una realización preferida del método de la invención.

En esta figura se han representado el primer terminal 10 de telecomunicación y la baliza 11 de la figura 1. Los demás elementos técnicos que intervienen en el método de la invención son un TSM 12 (Trusted Service Manager) y al menos un segundo terminal 13 de telecomunicación. El TSM es propiedad del Mobile Network Operator (Operador de red móvil - MNO) que gestiona las comunicaciones de los terminales 10 y 13 de telecomunicación (y de una flota de otros terminales de telecomunicación).

Aquí se supone que el usuario del primer terminal 10 de telecomunicación ha perdido un objeto (por ejemplo, sus llaves de casa) que está sujeto a su baliza 11, que se ha emparejado previamente (con respecto a la fig. 1).

En este caso, en una etapa 20, y a petición del usuario del primer terminal 10 de telecomunicación, una aplicación ubicada en este primer terminal 10 de telecomunicación o en su elemento de seguridad (UICC, eUICC o iUICC) genera un mensaje Msj, que es, preferiblemente, un AES de un alto y una suma de verificación opcional, por ejemplo, un MAC (Message Authentication Code). La suma de verificación se puede usar para verificar la integridad del alto, ya que esta suma de verificación se calcula al darse el alto. La clave para calcular el AES es la clave secreta SK.

El algoritmo AES se utiliza preferiblemente para cifrar el alto (y, opcionalmente, la suma de verificación) mediante la clave secreta SK. También se puede usar DES o 3DES. También se puede usar un esquema criptográfico asimétrico.

Este mensaje, que es un criptograma, se envía en una etapa 21 al TSM 12 (un servidor remoto) con un conjunto de ubicaciones que definen una indicación de ubicación aproximada de la baliza que define una zona de búsqueda. Esta ubicación aproximada es, por ejemplo, el último sitio en el que el usuario cree que perdió sus llaves (la última ubicación en la que recuerda que es probable que haya perdido las llaves, por ejemplo).

Una ubicación así se puede obtener a través de diversas aplicaciones, por ejemplo, Google™, si el usuario ha aceptado que Google™ registre sus posiciones pasadas y actuales (sitios en los que ha estado físicamente). Una interfaz API ubicada en el primer terminal 10 de telecomunicación también puede indicar las zonas en las que el usuario ha estado recientemente.

El TSM 12 envía entonces en una etapa 22 el mensaje Msj a todos los terminales que están en la zona de la ubicación definida.

La baliza 11 envía periódicamente, por ejemplo, cada minuto, un mensaje de anuncio dinámico "estoy aquí" con una dirección MAC (Media Address Control) temporal, a todos los terminales de telecomunicación circundantes en sus alrededores. Esta dirección MAC es un identificador temporal a efectos de privacidad (la baliza no puede ser rastreada) y es cambiada regularmente por la baliza 11.

Si uno de los segundos terminales de telecomunicación está en las proximidades de esta baliza 11, recibirá este mensaje dinámico, y podrá enviar el mensaje Msj a la baliza 11 (etapa 25) después de una autenticación mutua opcional (etapa 24). Esta autenticación mutua (usando pares de claves y un certificado) garantiza que la baliza es realmente una baliza que se ha emparejado según la figura 1 con un terminal que pertenece a la flota de terminales del MNO.

La baliza 11 descifra entonces el mensaje Msj recibido gracias a su clave SK registrada para recuperar el alto (etapa 26) y, opcionalmente, verifica la suma de verificación, en caso de que esté presente. La verificación opcional de la suma de verificación se realiza para verificar que el alto no se ha modificado durante las etapas 21 a 25.

La baliza puede, posiblemente después de que tenga éxito la verificación de suma de verificación opcional, enviar (etapa 27) el alto (y, opcionalmente, la MAC) al(a los) segundo(s) terminal(es) 13 de telecomunicación.

Este(estos) reenviará(n) entonces (en una etapa 28) el alto (y, opcionalmente, la suma de verificación [MAC]) al TSM 12 junto con la ubicación de su teléfono y, opcionalmente, su distancia a la baliza 11. Esta distancia puede obtenerse con precisión si la baliza y el segundo terminal 13 de telecomunicación tienen una conexión UWB. La conexión UWB saca partido al Time of Flight (Tiempo de vuelo - ToF), que es un método para medir la distancia entre dos transceptores de radio al multiplicar el ToF de la señal por la velocidad de luz.

Por lo tanto, las etapas 23, 25 y 27 se ejecutan preferiblemente en UWB para además permitir realizar un cálculo de una distancia demostrada entre el segundo terminal 13 y la baliza 11 gracias a la medición del ToF.

En una etapa 29, el TSM 12 reenvía el mensaje recibido al primer terminal 10 de telecomunicación. Este puede entonces verificar (etapa 30) el alto (y/o la MAC).

Si el alto recibido y/o la MAC recibida corresponde(n) a los que se enviaron en la etapa 21, el primer terminal 10 de telecomunicación ha autentificado la baliza 11 y conoce la ubicación de la misma. Opcionalmente, el usuario puede entonces pedir al primer terminal 10 de telecomunicación que envíe a la baliza 11 una orden (etapa 31) de que emita un sonido o luz. Por lo tanto, la baliza debe tener funcionalidades de telecomunicaciones, al menos para recibir una orden así. También es posible enviar del primer terminal 10 de telecomunicación al segundo terminal 13 de telecomunicación un mensaje (etapa 32) que pida al segundo terminal 13 de telecomunicación que envíe a la baliza 11 una orden (etapa 33) de que emita un sonido (pitido) o luz. De esta manera, el usuario del primer terminal 10 de telecomunicación puede encontrar fácilmente y recuperar la baliza.

La invención ayuda a determinar la ubicación de un objeto usando una red global de dispositivos de un OEM (un fabricante de teléfonos inteligentes, por ejemplo) sin revelar la identidad del dispositivo que recuperó el objeto buscado.

Las ventajas de la invención son las siguientes:

- La baliza 11 no tiene ningún identificador estático, por lo que no puede ser rastreada ni por el teléfono intermedio 13 ni por el servidor 12.
- Se introduce una autenticación fuerte, por lo que solo podrán interactuar teléfonos y balizas auténticos.
- Ninguna persona desconocida puede enviar una orden a la baliza (ya que se utiliza una clave secreta SK compartida).
- La ubicación precisa posibilitada por UWB solo puede usarse con una autenticación previa. Por lo tanto, aunque alguien detectase la baliza por análisis de protocolos, no podría acceder a su ubicación precisa.
- Se basa en servidores TSM existentes.
- La granularidad de la flota puede definirse a nivel de organización corporativa, de grupo familiar, de organización social, de asistentes a una exposición, etc.

REIVINDICACIONES

1. Un método para localizar una baliza (11), habiéndose emparejado dicha baliza (11) durante una etapa de emparejamiento para que se comparta una clave secreta entre dicha baliza (11) y un primer terminal (10) de telecomunicación, comprendiendo dicho método:

i-Enviar de dicho primer terminal (10) de telecomunicación a un servidor remoto (12):

-un alto cifrado mediante dicha clave secreta;
-una indicación de ubicación aproximada de dicha baliza (11) que define una zona de búsqueda,

ii-Enviar dicho alto cifrado de dicho servidor remoto (12) a al menos un segundo terminal (13) de telecomunicación presente en dicha zona de búsqueda;
iii-Una vez que haya recibido un mensaje dinámico procedente de dicha baliza (11), enviar dicho alto cifrado de dicho al menos segundo terminal (13) de telecomunicación a dicha baliza (11);
iv-Descifrar dicho alto cifrado en dicha baliza (11) y enviar dicho alto a dicho al menos segundo terminal (13) de telecomunicación;
v-Enviar de dicho al menos segundo terminal (13) de telecomunicación a dicho primer terminal (10) de telecomunicación, a través de dicho servidor remoto (12), dicho alto y la ubicación de dicho al menos segundo terminal (13) de telecomunicación;
vi-Verificar dicho alto en dicho primer terminal (10) de telecomunicación;
vii-Determinar en dicho primer terminal (10) de telecomunicación la ubicación de dicha baliza (11) basándose en la verificación de dicho alto y la ubicación de dicho segundo terminal (13) de telecomunicación.

2. Un método según la reivindicación 1, en donde las etapas -iii- y -iv- se ejecutan en UWB para calcular una distancia demostrada entre dicho segundo terminal y dicha baliza (11) gracias a la medición del tiempo de vuelo.

3. Un método según cualquiera de las reivindicaciones 1 y 2, en donde se utiliza un algoritmo AES para cifrar dicho alto mediante dicha clave secreta.

4. Un método según cualquiera de las reivindicaciones 1 a 3, en donde si en dicha etapa -vi- se indica que dicho alto es el que se envió en la etapa -i-:

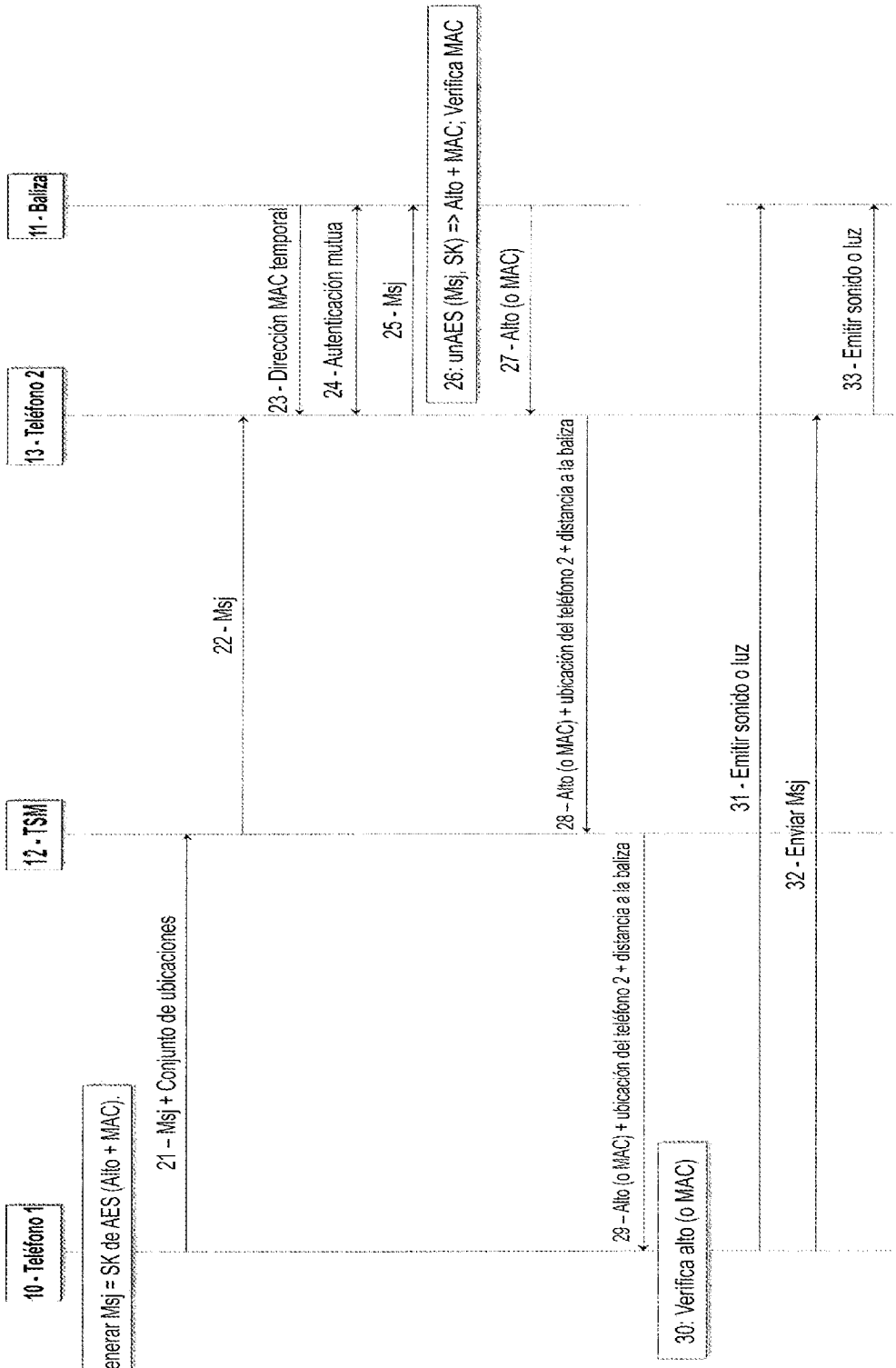
-dicho primer terminal (10) de telecomunicación envía a dicha baliza (11) una orden de que emita un sonido o luz, o
-dicho primer terminal (10) de telecomunicación envía a dicho segundo terminal (13) de telecomunicación un mensaje que pide a dicho segundo terminal (13) de telecomunicación que envíe a dicha baliza (11) una orden de que emita un sonido o luz.

5. Un método según cualquiera de las reivindicaciones 1 a 4, en donde dicho alto va acompañado de una suma de verificación.

Figura 1


10 - Teléfono 1
11 - Baliza
16 - Generar SK
15 - Autenticación mutua (mediante el uso de pares de claves y certificados)
17 - SK

Figura 2


10 - Teléfono 1
12 - TSM
13 - Teléfono 2
11 - Baliza
20: Generar Msj = SK de AES (Alto + MAC).
21 – Msj + Conjunto de ubicaciones
22 - Msj
23 - Dirección MAC temporal
24 - Autenticación mutua
25 - Msj
26: unAES (Msj, SK) => Alto + MAC; Verifica MAC
27 - Alto (o MAC)
28 – Alto (o MAC) + ubicación del teléfono 2 + distancia a la baliza
29 – Alto (o MAC) + ubicación del teléfono 2 + distancia a la baliza
30: Verifica alto (o MAC)
31 - Emitir sonido o luz
32 - Enviar Msj
33 - Emitir sonido o luz