(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 749 180**

(51) Int. CI.:

G01S 19/21 (2010.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.04.2018 PCT/IT2018/050068**

(87) Fecha y número de publicación internacional: **25.10.2018 WO18193487**

(96) Fecha de presentación y número de la solicitud europea: **19.04.2018 E 18724344 (9)**

(97) Fecha y número de publicación de la concesión europea: **10.07.2019 EP 3408687**

(54) Título: **Método y sistema de certificación de georreferenciación para dispositivos móviles**

(30) Prioridad:

20.04.2017 IT 201700043174

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.03.2020

(73) Titular/es:

ETUITUS S.R.L. (100.0%)
Università di Salerno, Via Giovanni Paolo II, 132
84084 Fisciano (SA), IT

(72) Inventor/es:

CATTANEO, GUISEPPE;
FARUOLO, POMPEO y
MANNETTA, MARCO

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Método y sistema de certificación de georreferenciación para dispositivos móviles

Esta invención se refiere a un método y sistema de georreferenciación para dispositivos móviles.

Más específicamente, la invención se refiere a un método de certificación de georreferenciación accionado por medio de una unidad central con uno o más de sensores o receptores de GNSS (Sistema de Satélite de Navegación Global) y uno o más dispositivos móviles que requieren la georreferenciación. El dispositivo móvil recopilará la información monitorizada por el sensor de GNSS instalado en el dispositivo móvil y la enviará a la unidad central, que comparará la información recibida con la que ha obtenido a través de sus sensores de GNSS relativos. El resultado de la comparación autorizará, o no, a la unidad central a emitir la certificación de georreferenciación.

Principios introductorios

Todos los sistemas de navegación por satélite están basados en el mismo enfoque: una red de satélites que orbitan alrededor de la Tierra que envían señales de radio para calcular la posición, velocidad y tiempo (PVT). Los dispositivos de recepción, conociendo las posiciones de cada satélite (efemérides), calculan la distancia de los satélites capturados y pueden calcular la posición relativa en la Tierra usando una técnica de posicionamiento conocida como "trilateración".

Más específicamente, el sistema de GPS NAVSTAR transmite simultáneamente diferentes códigos variables y mensajes de navegación en ciertas frecuencias de radio. Cada satélite envía dos tipos de códigos variables, uno denominado código C/A (Código de Adquisición Basta) y el otro denominado código P(Y) (código Y de precisión). Ambos de estos códigos son secuencias binarias pseudoaleatorias (PRN) específicas para cada satélite. De hecho, cada satélite de la constelación tiene un Identificador de Vehículo Espacial (SV ID) y un Número de Ruido Pseudoaleatorio (número PRN) que identifica de manera inequívoca los códigos generados por el satélite individual.

El código C/A es para uso civil y se transmite en texto sin cifrar en la frecuencia de radio L1 a intervalos repetidos. Incluso aunque sea un código PRN, el código C/A puede predecirse y puede reproducirse en el dispositivo móvil para sincronizarse con el generado por el satélite. El código P(Y) se encripta modulando con una secuencia encriptada denominada código W, actualizada de manera recular por el Departamento de Defensa de Estados Unidos, a partir de la cual se obtiene un código Y encriptado. El código P(Y) se transmite en las frecuencias de radio L1 y L2 y puede usarse para navegación exclusivamente para fines militares. Estos códigos no pueden usarse para navegación y posicionamiento en los dispositivos móviles comunes para uso civil. Estos no pueden desencriptarse y predecirse y aparecen como un ruido de fondo, pero dada su estructura y las frecuencias conocidas con las que se aplica el código, usando técnicas adecuadas, es posible detectarlos, trazarlos y usarlos conjuntamente con el código C/A para mejorar la posición de posicionamiento del último.

Un mensaje de navegación de 50 bit/s denominado LNAV (Navegación heredada) se añade en el GPS heredado anteriormente con las señales variables C/A y P(Y) L1. El mensaje de navegación comprende 3 tipos de información: fecha, hora y estado del satélite específico; posición en órbita del satélite único de la constelación (efemérides - válido durante 4 horas); estado de la constelación entera, posición aproximada de todos los satélites y modelos ionosféricos para la corrección de los errores de propagación de la señal de radio (almanaque - válido durante 180 días).

Para establecer de manera precisa la posición sobre la Tierra es necesario calcular la distancia de al menos 4 satélites de dicho receptor de GNSS. Cuanto mayor sea el número de satélites visibles en un cierto instante, mayor será la precisión del cálculo de la posición del dispositivo. Cada mensaje LNAV enviado contiene la indicación de tiempo de cuándo se generó. La indicación de tiempo se produce a través del reloj atómico a bordo del satélite. La hora del satélite se sincroniza regularmente a partir de la Tierra para corregir los errores inducidos por velocidad orbital y gravedad terrestre. El tiempo de propagación de señal se calcula comparando la indicación de tiempo generada en el satélite con la indicación de tiempo de llegada generada en el dispositivo móvil, conociendo la velocidad de propagación y los modelos de corrección ionosféricos globales relativos contenidos en el mensaje de LNAV.

Antecedentes de la técnica

Como se ha explicado anteriormente, la mayoría de los dispositivos móviles modernos tienen un sensor de GNSS de múltiples constelaciones y múltiples bandas para localizar de manera precisa la posición relativa. Las constelaciones de satélite globales principales son NAVSTAR GPS de los Estados Unidos y GLONASS de Rusia, pero se están generalizando en el mercado sensores que pueden obtener y procesar señales también de otros sistemas de satélites globales, tales como el futuro BEIDOU-2 de China y el futuro GALILEO de la Unión Europea.

Actualmente, la detección de la información no es muy fiable desde el punto de vista de seguridad, ya que puede manipularse fácilmente en los dispositivos móviles comunes. Existe equipo que puede reproducir o retransmitir señales de GNSS, que pueden referenciarse a una cierta posición, engañando la detección llevada a cabo por el sensor del dispositivo móvil (suplantación de identidad).

Se han propuesto diversos métodos en la bibliografía científica para verificar si una señal de GNSS detectada por un sensor es original o se ha modificado. Estos métodos en su mayoría ofrecen mecanismos para identificar posibles inconsistencias en la señal detectada, que están únicamente presentes en una señal reproducida artificialmente, pero no pueden siempre accionarse en dispositivos o son demasiado complejos para implementarse en dispositivos móviles comunes, que están caracterizados por potencia de procesamiento limitada y baja disponibilidad en términos de memoria y autonomía. Puede hallarse otra técnica anterior en SCHIELIN EMMANUEL ET AL: "On the Foundation of GNSS Authentication Mechanisms",GNSS 2012 - PROCEEDINGS OF THE 25TH INTERNATIONAL TECHNICAL MEETING OF THE SATELLITE DIVISION OF THE INSTITUTE OF NAVIGATION (ION GNSS 2012), THE INSTITUTE OF NAVIGATION, 8551 RIXLEW LANE SUITE 360 MANASSAS, VA 20109, Estados Unidos, 21 de septiembre de 2012 (21-09-2012), páginas 1194-1207

Objetivo de la invención

El objetivo de la invención es proporcionar un sistema y un método que resuelve el problema y supera las limitaciones de la técnica anterior, proporcionando una certificación de la georreferenciación llevada a cabo por un dispositivo móvil equipado con un sensor o receptor GNSS (Sistema de Satélite de Navegación Global).

El objeto de esta invención es un método y un sistema de acuerdo con las reivindicaciones adjuntas.

Descripción detallada de las realizaciones de la invención

Lista de dibujos

La invención se describe ahora, a modo de ejemplo y sin limitar el alcance de la invención, con referencia a los dibujos adjuntos, en los que:

- La Figura 1 muestra señales de GNSS, el servidor de certificación y el dispositivo móvil con la aplicación de cliente;
- La Figura 2 muestra un ESCENARIO 1: suplantando la identidad de la señal de GNSS con un único simulador de antena en un entorno aislado de señales enviadas de los satélites;
- La Figura 3 muestra un ESCENARIO 2: suplantando la identidad de la señal de GNSS con adquisición de las señales originales usando una antena y retransmisión de señales procesadas en un entorno aislado de señales enviadas de los satélites; y
- La Figura 4 muestra un ESCENARIO 3: suplantando la identidad de la señal de GNSS con un único simulador de antena de exteriores configurado para generar una señal que tiene una potencia mayor que la potencia de la señal de GNSS.

Debería observarse que los elementos de diferentes realizaciones pueden combinarse juntos para proporcionar realizaciones adicionales sin limitaciones de acuerdo con el concepto técnico de la invención, como pretende el técnico medio del sector, sin problemas.

Esta descripción también se refiere a la técnica anterior para su implementación, con respecto a las características detalladas no descritas, tales como por ejemplo, elementos de menor importancia generalmente usados en la técnica anterior en soluciones del mismo tipo.

Cuando se introduce un elemento siempre se pretende que pueda haber "al menos uno" o "uno o más".

Cuando se proporciona o presenta una lista de elementos en esta descripción significa que la invención "comprende" o como alternativa "consiste en" estos elementos.

Introducción

El objetivo de la invención es certificar la georreferenciación llevada a cabo por un dispositivo móvil equipado con un sensor o receptor de GNSS (Sistema de Satélite de Navegación Global).

Hablando en general, un sensor o receptor de GNSS es un dispositivo electrónico que puede obtener señales de radio de diferentes constelaciones de navegación de satélites globales.

La invención define un sistema en el que un usuario puede certificar la posición relativa de un servidor remoto, es decir un servidor de certificación, enviando los datos necesarios a dicho servidor para verificar dicha posición.

El servidor de certificación puede analizar tanto los datos de alto nivel, es decir, la estructura de los paquetes como los mensajes de navegación de la constelación de satélite de GNSS específico modulada en la señal de radio, y los datos sin procesar de bajo nivel con relación a las características de las señales de radio recibidas.

Para hacer a la verificación robusta, el servidor de certificación solicita el envío de diversos tipos de información, tal como, por ejemplo, los datos presentes en los mensajes de navegación de satélite de alto nivel y los datos en bruto

no procesados de bajo nivel con relación a las señales de radio obtenidas en el lado del cliente por los diversos sistemas de localización de satélite global.

El servidor de certificación comparará los datos con los de su posesión, (detectados usando los sensores de GNSS o receptores, procesados y registrados en el lado del servidor intervalos regulares de tiempo dentro de una ventana de tiempo específica) y puede identificar cualesquiera discrepancias y anomalías resultantes de intentos fraudulentos.

En el caso de datos coherentes producirá un certificado para certificar la posición del usuario.

Descripción del método

El método está basado en el modelo de interacción cliente-servidor: el servidor de certificación es la Autoridad encargada de Georreferenciación LA y un cliente está en ejecución en la APP de dispositivo móvil (APP indica tanto la aplicación de cliente como del dispositivo móvil). El cliente y el servidor de certificación están conectados a través de una red de comunicación de datos (mostrada en los dibujos con una línea de puntos discontinua) de acuerdo con la técnica anterior disponible.

El servidor de certificación LA proporcionará el servicio de georreferenciación seguro (certificación de la posición) a los usuarios cuando se solicita usar la aplicación de cliente APP. Un usuario que solicita la localización segura debe ejecutar la aplicación de cliente APP en el dispositivo móvil relativo; la aplicación de cliente APP recopilará la información monitorizada por el sensor de GNSS instalado en el dispositivo móvil y enviará al servidor de certificación LA.

El servidor de certificación LA opera en un área de competencia específica y, a través de diversos sensores de GNSS (denominados en este punto LA1, LA2 ... LAi ... LAx), localizados en dicho área de competencia y conectados junto con redes de cables y/o por medio inalámbrico, continuarán obteniendo las señales de GNSS.

La estructura de los paquetes, los mensajes de navegación de alto nivel (bits de datos), los datos procesados por el sensor de GNSS y las características de bajo nivel de las señales de radio se almacenarán y usarán en cada solicitud de georreferenciación segura recibida de un dispositivo móvil para verificar la autenticidad y certificar la posición.

Prerrequisitos

La aplicación de cliente APP debe poder acceder, además de a los mensajes de navegación de alto nivel (bits de datos) añadidos a los códigos PRN, a los datos sin procesar de bajo nivel con relación a las señales de radio detectadas por el receptor de GNSS a través de servicios necesarios proporcionados en los lados de hardware y/o software. Los datos de bajo nivel son código de pseudointervalo civil C/A L1, el código de señal militar encriptada P(Y), el efecto Doppler, onda portadora, fase, la relación de señal/ruido y otras características.

El usuario que usa la aplicación de cliente APP debe estar registrado con el servicio de georreferenciación seguro, que identifica tanto la solicitud de aplicación de cliente APP como el dispositivo móvil en el que se ejecuta (la denominada fase de inscripción).

Método detallado

El usuario inicia la aplicación de cliente APP para solicitar una georreferenciación segura. La aplicación de cliente APP solicita al servidor de certificación iniciar una sesión de georreferenciación. La comunicación cliente-servidor se realizará de una manera segura usando protocolos de comunicación encriptados.

El primer deber será sincronizar el reloj del dispositivo móvil con el del servidor de certificación LA, ejecutando un protocolo de sincronización de tiempo.

Posteriormente, la aplicación de cliente APP envía la siguiente información encriptada, durante un cierto periodo de tiempo y para cada señal de radio de satélite GPS L1 recibida en ese preciso instante:

1. los datos sin procesar de bajo nivel: valores del código C/A de código de pseudointervalo civil y fase relativa; valores relativos a la onda portadora de la señal, la fase, el desplazamiento Doppler, la potencia y la relación de señal/ruido (C/N_0 - densidad de portadora a ruido y/o SNR - relación de señal a ruido); valores que describen el patrón del código de señal militar encriptada P(Y);
2. los mensajes de navegación de satélite de alto nivel (bits de datos obtenidos y procesados en el lado de cliente) de todos los sistemas de satélite que son visibles y pueden detectarse por el sensor de GNSS específico instalado en el dispositivo móvil en ese preciso instante (GPS, GLONASS, BEIDOU, GALILEO), tanto a un nivel de protocolo (trama de datos) como los datos procesados por la APP de cliente en un formato de datos específico.

La ventana de tiempo en la que se obtendrán los datos es un parámetro seleccionado por quienquiera que esté proporcionando el servicio. La ventana de tiempo tendrá una amplitud mínima de entre 4 e 10 segundos.

El servidor, después de haber recibido estos datos, iniciará la etapa de verificación que realiza en primer lugar un análisis para cada único tipo de información y a continuación verifica todos los datos sin procesar de bajo nivel y datos de alto nivel para determinar cualesquiera inconsistencias. Se proporciona a continuación una descripción detallada de las comprobaciones que pueden accionar el servidor de certificación.

Verificación de las señales y los datos de GNSS

Con referencia a la Figura 1, cada servidor de certificación LA tiene disponible al menos dos receptores de GNSS de múltiples constelaciones y múltiples bandas/múltiples canales.

Se realizará una comparación en el lado del servidor de certificación LA de los datos sin procesar de las señales de radio, los datos de alto nivel (estructura de los paquetes y mensajes de navegación) y los datos procesados por los sensores de GNSS en la ventana de tiempo de referencia. Todas las diferencias y las inconsistencias entre información de GNSS obtenida en el lado del servidor de certificación (LA) y enviada al lado de cliente (APP) se etiquetarán como posibles intentos fraudulentos.

Para verificar y certificar la consistencia y la veracidad de la información recibida, dependiendo del tipo de datos disponible y enviado al lado de cliente, el servidor de certificación LA aplica las siguientes técnicas anti-suplantación de identidad organizadas en 4 etapas:

ETAPA *A: Control de la dirección de las señales, velocidad y movimiento de los satélites de GPS recibidos.*

En el lado del servidor de certificación LA, se requerirá lo siguiente para cada señal recibida del satélite de GPS (Figura 1 - satélites S1, S2, S3 y S4): los valores y la fase del código de PRN C/A del código L1, los valores de la onda portadora y de la fase de la señal de radio de bajo nivel y los valores del efecto Doppler generado por el desplazamiento relativo del satélite-receptor de GNSS - cambio continuo de la frecuencia de la señal emitida - (Tabla 1 - valores A1, A2, A3, A4 y A5). Usando diversos sensores de GNSS en el lado del servidor, instalados en el área de competencia donde opera el servidor de certificación LA, usando, por ejemplo, la técnica de interferometría de señales de radio (referencia bibliográfica "Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing" - J. Magiera, R. Katulski), se realizan cálculos, en una ventana de tiempo de referencia específica, de las direcciones de la señal de radio y la velocidad de los satélites con respecto a los sensores de GNSS del servidor de certificación LA. Los mismos valores (A1, A2, A3, A4, A5) también se obtienen en el lado de cliente y se envían al servidor de certificación LA para cálculo de la dirección de las señales y la velocidad de los satélites con respecto al dispositivo móvil.

La dirección de la señal y la velocidad de los satélites calculada en la ventana de tiempo de referencia entre el servidor de certificación LA y APP cliente debe ser igual; las discrepancias indican que la señal no es genuina.

ETAPA B: *Comparación de la potencia, relación de señal/ruido de la señal de radio y el ruido del código L1 del código de pseudointervalo del código C/A del GPS.*

El servidor de certificación LA verifica que los valores enviados del dispositivo móvil con relación a la potencia de las señales *(B1),* relación señal/ruido (B2) - (C/N_0 - densidad de portadora a ruido y/o SNR - relación de señal a ruido) - y ruido del código de pseudointervalo del código C/A L1 (B3) de todos los GPS de satélites de GPS capturados en la ventana de tiempo de referencia pertenecen a un intervalo predeterminado de valores que pueden registrarse realmente por el dispositivo móvil.

ETAPA C: *Comparación del código de GPS de pseudointervalo militar, código L1 encriptado P(Y)*.

Se trazará el patrón en el lado del servidor del código de pseudointervalo militar P(Y)-código (C3), que está encriptado y no es predecible, para cada satélite de GPS recibido dentro de la ventana de tiempo de referencia. Los valores de estos patrones obtenidos en el lado del servidor se compararán con los valores de los patrones obtenidos y enviados en el lado de cliente. Estos valores deben ser idénticos.

ETAPA D: *Comparación del paquete de datos y de los bits de datos contenidos en el mismo (telemetría, mensaje de navegación). La comparación de los datos de alto nivel procesados por el sensor de GNSS para todos los satélites capturados de las diversas constelaciones globales actualmente activas.*

El servidor de certificación LA comparará los datos obtenidos con los del cliente con relación a la estructura de los paquetes *(D1)* con mensajes de navegación relativos (bits de datos) - (D2) - y datos procesados por el sensor de GNSS (D3) de todos los satélites capturados en la ventana de tiempo de referencia. Los datos del cliente deben ser idénticos a los mismos valores obtenidos del servidor de certificación LA. Los datos de alto nivel incluyen la verificación de los intervalos de transmisión de las señales de satélite de GNSS; la verificación de la consistencia de las indicaciones de envío y llegada; la verificación de la corrección de los datos específicos de los diversos satélites capturados en el instante y lugar específicos: la estructura de los paquetes (D1 - tramas, sub-tramas y palabras), el mensaje de navegación contenido en el paquete (trama de datos - D2) y los datos de alto nivel procesados por el

sensor de GNSS (D3) deben ser todos idénticos.

Tabla 1 resumen de posibles datos a verificarse en el lado del servidor

Datos de bajo nivel		
ETAPA A	A1.	Valores de código de pseudointervalo de GPS predecible código C/A L1;
	A2.	Valores de fase de código de pseudointervalo de GPS código C/A L1;
	A3.	Valores de onda portadora de señal de radio de GPS;
	A4.	Valores de fase de la señal de radio de GPS;
	A5.	Valores de efecto Doppler de señal de radio de GPS;
ETAPA B	B1.	Valores de potencia de señal de radio de GPS;
	B2.	Valores de relación de señal/ruido (C/N_0 - densidad de portadora a ruido y/o SNR - relación de señal a ruido) de GPS;
	B3.	Valores de estadísticas con relación a ruido de código de pseudointervalo del código C/A L1 de GPS: ✓ Desviación típica de semi-eje mayor de elipse de error (en metros); ✓ Desviación típica de semi-eje menor de elipse de error (en metros); ✓ Orientación de semi-eje mayor de elipse de error (en grados); ✓ Desviación típica en metros de error de latitud (en metros); ✓ Desviación típica en metros de error de longitud (en metros); ✓ Desviación típica en metros de error de altitud (en metros);
ETAPA C	C1.	Valores con relación al patrón pseudoaleatorio de código militar impredecible encriptado P(Y);
	Datos de alto nivel	
ETAPA D	D1. Estructura de paquete de datos con relación a constelación de satélite específica. En el caso de estructura de GPS y bits de datos de trama, sub-tramas y palabras de telemetría: ✓ Preámbulo; ✓ Bits de paridad; ✓ Bits de sincronización. D2. Mensaje de navegación contenido en el paquete de datos de la constelación de satélite específica (trama de datos). En el caso de GPS las siguientes palabras: ✓ Corrección en las frecuencias convencionales, edad de datos (AODC) y coeficientes para el retardo ionosférico con relación a la frecuencia L1, enviados por el centro de control; ✓ Efemérides de cada satélite e instante de referencia AODE (Edad de Datos) enviadas por el centro de control; ✓ Almanaque de la constelación de satélite entera generada por el centro de control (efemérides truncada, correcciones de relojes, número de identificación de satélite, estado de satélite);	
	D3. Datos de alto nivel extraídos del mensaje de navegación y procesados por el receptor de GNSS. En el caso de GPS: ✓ Número total de satélites en vista; ✓ Número total de satélites en uso; ✓ Número de satélite de PRN; ✓ Elevación de satélite en grados (máx 90); ✓ Acimut de satélite en grados (de 000 a 359); ✓ Excentricidad; ✓ Velocidad de satélite con respecto a tierra; ✓ HDOP (Dilución de Precisión Horizontal); ✓ VDOP (Dilución de Precisión Vertical); ✓ PDOP (Posición (3D) Dilución de Precisión; ✓ TDOP (Dilución de Tiempo de Precisión); ✓ Fecha y hora; ✓ Número de la semana de sistema de GPS; ✓ Latitud de posición calculada; ✓ Longitud de posición calculada; ✓ Altura de receptor de GNSS por encima del nivel del mar; ✓ Separación de la geoda; ✓ Calidad de señal de GPS;	
	Datos de alto nivel	
	✓ Variación magnética;	

5

Resultados de verificaciones

Únicamente si todas las verificaciones anteriores (para todos los datos o un subconjunto de estos en la tabla) tienen un resultado positivo, el servidor de certificación LA certificará la posición del usuario, proporcionando a la aplicación de cliente APP con un certificado de georreferenciación firmado digitalmente con un valor legal y marcado digitalmente, que certifica la posición del usuario en ese momento particular.

En otras palabras, el método para la certificación de georreferenciación de un dispositivo móvil APP (equipado con reloj de dispositivo móvil y un sensor de GNSS móvil) por un servidor de certificación LA (equipado con sensor de GNSS de servidor y reloj de servidor), donde el dispositivo móvil y el servidor de certificación están conectados a través de una red de comunicación de datos, comprende las siguientes etapas:

A. ejecutar en el dispositivo móvil APP una aplicación configurada para gestionar la certificación APP en el lado del dispositivo móvil;
B. solicitar, a través de dicha aplicación, una certificación de georreferenciación a dicho servidor de certificación LA;
C. realizar una sincronización entre el reloj del dispositivo móvil y el reloj del servidor, realizando un protocolo de sincronización de tiempo de manera simultánea en el dispositivo móvil APP y el servidor de certificación LA;
D. obtener, mediante dicho sensor de GNSS móvil y para cada satélite de radio-visible S1-S4, una señal de radio de satélite de GNSS en cualquier instante de tiempo *t* de una ventana de tiempo predefinida;
E. obtener de dicho sensor de GNSS móvil de la etapa D y enviar a dicho servidor de certificación LA un conjunto de información derivada de dicha señal de radio de satélite de GNSS y relacionada con:

- un primer grupo de datos relacionado con potencia, relación de señal/ruido, código de pseudointervalo de ruido de código C/A L1,
- un segundo grupo de datos relacionado con código de pseudointervalo militar, código P(Y) L1 encriptado, datos de estructura del paquete de datos y de los bits de datos contenidos en el mismo que incluyen telemetría y mensaje de navegación, y
- un tercer grupo de datos relacionado con el efecto Doppler, onda portadora, fase;

F. obtener, por medio de dicho sensor de servidor de GNSS LA1, LA2 y para cada satélite de radio-visible S1-S4, una señal de radio de satélite de GNSS en cualquier instante de tiempo *t* de una ventana de tiempo predefinida;
G. obtener, de dicho sensor de la etapa F basándose en dicha señal de radio de satélite de GNSS de la etapa F, un primer, un segundo y un tercer conjunto de datos que corresponden a dicho primer, segundo y tercer conjunto de datos de la etapa E;
H. calcular, por dicho servidor de certificación LA:

- dirección, velocidad y desplazamiento de señal de cada satélite de radio visible S1-S4 que es radio-visible para el dispositivo móvil APP basándose en dicho tercer conjunto de datos;
- dirección, velocidad y desplazamiento de señal de cada satélite de radio visible S1-S4 que es radio-visible para el servidor de certificación LA basándose en dicho tercer conjunto de datos correspondiente;

I. comparar, por el servidor de certificación LA:

- dicho primer conjunto de datos y dicho primer conjunto de datos correspondiente, uno a uno, verificando que las diferencias caen en intervalos predefinidos;
- dicho segundo conjunto de datos y dicho segundo conjunto de datos correspondientes, uno a uno, verificando que son idénticos;
- dirección, velocidad y desplazamiento de señal del satélite de radio-visible que es radio-visible para el dispositivo móvil y dirección, velocidad y desplazamiento de señal del satélite de radio-visible que es radio-visible para el servidor, uno a uno, verificando que las diferencias caen en intervalos predefinidos adicionales;

L. únicamente en el caso donde todas las verificaciones de la etapa I son negativas, enviar, por el servidor de certificación LA al dispositivo móvil APP, un certificado de georreferenciación que incluye la fecha, dicha ventana de tiempo predeterminada y la posición del dispositivo móvil APP en dicha ventana de tiempo.

Innovaciones con respecto a la técnica anterior

La invención tiene ciertas peculiaridades sustanciales con respecto a la técnica anterior que pueden resumirse como sigue:

- uso de un servidor de certificación (que es una Autoridad de Georreferenciación confiable) que obtiene señales de GNSS independientemente de los dispositivos móviles;
- transmisión de las señales de GNSS obtenidas de los dispositivos móviles al servidor de certificación;
- comparación, por la unidad de certificación central, de acuerdo con criterios predeterminados, de los dos conjuntos de señales obtenidas independientemente; y

- emisión del certificado únicamente cuando se satisfacen los criterios anteriormente mencionados.

Resistencia del método a ataques de suplantación de identidad

Las señales de radio de los satélites de GNSS visibles llegan del espacio con diversos ángulos y cada satélite individual se mueve con una velocidad aproximada de 14.000 km por hora.

Cualquier simulador de GNSS en un entorno protegido intentará reproducir las señales de todos estos satélites visibles en un lugar y tiempo dados, intentando recrear, con respecto a la constelación de GPS el código predecible específico del código C/A L1.

Para reproducir todos los satélites de GNSS en vista, un hipotético atacante debería preparar un simulador para cada señal a emitirse. Estos simuladores necesitarían estar posicionados de una manera coherente con la posición real en el cielo del satélite relativo a simularse. Además de la señal de bajo nivel y el mensaje de navegación de alto nivel (bits de datos), cada simulador debería también simular el movimiento del satélite específico, intentando reproducir el efecto Doppler (desplazamiento) de cada señal de radio individual.

Este tipo de ataque es puramente teórico e impracticable en realidad, en vista de la precisión solicitada al replicar la posición y velocidad absolutas y relativas de todos los satélites en vista.

Por lo tanto, en la práctica, este tipo de ataque se lleva a cabo por medio de un simulador de GNSS equipado con una única antena que emite diversas señales de radio de GNSS que se modulan de manera adecuada para parecer como señales de radio de GNSS reales.

Si las señales de radio de GNSS provienen todas de una misma dirección con relación al dispositivo móvil, significa que ha habido un intento fraudulento.

El método por lo tanto debe oponerse a los atacantes que desean mostrar una posición diferente de la realmente ocupada. Debe ser posible detectar cualquier método de falsificación realizado que se inicia desde otra posición. Con referencia a la Figura 2, el escenario más complejo y sofisticado para oponerse es el de en el que un usuario desea falsificar la posición relativa aislando el dispositivo móvil de las señales de GNSS reales y transmitir diversas señales de GNSS falsas, creadas *ad hoc* en el laboratorio por medio de uno o más simuladores de señal de GNSS *(ESCENARIO* 1).

Con referencia a la Figura 3, de acuerdo con una variante a este escenario se irradia el dispositivo móvil, por medio de un emisor en el laboratorio, con una señal auténtica que proviene de la posición a declararse para el servicio o en la misma posición pero para procesarse de manera adecuada. En ese caso, el atacante debe detectar la señal auténtica y enviarla al simulador *(ESCENARIO* 2).

Con referencia a la Figura 4, otro posible escenario es el intento para irradiar el dispositivo objetivo únicamente con algunas señales no genuinas para manipular la posición. En este caso, es necesario irradiar las señales relativas con una potencia mayor para forzar el dispositivo objetivo para obtener el último en lugar de las señales de GNSS originales más débiles *(ESCENARIO* 3).

Con respecto a lo anterior, la etapa A del método de acuerdo con la invención puede identificar intentos de suplantación de identidad con señales simuladas en el laboratorio tales como en los ESCENARIOS 1 y 2.

En el ESCENARIO 3 es necesario considerar la potencia baja con la que llegan las señales de GNSS reales del espacio. Si el receptor de GNSS no está completamente aislado de señales externas, cualquier atacante que use un simulador para irradiar una señal no genuina debe usar una potencia de señal que es mayor que la del original, para engañar al dispositivo móvil e inducirlo a acoplarse con la señal creada *ad hoc* en lugar de la señal de radio de satélite débil original. La ETAPA B verifica la potencia de la señal; una potencia superior indica que la señal no es genuina. También en el caso de aislamiento completo, cualquier atacante podría tener que irradiar el dispositivo con un nivel de potencia correcto y recrear una relación de señal/ruido coherente y estadísticas coherentes del ruido del código de pseudointervalo de GPS del código C/A L1 para cada satélite a simularse.

Como un refuerzo adicional contra ataques de suplantación de identidad, las etapas C y D del método de acuerdo con la invención fuerzan a un atacante a enviar señales que se detectan eficazmente por los satélites y no se generan artificialmente; este es el caso para todos los satélites visibles y no solo para aquellos necesarios para calcular la posición. El atacante se fuerza a detectar las señales auténticas y, si fuera necesario, procesarlas para modificar la posición.

Se han descrito anteriormente las realizaciones preferidas y se han sugerido variantes a la invención, pero deberá entenderse que la invención puede modificarse y/o adaptarse por los expertos en el campo sin alejarse de esta manera del alcance del concepto inventivo, como se define en las reivindicaciones en el presente documento.

REIVINDICACIONES

1. Método de certificación de georreferenciación para la certificación de un dispositivo móvil (APP), equipado con un reloj de dispositivo móvil y un sensor de GNSS móvil, por un servidor de certificación (LA) equipado con un sensor de GNSS de servidor y reloj de servidor, estando conectados el dispositivo móvil y el servidor de certificación a través de una red de comunicación de datos, en la que realizan las siguientes etapas:

A. ejecutar en el dispositivo móvil (APP) una aplicación configurada para gestionar la certificación (APP) en el lado del dispositivo móvil;
B. solicitar, a través de dicha aplicación, una certificación de georreferenciación a dicho servidor de certificación (LA);
C. realizar una sincronización entre el reloj del dispositivo móvil y el reloj del servidor, realizando un protocolo de sincronización de tiempo simultáneamente en el dispositivo móvil (APP) y el servidor de certificación (LA);
D. obtener, mediante dicho sensor de GNSS móvil y para cada satélite de radio-visible (S1-S4), una señal de radio de satélite de GNSS en cualquier instante de tiempo t de una ventana de tiempo predefinida; estando el método caracterizado por
E. obtener de dicho sensor de GNSS móvil de la etapa D y enviar a dicho servidor de certificado (LA) un conjunto de información derivada de dicha señal de radio de satélite de GNSS relacionada con:

- un primer grupo de datos relacionado con potencia, relación de señal/ruido, código de pseudointervalo de ruido de código C/A L1,
- un segundo grupo de datos relacionado con código de pseudointervalo militar, código P(Y) L1 encriptado, datos de estructura del paquete de datos y de los bits de datos contenidos en el mismo que incluyen telemetría y mensaje de navegación, y
- un tercer grupo de datos relacionado con el efecto Doppler, onda portadora, fase;

F. obtener, por medio de dicho sensor de servidor de GNSS (LA1, LA2) y para cada satélite de radio-visible (S1-S4), una señal de radio de satélite de GNSS en cualquier instante de tiempo t de una ventana de tiempo predefinida;
G. obtener, de dicho sensor de la etapa F, basándose en dicha señal de radio de satélite de GNSS de la etapa F, un primer, un segundo y un tercer conjuntos de datos que corresponden a dicho primer, segundo y tercer conjuntos de datos de la etapa E;
H. calcular por dicho servidor de certificado (LA):

- dirección, velocidad y desplazamiento de señal de cada satélite de radio visible (S1-S4), que es radio-visible para el dispositivo móvil (APP), basándose en dicho tercer conjunto de datos;
- dirección, velocidad y desplazamiento de señal de cada satélite de radio visible (S1-S4), que es radio-visible para el servidor de certificación (LA), basándose en dicho tercer conjunto de datos correspondiente;

I. comparar, por el servidor de certificado (LA):

- dicho primer conjunto de datos y dicho primer conjunto de datos correspondiente, uno a uno, verificando que las diferencias caen en intervalos predefinidos;
- dicho segundo conjunto de datos y dicho segundo conjunto de datos correspondientes, uno a uno, verificando que son idénticos;
- dirección, velocidad y desplazamiento de señal del satélite de radio-visible que es radio-visible para el dispositivo móvil, y dirección, velocidad y desplazamiento de señal del satélite de radio-visible, que es radio-visible para el servidor, uno a uno, verificando que las diferencias caen en intervalos predefinidos adicionales;

L. únicamente en el caso donde todas las verificaciones de la etapa I son negativas, enviar, por el servidor de certificación (LA) al dispositivo móvil (APP), un certificado de georreferenciación que incluye la fecha, dicha ventana de tiempo predeterminada y la posición del dispositivo móvil (APP) en dicha ventana de tiempo.

2. Método de acuerdo con la reivindicación 1, en el que la comunicación entre el dispositivo móvil (APP) y el servidor de certificación (LA) se lleva a cabo usando protocolos de comunicación encriptados.

3. Método de acuerdo con la reivindicación 1 o 2, en el que la ventana de tiempo tiene una amplitud mínima entre 4 y 10 s.

4. Un método de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en el que dicho certificado de georreferenciación está firmado digitalmente e indicado en tiempo.

5. Método de acuerdo con una cualquiera de las reivindicaciones 1 a 3, en el que se incluye una fase preliminar en la que la aplicación móvil se registra en el servidor de certificación (LA).

6. Un método de acuerdo con una cualquiera de las reivindicaciones 1 a 5, en el que en la etapa H se usa una técnica de interferometría de señales de radio para calcular los valores de dirección, velocidad y desplazamiento de señal del

satélite.

7. Sistema de certificación de georreferenciación, que comprende:

- un dispositivo móvil (APP) equipado con un reloj de dispositivo móvil y un sensor de GNSS móvil,
- un servidor de certificación (LA) con sensor de GNSS de servidor y reloj de servidor,

caracterizado por que una aplicación está instalada en el dispositivo móvil (APP), que está configurada para realizar las etapas A-E del método de certificación de acuerdo con cualquiera de las reivindicaciones 1 a 6, y una aplicación está instalada en el servidor de certificación (LA) configurada para realizar las etapas C, F-L del método de certificación de acuerdo con cualquiera de las reivindicaciones 1 a 6.

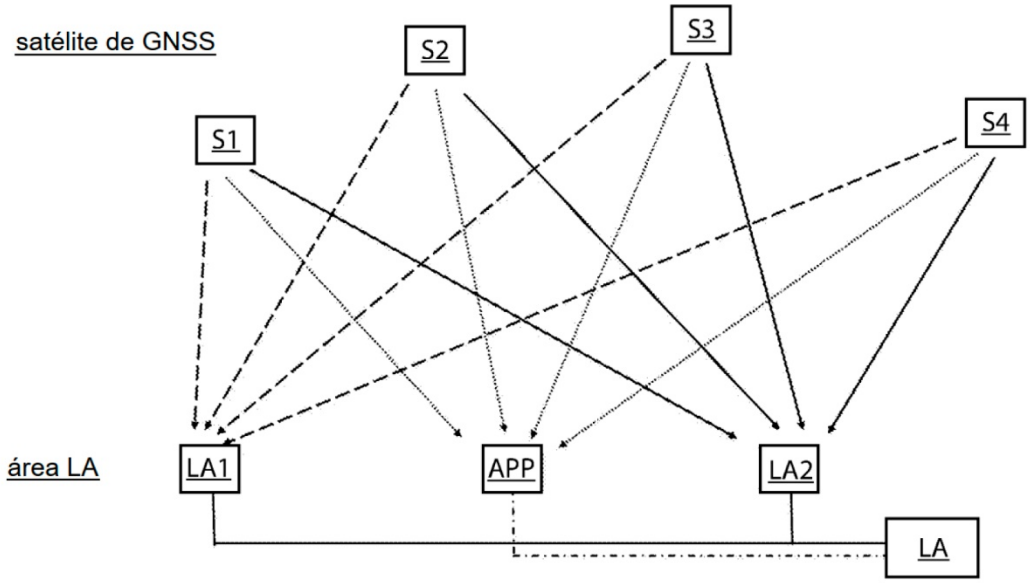
satélite de GNSS
S1
S2
S3
S4
área LA
LA1
APP
LA2
LA

Fig. 1

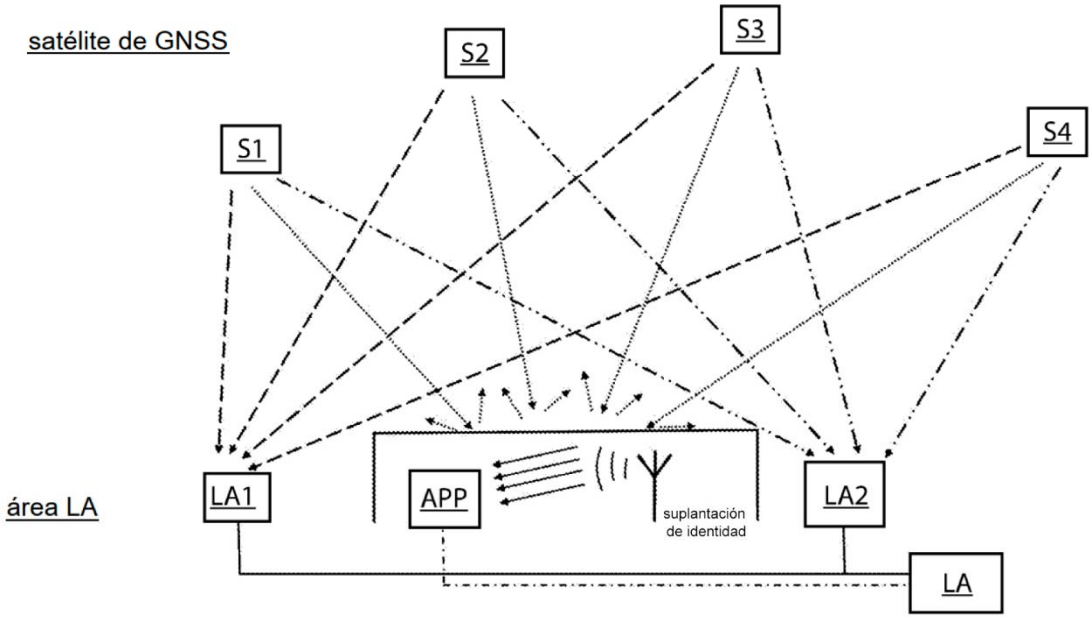
satélite de GNSS
S1
S2
S3
S4
área LA
LA1
APP
suplantación
de identidad
LA2
LA

Fig. 2

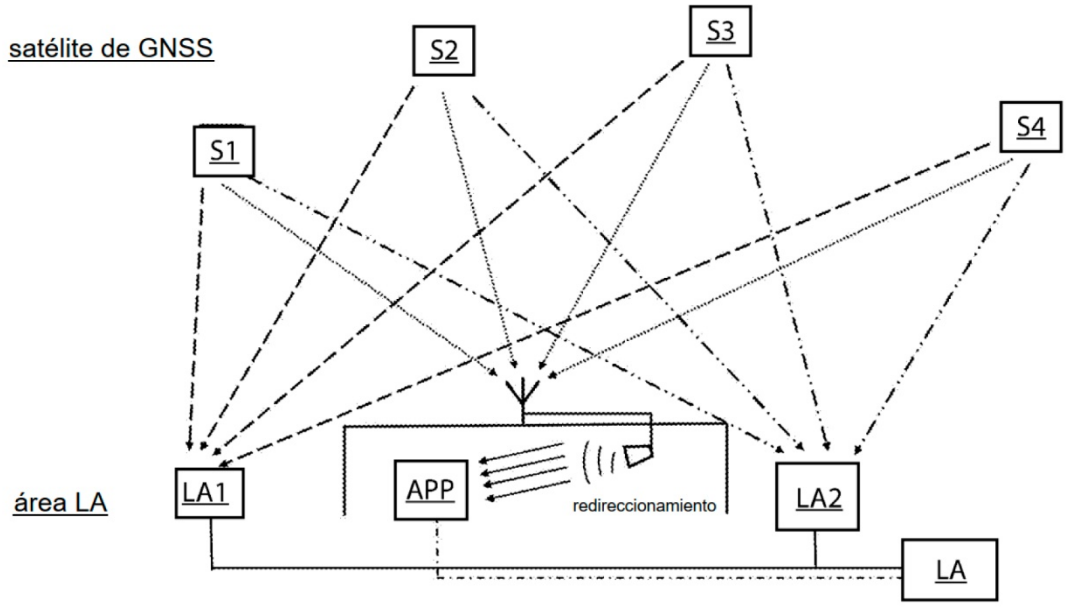
satélite de GNSS
S1
S2
S3
S4
área LA
LA1
APP
redireccionamiento
LA2
LA

Fig. 3

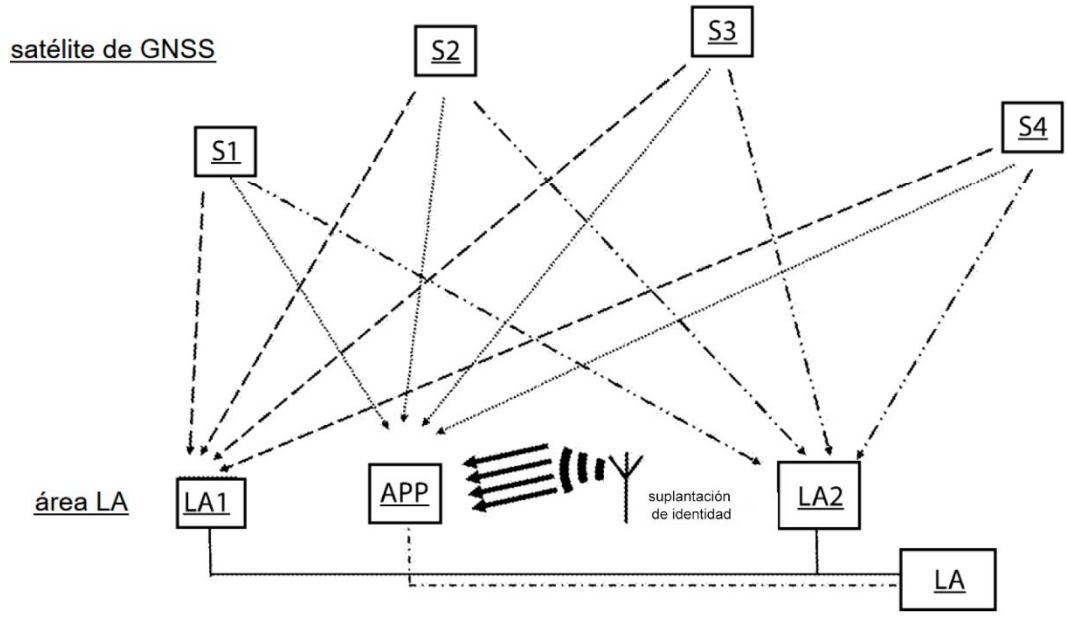
satélite de GNSS
S1
S2
S3
S4
área LA
LA1
APP
suplantación
de identidad
LA2
LA

Fig. 4