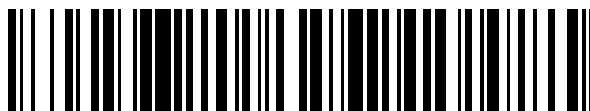


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 563 213**

51 Int. Cl.:

G01S 19/40 (2010.01)

G01S 19/14 (2010.01)

G01S 19/11 (2010.01)

G07B 15/06 (2011.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **19.10.2012 E 12189176 (6)**

97 Fecha y número de publicación de la concesión europea: **06.01.2016 EP 2584378**

54 Título: **Procedimiento y sistema de detección de fraude de información de posición de un dispositivo móvil**

30 Prioridad:

21.10.2011 FR 1103228

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

11.03.2016

73 Titular/es:

**THALES (100.0%)
45, rue de Villiers
92200 Neuilly Sur Seine, FR**

72 Inventor/es:

BARDOUT, YVES

74 Agente/Representante:

CARPINTERO LÓPEZ, Mario

ES 2 563 213 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 y sistema de detección de fraude de información de posición de un dispositivo móvil

El objeto de la presente invención se refiere a un procedimiento y a un sistema para autenticar la posición GNSS de un elemento o dispositivo móvil. Esta pretende detectar el enmascaramiento o la usurpación de emisor (término más conocido por el acrónimo anglosajón “spoofing”), y se aplica, por ejemplo, al campo de los sistemas de telepeaje en carretera, autopista, urbano y a cualquier otro sistema de vigilancia o de pago geolocalizado.

Un elemento móvil corresponde, por ejemplo, a una persona, un animal, un vehículo o incluso cualquier objeto.

Los terminales electrónicos móviles que implementan aplicaciones que requieren información sobre su posicionamiento geográfico constan de unos medios para estimar de la forma más precisa posible su posición. Para ello, se utilizan habitualmente unos sistemas de geolocalización por satélite, designándose estos sistemas con el acrónimo GNSS que procede de la expresión anglosajona “Global Navigation Satellite Systems”. Un ejemplo de sistema GNSS es el sistema GPS, acrónimo anglosajón de *Global Positioning System*.

La integridad de las posiciones es una gran necesidad en una aplicación del posicionamiento esencial desde un punto de vista legal (sistema de pago habitual: por ejemplo seguro, aparcamiento y red de carreteras), o una aplicación judicial (pulsera electrónica o vigilancia móvil), al igual que en una aplicación esencial desde el punto de vista de la seguridad de los bienes (seguimiento de contenedores), seguridad del usuario (asistencia a la conducción).

Los equipamientos utilizados en sistemas que implementan este tipo de aplicaciones habitualmente son inviolables e implementan unos medios de seguridad seguros. Sin embargo, la conexión por radio con los satélites es una señal abierta y vulnerable, a menos que se utilicen las señales de GNSS encriptadas que no son accesibles a estos mercados, debido a la difusión y a la gestión de las claves de acceso.

Por consiguiente, es posible que un usuario no colaborador o una persona malintencionada induzcan posiciones falsas en un receptor, sin tener que interferir en el equipo instalado a bordo (designado OBU o el término anglosajón “On Board Unit”), esto con un equipo de bajo coste de tipo receptor regenerador, y fácil de implementar de forma encubierta. Se pueden implementar estrategias más o menos complejas en un receptor-regenerador para inyectar una señal GNSS que corresponde a la trayectoria deseada para burlar la aplicación: por ejemplo, para evitar la generación de una alerta en un equipo de vigilancia, como la pulsera electrónica o los eventos de tarificación activados por el paso de puertas virtuales, en las aplicaciones de pago habituales, minimizando al mismo tiempo el riesgo de ser descubierto. Los sistemas considerados para estas aplicaciones no permiten a día de hoy impedir este tipo de fraudes.

La solución típica de tarificación se basa en el paso de un pórtico virtual o en el mundo anglosajón “virtual gate”, o también el posicionamiento en una zona de pago (un aparcamiento, el centro de una ciudad). La verificación del funcionamiento de los equipos de vehículo se hace estadísticamente sobre unos puntos de control fijos o móviles, donde la coherencia de los eventos de tarificación se controla a posteriori con las matrículas de los vehículos observados. Un equipo de fraude se puede diseñar, además, para que sea indetectable en estos controles, la posición de estos controles se publica hacia estos equipos de fraude mediante un servicio centralizado (información oficial para los puntos fijos o compartida por los usuarios, para los puntos móviles).

La solicitud de patente EP 2 203 022 utiliza una primera información de posición dada por un sistema GNSS y una segunda información de posición de la célula en la que se encuentra la estación de base a la cual está conectado un dispositivo móvil, y verifica que la posición del dispositivo móvil está incluida en la célula de base correspondiente a la información de posición de célula recibida.

La solicitud de patente WO 2009/090515 describe un sistema y un procedimiento para hacer seguro el peaje automático. En este caso, el procedimiento utiliza también dos fuentes diferentes para obtener la posición de un vehículo; p. ej. el sistema de seguimiento de posición y los sensores que son independientes de las señales de navegación.

De la técnica anterior se conocen diferentes métodos de control de la coherencia de las estimaciones de posición. Esta coherencia se puede verificar, por ejemplo, vigilando la potencia absoluta o relativa de las señales GNSS o por comparación con unas fuentes secundarias como unos sensores de movimiento, o la medición de otras señales de radio. En la solicitud de patente WO 2012/130891 se dan a conocer unos procedimientos originales que implementan la modelización del usuario y su entorno.

La coherencia de las mediciones también se puede verificar utilizando unas técnicas de tatuaje digital que permiten en particular que los terminales localicen los emisores de una red. Esta técnica se designa a menudo con la palabra inglesa “watermarking”. En la solicitud de patente WO 2009/037133 se da a conocer un ejemplo de implementación del tatuaje digital.

Por otra parte, la protección de las aplicaciones de localización supone unas medidas conocidas de protección contra la manipulación (conocido con el término anglosajón “anti-tampering”), en la protección de los intercambios, en la protección de los datos que proceden de otros sensores en el vehículo.

5 Dichos métodos no están hoy en día implementados en los receptores comerciales disponibles, y suponen para algunos un coste importante que se deriva de un trabajo de rediseño en el microprocesador y/o en el *software* de control. En particular, rediseñar el microprocesador o chip para receptores para el gran público representa un coste y una demora importantes. Otros métodos suponen la adición de sensores en el equipo móvil (inerciales, medición de señales de radiofrecuencia). En cualquier caso, estos no están garantizados y los ataques sofisticados pueden burlarlos al menos parcialmente.

10 La idea que implementa la presente invención, al contrario que en los enfoques existentes de la técnica anterior que solicitan en general la adición de datos de posición secundarios, o un tratamiento de la señal más elaborado en la recepción GNSS, consiste en particular en utilizar información de tipo cartográfica, sin tener que recurrir a otros sensores, en el caso de un funcionamiento normal del dispositivo.

15 El objeto de la invención se refiere a un procedimiento para autenticar la posición $X(t)$ de un elemento móvil, un elemento móvil que comprende al menos un receptor GNSS, r , que tiene la función de estimar la posición $X(t)$ de este elemento móvil, **caracterizándose** este procedimiento **porque** consta de al menos las siguientes etapas combinadas:

- determinar uno o varios datos asociados a la posición $X(t)$ de un receptor GNSS, r ;
- extraer de una base de datos cartográfica unos datos de referencia asociados a la posición $X(t)$;
- 20 • determinar al menos un indicador $I_c(X)$ de coherencia de la posición del elemento móvil que establece una coherencia entre unos aspectos observables GNSS, utilizando el primer dato asociado a la posición $X(t)$ de dicho receptor r y el dato de referencia procedente de la base cartográfica y a la posición $X(t)$;
- filtrar dicho o dichos indicadores $I_c(X)$, integrando estos valores en una trayectoria del elemento móvil para un intervalo, $[t_0, t_1]$, de tiempo dado;
- 25 • autenticar la posición $X(t)$ de dicho elemento móvil utilizando uno o varios de dichos indicadores $I_c(X)$ de coherencia y comparando dicho o dichos valores de los indicadores con un valor dado.

El establecimiento de la base cartográfica y el cálculo de indicador de coherencia se realizan en un dispositivo centralizado conectado mediante una red de comunicación a dichos elementos móviles.

30 El establecimiento de la base cartográfica y el cálculo de indicador de coherencia se realizan, por ejemplo, en el interior de dichos elementos móviles.

De acuerdo con una variante de realización, para autenticar la posición $X(t)$ de un elemento móvil, el indicador $I_c(X)$ de coherencia se calcula a partir de la posición de pseudolitos indicada en la base cartográfica.

35 Para autenticar la posición $X(t)$ de un elemento móvil, el indicador $I_c(X)$ de coherencia se puede calcular a partir de la o las direcciones θ_{map1} , θ_{map2} del segmento de carretera recorrido y/o la velocidad V_{map} estimada en este segmento, a partir de los datos indicados en la base cartográfica.

De acuerdo con otra forma de realización, para autenticar la posición $X(t)$ de un elemento móvil, el indicador $I_c(X)$ de coherencia se calcula a partir, por una parte, de la distancia recorrida $D_r(t)$, estimada por la velocidad medida $V_r(t)$, y, por otra parte, de la distancia D_{map} a vuelo de pájaro, o la distancia curvilínea en el gráfico de carreteras en la base cartográfica.

40 Para autenticar la posición $X(t)$ de un elemento móvil, el indicador $I_c(X)$ de coherencia se calcula, por ejemplo, a partir de la altitud Z_r medida, comparada con la Z_{map} , indicada en la base cartográfica.

Se mostrarán mejor otras características y ventajas de la presente invención con la lectura de la descripción de un ejemplo, dado a título ilustrativo y en modo alguno limitativo, adjunto de las figuras, que representan:

- La figura 1, un ejemplo de sistema de localización de un dispositivo móvil, como un vehículo, por satélite.
- 45 • La figura 2, un diagrama de los diferentes elementos que intervienen en el procedimiento y el sistema de acuerdo con la invención.
- La figura 3, una ilustración de la pertenencia de una posición de un elemento móvil en el área de visibilidad de un pseudolito.
- La figura 4, una ilustración de las tensiones de dirección/velocidad que ofrece la cartografía.
- 50 • La figura 5, una ilustración de comparación velocidad y distancia recorrida en el mapa.

En resumen, de manera genérica, el procedimiento de acuerdo con la invención, para autenticar la posición GNSS de un dispositivo móvil sin tener que recurrir a una segunda fuente de posición y utilizando la arquitectura de los receptores actualmente utilizados, consiste en particular en evaluar la coherencia espacial de la información de posicionamiento transferida a partir de la información cartográfica.

- La figura 1 representa un ejemplo de localización de un elemento 1 móvil, por ejemplo un vehículo por satélite. El sistema de localización consta, a bordo del vehículo 1, de un dispositivo 2 de localización y de difusión, denominado "dispositivo móvil", destinado a determinar la posición y/o la velocidad de un vehículo y a transmitir esta información de localización a un servidor 3 de posiciones encargado de almacenarlas y/o de utilizarlas. El dispositivo de localización y de difusión consta de un receptor 4 de señales de navegación GNSS (en inglés *Global Navigation Satellite System*) como un receptor GPS (*Global Positioning System*), emitidas por una constelación de satélites 5a, 5b y un emisor-receptor 6 de comunicación móvil.
- La información de posición se calcula mediante el receptor 4 GNSS por medio de la explotación de las señales 13a y 13b emitidas por los satélites 5a, 5b de acuerdo con unos métodos conocidos por el experto en la materia.
- La figura 2 esquematiza de manera simplificada la arquitectura del sistema de autenticación de posición de un dispositivo móvil de acuerdo con la invención.
- La trayectoria del receptor GNSS instalado a bordo en un dispositivo 1 móvil está compuesto por una sucesión de posiciones $X(t)$ GNSS estimadas en unos instantes t , 21, a las cuales está asociada una incertidumbre en la posición ΔX y una incertidumbre en el tiempo Δt . El dispositivo móvil se denomina "veraz" y las posiciones "auténticas" si se calculan las posiciones a partir de la señal "auténtica", es decir emitida por la constelación GNSS. El dispositivo móvil se denomina "fraudulento" y las posiciones "no auténticas" en el caso contrario.
- Un módulo 22 permite determinar unos indicadores de coherencia. Este módulo 22 recibe en particular los datos 23 geográficos, los valores de posición GNSS.
- Un módulo 24 tiene, en particular, como función detectar los datos o posiciones sospechosas.
- Se describen, a continuación, diferentes realizaciones del procedimiento.
- De acuerdo con una variante de realización, se utiliza, por ejemplo, una base cartográfica centralizada en uno o varios servidores accesibles desde cada uno de los receptores, que reciben los datos de posicionamiento. La zona de servicio de un servidor y de la base de datos se determina en una implementación mediante un equilibrio entre coste y rendimiento. En una implementación típica, una base cubrirá un país o una región.
- Una realización alternativa de implementación del procedimiento de acuerdo con la invención es utilizar una base cartográfica duplicada en cada equipo móvil. Los módulos 22 y 24 también se pueden realizar bien en el terminal o bien en un servidor central.
- Estas variaciones se refieren a la implementación o no del principio del procedimiento, explicado en la implementación centralizada.
- Un componente 24 de detección de datos sospechosos, tal como se describe en su principio general en la patente WO 2012/130891, por ejemplo, estima uno o varios indicadores, 22, estadísticos que llevan la referencia $Ic(X)$, y X en la posición de un receptor k en un instante dado.
- Un indicador al estar afectado por ruidos a la vez de los errores de medición de los receptores, de los errores de la cartografía y de los errores inherentes al principio de comparación, se aplican uno o varios filtros a los indicadores $Ic(X)$ estadísticos, por ejemplo integrando estos valores $Ic_{raw}(X)$ en una trayectoria del elemento móvil para un intervalo $[t_0, t_1]$ de tiempo, cuya duración se selecciona en función de la aplicación: $Ic_{filtrado}(X) = \int_{t_0}^{t_1} Ic_{raw}(X)$ en el que $Ic_{filtrado}$ corresponde al valor del indicador obtenido después del filtrado e Ic_{raw} corresponde a los valores que puede tomar el indicador en el intervalo $[t_0, t_1]$ de tiempo.
- A partir de estos valores filtrados, se puede construir una función de decisión sobre la autenticidad de la posición de un dispositivo móvil o de un receptor k montado en el dispositivo.
- Para ello, se puede utilizar tradicionalmente un valor lógico verdadero/falso, un estimador $p(X)$ de probabilidad de fraude o unos valores de posibilidad/necesidad según la lógica difusa de Lofti Zadeh (Zadeh, L. A. (1965), "Fuzzy sets", *Information and Control*, 8 (3), págs. 338-353; Novák, V., "Are fuzzy sets a reasonable tool for modeling vague phenomena?", *Fuzzy Sets and Systems*, 156 (2005), págs. 341-348), siendo este valor una representación numérica de un grado de confianza en la posición P_k del receptor k :
- un indicador lógico $L(X) = Ic(X) > T$, $\in \{0; 1\}$, en el que T es un valor umbral seleccionado, o un estimador $p(X) = f(Ic(X))$ de probabilidad, en el que $f: [0; \infty[\rightarrow [0; 1]$ es una función creciente que normaliza el indicador en $[0; 1]$. Esta función se selecciona a partir de un modelo o de un experimento para que sea un estimador válido de la probabilidad de fraude, ajustado mediante parámetros.
- Por ejemplo: $p(X) = 2/\pi \cdot \arctan(\beta Ic^m) \in [0; 1]$ es continuo y cumple con estos límites.

Los valores de parametrización son, por ejemplo, el valor umbral $T > 0$, o los factores $\beta > 0$ y $m > 0$. Estos valores permiten el ajuste de la decisión según la distribución observada del indicador utilizado en unas muestras representativas de trayectorias reales y de trayectorias falsificadas para un dispositivo móvil dado. β se define como la inversa del valor I_c que corresponde a una probabilidad de confianza de $\frac{1}{2}$ y m permite ajustar la “rampa” de la función.

Al ser $p(X)$ la probabilidad de enmascaramiento o en el mundo anglosajón “spoofing”, la complementaria $1-p(X)$ de este valor es una probabilidad de autenticidad. Esta probabilidad $p(X)$ del indicador $I_c(n, X)$ de confianza se obtiene a partir de uno de los indicadores de coherencia o indicadores estadísticos 22 o una combinación de algunos de estos indicadores aplicando los métodos conocidos del experto en la materia, los descritos en la patente WO 2012/130891, sí como al menos uno de los 4 tipos de indicador originales, el paso cerca de un pseudolito, la dirección/velocidad comparada con el segmento de carretera, la dirección/velocidad comparada con la trayectoria, la posición comparada con el modelo de terreno, que se describen a continuación, aprovechando la colaboración entre receptores.

A) Pseudolitos

En este método esquematizado en la figura 3, el sistema comprende un cierto número de emisores terrestres, denominados “pseudolitos”, que emiten una señal compatible de una constelación GNSS, que los receptores GNSS existentes utilizan para calcular su posición, de acuerdo con unos métodos conocidos por el experto en la materia: la posición del pseudolito se difunde en el mensaje de navegación, o mediante asistencia, o la conoce un servidor centralizado que calcula la posición de usuario en modo “mobile-assisted”. Por otra parte, este pseudolito se diferencia en el cálculo del punto por su PRN, y esto permite que el detector reconozca la recepción o no de un pseudolito, que lleva la referencia de la variable lógica: visible (PL).

La idea es instalar dichos pseudolitos en algunos puntos de control (lo que es potencialmente menos caro, más discreto, menos restrictivo que otros equipos de control). En un sistema de pago sensible a la posición, la implantación de un pseudolito en una “puerta virtual”, valida el evento de tarificación asociado a esta puerta. La autenticación de la posición consiste en comparar esta con la zona de cobertura del pseudolito. Al ser PL la zona de recepción, si r_{PL} es el radio estimado de recepción para un receptor y el entorno dado, la posición $X(t)$ del elemento móvil está en la cobertura del pseudolito si y solo si: $|X(t) - X_{PL}| \leq r_{PL}$, como se ilustra en la figura 3. El punto 30 corresponde a un elemento no visible y el punto 31 a un elemento visible.

Si la posición $X(t)$ del elemento móvil está en esta zona PL de cobertura sin que el pseudolito se incluya en el cálculo del punto, o la posición $X(t)$ no está en la zona PL mientras que el pseudolito está incluido en el cálculo del punto, entonces la señal utilizada para calcular la posición probablemente no es auténtica.

Se puede definir un indicador de coherencia:

$$IC_{PL}(X) = \text{si es visible (PL), entonces } |X(t) - X_{PL}| / r_{PL}, \text{ si no } r_{PL} / |X(t) - X_{PL}|$$

B) Coherencia de dirección y velocidad esquematizada en la figura 4

En esta variante de implementación, implementada en aplicaciones automovilísticas, la posición indicada por el receptor GNSS está asociada a una posición verosímil $X_m(t)$ en la red de carreteras correspondiendo con el mapa o “map-matching”. En este esquema, la línea de puntos 41 representa las diferentes posiciones $X(t)$ medidas para el vehículo en movimiento y la referencia 40 la posición correspondiente en el mapa de carreteras.

Al ser θ el ángulo calculado en el punto de referencia norte-sur habitualmente utilizado en el campo de la cartografía de carreteras, θ_r es el ángulo del vehículo calculado en el receptor en el punto de referencia terrestre, V_{map} es la velocidad definida por la cartografía, en función del segmento de carretera concernido, de la velocidad límite de conducción en este segmento, V_r es la velocidad medida por el receptor GNSS del vehículo móvil que hay que vigilar. La o las direcciones θ_{map1} , θ_{map2} del segmento de carretera (según si está clasificado de sentido único o de doble sentido) se compara con la del vehículo θ_r , al igual que la velocidad teórica V_{map} se compara con la velocidad medida V_r del vehículo. Un indicador lógico $L(X)$ salta cuando la diferencia es superior a un umbral $\Delta\theta$, ΔV respectivo para al menos una de estas variables:

$$L(X) = |\theta_r - \theta_{map1}| > \Delta\theta \quad \text{y} \quad |\theta_r - \theta_{map2}| > \Delta\theta \quad \text{o} \quad V_r > V_{map} + \Delta V$$

El valor umbral $\Delta\theta$ se obtiene, por ejemplo, mediante unos medios de evaluación previamente definidos.

Esta velocidad V_{map} teórica viene dada bien por la limitación de velocidad, bien por la evaluación de la velocidad a partir de la clasificación de las carreteras y de la topografía (curvas, cotas, etc.). Una velocidad inferior no se considera sospechosa. Evidentemente, esta indicación es ambigua puesto que una velocidad real excesiva hace saltar una falsa alarma.

Un indicador $I_{CDi}(X)$ continuo se calcula de la siguiente manera, en un instante t dado:

$$Ic_{Dir}(X) = \left| \theta_r(t) - \theta_{map}(t) \right| / \Delta\theta + \max(V_r(t) - V_{map}(t), 0) / \Delta V$$

Por otra parte, la comparación entre la posición X(t) indicada y la X_m(t) cartografiada en la red de carreteras, es otro indicador, descrito en la solicitud de patente WO 2012/130891.

C) Velocidad comparada con la trayectoria esquematizada en la figura 5

5 En esta variante de implementación, el indicador compara directamente la distancia Dist, que corresponde a la velocidad medida V_r veces el intervalo temporal entre 2 mediciones, con la calculada según la trayectoria constituida por el seguimiento de las posiciones X(t_k), llevando a cabo un cálculo de diferencia de puntos sucesivos, o incluso calculando la longitud en el gráfico de carreteras que une estos puntos sucesivos, lo que puede ser muy diferente si el intervalo de tiempo no es pequeño, o la trayectoria es sinuosa (vía de acceso, pasos en zig zag, etc.).

10 Este indicador establece una coherencia entre unos aspectos observables de la señal de cada satélite (esto es pseudo rango y frecuencia) que dependen de la trayectoria del móvil. La utilización de la cartografía permite en principio una medición bastante exacta del camino recorrido entre dos puntos, que debería corresponder a la velocidad definida en GNSS.

15 Al incluir el cálculo de longitud en el gráfico de carreteras, se detecta además un enmascaramiento apropiado en fase de código y frecuencia, pero que no habría utilizado este mismo gráfico para controlar la vinculación entre los dos.

Se puede calcular un indicador $Ic_{Dist}(X)$ a partir de la diferencia entre la distancia D_r(t_k) correspondiente a la velocidad medida en el receptor.

20 La velocidad GNSS multiplicada por la diferencia temporal entre dos instantes t_{k+1}-t_k y la distancia D_{map}(t_k) es la distancia medida entre dos puntos medidos X(t_k), X(t_{k+1}), o dos puntos proyectados X_m(t_k), X_m(t_{k+1}) en el gráfico de carreteras o la cartografía de carreteras:

$$Ic_{Dist}(X) = \left| D_r(t_k) - D_{map}(t_k) \right|$$

en la que

$$D_r(t_k) = S_r(t_k) \times (t_{k+1} - t_k)$$

25 y

$$D_{map}(t_k) = dist(X(t_k), X(t_{k+1})),$$

o

$$D_{map}(t_k) = dist(X_m(t_k), X_m(t_{k+1})),$$

siendo dist la distancia a vuelo de pájaro o la distancia curvilínea en el gráfico de carreteras.

30 D) Altitud comparada con el modelo de terreno

Para cualquier persona o vehículo terrestre de posición X = (x_r, y_r, z_r), proyectada en un mapa de terreno en un punto (X_{map}, y_{map}, z_{map}), la altitud z_r se supone conforme a la z_{map} del terreno, para la latitud y longitud x_r, y_r. El indicador se puede calcular a partir de esta diferencia en una trayectoria:

$$Ic_{Alt}(X) = \left| z_r(t) - z_{map}(t) \right|$$

35 z_{map} es la altitud de la proyección de la posición en un mapa de terreno, la cual puede o no tener en cuenta el "map-matching".

REIVINDICACIONES

1. Procedimiento para autenticar la posición $X(t)$ de un elemento (1) móvil, un elemento móvil que comprende al menos un receptor GNSS, que tiene una función de estimar la posición $X(t)$ de este elemento (1) móvil, constandingo este procedimiento, en combinación, al menos de las siguientes etapas:
- 5 • determinar uno o varios datos (21) asociados a la posición $X(t)$ de un receptor GNSS;
- extraer de una base (23) de datos cartográfica unos datos de referencia asociados a la posición $X(t)$;
- determinar al menos un indicador (22) de coherencia $I_c(X)$ de la posición del elemento (1) móvil que establece una coherencia entre unos aspectos observables GNSS, utilizando el primer dato asociado a la posición $X(t)$ de dicho receptor y el dato de referencia procedente de la base cartográfica y asociado a la posición $X(t)$;
- 10 • filtrar dicho o dichos indicadores $I_c(X)$, integrando estos valores en una trayectoria del elemento móvil para un intervalo $[t_0, t_1]$ de tiempo dado;
- autenticar (24) la posición $X(t)$ de dicho elemento (1) móvil utilizando uno o varios de dichos indicadores $I_c(X)$ de coherencia y comparando el valor filtrado de los indicadores con un valor dado.
- 15 2. Procedimiento de acuerdo con la reivindicación 1, **caracterizado porque** el establecimiento de la base (23) cartográfica y el cálculo del indicador de coherencia se realizan en un dispositivo centralizado conectado mediante una red de comunicación a dichos elementos (1) móviles.
3. Procedimiento de acuerdo con la reivindicación 1, **caracterizado porque** el establecimiento de la base (23) cartográfica y el cálculo de indicador de coherencia se realizan en el interior de dichos elementos (1) móviles.
- 20 4. Procedimiento de acuerdo con una de las reivindicaciones 1 a 3, **caracterizado porque** para autenticar la posición $X(t)$ de un elemento (1) móvil, el indicador $I_c(X)$ de coherencia se calcula a partir de la posición de pseudolitos indicada en la base cartográfica.
5. Procedimiento de acuerdo con una de las reivindicaciones 1 a 3, **caracterizado porque** para autenticar la posición $X(t)$ de un elemento (1) móvil, el indicador $I_c(X)$ de coherencia se calcula a partir de la o las direcciones θ_{map1} , θ_{map2} del segmento de carretera recorrido y/o la velocidad V_{map} estimada en este segmento, a partir de los datos indicados en la base cartográfica.
- 25 6. Procedimiento de acuerdo con una de las reivindicaciones 1 a 3, **caracterizado porque** para autenticar la posición $X(t)$ de un elemento (1) móvil, el indicador $I_c(X)$ de coherencia se calcula a partir, por una parte, de la distancia $D_r(t)$ recorrida, estimada por la velocidad $V_r(t)$ medida, y, por otra parte, de la distancia D_{map} a vuelo de pájaro, o la distancia curvilínea en el gráfico de carreteras en la base cartográfica.
- 30 7. Procedimiento de acuerdo con una de las reivindicaciones 1 a 3, **caracterizado porque** para autenticar la posición $X(t)$ de un elemento (1) móvil, el indicador $I_c(X)$ de coherencia se calcula a partir de la altitud z_r medida, comparada con la z_{map} indicada en la base (23) cartográfica.

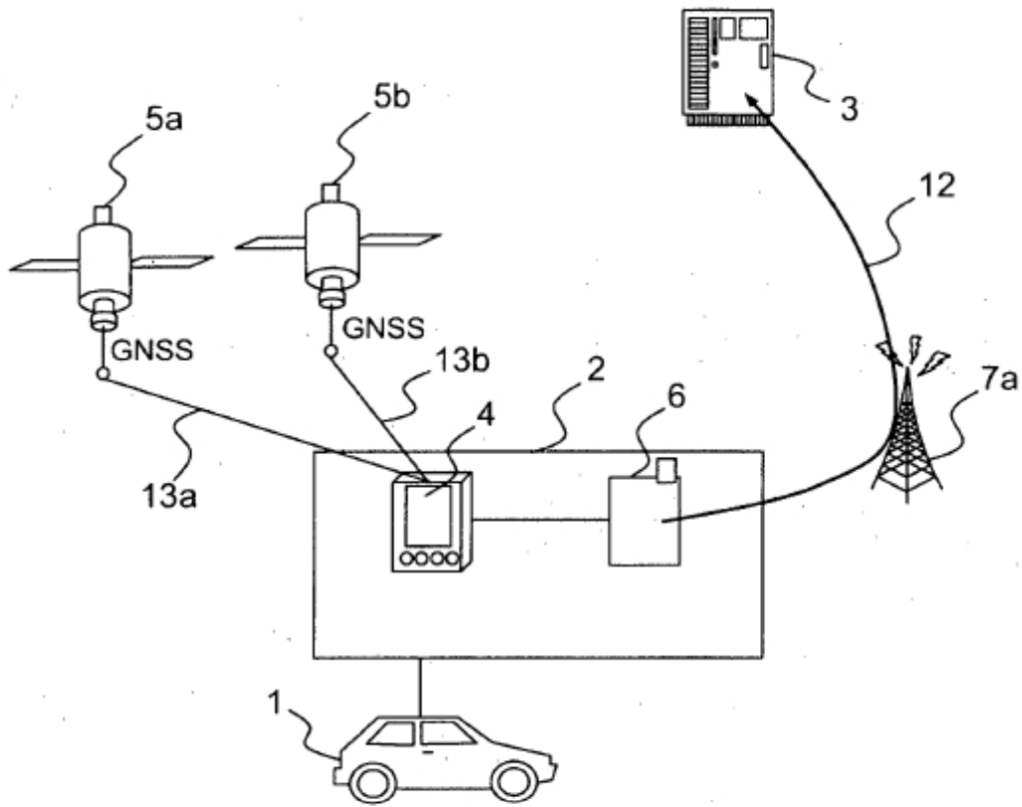


FIG.1

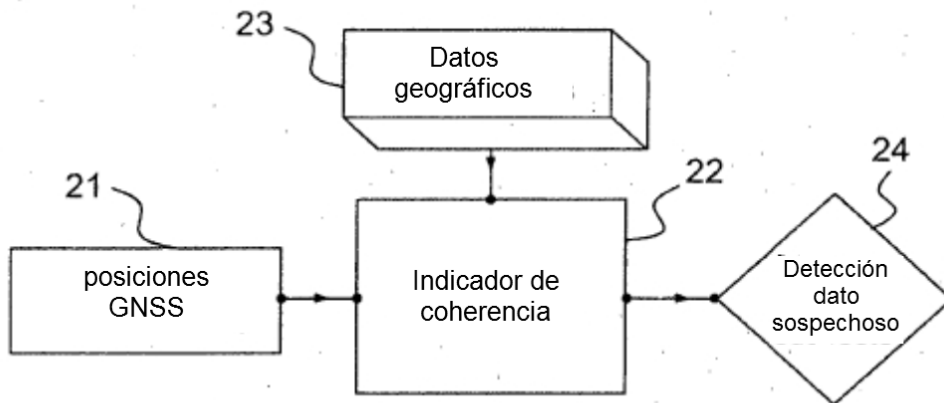


FIG.2

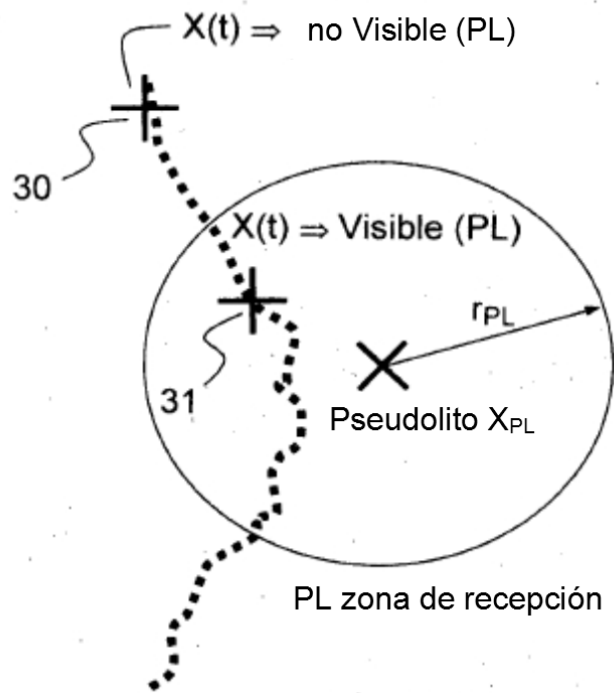


FIG.3

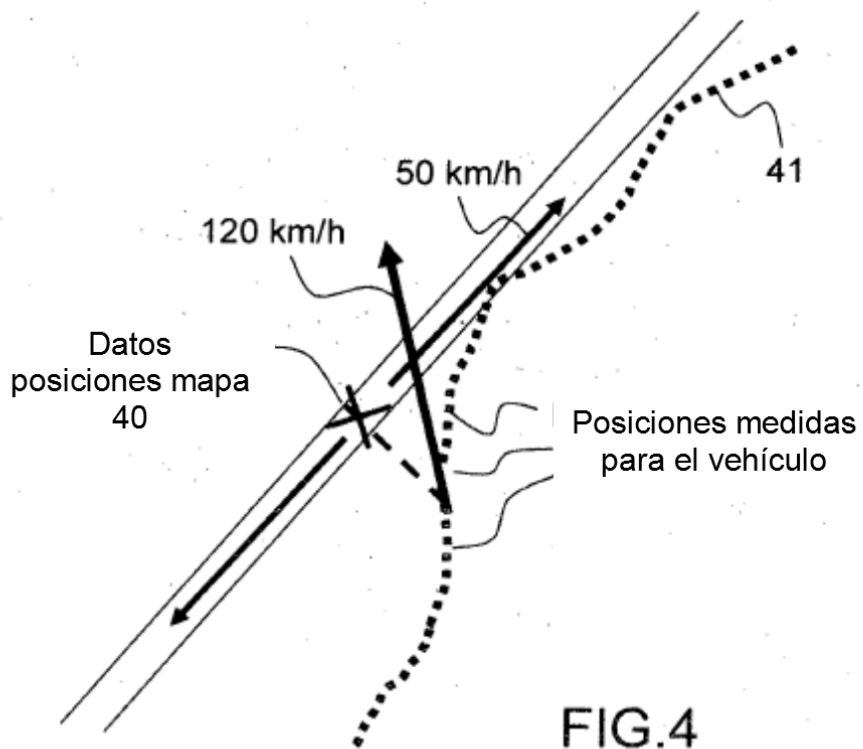


FIG.4

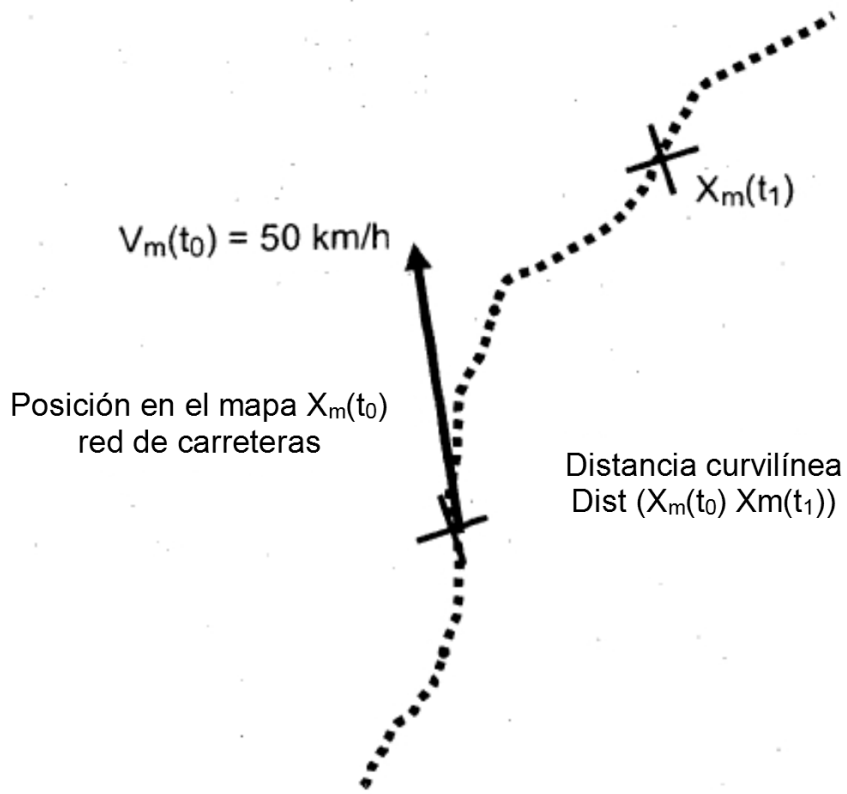


FIG.5