

METHOD AND SYSTEM FOR DETECTING FRAUDULENT POSITION DATA OF A MOBILE DEVICE

5 The subject of the present invention relates to a system for authenticating the GNSS position of a mobile device or element. Its purpose is to detect decoying or transmitter usurpation (a term better known as "spoofing") and it applies, for example, to the field of road, motorway or urban remote payment systems and to any other geographically located monitoring or payment system.

10 A mobile element corresponds, for example, to a person, an animal, a vehicle or to any object whatsoever.

 Mobile electronic terminals implementing applications requiring information on their geographic position comprise means for estimating their position
15 as accurately as possible. For this purpose, satellite geographic location systems are commonly used, these systems being denoted by the acronym GNSS, standing for "Global Navigation Satellite Systems". An example of a GNSS system is the GPS (Global Positioning System) system.

 The integrity of the positions is a major requirement in a positioning
20 application which is critical from a legal point of view (payment for use system: for example insurance, parking and road system), or a judicial application (wrist monitoring device or tags) just as it is in an application which is critical from the point of view of safety of goods (tracking containers) and safety of the user (driving assistance).

25 The equipments used in systems implementing these types of applications are usually tamper-resistant and use secure communication means. However, the radio link with the satellites is an open and vulnerable signal, unless encrypted GNSS signals are used which are not accessible to these markets, because of the distribution and management of access keys.

30 Consequently, it is possible for an uncooperative user or malicious person to induce false positions in a receiver, without having to interfere with the on-board equipment (denoted OBU, standing for "On Board Unit"), and to do this with a low-cost piece of equipment of the regenerative receiver type which is easy to

use surreptitiously. More or less complex strategies can be implemented in a regenerative receiver for injecting a GNSS signal corresponding to the path required for bypassing the application: for example in order to avoid the generation of a warning in monitoring equipment, like the wrist monitoring device or tariffing events triggered by passing through virtual gates in payment for use applications, and to do so whilst minimizing the risk of discovery. The systems envisaged for these applications do not at present make it possible to thwart such frauds.

The typical tariffing system is based on passing through a virtual gate, or on positioning in a charged zone (car park, town centre). The verification of the functioning of the equipment in vehicles is carried out statistically at fixed or mobile check points, where the consistency of the tariffing events is checked a posteriori with the registration numbers of the observed vehicles. Fraud equipment can furthermore be designed to be silent during these checks, the positions of these checks being published for these fraud equipments by a centralized service (official information for the fixed points or information shared by the users for the mobile points).

The patent application EP 2 203 022 uses a first piece of position information given by a GNSS system and a second piece of position information of the cell in which is located the base station to which a mobile device is connected, and checks that the position of the mobile device is included in the base cell corresponding to the received cell position information.

The patent application WO 2009/090515 describes a system and a method for making automatic payment secure. In this case the method again uses two different sources in order to obtain the position of a vehicle; i.e. the position tracking system and the sensors which are independent of the navigation signals.

Various methods of checking the consistency of position estimations are known in the prior art. This consistency can be checked for example by monitoring the absolute or relative power of the GNSS signals or by comparison with secondary sources like movement sensors or the measurement of other radio signals. Original procedures using the modelling of the user and his environment are disclosed in the patent application FR1100961.

The consistency of the measurements can also be checked using digital watermarking techniques notably allowing the terminals to locate the transmitters of a network. This technique is often referred to by the word "watermarking". An example of the use of digital watermarking is disclosed in the patent application WO 2009/037133.

Moreover, securing location applications assumes known anti-tampering protection measures in the securing of the exchanges and in the protection of data coming from other sensors in the vehicle.

Such methods are not at present implemented in commercially available receivers and some of them assume high cost resulting from re-design work at chip and/or control software level. In particular, redesigning the chip for mass produced receivers represents a high cost and a long delay. Other methods assume the adding of sensors in the mobile equipment (inertial, measurement of radio-frequency signals). In any case, they are not guaranteed and sophisticated attacks can at least partially bypass them.

The idea used by the present invention, unlike the existing approaches of the prior art which generally demand the adding of secondary position information or a more elaborate processing of the signal in the GNSS reception, notably consists in using cartographic information, without calling upon other sensors, in the case of normal functioning of the device.

The subject of the invention relates to a method for authenticating the position $X(t)$ of a mobile element, a mobile element comprising at least a GNSS receiver, r , having a function of estimating the position $X(t)$ of that mobile element, this method being characterized in that it comprises, in combination, at least the following steps:

- determining one or more items of data associated with the position $X(t)$ of a GNSS receiver, r ,
- extracting reference data associated with the position $X(t)$ from a cartographic database,

- determining at least one consistency indicator $Ic(X)$ using the first item of data associated with the said receiver r and the reference data coming from the cartographic database,
- filtering the said indicator or indicators $Ic(X)$, in order to improve the detection rate or the false alarm rate,
- authenticating the position $X(t)$ of the said mobile element using one or more of the said consistency indicators $Ic(X)$ in an authenticity decision function.

The filtering step is, for example, carried out by temporal integration of the indicator over a given period of time.

The establishment of the cartographic database and the calculation of the consistency indicator are carried out in a centralized device connected by a communications network to the said mobile elements.

The establishment of the cartographic database and the calculation of the consistency indicator are, for example, carried out within the said mobile elements.

According to a variant embodiment, in order to authenticate the position $X(t)$ of a mobile element, the consistency indicator $Ic(X)$ is calculated from the position of pseudolites indicated in the cartographic database.

In order to authenticate the position $X(t)$ of a mobile element, the consistency indicator $Ic(X)$ can be calculated from the direction or directions θ_{map1} , θ_{map2} of the road segment travelled and/or the speed V_{map} estimated over this segment, from data indicated in the cartographic database.

According to another embodiment, in order to authenticate the position $X(t)$ of a mobile element, the consistency indicator $Ic(X)$ is calculated from, on the one hand, the distance travelled $D_r(t)$, estimated by the measured speed $V_r(t)$, and on the other hand the distance as the bird flies D_{map} , or the curvilinear distance on the road graph in the cartographic database.

In order to authenticate the position $X(t)$ of a mobile element, the consistency indicator $Ic(X)$ is calculated, for example, from the measured altitude z_r , compared with that z_{map} indicated in the cartographic database.

Other features and advantages of the present invention will become more apparent on reading the description of an example given by way of illustration and in no way limitative with reference to the appended figures in which:

- Figure 1 shows an example of a satellite system for locating a mobile device, such as a vehicle,
- Figure 2 is a diagram of the different elements participating in the method and the system according to the invention,
- Figure 3 is an illustration of the inclusion of a position of a mobile element in the area of visibility of a pseudolite,
- Figure 4 is an illustration of the direction/speed constraints given by the cartography,
- Figure 5 is an illustration of comparison between speed and distance travelled on the map.

In brief, and in a generic manner, the method according to the invention, for authenticating the GNSS position of a mobile device without having recourse to a second position source and using the architecture of the receivers used at present, notably consists in evaluating the spatial consistency of the positioning information transferred from cartographic information.

Figure 1 shows an example of location of a mobile element 1, for example a vehicle, by satellite. The location system comprises, on board the vehicle 1, a locating and broadcasting device 2, called "mobile device", designed to determine the position and/or the speed of a vehicle and to transmit these items of locating information to a position server 3 responsible for storing and/or using them. The locating and broadcasting device comprises a receiver 4 of GNSS (Global Navigation Satellite System) navigation signals, such as a GPS (Global Positioning System) receiver, transmitted by a constellation of satellites 5a, 5b and a mobile communications transceiver 6.

The items of position information are calculated by the GNSS receiver 4 by means of the exploitation of signals 13a and 13b transmitted by the satellites 5a, 5b according to methods known to those skilled in the art.

Figure 2 is a simplified block diagram of the architecture of the system for authentication of the position of a mobile device according to the invention.

The path of the GNSS receiver on board a mobile device 1 is composed of a series of GNSS positions $X(t)$ estimated at times t , 21, with which are associated a position uncertainty ΔX and a time uncertainty Δt . The mobile device is called "true" and the positions "authentic" if the positions are calculated from
 5 "authentic" signal, that is to say transmitted by the GNSS constellation. The mobile device is called "fraudulent" and the positions "unauthentic" in the opposite case.

A module 22 makes it possible to determine consistency indicators. This module 22 notably receives the geographic data 23 and the GNSS position data.

A module 24 notably has the function of detecting suspect data or
 10 positions.

Different embodiments of the method are described below.

According to a variant embodiment, there is used, for example, a cartographic database centralized in one or more servers accessible from each of the receivers, which receive the positioning data. The service area of a server and of
 15 the database is determined in an implementation by a compromise between cost and performance. In a typical implementation, one base will cover a country or a region.

An alternative embodiment of implementation of the method according to the invention is to use a cartographic database duplicated in each item of mobile
 20 equipment. The modules 22 and 24 can also be produced either in the terminal or in a central server.

These variations relate to the implementation and not to the principle of the method, which is explained in the case of its centralized implementation.

A component for detecting suspect data 24, such as described in its
 25 general principle by patent No FR11/00961, for example, estimates one or more statistical indicators, 22, referenced $I_c(X)$, and X at the position of a receiver k at a given time.

As an indicator is affected by noise due to receiver measurement errors, cartographic errors and errors inherent in the principle of comparison, one or more
 30 filters are applied to the statistical indicators $I_c(X)$, for example by integrating these values $I_{c_{raw}}(X)$ over a path of the mobile element for a time period $[t_0, t_1]$, whose duration is chosen according to the application:

$Ic_{filtered}(X) = \int_{t_0}^{t_1} Ic_{raw}(X)$ where $Ic_{filtered}$ corresponds to the value of the indicator obtained after filtering and Ic_{raw} corresponds to the values that can be taken by the indicator over the time period $[t_0, t_1]$.

From these filtered values, it is possible to construct a function to decide on the authenticity of a position of a mobile device or of a receiver k fitted to the device.

For this purpose, it is typically possible to use a true/false logic value, a probability of fraud estimator $p(X)$ or values of possibility/necessity according to the fuzzy logic of Lofti Zadeh (Zadeh, L.A. (1965). "Fuzzy sets", Information and Control 8 (3): 338–353, Novák, V. "Are fuzzy sets a reasonable tool for modeling vague phenomena?", Fuzzy Sets and Systems 156 (2005) 341–348), this value being a numerical representation of a degree of confidence in the position P_k of the receiver k :

a logic flag $L(X) = Ic(X) > T$, $\in \{0;1\}$, where T is a chosen threshold value, or

a probability estimator $p(X) = f(Ic(X))$ where $f : [0; \infty[\rightarrow [0; 1]$ is an increasing function which normalises the indicator on $[0;1]$. This function is chosen from a model or by experimentation to be a valid estimator of the probability of fraud, adjusted using parameters.

For example: $p(X) = 2/\pi * \arctan(\beta Ic^m) \in [0;1]$ is continuous and satisfies these limits.

The parameterization values are, for example, the threshold value $T > 0$, or the factors $\beta > 0$ and $m > 0$. These values allow the adjustment of the decision according to the observed distribution of the indicator used over samples representative of real paths and of falsified paths for a given mobile device. β is defined as the inverse of the value Ic corresponding to a confidence probability of $1/2$ and m makes it possible to adjust the "slope" of the function.

$p(X)$ being the probability of spoofing, the complement $1-p(X)$ of this value is a probability of authenticity. This confidence indicator $Ic(n, X)$ probability $p(X)$ is obtained from one of the consistency indicators or statistical indicators 22 or a combination of certain of these indicators by applying methods known to those skilled in the art, those described in the patent FR11/00961, as well as one of the

four original types of indicator (passing close to a pseudolite, direction/speed compared with the road segment, direction/speed compared with the path, position compared with the model of the terrain) described below, exploiting the collaboration between receivers.

5 A) Pseudolites

In this method, shown diagrammatically in Figure 3, the system comprises a certain number of terrestrial transmitters called "pseudolites", transmitting a signal compatible with a GNSS constellation, which the existing GNSS receivers use for calculating their position, according to methods known to
 10 those skilled in the art: the position of the pseudolite being broadcast in the navigation message, or by assistance, or known by a centralized server which calculates the user position in "mobile-assisted" mode. Moreover, this pseudolite is distinguished in the calculation of the point by its PRN, and this fact allows the detector to recognize the reception or not from a pseudolite, referenced by the logic
 15 variable: visible(PL).

The idea is to install such pseudolites at certain control points (which is potentially less expensive, more discreet, and less restrictive than other control equipments). In a position-sensitive payment system, the installation of a pseudolite in a "virtual gate" validates the tariffing event associated with that gate. The
 20 authentication of the position consists in comparing the latter with the cover zone of the pseudolite. PL being the reception zone, if r_{PL} is the estimated reception radius for a receiver and the given environment, the position $X(t)$ of the mobile element is within the cover of the pseudolite if and only if: $|X(t) - X_{PL}| \leq r_{PL}$, as illustrated in Figure 3. The point 30 corresponds to an invisible element and the point 31 to a
 25 visible element.

If the position $X(t)$ of the mobile element is in this PL cover zone without the pseudolite being included in the calculation of the point, or if the position $X(t)$ is not in the PL zone whereas the pseudolite is included in the calculation of the point, then the signal used for calculating the position is in all likelihood not authentic.

30 It is possible to define a consistency indicator:

$$I_{CPL}(X) = \text{if visible(PL) then } |X(t) - X_{PL}| / r_{PL} \text{ otherwise } r_{PL} / |X(t) - X_{PL}|$$

B) Consistency of direction and speed shown diagrammatically in Figure 4.

In this variant embodiment, implemented in motor vehicle applications, the position indicated by the GNSS receiver is associated with a likely position $X_m(t)$ on the road system by "map-matching". In this diagram, the dotted line 41 represents the different positions $X(t)$ measured for the moving vehicle and the reference 40 represents the corresponding position on the road map.

θ being the angle calculated in the north-south reference system usually used in the road map field, θ_r being the angle of the vehicle calculated in the receiver in the terrestrial reference system, V_{map} being the speed defined by the cartography, as a function of the road segment in question, of the driving speed limit on this segment, V_r is the speed measured by the GNSS receiver of the moving vehicle to be monitored. The direction or directions θ_{map1} , θ_{map2} of the road segment (depending on whether it is classified as one-way or two-way) is compared with that of the vehicle θ_r , and, similarly, the theoretical speed V_{map} is compared with the measured speed V_r of the vehicle. A logic indicator $L(X)$ is set when the difference is greater than a respective threshold $\Delta\theta$, ΔV for at least one of these variables:

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

The threshold value $\Delta\theta$ is for example obtained by previously defined evaluation means.

This theoretical speed V_{map} is given either by the speed limit, or by the evaluation of the speed from the road classification and the topography (bends, elevations, ...). A lower speed is not considered suspicious. This indication is obviously ambiguous since a real excessive speed raises a false alarm.

A continuous indicator $I_{C_{Dir}}(X)$ is calculated as follows at a given time t :

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

Moreover, the comparison between the observed position $X(t)$ and the mapped position $X_m(t)$ on the road system is another indicator described in the patent FR1100961.

C) Speed compared with the path shown diagrammatically in Figure 5.

In this variant embodiment, the indicator directly compares the distance Dist, corresponding to the measured speed V_r times the time period between two measurements, with that calculated according to the path constituted by the series of positions $X(t_k)$, by carrying out a difference calculation for successive points, or by

calculating the length on the road graph which joins these successive points, which can differ greatly if the time period is not short or if the path is winding (access road, chicanes, ...).

This indicator establishes a consistency between observable
5 phenomena of the signal of each satellite (namely pseudo-range and frequency) which are dependent on the path of the moving object. The use of cartography in principle allows a rather exact measurement of the path travelled between two points, which should correspond to the speed defined in GNSS.

By including the calculation of length on the road graph, there is
10 furthermore detected a spoofing in the code and frequency phase but which would not have used this same graph for controlling the link between the two.

An indicator $Ic_{Dist}(X)$ can be calculated from the difference between the distance $D_r(t_k)$ corresponding to the speed measured in the GNSS receiver multiplied by the temporal difference between two times $t_{k+1} - t_k$ and the distance
15 $D_{map}(t_k)$ which is the distance measured between two measured points $X(t_k)$, $X(t_{k+1})$, or two projected points $X_m(t_k)$, $X_m(t_{k+1})$ on the road graph or road cartography:

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

$$D_r(t_k) = S_r(t_k) \times (t_{k+1} - t_k) \text{ and } D_{map}(t_k) = dist(X(t_k), X(t_{k+1})),$$

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

20 $dist$ being the distance as the bird flies or the curvilinear distance on the road graph.
D) Altitude compared with the terrain model.

For any person or land vehicle of position $X = (x_r, y_r, z_r)$, projected onto a land map at a point $(x_{map}, y_{map}, z_{map})$, the altitude z_r is assumed to conform with that z_{map} of the terrain, for the latitude and longitude x_r, y_r . The indicator can be
25 calculated from this difference on a path:

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

z_{map} is the altitude of the projection of the position on a land map, which may or may not take "map-matching" into account.

Claims

- 1 – Method for authenticating the position $X(t)$ of a mobile element (1), a mobile element comprising at least a GNSS receiver, r , having a function of estimating the position $X(t)$ of that mobile element (1), this method being characterized in that it comprises, in combination, at least the following steps:
- determining one or more items of data (21) associated with the position $X(t)$ of the GNSS receiver, r ,
 - extracting reference data associated with the position $X(t)$ of the said mobile element (1) from a map or road map cartographic database (23),
 - determining at least one consistency indicator (22) $I_c(X)$ using the first item of data associated with the said receiver r and the reference data coming from the cartographic database,
 - filtering the said indicator or indicators $I_c(X)$, in order to improve the detection rate or the false alarm rate,
 - authenticating (24) the position $X(t)$ of the said mobile element (1) using the result obtained by application of an authenticity decision function to one or more of the said consistency indicators $I_c(X)$.
- 2 – Method according to Claim 1, characterized in that the filtering step is a temporal integration of the indicator over a given period of time.
- 3 – Method according to Claim 1, characterized in that the establishment of the cartographic database (23) and the calculation of the consistency indicator are carried out in a centralized device connected by a communications network to the said mobile elements (1).
- 4 – Method according to Claim 1, characterized in that the establishment of the cartographic database (23) and the calculation of the consistency indicator are carried out within the said mobile elements (1).

5 – Method according to one of Claims 1 to 4, characterized in that in order to authenticate the position $X(t)$ of a mobile element (1), the consistency indicator $I_c(X)$ is calculated from the position of pseudolites indicated in the cartographic database.

5 6 – Method according to one of Claims 1 to 4, characterized in that in order to authenticate the position $X(t)$ of a mobile element (1), the consistency indicator $I_c(X)$ is calculated from the direction or directions θ_{map1} , θ_{map2} of a road segment travelled and/or the speed V_{map} estimated over this segment, from data indicated in the cartographic database.

10

7 – Method according to one of Claims 1 to 4, characterized in that in order to authenticate the position $X(t)$ of a mobile element(1), the consistency indicator $I_c(X)$ is calculated from, on the one hand, the distance travelled $D_r(t)$, estimated by the measured speed $V_r(t)$, and on the other hand the distance as the bird flies D_{map} , or
15 the curvilinear distance on a road graph in the cartographic database.

8 – Method according to one of Claims 1 to 4, characterized in that in order to authenticate the position $X(t)$ of a mobile element (1), the consistency indicator $I_c(X)$ is calculated from the measured altitude z_r , compared with that z_{map} indicated in the
20 cartographic database (23).