



**METHOD AND SYSTEM FOR DETECTING MOBILE DEVICE POSITION
INFORMATION FRAUD**

The subject of the present invention relates to a
5 method and a system for authenticating the GNSS
position, GNSS being an acronym deriving from the
expression "Global Navigation Satellite Systems", of a
mobile element or device. It aims to detect, not
jamming, but spoofing (the usurpation of a sender's
10 identity), and applies, for example, to the field of
road, motorway, urban remote toll systems and to any
other geolocated monitoring or payment system.

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

The mobile electronic terminals that implement
applications requiring information concerning their
geographical position comprise means for estimating
20 their position as accurately as possible. For this,
satellite geolocation systems are commonly used, these
systems being designated by the acronym GNSS. An
example of a GNSS system is the GPS system, GPS
standing for Global Positioning System.

25 The integrity of positions is a strong requirement in a
positioning application that is critical from a legal
point of view (pay-per-use system: insurance, parking
and road network notably), or a judicial application
30 (electronic bracelet or tag) just as in an application
that is critical from the viewpoint of security of
goods (tracking of containers), user safety (driving
assistance).

35 The equipment used in systems that implement this type
of application are usually inviolable and use secure
communication means. However, the radio link with the
satellites is an open and vulnerable signal, unless



to these markets because of the broadcasting and the management of the access keys.

It is consequently possible for a non-cooperative user
5 or an ill-intentioned person to induce false positions
in a receiver, even without interfering in the onboard
unit (OBU), and to do so with inexpensive equipment of
receiver-regenerator type, covering the antenna of the
receiver, that is also easy to set up surreptitiously.
10 Contrary to the equipment of jamming or of spoofing
emitting on a zone, attacking the service to the users
in this zone, such devices affect only a receiver, that
of the non-cooperative user. More or less complex
strategies can be implemented in a receiver-regenerator
15 to inject a GNSS signal corresponding to the desired
trajectory to bypass the application: for example, to
avoid the generation of an alert in monitoring
equipment, such as the electronic bracelet or the
charging events triggered by the passage through
20 virtual doors, in pay-per-use applications, and do so
while minimizing the risk of discovery. The systems
envisaged for these applications do not currently make
it possible to avoid such frauds.

25 The typical charging solution is based on passage
through a virtual gate or positioning in a paying area
(parking, town centre). The checking of the operation
of the vehicle equipment is done statistically on fixed
or mobile control points, where the consistency of the
30 charging events is checked a posteriori with the
registration details of the observed vehicles. Fraud
equipment can also be designed to be silent in these
checks, its position being published to such equipment
by a centralized service (official information for the
35 points that are fixed or shared by the users, for the
mobile points).

Different methods for checking the consistency of the position estimations do exist. This consistency can be checked by monitoring the absolute or relative strength of the GNSS signals or by comparison with secondary
5 sources such as motion sensors, or the measurement of other radio signals.

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

15 Moreover, the securing of the location applications presupposes known anti-tampering protection measures, on the securing of the exchanges, on the protection of the data originating from other sensors in the vehicle.

20 Such methods are not these days implemented in the available commercial receivers. For some, they assume a significant cost resulting from redesign work at the chip level and/or at the driver software level. In particular, redesigning the chip for receivers on the
25 consumer market represents a significant cost and leadtime. Other methods presuppose the addition of sensors in the mobile equipment: inertial units such as described in the application FR 1000588, measurement of radiofrequency signals or information of the cellular
30 network, for example, as described in the application FR 0807400. They are not guaranteed and sophisticated attacks can at least partially circumvent them.

The idea implemented by the present invention, unlike the existing approaches which generally require the
35 addition of secondary position information, or more sophisticated signal processing in the GNSS reception, is notably to use the information supplied by the receivers, of existing type, without requiring the use

of other sensors, in the case of normal operation of the device. This method is based on collaboration between receivers via a centralized infrastructure for example.

5

No hypothesis is made on the preliminary functioning of a receiver in normal mode without attack, but we shall suppose that proportion of receivers subject to cheating is enough weak so that statistical data can be
10 built, which are little affected by the possible devices of spoofing.

The receiver installed on a mobile vehicle collects the GNSS position information and transmits it to an
15 authentication module which combines and consolidates this information in a current and historical base, and computes confidence indicators on the measured trajectories from which a probability of fraud can be estimated, indicators which are based on:

- 20 • the quality of the signal received from a satellite, in a given area: the signal/noise density ratio, or C/N0 (carrier-to-noise density ratio), the user differential range error, better known by the acronym UDRE, or the global position quality: position
25 uncertainty,
- the signal quality compared to the history in this place,
- the azimuth, the elevation of the satellites seen compared to the historical map, and/or
- 30 • the associated cell in which a receiver may be located in a communication network.

The invention relates to a method for authenticating the position $P_1(t)$ of a mobile element, a mobile element
35 comprising at least one GNSS receiver, i, having a function for estimating the position $P_1(t)$ of this mobile element, from said signals "authentic" of the constellation GNSS, the aforementioned receiver being

potentially impacted by falsified signals, this method being characterized in that it comprises, in combination, at least the following steps:

- 5 • determining at least one datum associated with the position P_i of a GNSS receiver, i ,
- Transmitting and storing said data,
- aggregating a number of data associated with the position of a number of GNSS receivers belonging to a set $Ech(P_i)$, on a size of sample and a period of time superior to given thresholds, to
10 obtain a significant statistical data that is characteristic of the authentic signal,
- determining at least one consistency indicator $Ic(P_i)$, by comparing the first data associated with said receiver i and the aggregated data
15 obtained from the set Ech of receivers k , on an interval of time including at least a position $P_i(t)$,
- authenticating the position P_i of said mobile
20 element by using one or more of said consistency indicators $Ic(P_i)$ in an authenticity decision function or to raise a suspicion of fraud on behalf of the user of this receiver i , as regards the position P_i .

25

The aggregation and indicator computation steps are performed, for example, in a centralized device linked by a communication network to said mobile elements.

30 According to a variant the aggregation and indicator computation steps are performed within said mobile elements linked together and forming a network, following the principles of distributed computation.

35 To authenticate the position $P_i(t)$ of a mobile element the consistency indicator $Ic(P_i)$ is, for instance, computed on the basis of the strength $S_k(n, t)$ of signal received by the receiver k , by considering the

receivers k in the vicinity of the receiver 1, arranged at a range less than ε , at the instant (t_k) , with $t_k - t < \Delta t$, and Δt , ε being parameters of said consistency indicator, in which n is the pseudo range number (PRN) of a satellite in sight of the receivers.

According to a variant to authenticate the position $P_1(t)$ of a mobile element, according to a measurement associated with a satellite n , the method uses a set of samples obtained from a historical positions base, in which the position P_k of a sample at the instant t' and the orientation of the satellite n indicated by the azimuth, elevation pair $\alpha\theta(t',k)$ is sufficiently close to $P_1(t)$ and $\alpha\theta(t,1)$.

According to a variant to authenticate the position $P_1(t)$ of a mobile element, according to a global measure relating to all the satellites seen, the method uses a set of samples from a historical positions base, for which the position P_k at the instant t' is sufficiently close to $P_1(t)$.

The data aggregation step, for example, comprises, combining at least the following steps:

- the construction of a map of visibility of a satellite based on reports of positions of the receivers k stored in a database,
- analysis of the cloud of points in order to determine the density and the border,
- the computation of the probability estimate of finding a satellite n at a position P_1 as a function of the azimuth direction α , elevation θ , for an assumption as to the uncertainty of the direction ξ , and
- the probability $p(P_1, \{n\})$, as a consistency indicator is deduced from these probability estimates for each satellite PRN n , with $N_{sat} =$

$\text{card}(\{n\})$, in which $\{n\}$ is the set of the visible satellite numbers reported by the receiver i .

According to a variant the method constructs a table of
5 network cells based on the reports of the historical
positions X_h stored in the database and of contingent
information supplied by the communication network such
as the cell identity Cell-Id in a mobile cellular
network and in that it determines, as indicator of
10 consistency between the database and the candidate
position P_1 , a range metric between P_1 and the
aggregated positions X_h and in that it uses, as
authenticity function, the value of the probability
that the cell reported for the target receiver
15 corresponds to the position P_1) and the sample $E_{ch}(P_1)$
which serves as reference is the set of the positions
stored for this cell.

Method uses, for example, the measure and the decision
20 of authenticity in feedback on the selection of the
sample.

According to a variant said method uses a data
filtering mechanism excluding any past and future datum
25 concerning the terminal of a user for which at least a
suspicion of fraud is raised.

Method uses, for example, an obsolescence mechanism in
which the data for which the exactitude and utility are
30 diminished by age are deleted from the base, by
establishing obsolescence criteria adapted to the
datum, said criteria being chosen from the following
list:

- the code quality, strength, UDRE data are deleted
35 when the satellite n is the subject of a
notification by the control authority,

- the global quality, uncertainty and availability data are deleted when the constellation has been modified,
- 5 • the satellite visibility data are deleted when the positive spoofing indicator frequency on the same place to within ε is above an observed likelihood threshold,
- 10 • the cell data are deleted when the positive spoofing indicator frequency on the same cell is above an observed likelihood threshold,
- any datum is deleted when an age limit is reached,
- or any other criterion characterizing the possible obsolescence of the datum.

15 Method uses, for example, a data filtering mechanism excluding any past and future data relating to a place on which the false alarm rate exceeds a defined threshold.

20 The invention also relates to a system for authenticating the position $P_1(t)$ of a mobile element, a mobile element comprising at least one GNSS receiver, k , having a function for estimating the position $P_1(t)$ of this mobile element, characterized in that it comprises at least the following elements:

- a location and broadcasting device suitable for determining the position and/or the speed of a mobile element and for transmitting this location information to a position server responsible for storing and/or using said information,
- 30 • a receiver of GNSS navigation signals transmitted by a constellation of satellites and a mobile communication transceiver,
- 35 • a database containing reference data originating from these receivers,
- a processing module executing a data aggregation process,

- a module for determining consistency indicators which receives data, the GNSS position values and from the base,
- a module for detecting suspect data or positions of a mobile element.

Other features and advantages of the present invention will become more apparent on reading the description of an illustrative and nonlimiting example with appended figures which represent:

- Figure 1, an example of a system for locating a mobile device, such as a vehicle, by satellite,
- Figure 2, a diagram of the various elements involved in the method and the system according to the invention,
- Figure 3, an illustration of the space-time vicinity of a point P_1 ,
- Figure 4, an illustration of the satellite orientation and of the definition masking,
- Figure 5, a map according to azimuth and elevation of visibility at a point,
- Figure 6, the measurement of range to the cloud observed,
- Figure 7, an illustration of the spatial vicinity and orientation for a satellite observation at a point P_1 , and
- Figure 8, a representation of a cell reconstruction topology.

To sum up, generically, the method according to the invention for authenticating the GNSS position of a mobile device without having recourse to a second position source, and by using the architecture of the receivers currently used, consists notably in evaluating the temporal consistency and/or the spatial consistency of the positioning information transferred between a number of users.

Figure 1 represents an example of location of a mobile element 10 by satellite, the mobile element being able to be a vehicle. The location system comprises, onboard the vehicle 10, a location and broadcasting device 2, called "mobile device", intended to determine the position and/or the speed of a vehicle and to transmit this location information to a position server 3 responsible for storing it and/or using it. The location and broadcasting device comprises a receiver 4 of GNSS (Global Navigation Satellite System) signals, such as a GPS (Global Positioning System) receiver, transmitted by a constellation of satellites 5a, 5b and a mobile communication transceiver 6.

The position information is computed by the GNSS receiver 4 through the use of signals 13a and 13b transmitted by the satellites 5a, 5b according to methods known to those skilled in the art.

Figure 2 schematically represents, in a simplified manner, the architecture of the system for authenticating the position of a mobile device according to the invention.

The trajectory of the GNSS receiver installed on a mobile device consists of a series 21 of GNSS positions $P_1(t)$, estimated at instants t which have associated with them a position uncertainty ΔP and a time uncertainty Δt . The mobile device is said to be "true" and the positions are "authentic" if they are computed from "authentic" signals, that is to say signals transmitted by the GNSS constellation. The mobile device is said to be "fraudulent" and the positions "not authentic" in the contrary case.

35

The data 21 relative to a position P_1 of a receiver GNSS, k , will be transmitted and memorized in a centralized device, not represented on the figure for

reasons of simplification, within a database 24, the centralized device will be connected by a communication network to the mobile elements 10. Another way of process is to memorize these data within the mobile
5 elements 10, the aforementioned elements being interconnected and forming a network to exchange such data, according to the principles of the distributed calculus.

10 One of the objectives of the system is, notably, to determine the authenticity of the position of a GNSS receiver by using the collaboration between receivers k via a centralized infrastructure, for example the position server 3 (Figure 1) which allows for the
15 comparison of recent or historical positioning data supplied by the various user receivers, without identification, in order to guarantee respect for privacy. It is also possible to use a decentralized infrastructure by equipping each of the receivers k
20 with means suitable for executing the steps of the method according to the invention.

The sample E_{ch} of the reference data associated with the receivers which are taken into account to determine the
25 authenticity is, for example, obtained from a statistical base 24 which combines and consolidates data such as:

- the position, the speed, the direction, of a mobile device equipped with a GNSS receiver,
- 30 • the signal number from the satellite or PRN (Pseudo-Random Number), the value of the user differential range error (UDRE) and the ratio C/N_0 (carrier-to-noise density ratio) of the visible satellites.

35 The process according to the invention is going to select a relevant sample E_{ch} of data, from positions of the other receivers, for example, on criteria as the nearness or proximity in the space and according to

indicator type, nearness in orientation or of nearness in the time.

An optional almanac of the constellation of satellites, 5 23, supplies the (elevation, azimuth) pairs of the satellites theoretically visible by a receiver k . The values (elevation, azimuth) are either computed as and when needed, or stored with the other position data to speed up the computation of the indicator as will be 10 described below. The almanac 23 is used to determine the indicators of historical quality and visibility type.

The function of a processing module 22 is notably to 15 execute a data aggregation process according to methods known to those skilled in the art, by optimizing the statistical computations which are presented hereinbelow for each of the indicators described below. The statistical operation on this sample extracts an 20 average (the sum of measures on Ech divided by card (Ech)) or the border of a cloud of point (type of indicators " map of visibility " and " map of networks "). The result of this aggregation is a statistical data 25 little affected by equipments spoofing or swindler, the number of these equipments being weak in the sample Ech. This characteristic measure of the authentic signal, relevant for a position P_1 , is considered as an autonomous reference for the position P_1 .

30

As described in the following equations, the calculation of indicators, without contribution of technology of secondary positioning, and without period devoid of attacks, bases itself on no predetermined 35 data, but the reference emerges from stored data. The capacity of authentication appears after the initiation of the database, the quality of this reference being increasing with time since the

initialization of the device and the number of concerned receivers.

5 The module processing 22 contains, for example, at least one mechanism of filtering receiving the results, which modifies the composition of samples, and has the effect of decreasing the frequency of erroneous results.

10 The feedback in the device between decision of authenticity and selection of sample, realizes a learning process within the system formed by the receivers and the proposed device. This feedback on the selection of the sample is known to improve the
15 reliability of the device.

The function of the aggregation of data in a statistical base 24 is notably to retain, in an optimum manner, consistent data obtained from the authentic
20 signals received by the GNSS receivers. The use of this base 24 can be done with data obtained from terminals known to be true, or a large majority of true terminals is assumed from the outset. Three mechanisms are, for example, provided for aggregating data, aiming to
25 increase the robustness of the system to the errors present in the collected data, and therefore the detection efficiency.

A module 26 makes it possible to determine consistency
30 indicators. This module 26 notably receives the data from the almanac 23, the GNSS position values and from the base 24.

The function of a module 27 is notably to detect the
35 suspect data or positions.

The system comprises a filtering mechanism by which the doubtful data are excluded from the base 24, on the

basis of the available detection mechanisms, notably the data of a doubtful user (for whom there has been proven or assumed fraud). This filter excludes from the base any past and future datum concerning the terminal
5 of a user for whom at least a suspicion of fraud is raised by the spoofing detection, or by any other checking means. This filtering targets the quality of the base used as reference, in order not to depend on the proportion of honest users. The filtering mechanism
10 is, for example, implemented in the module 22.

A filtering mechanism excludes from the base 24, the places on which the detection is not reliable, in order to prevent the false alarms due to the highly variable
15 multiple paths and local environments. This filter excludes from the base any past and future datum concerning a place on which the false alarm rate exceeds a defined threshold.

20 An obsolescence mechanism is used to delete from the base 24 the data for which the exactitude and the utility are diminished by age, and does so by establishing obsolescence criteria suited to a datum. Examples of criteria are given below for several types
25 of data.

This method involves a set of mobile and connected terminals. Two implementations of the method are described: centralized and distributed.

30 The use is made, for example, of a database centralized in one or more servers that can be accessed from each receiver, which receive the positioning data. The service area of a server and of the database is
35 determined in an implementation by a trade-off between cost and performance. In a typical implementation, a base will cover a country or a region.

An alternative implementation of the method according to the invention is to use a database that is distributed between a number of servers in the communication network, or even the sharing of this
5 information between mobile equipment. The direct collaboration between receivers may be based on ad-hoc dynamic groups (a group being defined by a radius or a number of terminals).

10 The modules 26 and 27 may be implemented either in a GNSS terminal or in a central server 3. In the case of a totally decentralized implementation, each of the receivers reconstructs the data needed to compute the indicator by interacting with the receivers belonging
15 to the sample and itself evaluates the spoofing criteria.

These variations relate to the implementation and not the principle of the method, explained in the
20 centralized implementation. In this case, the techniques "known to those skilled in the art" in distributed computing, services qualified as "peer-to-peer", as well as the cognitive science field of collaborative problem solving, are applied in order to
25 perform the aggregation function and the indicator computation within the mobile device.

The algorithms used allow for the aggregation of data on a relevant scale according to the consolidated
30 datum. The aggregation of a sufficient number of positions, or the sample E_{ch} illustrated in Figure 3, as a vicinity of the point P_1 , increases the confidence in the average measurements, as long as the temporal and spatial deviation (limited by Δt and ε respectively) of
35 these positions does not result in the dispersion of these measurements. It will be noted that the data aggregation step uses statistical techniques "known to those skilled in the art", to optimize the search in

the base and the computations. In the formulae presented below, the sum of measurements on E_{ch} divided by $\text{card}(E_{ch})$ has been chosen for the aggregation means or aggregator. To optimize the detection, this value
5 may, in certain cases, be pre-computed, and stored in the base.

The module 27 for detecting suspect data or positions, may be identical to the one described in its general
10 principle by patent No. FR11/00961, for example, which estimates one or more statistical indicators, module 26, denoted $I_c(P_i)$ or $I_c(n, P_i)$ in which n corresponds to a satellite number, and P_i to the position of a receiver i at a given instant, from which it is
15 possible to construct a decision function concerning the position authenticity of a mobile device or of a receiver i mounted on the device. To this end, it is possible to use, typically, a true/false logic value, a fraud probability estimator $p(P_i)$ or
20 possibility/necessity values 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 -
25 348), this value being a digital representation of a degree of confidence in the position P_k of the receiver k :

- logic flag $L(P_i) = I_c(n, P_i) > T, \in \{0;1\}$, in which T is a chosen threshold, or
- 30 • probability estimator $p(P_i) = f(I_c(n, P_i))$ in which $f: [0; \infty[\rightarrow [0; 1]$ is an increasing function which standardizes the indicator on $[0;1]$. This function is chosen from a model or experimentation to be a valid estimator of the probability of fraud, adjusted using
35 parameters.

For example: $p(P_i) = 2/\pi \cdot \arctan(\beta \cdot I_c^m) \in [0;1]$ is continuous and satisfies these bounds.

The parameterizing values are, for example, the threshold value $T > 0$, or the factors $\beta > 0$ and $m > 0$. They allow for the adjustment of the decision according to the observed distribution of the indicator used on samples representative of real trajectories and of falsified trajectories for a given mobile device. β is defined as the inverse of the value I_c corresponding to a probability of confidence of $\frac{1}{2}$. m can be used to set the "ramp" of the function.

Since $p(P_1)$ is the probability of spoofing, the complement $1-p(P_1)$ to this value is a probability of authenticity. This probability $p(P_1)$ confidence indicator $I_c(n, P_1)$ is obtained from one of the consistency indicators or statistical indicators or a combination of some of these indicators by applying the methods known to those skilled in the art, those described in the patent FR11/00961, and at least one of the four original types of indicator: real time quality, historical quality, visibility, network, described below, using the collaboration between receivers.

Signal quality in real time

One possibility of implementing the invention consists in detecting the spoofing by using a signal quality index, when an apparatus transmits to a GNSS receiver GNSS signals generated or transformed from authentic signals (receiver-regenerators). In practice, such a device transmits a set of signals with propagation delays an alleged location. However, this "spoofing" cannot imitate the quality of the signal which is received at a given location. In practice, the spoofing device is not exactly at the alleged position; as a matter of fact it cannot, without a collaboration of

other receivers, be capable of reproducing the quality of the signal at this place.

5 The signal quality data computed for a receiver are compared to the signal quality data reported by the receivers that are closest, signal strength, uncertainty as to the user position, absence of position.

10 A real-time collaboration is possible by taking into account a significant population of receivers, which is the case of road toll. One alternative is to perform a historical comparison with data originating from the cooperative devices.

15

These characteristics of GNSS signals (received by the central server in the example of a centralized service) are managed, for example, in real-time collaboration:

- the satellite numbers being tracked by the receiver
20 (Tracked PRN) depend on the location, on the instant, on the obstacles, on the multiple paths,
- signal-noise ratio (C/N0) for each satellite (PRN) received, relative to the total signal, depends on the interference, reflections and maskings (notably
25 by foliage).

Signal/frequency noise ratio (C/N0) of the signal

30 The idea implemented by the method according to the invention is, in this exemplary embodiment, to construct an indicator comparing the C/N0, either absolute or relative (the instantaneous value divided by a chosen reference value, as the average over a given interval) of a signal received by a mobile device
35 to the average of C/N0 of a signal associated with other receivers in a given temporal sample.

Let $S_1(n, t)$ be the ratio C/N0 of the signal received on a first receiver 1, for a location or an alleged position $P_1(t)$. Since this value $S_1(n, t)$ depends on the receiver, on the antenna and on the installation thereof on the mobile element, the recommended method is to use a relative measurement in order to dispense with the differences between terminals k . $S_1(n, t)$ is subjected to random variations. In order to minimize the false alarm rate, the indicator Ic_s is expressed by integrating over the duration of this interval $[t_0; t_1]$, containing a sufficient number of measurements, this relative C/N0, divided by a chosen reference value, and this ratio being compared to the values of the relative C/N0 of the received signals $S_k(n, t)$, on a specific sample $E_{ch}(P_1)$ of receivers k . The position P_k of each of the receivers k is stored in the database and the method will consider the receivers k in the vicinity of the receiver 1 arranged at a range less than ε , at the instant (t_k) , $|t_k - t| < \Delta t$.

20

Let $E_{ch} = \{k \text{ such that } (P_k, P_1) < \varepsilon \text{ and } |t_k - t| < \Delta t\}$ (0)

in which $d(P_k, P_1)$ is the range between two transmitter positions or locations, and Δt , ε are parameters for the vicinity in time and space of the measurement $P_1(t)$ to be checked.

The indicator Ic_s of the C/N0 of the signal received by a receiver k over a time interval $[t_0; t_1]$ is expressed as follows:

30

$$Ic_s(n, P_1) = \int_{t_0}^{t_1} \left\| \frac{S_1(n, t)}{\dot{S}_1} - \frac{\sum_{E_{ch}} \frac{S_k(n, t_k)}{\dot{S}_k}}{card(E_{ch}(P_1))} \right\|^p \quad (1) \text{ with } E_{ch}(P_1) \text{ defined in (0)}$$

35 in which the notation $\dot{S}_k$ (dot over S_k) signifies a reference value of S_k as the average over a larger time

sample than the interval $[t_0; t_1]$, p being chosen according to statistical criteria ($p=1$ combines the deviations as absolute value, and $p=2$ as quadratic) and n is the number of a satellite in view of the receivers. The formula for the absolute C/N_0 is (1) with $\dot{S}_1 = \dot{S}_k = 1$.

User error

According to another way of proceeding, it is possible to determine an indicator based on statistics from measurements of quality of these signals received by the receiver k , such as user differential range error (UDRE) by satellite PRN, inherent in the transmitted signal. The position uncertainty also depends on these range errors between satellite and user, on the number of satellites used, on the indicator concerning the position of satellites, better known by the acronym DOP (Dilution of Precision), on the propagation delay in the ionosphere, and on the strengths (C/N_0). A consistency indicator is then constructed on the basis of the UDREs:

$$I_{C_U}(n, P_1) = \int_{t_0}^{t_1} \left\| \frac{U_1(n, t)}{\dot{U}_1} - \frac{\sum_{E_{ch}} \frac{U_k(n, t_k)}{\dot{U}_k}}{\text{card}(E_{ch}(P_1))} \right\|^p \quad (2)$$

25

in which $U_k(n, t_k)$ is the UDRE value computed by the receiver k at the time t , and the formula is similar to the formula (1), since the definition of $\dot{U}_k$, p and n in which the notation $\dot{U}_k$ (dot over U_k) signifies a reference value of U_k .

The absence of GNSS position, if the cases of startup of the receiver, or of failure of the receiver itself

35

are excluded, is due notably to interference, reflection and masking. Typically, in a road path, such interruptions appear when passing under a bridge or through a tunnel.

5

The absence of GNSS position is reflected by a logic value $O_1(t)$, which can be compared to the unavailabilities undergone by another user by using a "global" indicator determined as follows:

10

$$Ic_o(P_1) = \int_{t_0}^{t_1} \left\| O_1(t) - \frac{\sum_{E_{ch}} O_k(t_k)}{\text{card}(E_{ch}(P_1))} \right\|^p \quad (3)$$

It will be noted in the formulae (1), (2), (3) that the data are compared over times t , t_k which are very close
15 and the sample E_{ch} is defined at (0) by the instantaneous range of the receivers.

To combine these indicators $Ic_s(n, P_1)$ or $Ic_u(n, P_1)$ of "code" quality (by satellite) into a single "global"
20 indicator, an average is then applied to all the visible satellites according to the formula:

$$Ic_s(P_1) = \sum_{VIS} Ic_s(n, P_1) / \text{card}(VIS),$$

$$\text{or } Ic_u(P_1) = \sum_{VIS} Ic_u(n, P_1) / \text{card}(VIS),$$

)

25

2) Signal quality history

According to another implementation, it is possible to determine indicators by using historical data resulting
30 from a storage of positions for a number of users or receivers over time. These data have already been accumulated in proximity to the position P_k of a receiver to be checked. This method makes it possible to base the computation on a sufficient sample, when
35 the instantaneous sample E_{ch} is too small. However, it

does require filtering on azimuth and elevation, which conditions the measurements of the signal from a satellite, as illustrated in Figure 4. A distinction will be drawn for global measurements (relating to all
 5 the satellites seen, see formulae 5 and 6) or measurements for a satellite at the same elevation and azimuth relative to P_k (formulae 8 and 9).

The measurements of global signal quality, user and
 10 unavailability (I_{c_s} , I_{c_u} and I_{c_o}) may be associated with a single position, with no relation to time; thus, the global indicators use the definition of the sample $E_{ch} = \{k : d(P_k, P_1) < \varepsilon\}$.

15 Thus, the historical user uncertainty indicator and the set of samples considered are

$$I_{c_l}(P_1) = \int_{t_0}^{t_1} \left\| \frac{I_1(t)}{I_1} - \sum_{(t', k) \in E_{ch}} \frac{I_k(t')}{I_k} \right\| / \text{card}(E_{ch}(P_1)) \Big\|^p, \quad (5) \quad \text{with}$$

$E_{ch}(P_1)$ defined above.

20 Since the absence of GNSS reception is specified to a total masking situation, it is also possible to directly define the global indicator without reference to the orientation:

$$25 \quad I_{c_o}(P_1) = \int_{t_0}^{t_1} \left\| O_1(t) - \frac{\sum_{(t', k) \in E_{ch}(P_1)} O_k(t')}{\text{card}(E_{ch}(P_1))} \right\|^p, \quad (6)$$

with $E_{ch}(P_1)$ defined above.

The global quality data (uncertainty and availability)
 are deleted when the constellation has been modified
 30 (satellite removed or added).

However, the measurements on a satellite PRN (UDRE, C/N0) are mandatorily associated with the user position and with the orientation of the satellite. From this
 35 orientation of the satellite devolve the range to the

satellite, the maskings, the reflections at this point, which because of this determine the attenuation and the multiple-path, and ultimately the measured strength, and the pseudo-range error.

5

The C/No, UDRE data are initially associated in the base 24 with a receiver k and with an instant t, and, by derivation, with the satellite orientation, given by the two angles (azimuth, elevation) at the reported
10 point P(k), by computing, from the almanac 23, the position of the satellite n at the instant t.

The code quality data (strength, UDRE) are deleted when the satellite n is the subject of a notification by the
15 control authority (called NANU).

On a given satellite, the set $E_{ch}(P_1)$ of the samples taken into account for the computation of the indicators (I_{cs} , I_{cu} , I_{co}) on a measurement of strength
20 W_1 is defined in addition by a limit value ξ with a range function (as maximum, Euclidian) between the pair of angles (α, θ) representing the satellite orientations of the receiver k and the angles for the target receiver 1:

25
$$E'_{ch}(P_1) = \{t', k : d(P_k(t'), P_1(t)) < \varepsilon \text{ et } d((\alpha\theta(t, 1)), (\alpha\theta(t', k))) < \xi\} \quad (7)$$

in which α is the azimuth and θ the elevation of the satellite n for the user at P_k , at the instant t' , or the pair $\alpha\theta(t', k)$, and similarly $\alpha, \theta(t', k)$ for the
30 checked position P_1 at the instant t. This is illustrated in Figure 7 where each axis in fact represents two dimensions.

By modifying the formulae (1), (2), (3) to use the
35 history, the data are compared for the instants t' , and the sample $E'_{ch}(P_1)$ is defined in position and time, in addition to the range of the receivers by an angular orientation range of the satellite received. The

formulae (4), (5), (6) are thus obtained respectively for the indicators (I_{c_s} , I_{c_u} , I_{c_o}), in which the data are compared on one and the same time t .

- 5 The consistency indicator based on the signal strength, and the "pseudo range" error become, respectively:

$$I_{c_s}(n, P_1) = \int_{t_0}^{t_1} \left\| \frac{S_1(n, t)}{\dot{S}_1} - \frac{\sum_{(t', k) \in E'_{ch}(P_1)} \frac{S_k(n, t')}{\dot{S}_k}}{\text{card}(E'_{ch}(P_1))} \right\|^p, \quad (8) \quad \text{with } E'_{ch}(P_1) \text{ defined above.}$$

10

with t' a variable time over which the measurements are performed,

$$I_{c_u}(n, P_1) = \int_{t_0}^{t_1} \left\| \frac{U_1(n, t)}{\dot{U}_1} - \frac{\sum_{(t', k) \in E'_{ch}(P_1)} \frac{U_k(n, t')}{\dot{U}_k}}{\text{card}(E'_{ch}(P_1))} \right\|^p, \quad (9) \quad \text{with } E'_{ch}(P_1) \text{ defined above.}$$

15

These indicators can be consolidated for each observed satellite, as given by the formulae (4).

20 3) The visibility history map (azimuth, elevation)

Another consistency indicator 26 is based on the visibility of satellites. For this, the aggregation step 22 involves constructing a map of visibility of satellites based on the historical position reports, in any place defined typically by an interval of coordinates in a given reference, bearing in mind that the visibility is determined mainly by fixed obstacles such as assemblages, buildings and a density of leaves or forests. Thus, the possible orientation of the visible satellites is an envelope of all the

30

occurrences received by any receiver in a given position, illustrated in Figure 6.

This observed visibility being very variable in urban,
5 forested or mountainous zone, is a discriminating measure with regard to the real position. On the other hand, the visibility following the almanac can be identical on hundreds of km. The statistical method of construction of such a map of visibility thus presents
10 a decisive advantage of relevance as criterion of detection of spoofing with regard to the use of almanac, and on the other hand an economic advantage compared with other methods of forecast of the visibility.

15 A consistency indicator is defined between the visibility map and each satellite reported as being visible or not accordance to the position of a candidate or of a receiver. The reference procedure for
20 this principle is to compute the probability estimate $E(n, P_k)$ of seeing the satellite n at a point P_k , at the orientation (α, θ) , from the negative form of Figure 6, extracted from the cloud of the satellites of orientation (α, θ) seen at this point P_k , to within ε ,
25 the observations being stored in the historical base H .

The inclusion of an observation at a point Y , under the orientation (β, ρ) , in this cloud, is defined according to a measure of distance in a system of coordinates
30 chosen (for Example $\max_i (x_i - y_i) < \varepsilon$ or x_i , resp y_i being coordinates (latitude, longitude, height) in the WGS84 (World Geodetic System - on 1984) for the positions P_1 and Y), and in a similar way a distance between (α, θ) and (β, ρ) .

35

The **probability estimate** of a satellite visibility is computed as a function of the range inside or outside

of this cloud, and of the density of the cloud. The more dense the cloud is inside, and empty outside, the more "rigid" the function may be because the knowledge of the visibility is unambiguous. However, the appearance of dispersed orientations would be a sign of local conditions (partial or temporary maskings, or multiple-paths), which render the indicator less certain. In order to increase the detection robustness to these conditions, the satellite visibility data are deleted when the positive indicator (or spoofing) frequency at the same place (to within ε) is above an observed likelihood threshold (environmental filter as described above).

The probability estimate of finding a satellite n at a position P_1 as a function of the direction α_n , θ_n , (azimuth, elevation) given by the almanac, for an assumption concerning the uncertainty of the direction ξ , is obtained by the following formula:

$$E(n, X) = E(\alpha_n, \theta_n, \text{ knowing } X) = 1 - \frac{\text{Min}(d(\alpha, \theta, \alpha_n, \theta_n), (X_h, \alpha, \theta) \in H, d(X, X_h) \leq \varepsilon)}{\partial \alpha, \partial \theta}$$

in which (α, θ) are observations of satellites associated with a historical position X_h and

$(\delta \alpha, \delta \theta)$ the acceptable deviations defined by the cloud of the observations.

The statistical indicator deduced from these probability estimates is therefore the probability $P(P_1, \{n\})$ combining the probability for each satellite PRN n , which aggregates the probability with $N_{\text{sat}} = \text{card}(\{n\})$, in which $\{n\}$ is the set of the numbers of visible satellites reported by the target receiver, done by a known method.

4) The network history map (Position, Cell)

Figure 8 schematically represents another way of proceeding consisting in constructing a table of network cells from the reports of the historical positions X_h of a receiver $i=1$ in a cell, and
5 contingent information supplied by the communication network, upon the reporting of the positions by the mobile device, then using said table of cells to check the positions reported by the target receiver. The principle is illustrated with the cell identity Cell-Id
10 in a mobile cellular network obtained by the communication network according to a method known to those skilled in the art.

The collaborative building of this cross-reference
15 table cells and positions presents an economic advantage with regard to the network use of data existing as criterion of authentication.

The indicator of consistency between the database and
20 the candidate position X is a metric of range $d(P_1, X_h)$ between P_1 and the aggregated positions X_h in the database H .

The probability that the cell C_{id} reported for the
25 target receiver $i=1$ corresponds to the reported position P_1 is computed on the basis of the near positions stored in the base, or: $P(\text{cell}=C_{id}, \text{knowing } P_1)$
)=

$$p(\text{cellule} = C_{id}, \text{knowing } P_1) = \frac{\sum_{(X_h, C_{id'}) \in H} d(P_1, X_h)}{\sum_{(X_h, C_{id'}) \in H} d(P_1, X_h)} \quad (11)$$

30 in which this denominator is calculated only once for the complete base (or for all the $C_{id'}$), and the sample $E_{ch}(P_1)$ which serves as reference is the set of the positions of a receiver k stored for this cell. The learning of the field of each cell by the base
35 is illustrated in Figure 8.

It will be noted that the method uses the Cell-Id as a tag associated with the GNSS positions during the aggregation, and does not require any secondary position by a method of "network" type. In that, it
5 differs from the comparison of the GNSS position with the true network position, already described in the patent FR0807400.

The deletion of obsolete data can be triggered when a
10 number of alarms reflecting a possibility of fraud in the value of the position transmitted are raised on the same cell within a short time (above a likelihood threshold), which implicate the validity of these data, or simply after a fixed age. Since the data are stored
15 permanently, sufficient valid data remain for the check.

The aggregation of the data for statistical purposes comprises techniques "known to those skilled in the
20 art", in order to optimize the storage space and the search in the base and the statistical computations in the indicators. For example, the sums of measurements divided by $\text{card}(E)$ are aggregators of the data (k,t) on a subset of the base, which can in certain cases be
25 precomputed. Very close data can be replaced in the base by an average datum, without substantially modifying the principle explained.

It should be noted that it is essential to manage, in
30 this base, the obsolescence of the data, the relevance of the measurements observed being able to be challenged by modifications to the environment. For example, the coverage of a cell is modified with any change to the topology of the network.

35

The method and the system according to the invention make it possible to avoid subtle fraud mechanisms which would try to avoid the events triggering road charging

(areas or virtual gate) or attacks aimed at the security of goods or of people.

5 The solution ought to allow for a high fraud detection percentage, even subtle fraud, from inexpensive hardware equipment. No addition or modification is needed on the existing GPS receiver. It supplies incriminating information that may possibly serve as proof.

10

Finally, the use of these criteria outside of a pay-per-use context also makes it possible to improve the integrity in urban areas.

15 The collaboration of the users, most of them "non defrauders" (true terminals with authentic navigation signal) makes it possible to detect the "defrauding" users who report information inconsistent with this signal, and with no additional sensor in the mobile
20 equipment, and also with no change to the GPS receiver.

CLAIMS

1. Method for authenticating the position $P_i(t)$ of a mobile element (10), a mobile element comprising at least one GNSS receiver, k , having a function for estimating the position $P_i(t)$ of this mobile element (10), from said signals "authentic" of the GNSS constellation, the aforementioned receiver being potentially allocated by falsified signals, this method being characterized in that it comprises, in combination, at least the following steps:
- determining at least one datum (21) associated with the position P_i of a GNSS receiver, i ,
 - Transmitting and storing said data (21),
 - aggregating a number of data (22) associated with the position of a number of GNSS receivers belonging to a set $Ech(P_i)$, on a size of sample and a period of time superior to given thresholds, to obtain a significant statistical data (25) characteristic of the authentic signal,
 - determining at least one consistency indicator $Ic(P_i)$, (26), by comparing the first datum associated with said receiver i and the aggregated data (25) obtained from the set Ech of receivers k , on an interval of time including at least a position $P_i(t)$,
 - authenticating (27) the position P_i of said mobile element (10) by using one or more of said consistency indicators $Ic(P_i)$ in an authenticity decision function or to raise a suspicion of fraud on behalf of the user of this receiver i , as regards the position P_i .
2. Method according to Claim 1, characterized in that the aggregation and indicator computation steps are performed in a centralized device linked by a

communication network to said mobile elements (10).

3. Method according to Claim 1, characterized in that
5 the aggregation and indicator computation steps are performed within said mobile elements (10) linked together and forming a network, following the principles of distributed computation.
- 10 4. Method according to Claim 1, 2 or 3, characterized in that, to authenticate the position $P_1(t)$ of a mobile element (10), the consistency indicator $I_c(P_1)$ is computed on the basis of the strength $S_k(n, t)$ of signal received by the receiver k , by
15 considering the receivers k in the vicinity of the receiver 1, arranged at a range less than ε , at the instant (t_k) , with $t_k - t < \Delta t$, and Δt , ε being parameters of said consistency indicator, in which n is the satellite number in sight of the
20 receivers.
5. Method according to Claim 1, 2 or 3, characterized in that, to authenticate the position $P_1(t)$ of a mobile element, according to a measurement
25 associated with a satellite n , the method uses a set of samples obtained from a historical positions base, in which the position P_k of a sample at the instant t' and the orientation of the satellite n indicated by the azimuth, elevation pair $\alpha\theta(t', k)$ is sufficiently close to
30 $P_1(t)$ and $\alpha\theta(t, 1)$.
6. Method according to Claim 1, 2 or 3, characterized in that, to authenticate the position $P_1(t)$ of a
35 mobile element, according to a global measurement relating to all the satellites seen, the method uses a set of samples from a historical positions

base, for which the position P_k at the instant t' is sufficiently close to $P_1(t)$.

- 5 7. Method according to Claim 1, 2 or 3, characterized in that the data aggregation step comprises in combining at least the following steps:
- the construction of a map of visibility of a satellite based on reports of positions of the receivers k stored in a database (24),
 - 10 • analysis of the cloud of point in order to determine the density and the border,
 - the computation of the probability estimate of finding a satellite n at a position X as a function of the azimuth direction α ,
15 elevation θ , for an assumption as to the uncertainty of the direction ξ , and in that the probability $p(P_1, \{n\})$ is deduced from these probability estimates, as consistency indicator for each satellite PRN n , with N_{sat}
20 = $\text{card}(\{n\})$, in which $\{n\}$ is the set of the visible satellite numbers reported by the receiver k .
- 25 8. Method according to Claim 1, 2 or 3, characterized in that said method constructs a table of network cells based on the reports of the historical positions X_h stored in the database (24) and of contingent information supplied by the communication network such as the cell identity
30 Cell-Id in a mobile cellular network and in that it determines, as indicator of consistency between the database and the candidate position X , a range metric between X and the aggregated positions X_h and in that it uses, as authenticity function, the
35 value of the probability that the cell reported for the target receiver corresponds to the position X and the sample E_{ch} which serves as

reference is the set of the positions stored for this cell.

- 5 9. Method according to Claim 1, 2 or 3, characterized in that it uses, uses the measure and the decision of authenticity in feedback on the selection of the sample.
- 10 10. Method according to Claim 9, characterized in that it uses a data filtering mechanism excluding any past and future datum concerning the terminal of a user for which at least a suspicion of fraud is raised.
- 15 11. Method according to Claim 1, 2 or 3, characterized in that it uses an obsolescence mechanism in which the data for which the exactitude and utility are diminished by age are deleted from the base (24), by establishing obsolescence criteria adapted to
20 the datum, said criteria being chosen from the following list:
 - the code quality, strength, UDRE data are deleted when the satellite n is the subject of a notification by the control authority,
 - 25 • the global quality, uncertainty and availability data are deleted when the constellation has been modified,
 - the satellite visibility data are deleted when the positive spoofing indicator frequency on the
30 same place to within ϵ is above an observed likelihood threshold,
 - the cell data are deleted when the positive spoofing indicator frequency on the same cell is above an observed likelihood threshold,
 - 35 • any datum is deleted when an age limit is reached,
 - or any other criterion characterizing the possible obsolescence of the datum.

12. Method according to one of Claims 9, characterized
in that it uses a data filtering mechanism
excluding any past and future data relating to a
5 place on which the false alarm rate exceeds a
defined threshold.