



METHOD OF AND DEVICE FOR AUTHENTICATING A TRAJECTORY CALCULATED BASED ON RADIOLOCATION SIGNALS

5 The field of the invention relates to satellite navigation devices and more specifically to a device for and method of authenticating trajectories calculated based on radiolocation signals.

 With the improving performance of satellite navigation systems, the development of navigation applications is booming. For example, the
10 European satellite positioning system Galileo will enable payable services to be developed for commercial applications with enhanced reliability and guaranteed signal continuity. The signal will contain data relating to the additional commercial services offered. In exchange for payment, the Galileo operator may offer certain service guarantees. The main applications relate
15 to professional users who are ready to pay to have a service guaranteed by the Galileo operator, notably in the fields of geodesics, customs operators, network synchronization, management of maritime and road fleets, road tolls, etc. This service will be access controlled for the final users and for the value added service providers.

20 Vehicles that use these commercial services are equipped with radiolocation signal receivers and navigation data computers that exploit measurements of the radiolocation signals in order to determine, for example, service pricing. Consequently, the viability of the economic model of these commercial services relies on the authenticity of the navigation data.
25 In the field of radiolocation signal reception, it is essential to have measurements (called pseudoranges) supplied by satellites and ephemeris data. It is relatively easy to protect the ephemeris data to guarantee the origin and/or content. However, the characteristics of the measurement signals are in the public domain, and cannot therefore be protected. It is then easy to
30 emulate these signals in order for a user to obtain false geographic position coordinates. In practice, devices can easily be found on the Internet that can be used to spoof the pseudoranges, as can manuals enabling an individual to manufacture these spoofing devices.

 For example, in the case of a motorway toll service provider, a
35 user embeds a satellite signal receiver in the vehicle to authenticate his



position and the itinerary being followed. Depending on the itinerary taken (road, toll section, etc.), the navigation data can be used to evaluate the price to be paid by the user. The principle of the spoofing device involves sending signals that imitate those emitted by the geolocation satellites. At the receiver, these spoofing signals are of a higher power than that of the signals emitted by the satellites and thus cover the latter signals. The spoofing device therefore enables an ill-intentioned user to simulate an itinerary that exists but that is not being followed by the user and that describes a route without a paying section whereas the user is in fact located on a paying section. Generally, the spoofing device is a discrete module that the user places close to the receiver of the radiolocation signals.

A first known solution is disclosed in the European Patent EP 0 904 551 which can be used to safeguard against a spoofing device arranged close to the satellite signal reception device. This device analyses the characteristics of measured signals and detects whether they are signals emitted by a spoofing device or by a satellite.

A second solution is known that is disclosed in the French patent application FR 2 921 528 which safeguards against spoofing devices by concealing, in the signals emitted by a satellite, authentication data according to a distribution algorithm known only to the service operator. To counter this anti-spoofing method, an ill-intentioned user must know the hidden code and its distribution algorithm. This anti-spoofing method presents the disadvantage of having to apply a particular processing operation to the emitted satellite signals and a specific emission device at the satellite level leading to an excessive cost for the solution. This solution cannot therefore be used for receivers that exploit radiolocation signals from a navigation system that is already in place, such as, for example, the American GPS (Global Positioning System) system.

Also known from the prior art is the Internet publication entitled "GPS Spoofing Countermeasures" by Jon S Warner et al. which can be obtained by following the URL: http://www.homelandsecurity.org/bulletin/dual%20benefit/warner_gps_spoofing.html. This document relates to the security of GPS systems and describes a number of protection and detection methods countering GPS system spoofing techniques. This article notably describes simple and inexpensive

methods that can be adapted for the existing GPS systems. The seventh method described consists in using an accelerometer and a compass to calculate a relative position measured with the latter two sensors. This system then involves comparing two positions, one supplied by the GPS system and the other calculated in relation to a reference position. When the anti-spoofing system detects a position disagreement, the control authorities may be alerted to a spoofing attempt.

This method has the drawback that it is necessary to know an initial position in order to make the comparison and that it is affected by the bias in the measurement. Over a long measurement time, there is necessarily a deviation between the relative measurement and the GPS measurement.

The aim of the invention is to provide an inexpensive anti-spoofing solution for a radiolocation signal receiver that can operate regardless of the satellite navigation system that supplies the radiolocation signals.

More specifically, the invention relates to a method of authenticating a displacement trajectory calculated from radiolocation signals received by a receiver embedded in a mobile unit. The method comprises the following steps:

a first step of calculating a first profile of rotational movement of the mobile unit about a reference axis of the mobile unit based on data derived from the processing of the radiolocation signals;

a second step of calculating a second profile of rotational movement of the mobile unit about the same reference axis based on movement data derived from a measurement means independent of said radiolocation signals; and

a third step of comparing the first and the second rotational movement profiles of the mobile unit.

Advantageously, in a fourth step, when a difference is detected between the first profile and the second profile, the use of a spoofing device emitting a falsified radiolocation signal is flagged.

According to a first variant of the third step, the movement profiles are compared over a single profile portion.

According to a second variant of the third step, the movement profiles are compared over at least two distinct profile portions.

According to a variant of the method, the first and second rotational movement profiles are profiles representing the trend of the heading of the vehicle over time.

5 According to a variant of the method, the first and second rotational movement profiles are profiles representing the trend of a derivative n of the heading of the mobile unit over time, with n being at least equal to 1.

10 According to a variant of the method, the first and second rotational movement profiles are profiles representing the trend of an integration n of the heading of the mobile unit over time.

Preferably, the reference axis of the mobile unit is a vertical axis.

The invention also relates to the device for authenticating a displacement trajectory calculated from radiolocation signals received by a receiver embedded in a mobile unit. Advantageously, the device comprises a
15 means of measuring rotational movement of the mobile unit about a reference axis of the mobile unit, said measurement means being independent of the radiolocation signals and capable of measuring a rotational movement of the mobile unit, and it also comprises means for calculating a first rotational movement profile of the mobile unit about a
20 reference axis of the mobile unit based on data derived from the processing of the radiolocation signals and for calculating a second rotational movement profile of the mobile unit about the same reference axis based on data derived from the movement measurement means.

Advantageously, the measurement means is capable of
25 performing only rotational movement data measurements embedded in the mobile unit. According to a variant of the device, the movement measurement means comprises a rotational movement data measurement device of the gyro type. According to another variant of the device, the movement sensor is a gyroscope. According to another variant, the
30 measurement means comprise an assembly of several movement measurement devices embedded in the mobile unit, such as, for example, a motor vehicle antilock braking system (ABS).

According to a variant, the measurement means is an assembly comprising calculation means in communication with a communication
35 system capable of processing mobile location data so as to calculate a

rotational movement profile of the mobile unit. The communication system may notably be a cellular network or a wifi network.

The method and the device for authenticating a displacement trajectory calculated based on radiolocation signals form an inexpensive solution for countering satellite navigation receiver spoofing devices. In practice, the measurement and computation components needed to implement the trajectory calculation function have a cost that is derisory compared to a signal protection solution. Also, the authentication method according to the invention is compatible with any radiolocation signal and consequently it offers a high degree of integration on the market. Furthermore, the calculated rotational movement profile makes it possible to recognize a trajectory being followed and warn a service operator that a fraud attempt on the service is intended by the user. In this way, it is possible to stop any fraud of the service before it happens.

The invention will be better understood, and other advantages will become apparent, from reading the following non-limiting description, and from the appended figures in which:

Figure 1 represents a functional diagram of the authentication device as claimed;

Figure 2 represents a diagram of the authentication method as claimed;

Figure 3 represents a diagram symbolizing two distinct trajectories that can be followed by a mobile unit. A first trajectory is the trajectory actually followed by the mobile unit containing the device according to the invention and the second trajectory is a fictional trajectory possibly used by a spoofing system.

Figure 4 represents the heading profiles of the mobile unit according to each of the preceding trajectories.

Existing antispoofing methods and devices are implemented by modifying radiolocation signals, for example by integrating in the signal a hidden code that is very difficult to reproduce. The proposed invention does not involve protecting a signal from spoofing devices but rather checking that a signal received and used by the radiolocation signal receiver is the authentic signal. To illustrate the invention, we will describe the case of a motorway usage payment service, for which a service operator allows a user

to travel over payable sections in exchange for a price that varies according to the section travelled, as an indicative example. In this example, the mobile unit is a motor vehicle of car, motorbike or heavy goods vehicle etc. The mobile unit with the claimed device embedded does not represent a limitation of the scope of the invention. More generally, the mobile unit may be an air or ocean craft and also a non-transport mobile.

To put such a service in place, the user embeds in his vehicle a module that comprises a radiolocation signal receiver R which may be a receiver compatible with the American satellite navigation system GPS or a Galileo receiver compatible with the future European satellite navigation system, or any satellite navigation system. This module also comprises calculation means $\mu P1$ associated with the receiver that can process the radiolocation signals S1 in order to determine the itinerary and the trajectories followed by the vehicle benefitting from the service. Obviously, other data linked to the displacement of the vehicle may be calculated based on the radiolocation signal data.

The data representing the itinerary followed by the vehicle are then transmitted, via communication means (not represented in Figure 1) chosen by the operator, to a service management centre in order to evaluate the price to be paid. It is possible to mislead an operator to avoid paying for the service used by placing a spoofing device L close to the satellite signal receiver R. This spoofing device L emits signals S2 that imitate the signals S1 of the satellite navigation system in order to mislead the receiver R by supplying false data that may relate, in this case in point, to a nonpayable itinerary saved in a memory of the spoofing module L. The characteristics of the signals S2 are such that the signals S2 cover the signal S1 so that the receiver R sees only the signals S2.

In the context of this patent application, it would be tedious to detail in the description of the application the method of calculating the itinerary and trajectory based on data derived from the radiolocation signal receiver R and the calculation means $\mu P1$ for implementing the method. The methods and techniques for locating based on data derived from a radiolocation signal receiver R are known to those skilled in the art and widely disclosed in the prior art, and in addition are not the specific subject of

the Applicant's patent application. The object claimed covers any means of calculating a trajectory based on satellite navigation system data.

The computer μ P1 determines an itinerary and a trajectory of the vehicle. The computer μ P1 also determines, from the radiolocation signal S1 data, a rotational movement profile P1 of the vehicle M1, illustrated in Figure 3, representing the trend of the heading of the vehicle M1 over time within a navigation coordinate system REP. The coordinate system REP preferably comprises a vertical reference axis, not represented, passing through the vehicle M1 from top to bottom, and a reference base in the horizontal plane of the mobile unit M1 in the coordinate system REP within which the heading P1 of the mobile unit M1 varies. The rotational movement can be calculated in another coordinate system. The rotational movement profile, as represented in Figure 4, is the heading angle profile P1 taking the values P10, P11 and P12 during the trajectory T1. According to the calculated data, the rotational movement profile may also be an angular speed or angular acceleration profile. The computer μ P1 is incorporated into the same module as the receiver R. One and the same computer μ P1 of ASIC (Application Specific Integrated Circuit) or FPGA (field-programmable gate array) type for example, may implement the functions for reception and analysis of signals S1 and the profile calculation function. However, any other hardware distribution option for the functions may be implemented without limiting the scope of the claimed object.

The profile P1 is an authentic vehicle heading profile, that is to say, one which is calculated by the radiolocation signal receiver based on authentic signals S1 emitted by the satellites. However, when a spoofing device L is placed close to the receiver R and emits signals S2 that are more powerful than the signals S1, then the receiver R receives and analyses the signals S2 instead of the signals S1 and the computer μ P1 calculates the rotational movement profile based on the data derived from the signals S2, the signals S2 being spoofing signals that imitate signals emitted by satellites. The signals S2 are defined so as to simulate an itinerary T2 that a mobile unit M2 would follow. This itinerary T2 exists and represents a nonpayable route such that the service operator believes that the user has followed a free route whereas in fact the latter has travelled over a payable route. The rotational movement profile P2 represents the trend of the heading

of a vehicle M2 over time within a navigation coordinate system, the coordinate system comprising a vertical reference axis, that is not represented, that passes through the vehicle M2 from top to bottom, and a reference base in the horizontal plane of the mobile unit M2 in the coordinate system within which the heading P2 of the mobile unit M2 varies. The rotational movement profile, as represented in Figure 4, is the heading angle profile P2 that takes the values P20, P21 and P22 during the trajectory T2. According to the calculated data, the rotational movement profile may also be an angular speed or angular acceleration profile.

The device claimed also comprises a means C of measuring rotational movement of the mobile unit within a coordinate system identical to the coordinate system REP. The navigation coordinate system is therefore the same. The measurement means is a standalone sensor, that is to say, a sensor capable of performing on its own measurements of the rotational movement of the vehicle or, in the case of a set of sensors, the rotational movement measurements are deduced from the data produced by the set of sensors on their own. This sensor is therefore independent of the radiolocation signals based on which the radiolocation signal receiver determines the rotational movement profile P1. If the radiolocation signal receiver R is misled by a spoofing device L, the rotational movement measurements of the sensor remain authentic and represent the true dynamics of the mobile unit. The movement sensor is associated with a computer $\mu P2$ determining a rotational movement profile P3 based on data measured by the sensor. The rotational movement profile determined by the computer $\mu P2$, as represented in Figure 4, is the heading angle profile P3 that takes the values P30, P31 and P32 during the trajectory T1. According to the nature of the sensor, the rotational movement profile P3 may also be an angular speed or angular acceleration profile. The sensor may be a rate gyro measuring an angular speed, a gyroscope measuring an angle or a measurement device of inertial unit type commonly used in aircraft or missiles. The choice of the sensor depends on the desired accuracy and on the type of the mobile unit, and does not limit the scope of the object claimed. The computer $\mu P2$ is independent of the computer $\mu P1$ or, according to another hardware distribution option, is the same computer. The sensor C and the computer $\mu P2$ may form one and the same hardware assembly

independent of the computer $\mu P1$. The choice of the hardware distribution option for the functions does not limit the scope of the claimed object.

The device for authenticating the trajectory calculated based on the radiolocation signals S1 or S2 calculates two rotational movement profiles. A first profile P1 or P2 is derived from the radiolocation data (S1 or S2) received by the receiver and a second profile P3 is derived from the data measured by the standalone movement sensor. The trajectory T1 of Figure 3 describes an S-shaped trajectory describing a first 90° turn A to the right and a second 90° turn B to the left. Consequently, the profile P1 which is derived from the data from the radiolocation signal S1 and the profile P3 which is derived from the measurements of the sensor are identical or very close depending on the accuracy of the sensor. Even when the sensor exhibits a noise in the measurement and an observable bias, the shapes of the rotational movement profiles P1 and P3 are close while being slightly offset relative to one another, but are therefore taken to be identical (the result of correlation of the trajectory shapes being a high correlation). The trajectory T2 of Figure 3 describes a U-shaped trajectory describing a first 90° turn F to the left followed by a second 90° turn G also to the left. The profile P2 obtained from the false radiolocation data is therefore different from the profile P1 and from the profile P3.

The trajectory authentication device T1 calculated based on the radiolocation signal S1 or S2 also comprises a computer $\mu P3$ for comparing the profile P1 or P2 with the profile P3. If the compared profiles are identical then this means that the radiolocation signals received correspond to the trajectory measured by the standalone sensor. The device therefore authenticates the received radiolocation signals. However, if the profile P3 differs significantly from the profile P2 calculated from the radiolocation signals, then this means that the user is using a spoofing device and is seeking to defraud the operator. The authentication device therefore includes means for warning the operator that the user is trying to mislead the system. Preferably, these means are the same as the means for communicating trajectory data to the operator. This offers a significant advantage relative to a radiolocation signal protection solution because the defrauding user may be detected. The operator thus has a prevention means for stopping the fraud attempts.

The comparison function is able to perform a running correlation of the profiles P1 or P2 and P3, or else a correlation by profile portions. The comparison function may be configured so as to compare only the portions that include discriminating identification information, notably the profile portions that represent trajectory turns. The correlation by profile portion makes it possible to reduce the computational resources and consequently the energy consumption of the device. This is advantageous for embedded solutions.

The comparison function may be implemented by a computer $\mu P3$ that is independent of the first two computers $\mu P1$ and $\mu P2$, or, in another hardware distribution option, one and the same computer may carry the profile calculation and profile correlation functions. The choice of how the functional architecture is distributed does not represent a limitation.

Since the sensor is standalone and directly incorporated in the radiolocation signal reception module, according to a preferential embodiment, the anti-spoofing solution is almost impossible to circumvent. In practice, access to the data of the profile P3 must be made intrusively in the receiver module (if the latter incorporates the sensor) and the mechanical connection (more often than not by conductive track on the printed circuit board) must be cut. A second spoofing signal identical to the signal S2 could then be delivered to the correlation function. The rotational movement sensor solutions can at the present time be fully incorporated on the printed circuit and the signal tracks buried in the circuit. Such a solution makes the authentication device almost impossible to circumvent. However, according to another variant, the measurement means consists of an assembly of rotational movement sensors of an ABS system of a motor vehicle, or for example a communication system of cellular network type or wifi network type making it possible to determine trajectory profiles by calculating different position points of the mobile unit. The various technical solutions for calculating a movement profile of the mobile unit are independent of the receiver and of the profile computer associated with the geolocation signals emitted by the satellites.

The invention also relates to the method of authenticating the radiolocation signal. The authentication method as illustrated in Figure 2 comprises a number of steps which are itemized separately but whose

numbers do not in any way symbolize a running order or a processing order for the steps. The method of authenticating the trajectory calculated based on the radiolocation signals received by a receiver embedded in a mobile unit comprises a first step 100 of calculating a first rotational movement profile of the mobile unit about a reference axis of the mobile unit based on data derived from the radiolocation signal, a second step 101 of calculating a second rotational movement profile of the mobile unit about the same reference axis based on movement data derived from a sensor embedded in the mobile unit and a third step 102 of comparing the first and the second rotational movement profiles of the mobile unit. Preferably, the method comprises a fourth step 103 of authenticating the radiolocation signal used to flag a fraudulent use of the service to the operator. The calculated rotational movement profiles may be a profile representing the trend of the heading of the vehicle over time or a profile representing the trend of the angular speed of the heading of the vehicle over time or a profile representing the trend of the angular acceleration of the heading of the vehicle over time or a profile representing the trend of the integral of the measurement of the heading of the vehicle over time. Generally, the profile studied is representative of the movement of the vehicle. The type of profile depends on the measurement means used and the calculation processes executed on the measured data.

The invention applies to any field which exploits radiolocation signals to calculate the itinerary of a mobile unit. It relates to road, maritime or air services.

CLAIMS

1. Method of authenticating a displacement trajectory (T1) calculated
5 from radiolocation signals received by a receiver (R) embedded in a mobile unit (M1), characterized in that it comprises the following steps:
 - a first step (100) of calculating a first profile (P1 or P2) of rotational movement of the mobile unit about a reference axis of the mobile unit based on data derived from the processing of the radiolocation signals;
 - 10 - a second step (101) of calculating a second profile (P3) of rotational movement of the mobile unit about the same reference axis based on movement data derived from a measurement means (C) independent of said radiolocation signals; and
 - a third step (102) of comparing the first and the second
15 rotational movement profiles of the mobile unit.
2. Method according to Claim 1, characterized in that the movement profiles (P1, P3) are compared over a single profile portion.
3. Method according to Claim 1, characterized in that the movement profiles (P1, P3) are compared over at least two distinct profile portions.
- 20 4. Method according to any one of Claims 1 to 3, characterized in that the first and second rotational movement profiles (P1, P3) are profiles representing the trend of the heading of the mobile unit over time.
5. Method according to any one of Claims 1 to 3, characterized in that the first and second rotational movement profiles (P1, P3) are profiles
25 representing the trend of a derivative n of the heading of the mobile unit over time.
6. Method according to any one of Claims 1 to 3, characterized in that the first and second rotational movement profiles (P1, P3) are profiles representing the trend of an integration n of the heading of the mobile unit
30 over time.
7. Method according to Claim 1, characterized in that the reference axis of the mobile unit is a vertical axis.

8. Method according to Claim 1, characterized in that, when a difference is detected between the first profile and the second profile, the use of a spoofing device emitting a falsified radiolocation signal is flagged.

5 9. Device for authenticating a displacement trajectory (T1) calculated from radiolocation signals received by a receiver (R) embedded in a mobile unit (M1), characterized in that it comprises a means (C) of measuring rotational movement of the mobile unit about a reference axis of the mobile unit, said measurement means being independent of the radiolocation signals and capable of measuring a rotational movement of the mobile unit,
10 and in that it also comprises means ($\mu P1$, $\mu P2$) for calculating a first rotational movement profile of the mobile unit about a reference axis of the mobile unit based on data derived from the processing of the radiolocation signals and for calculating a second rotational movement profile of the mobile unit about the same reference axis based on data derived from the
15 movement measurement means (C).

10. Device according to Claim 9, characterized in that the measurement means (C) is capable of performing only rotational movement data measurements.

20 11. Device according to Claim 10, characterized in that the measurement means (C) comprises a rotational movement data measurement device embedded in the mobile unit.

25 12. Device according to Claim 10, characterized in that the measurement means (C) comprises an assembly of at least two measurement devices embedded in the mobile unit to determine the rotational movement data.

30 13. Device according to Claim 10, characterized in that the measurement means (C) is an assembly comprising calculation means in communication with a communication system capable of processing mobile location data so as to calculate a rotational movement profile of the mobile unit.