

DESCRIPTION

TITLE OF INVENTION: NAVIGATION MESSAGE RECEPTION DEVICE

5 CROSS REFERENCE TO RELATED APPLICATION

[0001]

This application is based on Japanese Patent Application No. 2014-37047 filed on February 27, 2014, the disclosure of which is incorporated herein by reference.

10

TECHNICAL FIELD

[0002]

The present disclosure relates to a navigation message reception device that receives a navigation message from an artificial satellite used for a satellite positioning system.

15

BACKGROUND ART

[0003]

Conventionally, there is known a technology that uses a receiver to receive a navigation message for positioning transmitted from an artificial satellite used for a satellite positioning system.

20

[0004]

Recently, however, a malicious person's falsification or impersonation of position information is increasing in response to development of a repeater to duplicate signals from the satellite or a simulator capable of imitatively generating signals from the satellite.

25

[0005]

Patent literature 1 discloses the technology to authenticate whether a receiver receives an authentic navigation message from an artificial satellite used for the satellite positioning system. According to the technology disclosed in
5 patent literature 1, the receiver accesses a database in an authentication center and acquires data used to authenticate a targeted satellite from a satellite number and the satellite time contained in a navigation message received from the satellite. The receiver uses the data acquired from the authentication center to
10 authenticate whether the received navigation message conforms to an authenticate navigation message from the satellite used for the satellite positioning system.

PRIOR ART LITERATURES

PATENT LITERATURE

15 [0006]

Patent Literature 1: JP-2013-130395A

SUMMARY OF INVENTION

[0007]

20 The inventors of the present application found the following concerning the technology disclosed in patent literature 1.

[0008]

According to the technology disclosed in patent literature 1, the receiver needs to communicate with the authentication center and authenticate all the
25 navigation messages from multiple satellites used for positioning every time the positioning is performed. Each receiver needs to frequently communicate with

the authentication center and causes an excessive amount of communication processing load on the authentication center.

[0009]

The present disclosure is made in consideration of the foregoing. It is an
5 object of the present disclosure to provide a navigation message reception device capable of determining whether a navigation message from an artificial satellite is authentic while suppressing a communication processing load at an authentication center used to authenticate a navigation message from an artificial satellite used for a satellite positioning system.

10 [0010]

A navigation message reception device in an example of the present disclosure comprises: a satellite receiver for receiving a navigation message from an artificial satellite used for a satellite positioning system; an authentication information receiver for receiving, from an authentication center, authentication
15 information corresponding to the navigation message received from the artificial satellite; and a center usage authentication portion for authenticating whether the navigation message received by the satellite receiver is authentic, by using the authentication information received by the authentication information receiver according to the navigation message. The navigation message contains
20 consistency information ensuring consistency between a plurality of the artificial satellites. The navigation message reception device further comprises: a consistency determination portion for determining whether information ensuring consistency with the consistency information contained in the navigation message successfully authenticated by the center usage authentication portion is contained
25 in a navigation message received by the satellite receiver from an unauthenticated satellite, the unauthenticated satellite being the artificial satellite other than a

source of the navigation message successfully authenticated by the center usage authentication portion; and a simplified determination portion for determining that the navigation message received by the satellite receiver is authentic when the consistency determination portion determines that the information ensuring the consistency is contained in the navigation message, and for not determining that the navigation message received by the satellite receiver is authentic when the consistency determination portion determines that the information ensuring the consistency is not contained in the navigation message.

[0011]

In the above navigation message reception device, when it is determined that information ensuring consistency with the consistency information contained in the navigation message successfully authenticated by the center usage authentication portion is contained in a navigation message received by the satellite receiver from an unauthenticated satellite that is the artificial satellite other than a source of the navigation message successfully authenticated by the center usage authentication portion, it is determined that the navigation message received by the satellite receiver from the unauthenticated satellite is authentic. Specifically, the navigation message reception device determines, without communicating with the authentication center, whether a navigation message is authentic based on whether the information ensuring the consistency with the consistency information contained in the navigation message successfully authenticated by the center usage authentication portion is contained.

[0012]

Because the consistency information is provided for ensuring the consistency between the plurality of artificial satellites, it is highly like that a navigation containing information ensuring consistency with the consistency

information contained in the navigation message successfully authenticated by the center usage authentication portion is authentic. Therefore, according to the above navigation message reception device, one navigation message is successfully authenticated by the center usage authentication portion, it becomes possible to determine, without communicating the authentication center, that other navigation messages highly likely to be authentic are also authentic. Because the navigation message reception device need not receive the authentication information from the authentication server, a communication processing load on the communication center can be reduced.

10 [0013]

As a result, it is possible to determine whether a navigation message from an artificial satellite is authentic, while suppressing a communication processing load at the authentication center used to authenticate a navigation message from an artificial satellite used for a satellite positioning system.

15

BRIEF DESCRIPTION OF DRAWINGS

[0014]

The foregoing and other objects, features and advantages of the present disclosure will become more apparent from the detailed description given below with reference to the accompanying drawings in which:

20

FIG. 1 is a diagram illustrating a schematic configuration of a simplified authentication system according to a first embodiment;

FIG. 2 is a block diagram illustrating a schematic configuration of an authentication center;

25

FIG. 3 is a block diagram illustrating a schematic configuration of an onboard device;

FIG. 4 is a flowchart illustrating a flow of an authentication-related process on the onboard device according to the first embodiment;

FIG. 5 is a flowchart illustrating a flow of a simplified determination process on the onboard device according to the embodiment;

5 FIG. 6 is a schematic diagram illustrating a process at S32; and

FIG. 7 is a flowchart illustrating a flow of a simplified determination process on the onboard device 200 according to a first modification.

EMBODIMENTS FOR CARRYING OUT INVENTION

10 [0015]

Embodiments of the present disclosure will be described with reference to the accompanying drawings.

[0016]

(First Embodiment)

15 As illustrated in FIG. 1, a simplified authentication system 1 according to the first embodiment includes a monitor station 110, an authentication center 120, a master control station 130, and an onboard device 200. A vehicle using the onboard device 200 is defined as vehicle A. The onboard device 200 corresponds to the navigation message reception device.

20 [0017]

<Schematic Configuration of the Simplified Authentication System 1>

The monitor station 110 receives GPS radio waves transmitted from GPS satellites 2a through 2c included in a GPS, one of satellite positioning systems. The GPS satellites 2a through 2c correspond to artificial satellites. The GPS
25 satellites 2a through 2c are hereafter represented as a GPS satellite 2 if the GPS satellites need not be distinguished from each other. As publicly known, the GPS

radio wave contains a navigation message. The monitor station 110 demodulates the received GPS radio wave, extracts a navigation message, and transmits it to the authentication center 120. The monitor station 110 may receive GPS radio waves from multiple GPS satellites 2. In this case, the
5 monitor station 110 extracts navigation messages from respective GPS radio waves and transmits the navigation messages to the authentication center 120.

[0018]

The authentication center 120 generates parity data from the navigation message and an H matrix serving as an encryption key. The authentication
10 center 120 transmits a signal containing the parity data to the master control station 130. The authentication center 120 also communicates with the onboard device 200. The authentication center 120 will be described in detail later with reference to FIG. 2.

[0019]

15 The master control station 130 transmits the parity data received from the authentication center 120 to a quasi-zenith satellite (hereinafter referred to as a QZS satellite) 3. The QZS satellite 3 broadcasts the navigation message containing the parity data to the earth.

[0020]

20 The onboard device 200 represents a navigation message authentication (NMA) onboard device. The onboard device 200 communicates with the authentication center 120 to authenticate that the navigation message received from the GPS satellite 2 is authentic. The authentication will be described in detail later with reference to FIG. 4.

25 [0021]

The onboard device 200 determines a current position of the onboard

device 200 using the navigation messages received from the multiple GPS satellites 2. The determination of the current position uses navigation messages received from at least three GPS satellites 2.

[0022]

5 The onboard device 200 performs a simplified determination process to determine, using a navigation message successfully authenticated in the onboard device 200 itself, whether a navigation message received from another GPS satellite 2 at approximately the same timing as the successfully authenticated is authentic without access to the authentication center 120. The onboard device
10 200 will be described in detail later with reference to FIG. 3.

[0023]

<Detailed Configuration of the Authentication Center 120>

As illustrated in FIG. 2, the authentication center 120 includes a controller 122, a data storage 124, and a communicator 126.

15 [0024]

The controller 122 is provided as a computer including a CPU, ROM, and RAM. The controller 122 controls the data storage 124 and the communicator 126. The CPU executes a program stored in the ROM while using a temporary storage function of the RAM, thereby functioning as a RAND message generator
20 1221, a SEED value generator 1222, an H matrix calculator 1223, a parity calculator 1224, and a signal processor 1225. The functions of the portions 1221 through 1225 may include functions disclosed in patent literature 1.

[0025]

The RAND message generator 1221 generates a RAND message from a
25 navigation message acquired from the monitor station 110. The RAND message contains TOW, TOC, AF0, and AF1 in order. TOW (time of week) is bit string

data contained in bit strings of the navigation message. TOC, AF0, and AF1 are clock correction parameters in ephemeris data. TOW, TOC, AF0, and AF1 are provided as data to specify a signal transmission time and correspond to a transmission time. The data is followed by AS Flag acting as an anti-spoof flag and PRN (Pseudo Random Noise) ID acting as a satellite number.

[0026]

RAND containing TOW and PRN ID can be provided as data to indicate which GPS satellite is used as the source at which time. TOW varies every six seconds. RAND contains PRN ID. Therefore, RAND is generated every six seconds for each GPS satellite 2 from which the monitor station 110 receives a GPS radio wave.

[0027]

The SEED value generator 1222 generates a random number using a PC clock as input to generate a SEED value.

[0028]

The H matrix calculator 1223 uses the SEED value generated by the SEED value generator 1222 to calculate an H matrix that maintains one-to-one correspondence to the SEED value. The publicly known hash function can be used for the H matrix. For example, the H matrix may be available as a parity check matrix for LDPC (Low Density Parity Check) coding. The H matrix may be also available as a generator matrix resulting from the parity check matrix.

[0029]

The parity calculator 1224 calculates parity data based on the RAND message generated by the RAND message generator 1221 and the H matrix calculated by the H matrix calculator 1223.

[0030]

The signal processor 1225 inserts the parity data and the RAND message into a navigation message originated from the QZS satellite 3. The parity data is calculated by the parity calculator 1224. The RAND message is used for this calculation. The signal processor 1225 transmits the navigation message after
5 the insertion to the master control station 130.

[0031]

In addition to the signal insertion, the controller 1225 causes the data storage 124 to store the parity data calculated by the controller 1224, the RAND message used for the parity data calculation, the H matrix, and the SEED value
10 used for the H matrix calculation so that these are associated with each other.

[0032]

The controller 1225 inserts the RAND message and the parity data into a navigation message transmitted from the QZS satellite 3 each time the controller 1221 generates a RAND message. Therefore, the RAND message generator
15 1221, the SEED value generator 1222, the H matrix calculator 1223, and the parity calculator 1224 also perform the processes each time the controller 1221 generates a RAND message.

[0033]

Suppose that the communicator 126 receives PRN ID, TOW, and a public
20 key transmitted from the onboard device 200. In this case, an H matrix selector 1226 selects an H matrix corresponding to the received PRN ID and TOW from H matrices stored in the data storage 124. The H matrix selector 1226 encrypts the selected H matrix using the public key and returns the encrypted H matrix to the onboard device 200.

25 [0034]

<Detailed Configuration of the Onboard Device 200>

The onboard device 200 includes a communicator 210 that includes a receiver 211. The receiver 210 receives a navigation message broadcast from the QZS satellite 3. As illustrated in FIG. 3, the onboard device 200 includes the communicator 210, a controller 220, and a satellite receiver 230.

5 [0035]

The communicator 210 includes the receiver 211 and a transmitter 212. The communicator 210 includes a wide area communication function. The wide area communication function supports several kilometers of communication distance and performs communication with a base station in the public network to enable communication with other communication devices available within a communication range of the public network. The wide area communication function enables the communicator 210 to communicate with the communicator 126 of the authentication center 120.

[0036]

15 The satellite receiver 230 receives radio waves originated from the GPS satellite 2 and the QZS satellite 3 at fixed cycles. For each fixed cycle, the satellite receiver 230 outputs to the controller 220 the navigation message received from the GPS satellite within the fixed cycle. When the navigation messages are received from multiple GPS satellites within one cycle, the navigation messages from these GPS satellites are output. The multiple navigation messages received within the one cycle can be considered as the navigation messages that are received in the same timing.

[0037]

25 The controller 220 is provided as a computer including a CPU, ROM, and RAM. The controller 220 controls the communicator 210 and the satellite receiver 230. The CPU executes a program stored in the ROM while using a

temporary storage function of the RAM, thereby executing an authentication-related process in FIG. 4 and a simplified determination process in FIG. 5.

[0038]

5 <Authentication-Related Process>

The controller 220 of the onboard device 200 performs the authentication-related process to be described with reference to a flowchart in FIG. 4. The authentication-related process relates to the authentication proving that a signal received by the satellite receiver 230 conforms to an authentic navigation message received from the GPS satellite 2. The flowchart in FIG. 4 may be performed each time the satellite receiver 230 receives GPS radio waves from three or more GPS satellites 2 within the above-mentioned one cycle.

[0039]

15 Suppose that the satellite receiver 230 may receive a signal from a repeater or a simulator and incorrectly assume that the signal is a navigation message contained in the GPS radio wave. In the above, the repeater is one that duplicates a signal from the GPS satellite 2. The simulator is one that can imitatively generate a signal from the GPS satellite 2.

[0040]

20 At S1, a current position of the device is determined based on navigation messages contained in the GPS radio waves received from three or more GPS satellites 2.

[0041]

25 At S2, a navigation message received from the QZS satellite 3 is acquired from the receiver 211. At S3, PRN ID and TOW are extracted from the navigation message acquired at S1.

[0042]

At S4, PRN ID and TOW extracted at S3 are transmitted along with a public key to the authentication center 120 from the transmitter 212. The H matrix is determined from PRN ID and TOW. The authentication center 120
5 encrypts the H matrix using the public key and transmits the H matrix to the onboard device 200. The H matrix, which is determined from PRN ID and TOW transmitted from the onboard device 200 to the authentication center 120, corresponds to authentication information.

[0043]

10 At S5, the H matrix transmitted from the authentication center 120 is acquired from the receiver 211. Namely, the H matrix that corresponds to the navigation message received from the GPS satellite 2 is received from the authentication center 120. S5 corresponds to an authentication information receiver. At S6, the encrypted H matrix acquired at S5 is encrypted using a
15 private key.

[0044]

At S7, a RAND message is generated from, of the navigation messages contained in the GPS radio waves received from the GPS satellites 2, a navigation message containing the same PRN ID as that transmitted at S4.

20 [0045]

At S8, comparison parity data is generated based on the RAND message generated at S7 and the H matrix decrypted at S6. At S9, it is determined whether the comparison parity data generated at S8 matches the parity data extracted at S3.

25 [0046]

The H matrix decrypted at S6 equals the H matrix that the authentication

center 120 uses to generate the parity data. The parity calculator 1224 of the authentication center 120 calculates parity data based on this H matrix and the RAND message.

[0047]

5 Accordingly, when the comparison parity data generated at S8 matches the parity data extracted at S3, the RAND message generated at S7 can be assumed to equal the RAND message generated by the authentication center 120.

[0048]

10 The process proceeds to S10 and determines that the authentication is successful when the comparison parity data generated at S8 matches the parity data extracted at S3 (S9: YES). When the authentication is successful, the process of FIG. 4 is ended. The process proceeds to S11 and determines that the authentication is unsuccessful when the comparison parity data generated at
15 S8 differs from the parity data extracted at S3 (S9: NO). When the authentication is unsuccessful, the process returns to S2 and the process is repeated until the authentication of at least one of the navigation messages used for the positioning at S1 is successful. In this way, the authentication-related process performs authentication according to a navigation message received from the GPS satellite
20 2 using the H matrix (i.e., authentication information) received from the authentication center 120. S9 through S11 correspond to a center usage authentication portion.

[0049]

<Simplified Determination Process>

25 The simplified determination process performed by the controller 320 of the onboard device 200 according to the first embodiment will be described with

reference to a flowchart in FIG. 5.. The flowchart in FIG. 5 may start when the authentication-related process successfully authenticates at least one of navigation messages used for positioning. The flowchart in FIG. 5 may be performed on each of navigation messages that are used for positioning and are not authenticated by the authentication-related process.

[0050]

At S21, of navigation messages used for positioning, an unauthenticated navigation message different from a navigation message (authenticated navigation message) successfully authenticated by the authentication-related process is acquired.

[0051]

At S22, it is determined whether there is a match between the transmission time contained in the unauthenticated navigation message acquired at S21 and the transmission time contained in the authenticated navigation message. The match here signifies not only a complete match but also an approximate match within a range of an error. The transmission time contained in the authenticated navigation message corresponds to consistency information. S22 corresponds to a consistency determination portion.

[0052]

An example of the process at S22 will be described with reference to FIG. 6. According to the example in FIG. 6, GPS satellites are used for positioning. The onboard device 200 uses the authentication center 120 to successfully authenticate a navigation message originated from the GPS satellite 2a. A navigation message originated from the GPS satellite 2b is not authenticated yet.

[0053]

The GPS satellite 2a originates the navigation message (i.e.,

authenticated navigation message) at transmission time T_{i1} . The GPS satellite 2b originates the navigation message (i.e., unauthenticated navigation message) at transmission time T_{i2} . The process at S22 determines whether there is a match between the transmission time (T_{i1}) of the authenticated navigation message and the transmission time (T_{i2}) of the unauthenticated navigation message.

[0054]

Multiple navigation messages received by the satellite receiver 230 within one cycle guarantee their transmission times to match when a repeater duplicating a signal from the GPS satellite 2 or a simulator capable of imitatively generating a signal from the GPS satellite 2 is not used.

[0055]

At S23, if it is determined that the transmission times match (S23: YES), it is determined that the unauthenticated navigation message contains the transmission time consistent with the transmission time contained in the authenticated navigation message, and the process proceeds to S24. At S24, it is determined the unauthenticated navigation message acquired at S21 is authentic and then the process is ended. If it is determined that the transmission times do not match (S23: NO), the process is ended. In this case, it is not determined that the unauthenticated navigation message acquired at S21 is authentic. S23 and S24 also correspond to the simplified determination portion.

[0056]

If the determination results in NO at S23, it may be determined that the unauthenticated navigation message acquired at S21 is unauthentic.

[0057]

<Summary of the First Embodiment>

According to the First embodiment, when the onboard device 200 successfully authenticates one of navigation messages used for positioning by using the authentication center 120, the other navigation messages used for positioning can be determined to be authentic or unauthentic based on the transmission times. Therefore, the onboard device 200 need not receive the H matrix from the authentication center 120 in terms of the other navigation messages used for positioning, reducing a communication processing load on the authentication center 120.

[0058]

The transmission times of the navigation messages used for positioning match when no repeater or simulator is used. The first embodiment determines a navigation message to be authentic or unauthentic based on whether the transmission time matches the successfully authenticated navigation message. Therefore, the first embodiment can prevent a navigation message from being determined to be authentic when a repeater or a simulator is used. The first embodiment can improve the accuracy to determine a navigation message to be authentic.

<First Modification>

There has been described the first embodiment that determines an unauthenticated navigation message to be authentic or unauthentic based on whether, of the navigation messages used for positioning, the transmission time contained in the authenticated navigation message matches the transmission time contained in the unauthenticated navigation message. However, this is not limiting.

[0059]

For example, there may be a configuration (first modification) that

determines an unauthenticated navigation message to be authentic or unauthentic based on where there is a match between satellite positions. Of the satellite positions, one satellite position is determined from orbit information about the GPS satellite 2 contained in the authenticated navigation message and the transmission time contained in the authenticated navigation message. Another satellite position is determined from orbit information about the GPS satellite 2 contained in the unauthenticated navigation message and the transmission time contained in the unauthenticated navigation message. The first modification equals the first embodiment except a partial difference in the process on the controller 220 of the onboard device 200. In detail, the first modification differs from the first embodiment in part of the simplified determination process the controller 220 performs.

[0060]

As publicly known, a navigation message contains ephemeris data and almanac data. The almanac data contains the orbit information about not only the GPS satellite 2 that is a source of the navigation message but also all GPS satellites 2 in orbit. Satellite positions of all the GPS satellites 2 can be calculated from the orbit information and the transmission time of the navigation message. The ephemeris data contains the orbit information about the GPS satellite 2 that is a source of the navigation message. A satellite position of the GPS satellite 2 that is a source of this navigation message can be calculated more accurately from the orbit information and the transmission time of the navigation message.

[0061]

The first modification uses, of the orbit information contained in the almanac data and the ephemeris data, the orbit information contained in the

almanac data. The orbit information contained in the almanac data is hereinafter simply referred to as the orbit information.

[0062]

<Simplified Determination Process According to the First Modification>

5 The controller 220 of the onboard device 200 according to the first modification performs the simplified determination process to be described with reference to a flowchart in FIG. 7. The flowchart in FIG. 7 may also start when the authentication-related process successfully authenticates at least one of navigation messages used for positioning. The flowchart in FIG. 7 may be also
10 performed on each of navigation messages that are used for positioning and are not authenticated by the authentication-related process.

[0063]

According to the example in FIG. 7, the GPS satellite 2a represents the GPS satellite 2 that is a source of an authenticated navigation message.

15 [0064]

At S31, like S21 above, an unauthenticated navigation message except the authenticated navigation message out of navigation messages used for positioning is acquired.

[0065]

20 At S32, a position of the GPS satellite 2a is calculated using the transmission time contained in the authenticated navigation message used for positioning and the orbit information about the GPS satellite 2a contained in the authenticated navigation message. The transmission time and the orbit information correspond to satellite position calculation information.

25 [0066]

At S33, a position of the GPS satellite 2a is calculated using the

transmission time contained in the unauthenticated navigation message used for positioning and the orbit information about the GPS satellite 2a contained in the unauthenticated navigation message. The description below explains why a satellite position of the GPS satellite 2a can be calculated from the orbit information contained in the unauthenticated navigation message received from the GPS satellite 2 other than the GPS satellite 2a that is a source of the authenticated navigation message. The GPS satellite 2 other than the GPS satellite 2a that is a source of the authenticated navigation message corresponds to an unauthenticated satellite.

10 [0067]

The orbit information contained in the almanac data also contains the orbit information about the GPS satellite 2a other than the GPS satellite 2 that is a source of the unauthenticated navigation message. As above, multiple navigation messages received by the satellite receiver 230 within one cycle guarantee their transmission times to match when the repeater or the simulator is not used. Therefore, a satellite position of the GPS satellite 2a can be calculated also from the transmission time and the orbit information contained in the unauthenticated navigation message.

[0068]

20 At S34, it is determined whether there is a match between the satellite position of the GPS satellite 2a calculated at S32 and the satellite position of the GPS satellite 2a calculated at S33. The match here signifies not only a complete match but also an approximate match within a range of an error. S34 corresponds to the consistency determination portion.

25 [0069]

The transmission times of the unauthenticated navigation message and

the authenticated navigation message used for positioning are supposed to match when the repeater or the simulator is not used. The satellite position of the GPS satellite 2a is calculated from the transmission time and the orbit information contained in the authenticated navigation message. Therefore, the same
5 satellite position as the satellite position of the GPS satellite 2a can be calculated from the transmission time and the orbit information contained in the unauthenticated navigation message when the repeater or the simulator is not used. Therefore, the satellite position of the GPS satellite 2a calculated at S32 matches the satellite position of the GPS satellite 2a calculated at S33 when the
10 repeater or the simulator is not used.

[0070]

When it is determined at S35 that the satellite positions match (S35: YES), it is determined that the unauthenticated navigation message contains the orbit information and the transmission time consistent with the orbit information and the
15 transmission time contained in the authenticated navigation message, and the process proceeds to S36. At S36, it is determined that the unauthenticated navigation message acquired at S31 is authentic, and then the process is ended. When it is determined that the satellite positions do not match (S35: NO), it is determined that the unauthenticated navigation message acquired at S31 is
20 unauthentic, and the process is ended. S35 and S36 also correspond to the simplified determination portion.

[0071]

If the determination results in NO at S35, it may be determined that the unauthenticated navigation message acquired at S31 is unauthentic.

25 [0072]

<Summary of the First Modification>

According to the first modification similarly to the first embodiment, when the onboard device 200 successfully authenticates one of navigation messages used for positioning by using the authentication center 120, the other navigation messages used for positioning can be determined to be authentic or unauthentic based on a satellite position calculated from the orbit information and the transmission time. Therefore the onboard device 200 need not receive the H matrix from the authentication center 120 in terms of the other navigation messages used for positioning, reducing a communication processing load on the authentication center 120.

[0073]

The use of a repeater or a simulator causes a difference between transmission times contained in the navigation messages used for positioning and consequently a difference between satellite positions of the same GPS satellite 2 calculated from the transmission time and the orbit information. The first embodiment determines a navigation message to be authentic or unauthentic based on whether the satellite position matches the successfully authenticated navigation message. Therefore, the first embodiment can prevent a navigation message from being determined to be authentic when a repeater or a simulator is used, and accordingly, the first embodiment can improve the accuracy to determine a navigation message to be authentic.

[0074]

The first modification has described the example in which a satellite position of the GPS satellite 2a that is a source of an authenticated navigation message is used for the match between satellite positions. Alternatively, a satellite position of the GPS satellite 2 other than the GPS satellite 2a may be used as long as the GPS satellite 2 is a source of a navigation message used for

positioning.

[0075]

<Second Modification>

There has been described the embodiment that uses only navigation
5 messages received from the GPS satellite 2 for positioning. However, a
navigation message received from the QZS satellite 3 may be used for positioning.
In this case, the navigation message received from the QZS satellite 3 may be
also authenticated similarly to the case of the GPS satellite 2.

[0076]

10 An example of the second modification is to generate a RAND message
from the navigation message that the monitor station 110 receives from the QZS
satellite 3. The authentication center 120 generates parity data based on the
RAND message. The generated parity data is transmitted to the master control
station 130. The master control station 130 transmits the parity data to the QZS
15 satellite 3. The QZS satellite 3 broadcasts a navigation message containing the
parity data to the earth.

[0077]

The onboard device 200 may generate a RAND message from the
navigation message received from the QZS satellite 3. The onboard device 200
20 may generate comparison parity data from the RAND message and the H matrix
acquired from the authentication center 120. The onboard device 200 may
authenticate navigation messages by comparing the generated comparison parity
data with the parity data received from the QZS satellite 3.

[0078]

25 <Third Modification>

Although the authentication method in the above embodiment is of a type

of authenticating a navigation message, this is a mere example. As long as an authentication method is of a type requiring an access to a certification organization, other configurations may be employed in the authentication method (third modification).

5 [0079]

<Fourth Modification>

Although the above embodiment illustrates the onboard device 200 used for vehicles, this is not limiting. For example, a navigation message reception device comparable to the onboard device 200 may be applied to a mobile terminal
10 carried by a user.

[0080]

Although embodiments and the configurations have been illustrated, embodiments and the configurations of the present disclosure are not limited to those illustrated above. For example, the scope of embodiments and
15 configurations according to the present disclosure also includes an embodiment and a configuration resulting from any combination of technical elements disclosed in different embodiments and configurations.

CLAIMS

1. A navigation message reception device comprising:

5 a satellite receiver for receiving a navigation message from an artificial satellite used for a satellite positioning system;

an authentication information receiver for receiving, from an authentication center, authentication information corresponding to the navigation message received from the artificial satellite; and

10 a center usage authentication portion for authenticating whether the navigation message received by the satellite receiver is authentic, by using the authentication information received by the authentication information receiver according to the navigation message;

wherein the navigation message contains consistency information ensuring consistency between a plurality of the artificial satellites,

15 the navigation message reception device further comprising:

a consistency determination portion for determining whether information ensuring consistency with the consistency information contained in the navigation message successfully authenticated by the center usage authentication portion is contained in a navigation message received by the satellite receiver from an
20 unauthenticated satellite, wherein the unauthenticated satellite is the artificial satellite other than a source of the navigation message successfully authenticated by the center usage authentication portion; and

a simplified determination portion

25 for determining that the navigation message received by the satellite receiver is authentic when the consistency determination portion determines that

the information ensuring the consistency is contained in the navigation message ,and

for not determining that the navigation message received by the satellite receiver is authentic when the consistency determination portion
5 determines that the information ensuring the consistency is not contained in the navigation message.

2. The navigation message reception device according to claim 1, wherein:

10 the consistency information is a transmission time of the navigation message; and

based on whether there is a match between a transmission time contained in the navigation message successfully authenticated by the center usage authentication portion and a transmission time contained in the navigation
15 message received by the satellite receiver from the unauthenticated satellite, the consistency determination portion determines whether the information ensuring the consistency is contained.

3. The navigation message reception device according to claim 1, wherein:
20

the navigation message contains satellite position calculation information enabling to calculate satellite positions of not only the artificial satellite that is a source of the navigation message but also another artificial satellite;

the consistency information is the satellite position calculation information;
25 and

based on whether there is a match between a satellite position of the

unauthenticated satellite calculated from the satellite position calculation information contained in the navigation message successfully authenticated by the center usage authentication portion and a satellite position of the unauthenticated satellite calculated from the satellite position calculation information contained in a
5 navigation message received by the satellite receiver from the unauthenticated satellite, the consistency determination portion determines whether the information ensuring the consistency is contained.