

DESCRIPTION

TITLE OF INVENTION: NAVIGATION MESSAGE RECEPTION DEVICE

5 CROSS REFERENCE TO RELATED APPLICATION

[0001]

This application is based on Japanese Patent Application No. 2014-37048 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 each of
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 according to 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,
15 authentication information corresponding to the navigation message received from the artificial satellite; 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; a continuity determination portion
20 for, when the satellite receiver receives a new navigation message from the artificial satellite that is a source of the navigation message authenticated by the center usage authentication portion, determining whether or not there is continuity between the navigation message authenticated by the center usage authentication portion and the new navigation message; and a simplified
25 determination portion for determining that the new navigation message is authentic when the continuity determination portion determines that there is

continuity between the new navigation message and the navigation message authenticated by the center usage authentication portion, and determining that the new navigation message is unauthentic when the continuity determination portion determines that there is no continuity between the new navigation message and the navigation message authenticated by the center usage authentication portion.

[0011]

In this navigation message reception device, when it is determined that there is the continuity between the navigation message authenticated by the center usage authentication portion and the navigation message newly received from the artificial satellite that is a source of the authenticated navigation message, it is determined that the new navigation message is authentic. Specifically, without communication with the authentication center, the navigation message reception device determines whether a navigation message is authentic based the continuity with the navigation message authenticated by the center usage authentication portion.

[0012]

When a navigation message is originated from the same artificial satellite as the navigation message successfully authenticated by the center usage authentication portion and has continuity with the authenticated navigation message, the navigation message is highly likely to be authentic. Therefore, when the center usage authentication portion of the navigation message reception device authenticates a navigation message from a certain artificial satellite, the navigation message reception device can determine, without communication with the authentication center, that a navigation message thereafter originated from this certain artificial satellite and highly likely to be authentic is authentic.

Therefore, the onboard device need not receive authentication information from the authentication center, reducing a communication processing load at the authentication center.

[0013]

5 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.

10 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:

15 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;

20 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 first embodiment;

25 FIG. 6 is a schematic diagram illustrating a process at S24;

 FIG. 7 is a flowchart illustrating a flow of a simplified determination

process on the onboard device according to a first modification; and

FIG. 8 is a schematic diagram illustrating a process at S35.

EMBODIMENTS FOR CARRYING OUT INVENTION

5 [0015]

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

[0016]

(First Embodiment)

10 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.

15 [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
20 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
25 receive GPS radio waves from multiple GPS satellites. In this case, the 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 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]

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]

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.

[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]

The onboard device 200 performs a simplified authentication process to

determine whether a newly received navigation message is authentic, using a navigation message already authenticated in the past without access to the authentication center 120. The onboard device 200 will be described in detail later with reference to FIG. 3.

5 [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.

[0024]

10 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 1221, a SEED value generator 1222, an H matrix calculator 1223, a parity
15 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 navigation message acquired from the monitor station 110. The RAND message
20 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
25 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
5 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]

10 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
15 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.

20 [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
25 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 used for the H matrix calculation so that these are associated with each other.

5 [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 1221, the SEED value generator 1222, the H matrix calculator 1223, and the
10 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 key transmitted from the onboard device 200. In this case, an H matrix selector
15 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.

[0034]

20 <Detailed Configuration of the Onboard Device 200>

The onboard device 200 includes a communicator 210 that includes a receiver 211. The receiver 211 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.

25 [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]

The satellite receiver 230 periodically receives radio waves originated from the GPS satellite 2 and the QZS satellite 3.

[0037]

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]

<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.

[0039]

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]

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]

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 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]

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 private key.

[0044]

5 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.

[0045]

10 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.

[0046]

15 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]

20 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]

25 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). The process proceeds to S11 and determines

that the authentication is unsuccessful when the comparison parity data generated at S8 differs from the parity data extracted at S3 (S9: NO). In this way, the authentication-related process performs authentication according to a navigation message received from the GPS satellite 2 using the H matrix (i.e., authentication information) received from the authentication center 120. The process proceeds to S12 after S10 and S11. S9 through S11 correspond to a center usage authentication portion.

[0049]

At S12, it is determined whether the determination about the successful or unsuccessful authentication is completed in terms of all navigation messages used for the positioning at S1. The process in FIG. 4 is ended if the determination about the successful or unsuccessful authentication is completed (S12: YES). The process returns to S2 if the determination about the successful or unsuccessful authentication is not completed in terms of at least one of all navigation messages used for the positioning at S1 (S12: NO).

[0050]

The onboard device 200 uses nonvolatile memory such as backup RAM of the controller 220 to store the time of receipt of an authenticated navigation message in association with the authenticated navigation message. The authenticated navigation message signifies a navigation message that the authentication-related process in FIG. 4 authenticates successfully. Only the satellite number and the transmission time contained in the authenticated navigation message may be stored in association with the reception time.

[0051]

<Simplified Determination Process>

The description below explains a simplified determination process

performed by the controller 220 of the onboard device 200 according to the first embodiment with reference to a flowchart in FIG. 5. The flowchart in FIG. 5 may start when the satellite receiver 230 of the onboard device 200 receives a navigation message from GPS satellite 2, for example. When the satellite receiver 230 receives multiple navigation messages from the GPS satellites 2 within one cycle of successive output from the satellite receiver 230 to the controller 220, the flowchart in FIG. 5 may be performed on each of the navigation messages from the multiple GPS satellites 2.

[0052]

10 At S21, a navigation message received by the satellite receiver 230 is acquired from the satellite receiver 230.

[0053]

 At S22, it is determined whether a satellite number contained in the navigation message acquired at S21 matches a satellite number contained in the authenticated navigation message stored in the memory of the controller 220.

[0054]

 The process proceeds to S24 if the satellite numbers are determined to match at S23 (S23: YES). The process is ended if the satellite numbers are determined to differ from each other at S23 (S23: NO). The satellite numbers may be also determined to differ from each other when no authenticated navigation message is stored in the memory of the controller 220.

[0055]

 At S24, it is determined whether there is continuity between the authenticated navigation message and the navigation message that is acquired at S21 and is determined at S23 to contain the matching satellite number. In detail, it is determined whether the transmission time contained in the navigation

message newly received by the satellite receiver 230 and the transmission time contained in the authenticated navigation message have continuity corresponding to a reception time difference from the reception time of the authenticated navigation message to the reception time of the newly received the navigation message. S24 corresponds to a continuity determination portion.

[0056]

An example of the process at S24 will be described using FIG. 6. As a precondition for the example in FIG. 6, the onboard device 200 successfully authenticates a navigation message originated from the GPS satellite 2a using the authentication center 120. The onboard device 200 thereafter receives the navigation message originated from the GPS satellite 2a.

[0057]

Transmission time $Ti1$ is assumed to be a transmission time of the authenticated navigation message, namely, the navigation message that the onboard device 200 successfully authenticates using the authentication center 120. Reception time $To1$ is assumed to be a time of receipt of this navigation message by the onboard device 200. Transmission time $Ti2$ and reception time $To2$ are assumed to be a transmission time and a reception time of a navigation message the onboard device 200 newly receives from the GPS satellite 2a thereafter.

[0058]

In the process at S24, the reception time ($To1$) of the authenticated navigation message is subtracted from reception time ($To2$) of the navigation message acquired at S21 to find a reception time difference ($To2 - To1$) which is a difference from the reception time of the authenticated navigation message to the reception time of the navigation message acquired at S21.

[0059]

It is then determined whether there is a match between the time ($Ti1 + (To2 - To1)$) resulting from adding the calculated reception time difference ($To2 - To1$) to the transmission time ($Ti1$) contained in the authenticated navigation message and the transmission time ($Ti2$) contained in the navigation message acquired at S21. The match here signifies not only a complete match but also an approximate match within a range of an error. The match here can be rephrased as consistency.

[0060]

It is determined that there is the continuity between the transmission time contained in the authenticated navigation message and the transmission time contained in the navigation message acquired at S21 if a match is determined between the time ($Ti1 + (To2 - To1)$) and the transmission time ($Ti2$). It is determined that there is no continuity if no match is determined.

[0061]

In an alternative configuration, the process at S24 may determine whether there is a match between the time ($To2 - To1$) resulting from subtracting the reception time ($To1$) of the authenticated navigation message from the reception time ($To2$) of the navigation message acquired at S21 and the time ($Ti2 - Ti1$) resulting from subtracting the transmission time ($Ti1$) contained in the authenticated navigation message from the transmission time ($Ti2$) contained in the navigation message acquired at S21.

[0062]

It may be determined that there is the continuity between the transmission time contained in the authenticated navigation message and the transmission time contained in the navigation message acquired at S21 if a match is determined

between the time (To2 - To1) and the time (Ti2 - Ti1). The controller 220 may determine no continuity if no match is determined.

[0063]

5 At S25 in FIG. 5, when it is determined that there is the continuity between the transmission time contained in the authenticated navigation message and the transmission time contained in the navigation message acquired at S21 (S25: YES), the process proceeds to S26. At S26, it is determined that the navigation message acquired at S21 is authentic and the process is ended.

[0064]

10 When it is determined that there is no continuity between the transmission time contained in the authenticated navigation message and the transmission time contained in the navigation message acquired at S21 (S25: NO), it is determined that the navigation message acquired at S21 is unauthentic and the process is ended. S25 and S26 correspond to a simplified determination portion.

15 [0065]

In an alternative configuration, if the determination results in NO at S25, it may be determined that the navigation message acquired at S21 is unauthentic.

[0066]

20 The first embodiment may delete the authenticated navigation message stored in the memory of the controller 220 when a timer to measure the reception time, i.e., the time the satellite receiver 230 receives a navigation message, indicates a lapse of time that causes a time lag in excess of a range within which the time or an interval of time is assumed to be consistent in the process at S24. After the authenticated navigation message is deleted, the controller 220 may use
25 the authentication center 120 to authenticate a navigation message newly received from the same GPS satellite 2 and store the successfully authenticated

navigation message as an authenticated navigation message in the memory.

[0067]

<Summary of the First Embodiment>

According to the first embodiment, the onboard device 200 authenticates
5 a navigation message using the authentication center 120. Once the
authentication is successful, the onboard device 200 can determine whether a
newly received navigation message is authentic, based on the authenticated
navigation message and the reception time stored in the memory, when the newly
received navigation message is received from the GPS satellite 2 equal to the
10 source of the successfully authenticated navigation message. Therefore, the
onboard device 200 need not receive the H matrix from the authentication center
120 in terms of a newly received navigation message, reducing a communication
processing load on the authentication center 120.

[0068]

15 When a repeater or a simulator is used, the continuity corresponding to a
reception time difference is not ensured between the transmission time contained
in the authenticated navigation message and the transmission time of the
navigation message newly received by the onboard device 200.

[0069]

20 According to the first embodiment, when the continuity corresponding to a
reception time difference may not be ensured between the transmission time
contained in the authenticated navigation message and the transmission time of
the navigation message newly received by the onboard device 200, the newly
received navigation message is not determined to be authentic. Therefore, the
25 embodiment can prevent a navigation message from being determined to be
authentic when a repeater or a simulator is used, and can improve the accuracy to

assume a navigation message to be authentic.

[0070]

<First Modification>

There has been described the first embodiment that determines whether a
5 received navigation message is authentic depending on whether the continuity
corresponding to a reception time difference exists between the transmission time
contained in the authenticated navigation message and the transmission time of a
navigation message newly received by the onboard device 200 in terms of the
same GPS satellite 2. However, this is not limiting.

10 [0071]

For example, a configuration (hereinafter referred to as a first
modification) may determine whether a received navigation message is authentic
depending on whether the continuity exists between two pseudo-distances,
namely, between one pseudo-distance determined from the transmission time and
15 the reception time of the authenticated navigation message and the other
pseudo-distance determined from the transmission time and the reception time of
a newly received navigation message. The first modification equals the first
embodiment except that the controller 220 of the onboard device 200 performs a
partially different process. In detail, the first modification differs from the first
20 embodiment in part of the simplified determination process performed by the
controller 220.

[0072]

<Simplified Determination Process in the First Modification>

The simplified determination process performed by the controller 220 of
25 the onboard device 200 according to the first modification will be described with
reference to a flowchart in FIG. 7. The flowchart in FIG. 7 may also start when

the satellite receiver 230 of the onboard device 200 receives a navigation message from GPS satellite 2, for example. The flowchart in FIG. 7 may be also performed on each of navigation messages from the multiple GPS satellites 2 when the satellite receiver 230 receives the navigation messages from the GPS satellites 2 within one cycle of successive output from the satellite receiver 230 to the controller 220.

[0073]

At S31, a reception time difference is determined. The reception time difference is a difference between the reception time of the authenticated navigation message stored in the memory of the controller 220 and the reception time of a navigation message newly received by the satellite receiver 230. The process proceeds to S32 if the reception time difference is within a specified time period (S31: YES). When the reception time difference exceeds the specified time period (S31: NO), it is determined that the navigation message newly received by the satellite receiver 230 is unauthentic and the process is ended.

[0074]

The specified time period is so estimated that the pseudo-distance determined from the transmission time of a navigation message from the GPS satellite 2 and the reception time of the navigation message at the satellite receiver 230 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 is unlikely to cause a difference greater than or equal to a threshold value used for S35 described later. The specified time period can be set to any value.

[0075]

The pseudo-distance signifies a distance between the GPS satellite 2 and the satellite receiver 230 calculated by multiplying the light speed and the

propagation time that is determined from the transmission time at the GPS satellite 2 and the reception time at the satellite receiver 230.

[0076]

The process at S32 through S34 equals that at S21 through S23. At S35,
5 it is determined whether the continuity exists between the authenticated navigation message and the navigation message that is newly acquired by the satellite receiver 230 and is determined at S34 to contain the matching satellite number. In detail, it is determined whether the continuity exists between two pseudo-distances. One pseudo-distance is found from the transmission time
10 contained in the authenticated navigation message and the reception time of the authenticated navigation message. The other pseudo-distance is found from the transmission time contained in the navigation message newly received by the satellite receiver 230 and the reception time of the navigation message. S35 also corresponds to a continuity determination portion.

15 [0077]

The pseudo-distance signifies a distance between the GPS satellite 2 and the satellite receiver 230 calculated by multiplying the light speed and the propagation time that is determined from the transmission time at the GPS satellite 2 and the reception time at the satellite receiver 230.

20 [0078]

An example of the process at S35 will be described using FIG. 8. As a precondition for the example in FIG. 8, the onboard device 200 successfully authenticates a navigation message originated from the GPS satellite 2a using the authentication center 120. The onboard device 200 thereafter receives the
25 navigation message originated from the GPS satellite 2a.

[0079]

Pseudo-distance p_1 is found from the transmission time of the authenticated navigation message and the reception time of the authenticated navigation message. Pseudo-distance p_2 is found from the transmission time of a navigation message thereafter newly received by the satellite receiver 230 from the GPS satellite 2a and the reception time of the navigation message.

[0080]

At S35, the pseudo-distance (p_1) is calculated by multiplying the light speed and the propagation time that is determined from the transmission time of the authenticated navigation message and the reception time of the authenticated navigation message. The pseudo-distance (p_2) is calculated by multiplying the light speed and the propagation time that is determined from the transmission time of a navigation message newly received by the satellite receiver 230 and the reception time of the navigation message.

[0081]

The pseudo-distance (p_2) is subtracted from the pseudo-distance (p_1) to find the absolute value of the difference ($|p_1 - p_2|$), and it is determined whether the absolute value is smaller than a threshold value. The threshold value here approximates to the upper limit of a change in the pseudo-distance between the GPS satellite 2 and the satellite receiver 230 when a repeater or a simulator as above is not used. The change is supposed to occur due to a lapse of the specified time period at S31.

[0082]

It is determined that there is the continuity between the authenticated navigation message and the navigation message newly received by the satellite receiver 230 if the difference is smaller than the threshold value. It is determined that there is no continuity if the difference is greater than or equal to the threshold

value.

[0083]

At S36 in FIG. 7, when it is determined that there is the continuity between the authenticated navigation message and the navigation message newly received by the satellite receiver 230 (S36: YES), the process proceeds to S37. At S37, it is determined that the navigation message newly received by the satellite receiver 230 is authentic and the process is ended.

[0084]

The specified time period at S31 is provided as a condition that allows S36 to determine the presence and absence of the continuity of navigation messages with no use of a repeater or a simulator as above.

[0085]

When no continuity is determined between the authenticated navigation message and the navigation message newly received by the satellite receiver 230 (S36: NO), it is determines that the navigation message newly received by the satellite receiver 230 is unauthentic and the process is ended. S36 and S37 also correspond to the simplified determination portion.

[0086]

<Summary of the First Modification>

According to the first modification, like the first embodiment, the onboard device 200 authenticates a navigation message using the authentication center 120. Once the authentication is successful, the onboard device 200 can determine whether a newly received navigation message is authentic, based on the authenticated navigation message and the reception time stored in the memory, when the newly received navigation message is received from the GPS satellite 2 equal to the source of the successfully authenticated navigation

message. Therefore, the onboard device 200 need not receive the H matrix from the authentication center 120 in terms of a newly received navigation message, reducing a communication processing load on the authentication center 120.

[0087]

5 When a repeater is used to duplicate a signal from the GPS satellite 2, a delay in the reception time of a navigation message occurs with respect to the authentic navigation message. When a simulator capable of imitatively generating a signal from the GPS satellite 2 is used, a discrepancy in the transmission time or the reception time of a navigation message occurs with
10 respect to the authentic navigation message. Specifically, when a repeater or a simulator is used, a pseudo-distance determined from the transmission time and the reception time greatly varies and the continuity is lost.

[0088]

15 In the first modification, a newly received navigation message is determined to be authentic if no continuity is found between two pseudo-distances, namely, one pseudo-distance determined from the transmission time contained in the authenticated navigation message and the reception time of the authenticated navigation message and the other pseudo-distance determined from the transmission time and the reception time of the newly received navigation
20 message. The first modification can prevent a navigation message from being determined to be authentic when a repeater or a simulator is used, and can improve the accuracy to determine a navigation message to be authentic.

[0089]

<Second Modification>

25 The embodiment has described the example of using only a navigation message received from the GPS satellite 2 for positioning. A navigation

message received from the QZS satellite 3 may be used for positioning. In this case, a navigation message received from the QZS satellite 3 may be authenticated similarly to the GPS satellite 2.

[0090]

5 As an example of the second modification, the monitor station 110 receives a navigation message from the QZS satellite 3 and generates a RAND message from the received navigation message. The authentication center 120 generates parity data based on the RAND message. The authentication center 120 transmits the generated parity data to the master control station 130. The
10 master control station 130 transmits the parity data to the QZS satellite 3. The QZS satellite 3 broadcasts a navigation message containing the parity data to the earth.

[0091]

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

20 [0092]

<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
25 organization, other configurations may be employed in the authentication method (hereinafter referred to as a third modification).

[0093]

<Fourth Modification>

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

[0094]

Although embodiments and the configurations have been illustrated, embodiments and the configurations of the present disclosure are not limited to
10 those illustrated above. For example, the scope of embodiments and 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 (200) comprising:

5 a satellite receiver (230) for receiving a navigation message from an artificial satellite used for a satellite positioning system;

an authentication information receiver (S5) for receiving, from an authentication center, authentication information corresponding to the navigation message received from the artificial satellite;

10 a center usage authentication portion (S9 to S11) 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;

15 a continuity determination portion (S24, S35) for, when the satellite receiver receives a new navigation message from the artificial satellite that is a source of the navigation message authenticated by the center usage authentication portion, determining whether or not there is continuity between the navigation message authenticated by the center usage authentication portion and the new navigation message; and

20 a simplified determination portion (S25, S26, S36, S37) for determining that the new navigation message is authentic when the continuity determination portion determines that there is continuity between the new navigation message and the navigation message authenticated by the center usage authentication portion and

25 determining that the new navigation message is unauthentic when the continuity determination portion determines that there is no continuity between the new navigation message and the navigation message authenticated

by the center usage authentication portion.

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

5 the navigation message contains a transmission time thereof; and

the continuity determination portion (S24) determines whether or not an
transmission time contained in the navigation message authenticated by the
center usage authentication portion and an transmission time contained in the
new navigation message have therebetween continuity that corresponds to a
10 reception time difference between a reception time of the authenticated navigation
message and a reception time of the new navigation message.

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

15 the navigation message contains a transmission time thereof;

the new navigation message is a navigation message that is received by
the satellite receiver within a specified time period from a reception time of the
navigation message authenticated by the center usage authentication portion; and

when a difference between two pseudo-distances, one of which is
20 determined from a transmission time and a reception time of the navigation
message authenticated by the center usage authentication portion and the other
of which is determined from a transmission time and a reception time of the new
navigation message, is smaller than a threshold value, the continuity
determination portion (S35) determines that there is the continuity between the
25 navigation message authenticated by the center usage authentication portion and
the new navigation message.