

DESCRIPTION

TITLE OF INVENTION: NAVIGATION MESSAGE AUTHENTICATION TYPE
POSITIONING APPARATUS

CROSS REFERENCE TO RELATED APPLICATIONS

5 [0001]

The present application is based on Japanese Patent Application No. 2014-21633 filed on February 6, 2014, the disclosure of which is incorporated herein by reference.

TECHNICAL FIELD

10 [0002]

The present disclosure relates to a navigation message authentication type positioning apparatus that authenticates a navigation message received from an artificial satellite used in a satellite positioning system.

15 BACKGROUND ART

[0003]

Conventionally, a technique is known that receives a navigation message transmitted from an artificial satellite used in a satellite positioning system with a receiver to determine a position.

20 [0004]

Due to the recent development of a repeater that duplicates a signal from an artificial satellite, a simulator that is capable of artificially generating a signal from an artificial satellite, or the like, a malicious person may perform falsification or spoofing of position information.

25 [0005]

Patent Literature 1 discloses a technique which authenticates whether a navigation message received by a receiver is an authentic navigation message from an artificial satellite used in a satellite positioning system. In the technique disclosed in Patent Literature 1, the receiver
5 accesses a database in an authentication center, and acquires data used to authenticate a target artificial satellite from the satellite number and satellite time included in the navigation message received from an artificial satellite. Then, using the data acquired from the authentication center, the receiver authenticates whether the received navigation message is an authentic
10 navigation message from the artificial satellite used in the satellite positioning system.

[0006]

The inventors of the present application have found the following.

[0007]

15 In the technique disclosed in Patent Literature 1, when there are multiple artificial satellites from which navigation messages can be received by the host apparatus, it is necessary to perform communication with the authentication center for the navigation messages from all the artificial satellites and authenticate whether the navigation messages are authentic
20 navigation messages. In general, at one location, navigation messages can be received from artificial satellites the number of which is greater than the number of artificial satellites required for positioning. Accordingly, when authentication of navigation messages is performed for all the artificial satellites from which the navigation messages have successfully been
25 received, processing loads resulting from communication and arithmetic operations in the authentication center and the host apparatus and the time required for authentication may enormously increase.

PRIOR ART LITERATURE

PATENT LITERATURE

30

[0008]

Patent Literature 1: JP 2013-130395 A

SUMMARY OF INVENTION

[0009]

It is an object of the present disclosure to provide a navigation message authentication type positioning apparatus that allows higher accuracy positioning to be performed, while reducing the time required for authentication and processing loads.

[0010]

A navigation message authentication type positioning apparatus according to an example of the present disclosure includes: a satellite receiver that receives a navigation message from an artificial satellite used in a satellite positioning system; an authentication information acquisition portion that acquires, from an authentication center, authentication information in accordance with the navigation message received from the artificial satellite; an authentication portion that authenticates that the navigation message received by the satellite receiver is authentic, by using the authentication information acquired by the authentication information acquisition portion; and a positioning portion that determines a position of the navigation message authentication type positioning apparatus (a host apparatus) based on the navigation message received by the satellite receiver from multiple artificial satellites. The navigation message authentication type positioning apparatus includes: an evaluation value specification portion that specifies a signal quality evaluation value that evaluates a signal quality of the navigation message received by the satellite receiver; and a selection portion that selects, based on the signal quality evaluation value specified by the evaluation value specification portion and from among the artificial satellites from which the satellite receiver has successfully received the navigation message, the artificial satellite that has transmitted the navigation message having the signal quality that is rated excellent. The authentication information acquisition portion acquires only the authentication information in accordance with the navigation message received from the artificial satellite selected by the selection portion. The authentication portion authenticates that the navigation message received by the satellite receiver from the artificial satellite selected by the selection

portion is authentic, by using the authentication information acquired by the authentication information acquisition portion. The positioning portion determines the position of the navigation message authentication type positioning apparatus based on the navigation message received from the
5 artificial satellite selected by the selection portion.

[0011]

According to this configuration, it is sufficient to narrow down the artificial satellites from which the satellite receiver has successfully received the navigation messages to the artificial satellite selected by the selection
10 portion, acquire only the authentication information in accordance with the navigation message received from the selected artificial satellite, and authenticate the received navigation message. Thus, it may be possible to reduce the time required for authentication and processing loads compared to a case of acquiring the authentication information in accordance with the
15 navigation messages received from all the artificial satellites from which the satellite receiver has successfully received the navigation messages and authenticating the received navigation messages.

[0012]

In addition, the selection portion selects the artificial satellite that
20 has transmitted the navigation message having the signal quality that can be rated as excellent based on the signal quality evaluation value specified by the evaluation value specification portion, and the positioning portion determines the position of the host apparatus based on the navigation message received from the selected artificial satellite. This may increase
25 the possibility of positioning using the navigation message having the excellent signal quality. Thus, it may be possible to perform positioning with higher accuracy, while reducing the time required for authentication and processing loads.

BRIEF DESCRIPTION OF DRAWINGS

30 [0013]

The above and other aspects, features and advantages of the present disclosure will become more apparent from the following detailed description made with reference to the accompanying drawings. In the drawings:

5 FIG. 1 is a diagram showing an example of a schematic configuration of a navigation message authentication system in a first embodiment;

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

10 FIG. 3 is a block diagram showing an example of a schematic configuration of a first vehicle onboard apparatus;

 FIG. 4 is a flowchart showing an example of the flow of a first authentication target satellite selection process in the first vehicle onboard apparatus in the first embodiment;

15 FIG. 5 is a diagram showing an example of a selected satellite list;

 FIG. 6 is a flowchart showing an example of the flow of an authentication related process in the first vehicle onboard apparatus in the first embodiment;

20 FIG. 7 is a flowchart showing an example of the flow of a positioning process in the first vehicle onboard apparatus in the first embodiment;

 FIG. 8 is a flowchart showing an example of the flow of an NMA related information transmission process in the first vehicle onboard apparatus in the first embodiment;

25 FIG. 9 is a diagram showing an example of NMA related information;

 FIG. 10 is a block diagram showing an example of a schematic configuration of a second vehicle onboard apparatus;

30 FIG. 11 is a flowchart showing an example of the flow of a second authentication target satellite selection process in the second vehicle onboard apparatus in the first embodiment;

 FIG. 12 is a flowchart showing an example of the flow of the first authentication target satellite selection process in the first vehicle onboard apparatus in a first modification;

FIG. 13 is a flowchart showing an example of the flow of the first authentication target satellite selection process in the first vehicle onboard apparatus in a second modification; and

5 FIG. 14 is a flowchart showing an example of the flow of the first authentication target satellite selection process in the first vehicle onboard apparatus in a third modification.

PREFERRED EMBODIMENTS FOR CARRYING OUT INVENTION

[0014]

The following will describe the embodiments of the present
10 disclosure using the drawings.

[0015]

(First embodiment)

As shown in FIG. 1, a navigation message authentication system 1
in a first embodiment includes a monitor station 110, an authentication center
15 120, a master control station 130, a first vehicle onboard apparatus 200, and
a second vehicle onboard apparatus 300. It is supposed that a vehicle
using the first vehicle onboard apparatus 200 is a vehicle A, and a vehicle
using the second vehicle onboard apparatus 300 is a vehicle B. Each of the
first vehicle onboard apparatus 200 and the second vehicle onboard
20 apparatus 300 corresponds to a navigation message authentication type
positioning apparatus in the present disclosure.

[0016]

<Schematic configuration of navigation message authentication
system 1>

25 The monitor station 110 receives the GPS waves transmitted from
GPS satellites 2a to 2f included in a GPS as one of satellite positioning
systems. The GPS satellites 2a to 2f correspond to an artificial satellite in
the present disclosure. The GPS satellites 2a to 2f will be hereinafter
referred to as a GPS satellite 2 when no distinction is made therebetween.
30 As is known, a GPS wave includes a navigation message. The monitor
station 110 demodulates the received GPS wave, extracts the navigation

message therefrom, and sends the navigation message to the authentication center 120. When GPS waves are received from multiple GPS satellites 2, the navigation message is extracted from each of the GPS waves and is sent to the authentication center 120.

5 [0017]

As is known, the navigation message includes Ephemeris data and Almanac data. The Almanac data includes orbit information about not only the GPS satellites 2 as the transmitters of the navigation messages but also all the GPS satellites 2 on an orbit. From the orbit information and the
10 transmission times of the navigation messages, the satellite positions of all the GPS satellites 2 can be calculated. The Ephemeris data includes orbit information about the GPS satellites 2 as the transmitters of the navigation messages. From the orbit information and the transmission times of the navigation messages, it may be possible to calculate the satellite position of
15 the GPS satellites 2 as the transmitters of the navigation messages with higher accuracy.

[0018]

The authentication center 120 produces parity data from a navigation message and an H matrix, which is a cryptography key. Then,
20 the authentication center 120 sends a signal including the parity data to the master control station 130. The authentication center 120 also performs communication with the first vehicle onboard apparatus 200 and the second vehicle onboard apparatus 300. The authentication center 120 will be described in detail later using FIG. 2.

25 [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 QZS satellite) 3. The QZS satellite 3 broadcasts the navigation message including the parity data toward the ground.

30 [0020]

The first vehicle onboard apparatus 200 is a navigation message authentication (NMA) type vehicle onboard apparatus. The first vehicle onboard apparatus 200 communicates with the authentication center 120 to

authenticate that the navigation message received from the GPS satellite 2 is an authentic navigation message. A detailed description of the authentication will be given later using FIG. 6. The first vehicle onboard apparatus 200 performs a process which selects in advance the target GPS
5 satellite 2 to be subjected to the authentication.

[0021]

Besides, the first vehicle onboard apparatus 200 determines the present position of the host apparatus by using the navigation messages received from the multiple GPS satellites 2. To determine the present
10 position, the first vehicle onboard apparatus 200 uses the navigation messages received from at least three of the GPS satellites 2. The first vehicle onboard apparatus 200 further transmits information (hereinafter referred to as NMA related information) about the GPS satellite 2 as the transmitter of the navigation message that has succeeded in authentication.
15 A detailed description of the first vehicle onboard apparatus 200 will be given later using FIG. 3.

[0022]

The second vehicle onboard apparatus 300 is also a navigation message authentication type vehicle onboard apparatus, similarly to the first
20 vehicle onboard apparatus 200. The second vehicle onboard apparatus 300 also performs the authentication and positioning, similarly to the first vehicle onboard apparatus 200. In addition, the second vehicle onboard apparatus 300 receives the NMA related information transmitted from the first vehicle onboard apparatus 200, and performs a process that selects in
25 advance the target GPS satellite 2 to be subjected to authentication using the NMA related information. A detailed description of the second vehicle onboard apparatus 300 will be given later using FIG. 10.

[0023]

<Detailed configuration of authentication center 120>

30 As shown in FIG. 2, the authentication center 120 includes a control portion 122, a data memory portion 124, and a communication portion 126.

[0024]

The control portion 122 is a computer including a CPU, a ROM, a RAM, or the like, and controls the data memory portion 124 and the communication portion 126. The CPU executes a program stored in the ROM using a temporary storing function of the RAM so as to function as a
5 RAND message generation portion 1221, a SEED value generation portion 1222, an H matrix calculation portion 1223, a parity calculation portion 1224, and a signal processing portion 1225. It should be noted that the functions of the portions 1221 to 1225 may be the same as the functions disclosed in Patent Literature 1.

10 [0025]

The RAND message generation portion 1221 produces a RAND message from the navigation message acquired from the monitor station 110. In the RAND message, from the bit strings of the navigation message, TOC, AF0, and AF1, which are clock correction parameters included in the data of
15 a TOW (time of week) bit string and the Ephemeris data are arranged in order. TOW, TOC, AF0, and AF1 are data that specify the transmission time of a signal. Besides, AS Flag showing an anti-spool flag and a PRN (Pseudo Random Noise) ID showing a satellite number are added subsequently.

[0026]

20 RAND including TOW and PRN ID is data showing when and which one of the GPS satellites transmitted a signal. In addition, since TOW changes every 6 seconds and RAND includes PRN ID, it follows that RAND is generated every 6 seconds for each one of the GPS satellites 2 from which the monitor station 110 have received the navigation messages.

25 [0027]

The SEED value generation portion 1222 receives a PC clock as an input to generate a random number, generating a SEED value.

[0028]

30 The H matrix calculation portion 1223 uses the SEED value generated by the SEED value generation portion 1222 to calculate the H matrix corresponding to the SEED value on a one-by-one basis. As the H matrix, a known hash function may be used appropriately and a parity check matrix for performing, for example, LDPC (Low Density Parity Check) coding

may be used appropriately. Further, a generator matrix determined from the parity check matrix may be used.

[0029]

5 The parity calculation portion 1224 calculates the parity data based on the RAND message generated by the RAND message generation portion 1221 and the H matrix calculated by the H matrix calculation portion 1223.

[0030]

10 The signal processing portion 1225 inserts the parity data calculated by the parity calculation portion 1224 and the RAND message used for the calculation into the navigation message to be transmitted from the QZS satellite 3. Then, the signal processing portion 1225 sends the navigation message into which the parity data and the RAND message have been inserted to the master control station 130.

[0031]

15 Simultaneously with the signal insertion, the signal processing portion 1225 also associates the parity data calculated by the parity calculation portion 1224, the RAND message used for the calculation of the parity data, the H matrix, and the SEED value used for the calculation of the H matrix with each other, and stores them in the data memory portion 124.

20 [0032]

Every time the RAND message generation portion 1221 generates the RAND message, the signal processing portion 1225 inserts the RAND message and the parity data into the navigation message to be transmitted from the QZS satellite 3. Accordingly, the RAND message generation
25 portion 1221, the SEED value generation portion 1222, the H matrix calculation portion 1223, and the parity calculation portion 1224 also perform the processes every time the RAND message generation portion 1221 generates a RAND message.

[0033]

30 When PRN ID, TOW, and the public key transmitted from the first vehicle onboard apparatus 200 are received by the communication portion 126, the H matrix selection portion 1226 selects the H matrix corresponding to the received PRN ID and TOW from among the H matrixes stored in the

data memory portion 124. Then, the H matrix selection portion 1226 encrypts the selected H matrix using the public key, and returns the encrypted H matrix to the first vehicle onboard apparatus 200.

[0034]

5 <Detailed configuration of first vehicle onboard apparatus 200>

The navigation message broadcasted by the QZS satellite 3 is received by a reception portion 211 included in a communication portion 210 of the first vehicle onboard apparatus 200. As shown in FIG. 3, the first vehicle onboard apparatus 200 includes the communication portion 210, a
10 control portion 220, and a satellite receiver 230.

[0035]

The communication portion 210 includes the reception portion 211 and a transmission portion 212. The communication portion 210 includes a narrow area communication function and a wide area communication
15 function. The narrow area communication function covers a communication distance of, for example, several hundreds of meters. The wide area communication function covers a communication distance of, for example, several kilometers, and by performing communication with a base station in a public communication network, the communication portion 210 can perform
20 communication with another communication apparatus within the communication distance in the public communication network. Using the narrow area communication function, the communication portion 210 performs a vehicle-to-vehicle communication with a communication portion 310 of the second vehicle onboard apparatus 300. Using the wide area
25 communication function, the communication portion 210 performs communication with the communication portion 126 of the authentication center 120.

[0036]

The satellite receiver 230 receives the electric waves transmitted
30 from the GPS satellites 2 and the QZS satellite 3 at fixed periods.

[0037]

The control portion 220 is a computer including a CPU, a ROM, a RAM, or the like, and controls the communication portion 210 and the

satellite receiver 230. The CPU executes a program stored in the ROM using the temporary storing function of the RAM to thus perform various processes such as the first authentication target satellite selection process shown in FIG. 4, the authentication related process shown in FIG. 6, the
5 positioning process shown in FIG. 7, and the NMA related information transmission process shown in FIG. 8.

[0038]

The outline of the authentication related process is a process related to the authentication of the signal received by the satellite receiver
10 230 as the authentic navigation message received from the GPS satellite 2. The first authentication target satellite selection process is a process that selects, from among the GPS satellites 2 from which the satellite receiver 230 can receive navigation messages, the target GPS satellites 2 to be subjected to the authentication related process. The positioning process is a process
15 that determines the present position of the host apparatus based on the navigation messages received by the satellite receiver 230 from the multiple GPS satellites 2 selected by the first authentication target satellite selection process. The NMA related information transmission process is a process which transmits the NMA related information including identification
20 information which allows the GPS satellites 2 selected by the first authentication target satellite selection process to be identified and authentication information showing whether the navigation messages from the GPS satellites 2 have succeeded in authentication.

[0039]

25 <First authentication target satellite selection process>

The first authentication target satellite selection process in the control portion 220 of the first vehicle onboard apparatus 200 using the flowchart shown in FIG. 4 will be explained. The flowchart in FIG. 4 may be configured appropriately to be started when the navigation message received
30 by the satellite receiver 230 from the GPS satellite 2 is output from the satellite receiver 230.

[0040]

The satellite receiver 230 receives the navigation messages from the multiple GPS satellites 2 within one cycle of output sequentially performed from the satellite receiver 230 to the control portion 220 and outputs the multiple navigation messages. The following description will be given herein by using, as an example, the case where the navigation messages from all the GPS satellites 2 that can be observed at the present position of the first vehicle onboard apparatus 200 are received by the satellite receiver 230 within the one cycle mentioned above and the multiple navigation messages are output to the control portion 220.

10 [0041]

In S1, the navigation messages from all the GPS satellites 2 that can be observed at the present position, which are output from the satellite receiver 230, are acquired. All the GPS satellites 2 that can be observed at the present position are hereinafter referred to merely as all observation GPS satellites 2.

15 [0042]

In S2, the process (hereinafter referred to as the selection related process) in subsequent S3 to S7 is started for each of the all observation GPS satellites 2. It is supposed herein that the number of the all observation GPS satellites 2 is equal to i , and the selection related process is repeatedly performed in succession on the first GPS satellite 2 through the i -th GPS satellite 2. In S2, the selection related process is started on the assumption that the ordinal number of the present target GPS satellite 2 is given by $x = 1$. The order in which all observation GPS satellites 2 are sequenced may be a magnitude order of PRN ID, may be based on another criterion, or may randomly be determined.

25 [0043]

In S3, the signal-to-noise ratio (hereinafter referred to as SN ratio) of the navigation message acquired from the x -th GPS satellite 2 in S1 is specified. As an example, the value detected by the SN ratio detection circuit included in the satellite receiver 230 may be specified as the SN ratio of the navigation message acquired in S1. As is known, an SN ratio is a logarithmic representation of the ratio of noise to a signal, and shows that, as

the value thereof is greater, the quality of the signal is more excellent. Accordingly, the SN ratio corresponds to a signal quality evaluation value in the present disclosure, and S3 corresponds to an evaluation value specification portion in the present disclosure.

5 [0044]

In S4, it is determined whether the SN ratio specified in S3 is equal to or greater than a threshold value. The threshold value mentioned herein may appropriately be an SN ratio having a signal quality that is excellent enough to say that the possibility of causing an error in the result of
10 positioning is low and has a value that can arbitrarily be set. When it is determined that the SN ratio specified in S3 is equal to or greater than a threshold value (YES in S4), the process moves to S5. When it is determined that the SN ratio specified in S3 is less than the threshold value (NO in S4), the process moves to S6.

15 [0045]

In S5, the GPS satellite 2 having the SN ratio specified in S3 and determined to be equal to or greater than the threshold value is selected as a target GPS satellite 2 to be subjected to the authentication related process, and then the process moves to S6. Accordingly, S5 corresponds to a
20 selection portion in the present disclosure.

[0046]

In S6, when the selection related process on each of the all observation GPS satellites 2 is completed, that is, when $x = i$ is satisfied (YES in S6), the process moves to S8. By contrast, when $x = i$ is not satisfied (NO
25 in S6), the process moves to S7.

[0047]

In S7, the $(x+1)$ -th GPS satellite 2 is newly set as the target of the selection related process, and the process returns to S4 to be repeated.

[0048]

30 In S8, when the selection related process on each of the all observation GPS satellites 2 is completed (that is, when $x = 1$ is satisfied), a list (hereinafter referred to as a selected satellite list) of the GPS satellites 2 selected in S5 is produced and stored in the memory of the control portion

220, and the process in FIG. 4 terminates. The selected satellite list stored in the memory is sequentially updated every time the first authentication target satellite selection process is newly performed.

[0049]

5 For example, the selected satellite list may be produced appropriately as a list in which the PRN IDs of all the GPS satellites 2 selected in S5 are listed. It is also preferable to store the SN ratios (that is, signal quality evaluation values) specified in S3 in association with the PRN IDs of the GPS satellites 2 in the memory.

10 [0050]

As an example, the selected satellite list may be configured appropriately such that, as shown in FIG. 5, the SN ratios as the signal quality evaluation values are associated with the PRN IDs of the GPS satellites 2. It is supposed that, in the example shown in FIG. 5, the GPS satellites 2a to 2f are the all observation GPS satellites 2 and the GPS satellite 2a having the PRN ID of 1, the GPS satellite 2b having the PRN ID of 5, the GPS satellite 2c having the PRN ID of 10, and the GPS satellite 2e having the PRN ID of 24 have been selected by the first authentication target satellite selection process.

20 [0051]

<Authentication related process>

A description will be given of the authentication related process in the control portion 220 of the first vehicle onboard apparatus 200 using the flowchart shown in FIG. 6. The flowchart in FIG. 6 may be configured appropriately to be started when the target GPS satellite 2 to be subjected to the authentication related process is selected by the first authentication target satellite selection process shown in FIG. 4.

[0052]

30 It is supposed that there may be a case where the satellite receiver 230 has erroneously received a signal from a repeater repeating a signal from the GPS satellite 2 or a signal from a simulator capable of simulatively generating a signal from the GPS satellite 2 as the navigation message included in a GPS wave.

[0053]

In S21, the navigation messages included in the GPS waves received from the GPS satellites 2 selected by the first authentication target satellite selection process shown in FIG. 4 are acquired from the satellite receiver 230.

[0054]

In S22, the navigation message received from the QZS satellite 3 is acquired from the reception portion 211. In S23, from each of the navigation messages acquired in S21, the PRN ID and the TOW are extracted.

10 [0055]

In S24, PRN ID and TOW extracted in S23 are transmitted together with the public key from the transmission portion 212 to the authentication center 120. The authentication center 120 encrypts the H matrix determined by PRN ID and TOW using the public key, and transmits the H matrix to the first vehicle onboard apparatus 200. The H matrix determined by PRN ID and TOW transmitted from the first vehicle onboard apparatus 200 to the authentication center 120 corresponds to authentication information in the present disclosure.

[0056]

20 In S25, the H matrix transmitted from the authentication center 120 is acquired from the reception portion 211. Accordingly, S25 corresponds to authentication information acquisition portion in the present disclosure. In S26, the encrypted H matrix acquired in S25 is decrypted using the secret key.

25 [0057]

In S27, the RAND message is generated from the navigation message that includes the PRN ID identical with the PRN ID transmitted in S24 of the navigation messages included in the GPS wave received from the GPS satellites 2.

30 [0058]

In S28, a comparison parity data is generated based on the RAND message produced in S27 and the H matrix decrypted in S26. In S29, it is

determined whether the comparison parity data produced in S28 matches the parity data extracted in S23.

[0059]

5 The H matrix decrypted in S26 is identical with the H matrix used by the authentication center 120 to produce the parity data. In addition, the parity data calculation portion 1224 of the authentication center 120 has calculated the parity data based on the H matrix and the RAND message.

[0060]

10 Accordingly, when the comparison parity data generated in S28 matches the parity data extracted in S23, it can be considered that the RAND message generated in S27 is identical with the RAND message generated by the authentication center 120.

[0061]

15 When the comparison parity data produced in S28 matches the parity data extracted in S23 (YES in S29), the process advances to S30, and determines that the authentication has succeeded. By contrast, when the two parity data items do not match (NO in S29), the process advances to S31 and determines that the authentication has failed. Accordingly, S29 to S31 correspond to an authentication portion in the present disclosure. After S30
20 and S31, the process advances to S32.

[0062]

In S32, when the determination of whether the authentication has succeeded or failed is completed for each of the navigation messages from all the GPS satellites 2 selected by the first authentication target satellite
25 selection process shown in FIG. 4 (YES in S32), the process in FIG. 6 terminates. By contrast, when the determination of whether the authentication has succeeded or failed has not be completed even for one of the navigation messages (NO in S32), the process returns to S22 to be repeated.

30 [0063]

Incidentally, there may not need to authenticate the navigation messages from all the GPS satellites 2 selected by the first authentication target satellite selection process. The configuration may also be such that

all the selected GPS satellites 2 are narrowed down to the GPS satellites 2 required for a positioning process described later or authentication is performed for at least one of the GPS satellites 2 required for the positioning process described later.

5 [0064]

<Positioning process>

A description will be given of the positioning process in the control portion 220 of the first vehicle onboard apparatus 200 using the flowchart shown in FIG. 7. The flowchart in FIG. 7 may be configured appropriately to
10 be started when the target GPS satellites to be subjected to the authentication related process are selected by the first authentication target satellite selection process shown in FIG. 4.

[0065]

In S41, from among the GPS satellites 2 selected by the first
15 authentication target satellite selection process shown in FIG. 4, the GPS satellites 2 the number of which is required for positioning are selected. The number of the GPS satellites 2 required for positioning may be either 4 or 3. When the GPS satellites 2 the number of which is required for positioning are selected, the GPS satellites 2 may be selected either in the order of the PRN
20 IDs in the selected satellite list (referring to FIG. 5) or in decreasing order of SN ratio as the signal quality evaluation value. When the GPS satellites 2 are selected in decreasing order of signal quality evaluation value, S41 also corresponds to the selection portion in the present disclosure.

[0066]

25 In S42, using the navigation messages received from the GPS satellites 2 selected in S41, the present position of the first vehicle onboard apparatus 200 is calculated by a known method, and the process in FIG. 7 terminates. Accordingly, S42 corresponds to a positioning portion in the present disclosure.

30 [0067]

Incidentally, in the positioning process, the positioning may be performed by using only the navigation messages that have succeeded in authentication in the authentication related process or the positioning may be

performed before the authentication related process. When the positioning performed before the authentication related process, and the authentication messages used for positioning include the one that has failed in authentication, positioning is performed again using only the navigation messages that have succeeded in authentication, the result of the positioning is not used or the result of the positioning is used only after the low reliability thereof is indicated.

[0068]

<NMA related information transmission process>

10 A description will be given of the NMA related information transmission process in the control portion 220 of the first vehicle onboard apparatus 200 using the flowchart shown in FIG. 8. The NMA related information transmission process shown in FIG. 8 and the authentication related process shown in FIG. 6 are performed in parallel. It is supposed that, even when authentication in the authentication related process has not been completed for all the GPS satellites 2 selected by the first authentication target satellite selection process, the flowchart in FIG. 8 starts. The flowchart in FIG. 8 may be configured appropriately to be started at, for example, fixed periods.

20 [0069]

In the NMA related information transmission process shown in the flowchart in FIG. 8, NMA related information including identification information that identifies the GPS satellites 2 selected by the first authentication target satellite selection process and authentication information that shows whether the authentication of the navigation messages from the GPS satellites 2 has succeeded is transmitted. The NMA related information transmitted from the first vehicle onboard apparatus 200 is used in the second vehicle onboard apparatus 300 to select the target GPS satellites 2 to be subjected to the authentication related process.

30 [0070]

In S51, it is determined for each of the GPS satellites 2 included in the selected satellite list produced in the first authentication target satellite

selection process shown in FIG. 4 whether authentication has succeeded in the authentication related process shown in FIG. 6.

[0071]

In S52, the NMA related information including the respective PRN
5 IDs of the GPS satellites 2 included in the selected satellite list and
information (hereinafter referred to as authentication information) about
whether each of the GPS satellites 2 has succeeded in authentication, which
has been determined in S51, is transmitted using the narrow area
communication function of the transmission portion 212, and the process
10 terminates. Accordingly, each of the PRN IDs corresponds to identification
information in the present disclosure and the transmission portion 212
corresponds to a transmission portion in the present disclosure.

[0072]

Using FIG. 9, a description will be given of an example of the NMA
15 related information. The NMA related information may be configured
appropriately such that, as shown in FIG. 9, the PRN ID of each of the GPS
satellites 2 is associated with information showing whether the GPS satellite
2 shown by the PRN ID has succeeded in authentication. As shown in, for
example, FIG. 9, the information showing whether the GPS satellite 2 has
20 succeeded in authentication may appropriately be a binary flag representing
either one of the two states where authentication has succeeded
("Succeeded" in the drawing) and where authentication has failed or has not
succeeded yet ("Not Yet" in the drawing). Alternatively, information
representing any of three states where authentication has succeeded, where
25 authentication has failed, and where authentication has not succeeded yet
may also be used.

[0073]

In the following description, it is supposed that, in the present
embodiment, the NMA related information transmitted from the transmission
30 portion 212 is received by the second vehicle onboard apparatus 300.

[0074]

<Detailed configuration of second vehicle onboard apparatus 300>

With referring to FIG. 10, the second vehicle onboard apparatus 300 as a receiver of the NMA related information will be explained. As shown in FIG. 10, the second vehicle onboard apparatus 300 includes the communication portion 310, a control portion 320, and a satellite receiver 330.

5 The communication portion 310 performs wireless communication with the communication portion 210 included in the first vehicle onboard apparatus 200.

[0075]

The communication portion 310 includes a reception portion 311 and a transmission portion 312. Similarly to the communication portion 210, the communication portion 310 includes a narrow area communication function and a wide area communication function. Similarly to the satellite receiver 230, the satellite receiver 330 receives electric waves transmitted from the GPS satellites 2 and the QZS satellite 3 at fixed periods.

10

15 [0076]

The control portion 320 is a computer including a CPU, a ROM, a RAM, or the like, and controls the communication portion 310 and the satellite receiver 330. The CPU executes a program stored in the ROM using the temporary storing function of the RAM to thus perform various processes such as the second authentication target satellite selection process shown in FIG. 11, the authentication related process as shown in FIG. 5, the positioning process as shown in FIG. 6, and the NMA related information transmission process as shown in FIG. 7.

20

[0077]

The outline of the second authentication target satellite selection process is a process which selects the target GPS satellites 2 to be subjected to the authentication related process from among the GPS satellites 2 from which the satellite receiver 330 can receive navigation messages using also the NMA related information received from the first vehicle onboard apparatus 200.

25

30

[0078]

The control portion 320 acquires the NMA related information received by the reception portion 311 from the first vehicle onboard

apparatus 200 and stores the NMA related information in a memory. The reception portion 311 corresponds to the reception portion in the present disclosure. The NMA related information stored in the memory may be configured appropriately to be processed in association with, for example,
5 each of the first vehicle onboard apparatus 200 as the transmitter and updated to new NMA related information from the same first vehicle onboard apparatus 200 when the new NMA related information is received therefrom.

[0079]

<Second authentication target satellite selection process>

10 The second authentication target satellite selection process in the control portion 320 of the second vehicle onboard apparatus 300 using the flowchart shown in FIG. 11 will be explained. The flowchart in FIG. 11 may be configured appropriately to be started when the navigation message received by the satellite receiver 330 from the GPS satellite 2 is output from
15 the satellite receiver 330 in the state where the NMA related information received from the first vehicle onboard apparatus 200 has been stored in the memory.

[0080]

In S61, the navigation messages from all the GPS satellites 2 that
20 can be monitored at the present position (that is, the all observation GPS satellites 2) that are output from the satellite receiver 300 are acquired.

[0081]

In S62, from the NMA related information received from the first vehicle onboard apparatus 200, the PRN IDs of the GPS satellites 2 which
25 have succeeded in the authentication of the navigation message are extracted. As an example, the PRN IDs associated with authentication information showing successful authentication may be extracted from the NMA related information. It is supposed that the number of the GPS satellites 2 which have succeeded in authentication is equal to k , and the
30 PRN IDs from the PRN ID (hereinafter referred to as PRN[1]) of the first GPS satellite 2 which has succeeded in authentication to the PRN ID (hereinafter referred to as PRN[k]) of the k -th GPS satellite 2 which has succeeded in authentication are extracted.

[0082]

In S63, the subsequent process in S64 to S72 (hereinafter referred to as the selection related process) is started for each of the all observation GPS satellites 2. Similar to S2 of the first authentication target satellite selection process, it is supposed that the number of the all observation GPS satellites 2 is equal to i , and the selection related process is repeatedly performed in succession on the all observation GPS satellites 2 from the first GPS satellite 2 to the i -th GPS satellite 2. In S63, the selection related process is started on the assumption that the present ordinal number of the present target GPS satellite 2 is given by $x = 1$.

[0083]

In S64, similar to S3, the SN ratio of the navigation message acquired from the x -th GPS satellite 2 in S61 is specified. Accordingly, S64 also corresponds to the evaluation value specification portion in the present disclosure.

[0084]

In S65, similar to S4, it is determined whether the SN ratio specified in S64 is equal to or greater than a threshold value. When the SN ratio specified in S64 is determined to be equal to or greater than the threshold value (YES in S65), the process moves to S66. By contrast, when the SN ratio specified in S64 is determined to be less than the threshold value (NO in S65), the process moves to S71.

[0085]

In S66, a process (hereinafter referred to as a correspondence determination process) determining whether all the PRN IDs extracted in S62 include the PRN ID corresponding to the PRN ID of the present target GPS satellites 2 of the selection related process is started. The correspondence determination process is repeatedly performed in succession on the PRN [1] through the PRN [k]. In S66, the correspondence determination process is started on the assumption that the ordinal number of the PRN ID of the present target GPS satellite 2 that has succeeded in authentication is given by $y = 1$.

[0086]

In S67, when it is determined that there is a match between the PRN ID of the present target GPS satellite 2 that has succeeded in authentication and the PRN ID of the present target GPS satellite 2 of the selection related process (an answer to whether $\text{PRN}[y] = x$ is satisfied is YES in FIG. 11), the process moves to S68. By contrast, when it is determined that there is no match therebetween (an answer to whether $\text{PRN}[y] = x$ is satisfied is NO in FIG. 11), the process moves to S69.

[0087]

A case where it is determined that there is a match in S67 can also be said otherwise to be a case where it is determined that the authentication of the navigation message from the present target GPS satellite 2 of the selection related process has already succeeded in the first vehicle onboard apparatus 200.

[0088]

In S68, the GPS satellite 2 that has the SN ratio specified in S64 and determined to be equal to or greater than the threshold value and that has been determined to have succeeded in the authentication of the navigation message in the first vehicle onboard apparatus 200 in S67 is selected as the target GPS satellite 2 to be subjected to the authentication related process and then the process moves to S71. Accordingly, S68 corresponds to the selection portion in the present disclosure.

[0089]

In S69, when the selection related process is completed for all the PRN IDs extracted in S62, that is, when $y = k$ is satisfied (YES in S69), the process moves to S71. By contrast, when $y = k$ is not satisfied (NO in S69), the process moves to S70.

[0090]

In S70, the PRN ID of the $(y+1)$ -th GPS satellite 2 that has succeeded in authentication is supposed to be the new target of the correspondence determination process and the process returns to S67 to be repeated.

[0091]

In S71, when the selection related process is completed for the all observation GPS satellites 2, that is, when $x = i$ is satisfied (YES in S71), the process moves to S73. By contrast, when $x = i$ is not satisfied (NO in S71), the process moves to S72.

5 [0092]

In S72, the $(x+1)$ -th GPS satellite 2 is supposed to be the new target of the selection related process and the process returns to S64 to be repeated.

[0093]

10 In S73, when the selection related process is completed with the all observation GPS satellites 2 (that is, when $x = i$ is satisfied), similar to S8, the selected satellite list of all the GPS satellites 2 selected in S68 is produced and stored in the memory of the control portion 220, and the process in FIG. 11 terminates. The selected satellite list stored in the memory is
15 sequentially updated every time the second authentication target satellite selection process is newly performed.

[0094]

Incidentally, in the second authentication target satellite selection process, as long as the configuration is such that the GPS satellites 2 having
20 succeeded in authentication are preferentially selected in the first vehicle onboard apparatus 200, the configuration is not limited to a configuration in which the target GPS satellites 2 are narrowed down to the GPS satellites 2 which have succeeded in authentication in the first vehicle onboard apparatus 200 and then a selection is made. For example, even though the
25 GPS satellites 2 have not succeeded in authentication yet in the first vehicle onboard apparatus 200, the navigation messages from the GPS satellites 2 that have succeeded in authentication in the first vehicle onboard apparatus 200 for the positioning process may be preferentially used as long as the SN ratios are equal to or greater than the threshold value. In this case also,
30 when the authentication information included in the NMA related information is information allowing for a distinction to be made between the GPS satellite 2 that has not succeeded yet in authentication and the GPS satellite 2 that has failed in authentication, it may be preferable not to select the GPS

satellite 2 that has failed in authentication even though the SN ratio is equal to or greater than the threshold value.

[0095]

5 In the second vehicle onboard apparatus 300, on each of the navigation messages from the GPS satellites 2 selected by the second authentication target satellite selection process, the authentication related process as shown in FIG. 5 and the positioning process as shown in FIG. 6 are performed. Alternatively, the second vehicle onboard apparatus 300 may also be configured such that, by the NMA related information
10 transmission process as shown in FIG. 7, the NMA related information about the GPS satellites 2 as the transmitters of the navigation messages that have succeeded in authentication in the second vehicle onboard apparatus 300 is transmitted to the outside by wireless communication.

[0096]

15 <Summarization of first embodiment>

According to the first embodiment, the first vehicle onboard apparatus 200 narrows down the GPS satellites 2 from which the satellite receiver 230 has successfully received the navigation messages to the GPS satellites 2 selected in the first authentication target satellite selection
20 process, and then performs the authentication related process related to the received navigation messages only on the selected GPS satellites 2. It may be possible to reduce the time required for authentication and processing loads in the first vehicle onboard apparatus 200 and the authentication center 120 in comparison with the case where the authentication related process is
25 performed on all the GPS satellites 2 from which the satellite receiver 230 has successfully received the navigation messages.

[0097]

In the first authentication target satellite selection process, the GPS satellites 2 that have provided the SN ratios which are high enough to say
30 that the navigation messages have excellent signal qualities are selected. Accordingly, by performing the positioning process based on the navigation messages received from the selected GPS satellites 2, it may be possible to perform positioning using the navigation messages that have the excellent

signal qualities. It may be possible to allow the first vehicle onboard apparatus 200 to perform positioning more accurately, while reducing the time required for authentication and processing loads.

[0098]

5 According to the first embodiment, the second vehicle onboard apparatus 300 also narrows down the GPS satellites 2 from which the satellite receiver 330 has successfully received the navigation messages to the GPS satellite 2 selected by the second authentication target satellite selection process, and then performs the authentication related process only
10 on the selected GPS satellites 2. Accordingly, it may be possible to reduce the time required for authentication and processing loads in the second vehicle onboard apparatus 300 and the authentication center 120.

[0099]

15 In the second authentication target satellite selection process, the GPS satellites 2 which have succeeded in authentication in the first vehicle onboard apparatus 200 are preferentially selected based on the NMA related information transmitted from the first vehicle onboard apparatus 200. It may be possible that the GPS satellites 2 each having a high probability of succeeding in authentication even in the second vehicle onboard apparatus
20 300 is preferentially selected. Thus, the possibility of selecting the GPS satellites 2 which may fail in authentication in the second vehicle onboard apparatus 300 is lowered, so that it may be possible to reduce the labor of performing useless authentication.

[0100]

25 In addition, in the second authentication target satellite selection process also, the GPS satellites 2 that have provided the SN ratios which are high enough to say that the navigation messages have excellent signal qualities are selected. Accordingly, by performing the positioning process based on the navigation messages received from the selected GPS satellites
30 2, it may be possible to perform positioning with higher accuracy.

[0101]

 The GPS satellites 2 selected in the first authentication target satellite selection process in the first vehicle onboard apparatus 200 have

high possibilities of having excellent signal qualities. Accordingly, the possibility may be high that the same applies also to the second vehicle onboard apparatus 300 located around the first vehicle onboard apparatus 200. The probability may be high that the individual situations in which the first and second vehicle onboard apparatus 200 and 300 are placed are similar to each other.

[0102]

In the configuration of first embodiment, the NMA related information is received by vehicle-to-vehicle communication from the first vehicle onboard apparatus 200. Accordingly, the distance between the second vehicle onboard apparatus 300 which receives the NMA related information and the first vehicle onboard apparatus 200 as the transmitter is relatively short. Therefore, by preferentially selecting the GPS satellites 2 that have succeeded in authentication in the first vehicle onboard apparatus 200 based on the NMA related information, it is possible for the second vehicle onboard apparatus to preferentially select the GPS satellites which have transmitted the navigation messages having excellent signal qualities. Thus, it is possible for the second vehicle onboard apparatus 300 to perform positioning with higher accuracy, while reducing the time required for authentication and processing loads.

[0103]

In the present embodiment, the second vehicle onboard apparatus 300 corresponds to a navigation message authentication type positioning apparatus, and the first vehicle onboard apparatus 200 corresponds to a different navigation message authentication type positioning apparatus.

[0104]

<First modification>

In the first embodiment, the description has been given of the configuration in which, in the first authentication target satellite selection process in the first vehicle onboard apparatus 200, all the GPS satellites 2 determined to have the SN ratios which are equal to or greater than the threshold value are selected. The configuration is not necessarily limited to this. For example, a configuration (hereinafter referred to as a first

modification) may also be used in which a predetermined plural number of GPS satellites 2 that have transmitted the navigation messages having the signal qualities that can be rated more excellent are selected in decreasing order of signal quality.

5 [0105]

The navigation message authentication system 1 in a first modification using the drawings will be explained. Incidentally, for the convenience of description, members having the same functions as those of the members shown in the drawings used to describe the embodiment are designated by the same reference numerals and a description thereof is omitted.

[0106]

The navigation message authentication system 1 in the first modification is the same as the navigation message authentication system 1 in the first embodiment except that a part of the first authentication target satellite selection process is different.

[0107]

<First authentication target satellite selection process in first modification>

20 A description will be given herein of the first authentication target satellite selection process in the control portion 220 of the first vehicle onboard apparatus 200 in the first modification using the flowchart shown in FIG. 12. Similarly to the flowchart in FIG. 4, the flowchart in FIG. 12 may also be configured appropriately to be started when the navigation message received by the satellite receiver 230 from the GPS satellite 2 is output from the satellite receiver 230.

[0108]

30 The process in S81 to S87 is the same as in S1 to S7. Accordingly, S83 also corresponds to the evaluation value specification portion in the present disclosure, and S85 also corresponds to the selection portion in the present disclosure.

[0109]

In S88, a predetermined number of the GPS satellites 2 having higher SN ratios included in the selected satellite list stored in the memory of the control portion 22 are further selected from among all the GPS satellites 2 selected in S85 in decreasing order of SN ratio. Accordingly, S88 also
5 corresponds to the selection portion in the present disclosure. The predetermined number may appropriately be the number of the GPS satellites 2 required for the positioning process, which is, for example, four.

[0110]

In S89, the selected satellite list of the GPS satellites 2 selected in
10 S88 is produced and stored in the memory of the control portion 220. The process in FIG. 12 terminates. The selected satellite list stored in the memory is sequentially updated every time the first authentication target satellite selection process is newly performed.

[0111]

15 <Summarization of first modification>

According to the first modification, in the same manner as in the first embodiment, it is possible to allow the first vehicle onboard apparatus 200 to perform positioning with higher accuracy, while reducing the time required for authentication and processing loads. According to the first modification, the
20 predetermined number of GPS satellites 2 that provide higher SN ratios are further selected in decreasing order of SN ratio. It may be possible to perform positioning using the navigation messages having particularly excellent signal qualities. Thus, it may be possible to allow the first vehicle onboard apparatus 200 to perform positioning with much high accuracy,
25 while further reducing the time required for authentication and processing loads.

[0112]

<Second modification>

The description has been given of the configuration in which, in the
30 first authentication target satellite selection process in the first vehicle onboard apparatus 200, the GPS satellites 2 having the SN ratios determined to be equal to or greater than the threshold value are selected, but the configuration is not limited to this. For example, a configuration (hereinafter

referred to as a second modification) may also be used in which the GPS satellites 2 are selected using elevation angles of the GPS satellites 2 as a condition for selection.

[0113]

5 A description will be given herein of the navigation message authentication system 1 in the second modification using the drawings. Incidentally, for the convenience of description, members having the same functions as those of the members shown in the drawings used to describe the embodiment are designated by the same reference numerals and a
10 description thereof is omitted.

[0114]

 The navigation message authentication system 1 in the second modification is the same as the navigation message authentication system 1 in the first embodiment except that a part of the first authentication target
15 satellite selection process is different.

[0115]

 <First authentication target satellite selection process in second modification>

 A description will be given herein of the first authentication target
20 satellite selection process in the control portion 220 of the first vehicle onboard apparatus 200 in the second modification using the flowchart shown in FIG. 13. The flowchart in FIG. 13 is obtained by replacing only the process in S3 and S4 in the flowchart in FIG. 4, and shows only the extracted part of the process in S3a and S4a as a replacement for the process in S3
25 and S4.

[0116]

 In S3a subsequent to S2, the satellite position of the x-th GPS satellite 2 is calculated from the orbit information included in the navigation message obtained from the x-th GPS satellite 2 in S1 and from the
30 transmission time of the navigation message. Then, from the calculated satellite position and the present position of the first vehicle onboard apparatus 200, the elevation angle of the x-th GPS satellite 2 is specified.

[0117]

The orbit information may be either the Ephemeris data or the Almanac data but, from the viewpoint of accuracy, the Ephemeris data is preferred. The configuration may appropriately be such that, as the present position of the first vehicle onboard apparatus 200, the value obtained in the previous positioning is used as long as the travel distance from the previously determined position is less than a predetermined distance (for example, 100 m). Alternatively, a position estimated by autonomous navigation using the position obtained in the previous positioning may be used as a reference point.

10 [0118]

The elevation angle is the angle formed between the straight line connecting the GPS satellite 2 and the present position of the first vehicle onboard apparatus 200 and a horizon plane based on the present position. It is known that, as the elevation angle is smaller, a measurement error increases. In other words, the elevation angle shows that, as the elevation angle is larger, a navigation message having a more excellent signal quality is obtained. Accordingly, the elevation angle corresponds to the signal quality evaluation value in the present disclosure, and S3a corresponds to the evaluation value specification portion in the present disclosure.

20 [0119]

In S4a, it is determined whether the elevation angle specified in S3a is equal to or greater than a threshold value. The threshold value mentioned herein may appropriately be an elevation angle which can provide a signal quality excellent enough to say that the possibility of causing an error in the result of positioning is low and has a value that can arbitrarily be set. When the elevation angle specified in S3a is determined to be equal to or greater than the threshold value (YES in S4a), the process moves to S5. By contrast, when the angle is determined to be less than the threshold value (NO in S4a), the process moves to S6.

30 [0120]

In S5 in the second modification, the GPS satellite 2 having the elevation angle specified in S3a and determined to be equal to or greater than the threshold value is selected as the GPS satellite 2 as the target GPS

satellite 2 to be subjected to the authentication related process and the process moves to S6. In S8 in the second modification, the selected satellite list in which the PRN IDs of all the GPS satellites 2 selected in S5 are associated with the elevation angles (that is, signal quality evaluation values)
5 specified in S3a is stored in the memory.

[0121]

<Summarization of second modification>

According to the second modification, in the first authentication target satellite selection process, the GPS satellites 2 are selected which
10 have elevation angles sufficient to say that the signal qualities of the obtained navigation messages are excellent. Therefore, by performing the positioning process based on the navigation messages received from the selected GPS satellites 2, it may be possible to perform positioning using the navigation messages having the excellent signal qualities.

15 [0122]

<Third modification>

The description has been given of the configuration in which, in the first authentication target satellite selection process in the first vehicle onboard apparatus 200, the GPS satellites 2 are selected which have the SN
20 ratios determined to be equal to or greater than the threshold value, but the configuration is not necessarily limited to this. For example, a configuration (hereinafter referred to as a third modification) may also be used in which the GPS satellites 2 are selected using the distances between the geometric distances between the GPS satellites 2 and the first vehicle onboard
25 apparatus 200 and the pseudo-distances therebetween as a condition for selection.

[0123]

Here, a description will be given of the navigation message authentication system 1 in the third modification using the drawings.
30 Incidentally, for the convenience of description, members having the same functions as those of the members shown in the drawings used to describe the embodiment are designated by the same reference numerals and a description thereof is omitted.

[0124]

The navigation message authentication system 1 in the third modification is the same as the navigation message authentication system 1 in the first embodiment except that a part of the first authentication target
5 satellite selection process is different.

[0125]

<First authentication target satellite selection process in third modification>

A description will be given herein of the first authentication target
10 satellite selection process in the control portion 220 of the first vehicle onboard apparatus 200 in the second modification using the flowchart shown in FIG. 14. The flowchart in FIG. 14 is obtained by replacing only the process in S3 and S4 in the flowchart in FIG. 4, and shows only the extracted part of the process in S3b and S4b as a replacement for the process in S3
15 and S4.

[0126]

In S3b subsequent to S2, the satellite position of the x-th GPS satellite 2 is calculated from the orbit information included in the navigation message obtained in S1 from the x-th GPS satellite 2 and from the
20 transmission time of the navigation message. Then, from the calculated satellite position and the present position of the first vehicle onboard apparatus 200, the geometric distance between the x-th GPS satellite 2 and the first vehicle onboard apparatus 200 is calculated.

[0127]

25 The orbit information may be either the Ephemeris data or the Almanac data but, from the viewpoint of accuracy, the Ephemeris data is preferred. As the present position of the first vehicle onboard apparatus 200, the value obtained in the previous positioning may be used as long as the travel distance from the previously determined position is less than a
30 predetermined distance (for example, 100 m). Alternatively, a position estimated by autonomous navigation using the position obtained in the previous positioning as a reference point may also be used.

[0128]

In S3b, the pseudo-distance determined from the transmission time included in the navigation message acquired in S1 from the x-th GPS satellite 2 and from the reception time when the navigation message was received by the first vehicle onboard apparatus 200 is calculated. Needless to say, the
5 pseudo-distance is the distance between the GPS satellite 2 and the first vehicle onboard apparatus 200 which is calculated by multiplying, by a light speed, a propagation time determined from the time of transmission from the GPS satellite 2 and from the time of reception by the first vehicle onboard apparatus 200.

10 [0129]

Then, in S3b, the distance (hereinafter referred to as a distance difference) between the geometric distance between the x-th GPS satellite 2 and the first vehicle onboard apparatus 200 and the pseudo-distance therebetween is specified. Since the pseudo-distance is the distance
15 determined from the propagation time, a difference with the geometric distance may be produced under the influence of a multipath. When the multipath occurs, the signal quality deteriorates. Therefore, as the distance difference is smaller, the signal quality is more excellent. The distance difference corresponds to the signal quality evaluation value in the present disclosure, and S3b corresponds to the evaluation value specification portion
20 in the present disclosure.

[0130]

In S4b, it is determined whether the distance difference specified in S3b is equal to or less than a threshold value. The threshold value
25 mentioned herein may appropriately be a distance difference which can provide the signal quality excellent enough to say that the possibility of causing an error in the result of positioning is low and has a value that can arbitrarily be set. When the distance difference specified in S3b is determined to be equal to or less than the threshold value (YES in S4b), the
30 process moves to S5. By contrast, when the distance difference is determined to be greater than the threshold value (NO in S4b), the process moves to S6.

[0131]

In S5 in the third modification, the GPS satellites 2 each having the distance difference specified in S3b and determined to be equal to or less than the threshold value are selected as the target GPS satellites 2 to be subjected to the authentication related process, and the process moves to S6.

- 5 In S8 in the third modification, the selected satellite list in which the PRN IDs of all the GPS satellites 2 selected in S5 are associated with the specified distance differences (that is, the signal quality evaluation values) selected in S3b is stored in the memory.

[0132]

- 10 <Summarization of third modification>

According to the third modification also, in the first authentication target satellite selection process, the GPS satellites 2 are selected which have distance differences sufficient to say that the signal qualities of the obtained navigation messages are excellent. Therefore, by performing the
15 positioning process based on the navigation messages received from the selected GPS satellites 2, it may be possible to perform positioning using the navigation messages having the excellent signal qualities.

[0133]

<Fourth modification>

- 20 In each of the second modification and the third modification, the configuration has been shown in which the elevation angles or the distance differences between the geometric distances and the pseudo-distances are used as the condition for selecting the GPS satellites 2 instead of the SN ratios, but the configuration is not limited to this. For example, the GPS
25 satellites 2 are selected by combining these conditions. For example, when all the conditions are combined, in the selected satellite list, the PRN IDs of all the GPS satellites 2 selected in S5 are associated with the SN ratios, the elevation angles, and the distance differences between the geometric distances and the pseudo-distances each related to the GPS satellites 2.

- 30 [0134]

<Fifth modification>

The configuration of any of second to fourth modifications may be combined with the configuration of first modification in which the

predetermined plural number of GPS satellites 2 which have transmitted the navigation messages having the signal qualities that can be rated as more excellent are selected in decreasing order of signal quality .

[0135]

5 For example, in the case of combining the first modification and the fourth modification, the GPS satellites 2 are ranked by giving a top priority to any of signal quality evaluation values such as the SN ratio, the elevation angle, and the distance difference between the geometric distance and the pseudo-distance, and then a predetermined number of the higher-order GPS
10 satellites 2 may be selected.

[0136]

 Alternatively, it may also be possible to weight each of signal quality evaluation values such as the SN ratio, the elevation angle, and the distance difference between the geometric distance and the pseudo-distance and use
15 a function or the like for generally evaluating the signal qualities from the individual parameters. That is, a function is designed using the SN ratio, the elevation angle, and the distance difference between the geometric distance and the pseudo-distance as variables and having an output value which is larger as the SN ratio is larger, as the elevation angle is larger, and as the
20 distance difference is smaller to select a predetermined number of the higher-order GPS satellites 2 with which the output values of the function are larger.

[0137]

<Sixth modification>

25 The configurations of first to fifth modifications may also be applied to the second authentication target satellite selection process in the second vehicle onboard apparatus 300.

[0138]

<Seventh modification>

30 In the above embodiments, the configuration is shown in which the first vehicle onboard apparatus 200 transmits the NMA related information by vehicle-to-vehicle communication to the second vehicle onboard apparatus 300. The configuration is not necessarily limited to this. For example, by

using a roadside device as a relay device, the NMA related information is transmitted from the first vehicle onboard apparatus 200 by road-to-vehicle communication to the second vehicle onboard apparatus 300. Alternatively, by using a public communication network, the NMA related information is
5 transmitted from the first vehicle onboard apparatus 200 to the second vehicle onboard apparatus 300.

[0139]

<Eighth modification>

In the above embodiments, a case where only the navigation
10 messages received from the GPS satellites 2 are used for positioning is described as an example. The navigation message received from a QZS satellite 3 may be used for positioning. In this case, the authentication of the navigation message received from the QZS satellite 3 is also performed in the same manner as in the case of the GPS satellites 2.

15 [0140]

In an example of the eighth modification, a RAND message is generated from the navigation message received by the monitor station 110 from the QZS satellite 3, and parity data is produced based on the RAND message in the authentication center 120. Then, the produced parity data is
20 sent to the master control station 130, and transmitted from the master control station 130 to the QZS satellite 3. The QZS satellite 3 broadcasts the navigation message including the parity data toward the ground.

[0141]

The first vehicle onboard apparatus 200 and the second vehicle
25 onboard apparatus 300 in each of the embodiments including and subsequent to the second embodiment produces a RAND message from the navigation message received from the QZS satellite 3 and produces comparison parity data from the RAND message and the H matrix acquired from the authentication center 120. Authentication may be performed by
30 comparing the parity data received from QZS satellite 3 to the produced comparison parity data.

[0142]

<Ninth modification>

The navigation message authenticating authentication method described in the embodiment is a mere example. Another configuration using another authentication method may be used as long as the authentication method needs an access to an authentication facility.

5 [0143]

<Tenth modification>

In the embodiment, the description is given using the first vehicle onboard apparatus 200 and the second vehicle onboard apparatus 300 used in a vehicle as an example, but the configuration is not limited to this. The same navigation message reception apparatus as the first vehicle onboard apparatus 200 and the second vehicle onboard apparatus 300 may be applied to a mobile terminal to be carried by a user or the like.

[0144]

According to the navigation message authentication type positioning apparatus according to one example of the present disclosure, it is sufficient to narrow down the artificial satellites from which a satellite receiver has successfully received navigation messages to the artificial satellite selected by a selection portion, acquire only authentication information in accordance with the navigation message received from the selected artificial satellite, and authenticate the received navigation message. Thus, it may be possible to reduce the time required for authentication and processing loads in comparison with the case of acquiring the authentication information in accordance with the navigation messages received from all the artificial satellites from which the satellite receiver has successfully received the navigation messages and authenticating the received navigation messages.

[0145]

In addition, the selection portion selects the artificial satellite which has transmitted the navigation message having the signal quality that can be rated as excellent based on the signal quality evaluation value specified by the evaluation value specification portion, and the positioning portion determines the position of the navigation message authentication type positioning apparatus based on the navigation message received from the selected artificial satellite. This increases the possibility of positioning using

the navigation message having the excellent signal quality. Thus, it may be possible to perform positioning with higher accuracy, while reducing the time required for authentication and processing loads.

[0146]

5 A flowchart or a process corresponding to the flowchart described in the present application includes several steps (or referred to as sections). Each step is represented as S1, for example. Each step may be divided into sub-steps. Several steps may be combined into one step. Furthermore, each step can be also referred to as a device, module, or means.

10 [0147]

 It is to be understood that the disclosure is not limited to the embodiments. The present disclosure can be modified variously within the scope of the present disclosure. Embodiments obtained by appropriate combination of technical features each disclosed in different embodiments
15 are included in the scope of the present disclosure.

CLAIMS

1. A navigation message authentication type positioning apparatus,
comprising:

5 a satellite receiver that receives a navigation message from an
artificial satellite among a plurality of artificial satellites used in a satellite
positioning system;

an authentication information acquisition portion that acquires, from
an authentication center, authentication information in accordance with the
navigation message received from the artificial satellite, wherein the
10 authentication information is used in authentication of the navigation
message;

an authentication portion that authenticates that the navigation
message received by the satellite receiver is authentic, by using the
authentication information acquired by the authentication information
15 acquisition portion;

a positioning portion that determines a position of the navigation
message authentication type positioning apparatus based on the navigation
message received by the satellite receiver from the artificial satellite;

an evaluation value specification portion that specifies a signal
20 quality evaluation value that evaluates a signal quality of the navigation
message received by the satellite receiver; and

a selection portion that selects, based on the signal quality
evaluation value specified by the evaluation value specification portion and
from among all of the artificial satellites from which the satellite receiver has
25 successfully received navigation messages, the artificial satellite that has
transmitted the navigation message having the signal quality that is rated
excellent,

wherein:

the authentication information acquisition portion acquires only the
30 authentication information in accordance with the navigation message
received from the artificial satellite selected by the selection portion from
among the all of the artificial satellites from which the satellite receiver has
successfully received navigation messages;

the authentication portion authenticates that the navigation message received by the satellite receiver from the artificial satellite selected by the selection portion is authentic, by using the authentication information acquired by the authentication information acquisition portion; and

5 the positioning portion determines the position of the navigation message authentication type positioning apparatus based on the navigation message received from the artificial satellite selected by the selection portion.

2. The navigation message authentication type positioning
10 apparatus according to claim 1, wherein:

the selection portion selects, based on the signal quality evaluation value specified by the evaluation value specification portion and from among all of the artificial satellites from which the satellite receiver has successfully received navigation messages, a predetermined plurality of the artificial
15 satellites having transmitted the navigation message having the signal quality that is rated as more excellent in decreasing order of signal quality.

3. The navigation message authentication type positioning apparatus according to claim 1 or 2, wherein:

20 the evaluation value specification portion specifies, as the signal quality evaluation value, a signal-to-noise ratio of the navigation message received by the satellite receiver.

4. The navigation message authentication type positioning
25 apparatus according to any one of claims 1 to 3, wherein:

the evaluation value specification portion specifies, as the signal quality evaluation value, an elevation angle of the artificial satellite determined by using orbit information of the artificial satellite included in the navigation message received by the satellite receiver.

30

5. The navigation message authentication type positioning apparatus according to any one of claims 1 to 4, wherein:

the evaluation value specification portion specifies, as the signal quality evaluation value, a difference between

5 a geometric distance between the artificial satellite and the navigation message authentication type positioning apparatus, the geometric distance being obtained by using orbit information of the artificial satellite included in the navigation message received by the satellite receiver and
10 a pseudo-distance between the artificial satellite and the navigation message authentication type positioning apparatus, the pseudo-distance being determined from a propagation time of the navigation message received by the satellite receiver.

6. The navigation message authentication type positioning apparatus according to any one of claims 1 to 5, further comprising:

15 a transmission portion that transmits to an outside of the navigation message authentication type positioning apparatus, information including identification information that identifies the artificial satellite selected by the selection portion and
20 the authentication information about the artificial satellite selected by the selection portion showing whether authentication has succeeded in the authentication portion.

7. The navigation message authentication type positioning apparatus according to any one of claims 1 to 6, further comprising:

25 a reception portion that receives information transmitted from a different navigation message authentication type positioning apparatus, which is different from the navigation message authentication type positioning apparatus, the information including
30 identification information that identifies the artificial satellite selected by the selection portion of the different navigation message authentication type positioning apparatus and

the authentication information about the artificial satellite selected by the selection portion showing whether authentication has succeeded in the authentication portion of the different navigation message authentication type positioning apparatus,

5 wherein:

the selection portion of the navigation message authentication type positioning apparatus preferentially selects the artificial satellite that has succeeded in the authentication of the navigation message in the different navigation message authentication type positioning apparatus based on the
10 identification information and the authentication information, which are received by the reception portion.