

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. 2014-21632 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 which receives a navigation message transmitted from an artificial satellite used in a satellite positioning system with the receiver of a positioning apparatus and determines a
20 position.

[0004]

However, 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
25 person may perform falsification or spoofing of position information.

[0005]

Patent Document 1 discloses a technique which authenticates whether a navigation message received by a receiver (that is, a positioning apparatus) is an authentic navigation message from an artificial satellite used in a satellite positioning system. In the technique disclosed in Patent Document 1, the positioning apparatus 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 positioning apparatus authenticates whether the received navigation message is an authentic navigation message from the artificial satellite used in the satellite positioning system.

[0006]

A restart method referred to as a hot start has also conventionally been known in which, even when there is a short lasting power OFF state in a positioning apparatus, Ephemeris data as orbit information included in a navigation message is stored in a backup memory to omit re-collection of the Ephemeris data and expedite a positioning start time (referring to, for example, Patent Literature 2).

[0007]

A restart method referred to as a warm start has also been known in which Almanac information as orbit information is stored in a backup memory to omit re-collection of the Almanac data and expedite a positioning start time. The Ephemeris data is more detailed information than the Almanac data and has an expiration date shorter than that of the Almanac data.

[0008]

The warm start is the restart method when the power OFF period of the positioning apparatus has continued beyond the expiration date of the Ephemeris data held in the backup memory, but has not been beyond the expiration date of the Almanac data held in the backup memory. Although the positioning start time when a warm start is made is delayed later than when a hot start is made since it is necessary to collect the Ephemeris data,

the positioning start time can be expedited since it is unnecessary to re-collect the Almanac data.

[0009]

5 The inventor of the present application has found the following with regard to a navigation message authentication type positioning apparatus.

[0010]

10 When the technique disclosed in Patent Literature 1 is used at the time of the hot start or the warm start, in order to perform positioning with high reliability, it is necessary to communicate with an authentication center after the restart of the positioning apparatus and authenticate whether the navigation message is an authentic navigation message. Accordingly, the positioning start time may be delayed later since communication is performed with the authentication center to authenticate the navigation message.

PRIOR ART LITERATURES

15 PATENT LITERATURES

[0011]

Patent Literature 1: JP 2013-130395 A

Patent Literature 2: JP 2000-292521 A

SUMMARY OF INVENTION

20 [0012]

It is an object of the present disclosure to provide a navigation message authentication type positioning apparatus that can suppress a delay in positioning start time at the time of a hot start or a warm start, while allowing more reliable positioning to be performed.

25 [0013]

A navigation message authentication type positioning apparatus according to one 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
5 the authentication information acquired by the authentication information acquisition portion; a positioning portion that determines a position of the host apparatus (the navigation message authentication type positioning apparatus) based on navigation messages received by the satellite receiver from a plurality of artificial satellites. The navigation message authentication
10 type positioning apparatus includes a storage portion that stores satellite information including at least orbit information about the artificial satellite of the navigation message received by the satellite receiver and an authentication result of the navigation message by the authentication portion even during power OFF period of the navigation message authentication type
15 positioning apparatus; an acquisition portion that acquires, when the navigation message authentication type positioning apparatus is restarted, the artificial satellites by using the orbit information stored in the storage portion; a consistency determination portion that determines, when the navigation message having the authentication result of a succeeded
20 authentication stored in the storage portion exists, whether the navigation message has a consistency with a navigation message received from the artificial satellite as a transmitter of the navigation message after restart of the navigation message authentication type positioning apparatus by using information included in the satellite information of the navigation message
25 stored in the storage portion; and a selection portion that selects, when the consistency determination portion determines that the consistency exists, the artificial satellite as the transmitter of the navigation message determined to have the consistency as the artificial satellite used for positioning in the positioning portion. The positioning portion determines the position of the
30 navigation message authentication type positioning apparatus by using the navigation message received from the artificial satellite that is selected by the selection portion among the artificial satellites acquired by the acquisition portion.

[0014]

According to this configuration, when the host apparatus is restarted, the acquisition portion acquires the artificial satellites using the orbit information stored in the storage portion, so that it may be possible to make a hot start or a warm start. With respect to the identical artificial satellite, when the navigation message succeeded in authentication in the authentication portion before the power of the host apparatus is turned OFF has a consistency with the navigation message after the restart of the host apparatus, it is likely that the navigation message received after the restart is also authentic. Accordingly, the navigation message determined to have the consistency in the consistency determination portion also has the high possibility of being authentic. When using the navigation message received after the restart from the artificial satellite as the transmitter of the navigation message, it may be possible to perform the positioning with higher reliability. Therefore, by using the navigation message received from the artificial satellite selected by the selection portion, it may be possible to perform more reliable positioning.

[0015]

In addition, the positioning portion determines the position of the host apparatus using the navigation message received from the artificial satellite selected by the selection portion from among the artificial satellites acquired by the acquisition portion. It may be possible to perform more reliable positioning when a hot start or a warm start is made. According to the present disclosure, by using the navigation message received from the artificial satellite selected by the selection portion, it may be possible to perform more reliable positioning without performing authentication in the authentication portion using the authentication information acquired by the authentication information acquisition portion. Therefore, for the artificial satellite selected by the selection portion, it may be possible to reduce the time required for performing authentication using the authentication information acquired by the authentication information acquisition portion and suppress a delay in positioning start time when a hot start or a warm start is made.

BRIEF DESCRIPTION OF DRAWINGS

[0016]

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:

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;

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 an authentication related process in the first vehicle onboard apparatus;

FIG. 5 is a diagram showing an example of temporarily stored information stored in the memory of the first vehicle onboard apparatus;

FIG. 6 is a flowchart showing an example of the flow of a restart method selection process in the first vehicle onboard apparatus;

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

FIG. 8 is a diagram showing an example of an authentication information list stored in the memory of the first vehicle onboard apparatus;

FIG. 9 is a flowchart showing an example of the flow of a positioning information transmission process in the first vehicle onboard apparatus;

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

FIG. 11 is a flowchart showing an example of the flow of the initial positioning related process in the first vehicle onboard apparatus in a first modification;

FIG. 12 is a flowchart showing an example of the flow of an authentication confirmation information transmission process in the first vehicle onboard apparatus in a fourth modification;

FIG. 13 is a diagram showing an example of an authentication information list transmitted from the first vehicle onboard apparatus, which
5 shows an example of authentication confirmation information;

FIG. 14 is a flowchart showing an example of the flow of a confirmation process in the second vehicle onboard apparatus in the fourth modification; and

FIG. 15 is a diagram showing an example of the authentication information list stored in the memory of the second vehicle onboard apparatus.
10

PREFERRED EMBODIMENTS FOR CARRYING OUT INVENTION

[0017]

Hereinafter, the embodiments of the present disclosure will be
15 explained with reference to the drawings.

[0018]

(First Embodiment)

As shown in FIG. 1, a navigation message authentication system 1
20 in a first embodiment includes a monitor station 110, an authentication center 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
25 first vehicle onboard apparatus 200, the second vehicle onboard apparatus 300 corresponds to a navigation message authentication type positioning apparatus in the present disclosure.

[0019]

<Schematic configuration of navigation message authentication
30 system 1>

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
5 referred to as a GPS satellite 2 when no distinction is made therebetween. 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,
10 the navigation message is extracted from each of the GPS waves and is sent to the authentication center 120.

[0020]

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

[0021]

25 The authentication center 120 produces parity data from a navigation message and an H matrix, which is a cryptography key. Then, 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
30 vehicle onboard apparatus 300. The authentication center 120 will be described in detail later using FIG. 2.

[0022]

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.

5 [0023]

Each of the first vehicle onboard apparatus 200 and the second vehicle onboard apparatus 300 is a navigation message authentication (NMA) vehicle onboard apparatus. Each of the first vehicle onboard apparatus 200 and the second vehicle onboard apparatus 300 performs
10 communication with the authentication center 120, and authenticates that the navigation message received from the GPS satellites 2 is an authentic navigation message. The authentication will be explained in detail later using FIG. 4. Each of the first vehicle onboard apparatus 200 and the second vehicle onboard apparatus 300 also determines the present positions
15 using the navigation messages received from multiple GPS satellites 2. To determine the present position, each of the first vehicle onboard apparatus 200 and the second vehicle onboard apparatus 300 uses the navigation messages received from at least three of the GPS satellites 2. The first vehicle onboard apparatus 200 and the second vehicle onboard apparatus
20 300 will be described in detail later.

[0024]

<Detailed configuration of authentication center 120>

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

25 [0025]

The control portion 122 is a computer including a CPU, a ROM, a RAM, or the like, and controls the data storage 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
30 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 Document 1.

[0026]

The RAND message generation portion 1221 produces a RAND
5 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 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
10 signal. Besides, AS Flag showing an anti-spool flag and a PRN (Pseudo Random Noise) ID showing a satellite number are subsequently added.

[0027]

RAND including TOW and PRN ID is data showing when and which
one of the GPS satellites transmitted a signal. In addition, since TOW
15 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.

[0028]

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

[0029]

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
25 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.

[0030]

30 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.

[0031]

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.

[0032]

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 storage portion 124.

[0033]

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 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.

[0034]

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 storage 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.

[0035]

<Detailed configuration of first vehicle onboard apparatus 200>

The navigation message broadcast 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 control portion 220, and a satellite receiver 230.

[0036]

5 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 function. The narrow area communication function covers a communication distance of, for example, several hundreds of meters. The wide area
10 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 communication with another communication apparatus within the communication distance in the public communication network. Using the
15 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 communication function, the communication portion 210 performs communication with the communication portion 126 of the authentication
20 center 120.

[0037]

 The satellite receiver 230 receives the electric waves transmitted from the GPS satellites 2 and the QZS satellite 3 at a constant period. Then, the satellite receiver 230 outputs the navigation messages included in the
25 received electric waves to the control portion 220. When the navigation messages from the multiple GPS satellites 2 are received by the satellite receiver 330 within a single cycle of output sequentially performed from the satellite receiver 230 to the control portion 220, the navigation messages from the multiple GPS satellites 2 are output to the control portion 220 within
30 a single cycle.

[0038]

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

210 and the satellite receiver 230. It is supposed that the memory includes a ROM, a RAM, or the like, and that the memory 220a is a non-volatile temporary storage memory such as a backup RAM, or the like. The CPU executes a program stored in the ROM using the temporary storing function of the RAM so as to perform various processes such as an authentication related process (referring to FIG. 4), a temporary storage process and a restart method selection process (referring to FIG. 6), an initial positioning related process (FIG. 7), and an authentication information storage process and a positioning information transmission process (referring to FIG. 9).

10 [0039]

The outline of the authentication related process is a process related to the authentication in which the signal received by the satellite receiver 230 corresponds to an approved navigation message received from the GPS satellite 2. The temporary storage process is a process which temporarily stores, in the memory 220a, the information included in the navigation message and an authentication result of the authentication related process with respect to the navigation message.

[0040]

The restart selection process is a process performed when the power of the first vehicle onboard apparatus 200 is turned OFF once and then turned ON again. The initial positioning related process is a process related to an initial positioning performed at the time of a hot start or a warm start. The authentication information storage process is a process storing authentication information about the GPS satellite 2 used for the positioning such as NMA authentication information and deemed authentication information, in the memory 220a. The positioning information transmission process is a process transmitting the determined position and the authentication information about the GPS satellite 2 used to determine the position.

30 [0041]

<Authentication related process>

The authentication related process in the control portion 220 of the first vehicle onboard apparatus 200 will be explained with reference to the

flowchart in FIG. 4. The flowchart in FIG. 4 may be configured appropriately to be started when, for example, the control portion 220 receives an output of the navigation message received by the satellite receiver 230 from the GPS satellite 2. In this explanation, it is supposed that navigation messages of the multiple GPS satellites 2 are outputted in a single cycle, and processes are repeated so as to authenticate the navigation messages from the multiple GPS satellites 2.

[0042]

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

[0043]

In S1, the navigation message, which is output from the satellites receiver 230, included in the GPS waves received from the GPS satellites 2 is acquired.

[0044]

In S2, the navigation message received from the QZS satellite 3 is acquired from the reception portion 211. In S3, from the navigation message acquired in S1, PRN ID and TOW are extracted.

[0045]

In S4, PRN ID and TOW extracted in S3 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.

[0046]

In S5, the H matrix transmitted from the authentication center 120 is acquired from the reception portion 211. Accordingly, S5 corresponds to

authentication information acquisition portion in the present disclosure. In S6, the encrypted H matrix acquired in S5 is decrypted using the secret key.

[0047]

5 In S7, the RAND message is generated from the navigation message which is among the navigation messages included in the GPS wave received from the GPS satellites 2 and includes the identical PRN ID as PRN ID transmitted in S4.

[0048]

10 In S8, a comparison parity data is generated based on the RAND message produced in S7 and the H matrix decrypted in S6. In S9, it is determined whether the comparison parity data produced in S8 matches the parity data extracted in S3.

[0049]

15 The H matrix decrypted in S6 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.

[0050]

20 Accordingly, when the comparison parity data generated in S8 matches the parity data extracted in S3, it can be considered that the RAND message generated in S7 is identical with the RAND message generated by the authentication center 120.

[0051]

25 When the comparison parity data produced in S8 matches the parity data extracted in S3 (YES in S9), the process shifts to S10, and determines that the authentication has succeeded. On the other hand, when the two parity data items do not match (NO in S9), the process shifts to S11, and determines that the authentication has failed. Accordingly, S9 to S11 correspond to an authentication portion in the present disclosure. After S10
30 and S11, the process shifts to S12.

[0052]

In S12, when the determination of whether authentication has succeeded or failed is completed for all the target GPS satellites 2, that is,

each of all the navigation messages from all the GPS satellites 2 that have been output within a single cycle from the satellite receiver 230 (YES in S12), the process in FIG. 4 terminates. On the other hand, when the determination of whether authentication has succeeded or failed is not completed even for one of all the target GPS satellites 2 (NO in S12), the process returns to S12 to be repeated. The authentication in the authentication related process is referred to as NMA authentication.

[0053]

Incidentally, it is unnecessary to authenticate each of the navigation messages from all the GPS satellites 2 that have been output within a single cycle from the satellite receiver 230. All the GPS satellites 2 may be narrowed down to the GPS satellites 2 the number of which is necessary for positioning, for example, four or to the GPS satellites 2 the number of which is necessary for the initial positioning related process, which is described later, and then authentication may be performed.

[0054]

<Temporary storage process>

The control portion 220 of the first vehicle onboard apparatus 200 performs a temporary storage process that temporarily stores, in the memory 220a, the information included in the latest navigation message output from the satellite receiver 230 and the authentication result (NMA authentication information) of the navigation message in the authentication related process. When the navigation messages of the multiple GPS satellites 2 are output within a single cycle from the satellite receiver 230, the multiple navigation messages correspond to all the latest navigation messages.

[0055]

The information (hereinafter referred to as temporarily stored information) stored in the memory 220a in the temporary storage process includes PRN ID, orbit information such as the Ephemeris data and the Almanac data, which are included in the navigation message, a transmission time, the time when the navigation message is received, the NMA authentication information, or the like. The Ephemeris data corresponds to

the orbit information needed for a hot start. The Almanac data corresponds to the orbit information needed for a warm start.

[0056]

An example of the temporarily stored information will be explained with reference to FIG. 5. In the example of FIG. 5, it is supposed that, for example, the four GPS satellites 2 which are GPS satellites 2a to 2d can be monitored from the first vehicle onboard apparatus 200 and the navigation messages from the GPS satellites 2a and 2b have succeeded in NMA authentication. It is supposed that PRN ID of the GPS satellite 2a is "1", PRN ID of the GPS satellite 2b is "3", PRN ID of the GPS satellite 2c is "5", and PRN ID of the GPS satellite 2d is "10".

[0057]

As shown in FIG. 5, the temporarily stored information stored in the memory 220a may be configured appropriately such that each of the GPS satellites 2 as the transmitters of the navigation messages is associated with PRN ID, the NMA authentication information showing whether the GPS satellite 2 shown by PRN ID has succeeded in NMA authentication, the orbit information, the transmission time, and the reception time. The orbit information, the transmission time, and the reception time correspond to satellite information in the present disclosure.

[0058]

As shown in, for example, FIG. 5, the NMA authentication information may appropriately be a binary flag representing either one of the two states where authentication has succeeded ("T" in the drawing) and where authentication has failed or has not succeeded yet ("F" in the drawing). Alternatively, information representing any of the three states where authentication has succeeded, where authentication has failed, and where authentication has not succeeded yet may also be used. Accordingly, in the example in FIG. 5, the GPS satellites 2a, 2b have "T" and the GPS satellites 2c, 2d have "F".

[0059]

It is supposed that, when the control portion 220 receives the navigation messages corresponding to a single cycle which have been newly

output from the satellite receiver 230, the temporarily stored information stored in the memory 220a is sequentially updated based on the newly output navigation messages. Consequently, temporarily stored information about the GPS satellites 2 that can be monitored by the first vehicle onboard apparatus 200 at the present position continues to be left. The NMA related information may be configured appropriately to be sequentially updated at times other than when the control portion 220 receives the navigation messages corresponding to a single cycle which have been newly output from the satellite receiver 230. The details are as follows.

10 [0060]

In the authentication related process, the NMA authentication is sequentially performed for each of all the target GPS satellites 2. However, it takes time to perform the NMA authentication even for one GPS satellite 2 to result in a situation where, by the time when the NMA authentication is performed for each of all the target GPS satellites 2, the NMA authentication has been performed only for some of the target GPS satellites 2. Accordingly, the NMA authentication information may be configured appropriately to be updated every time the NMA authentication is newly performed for the GPS satellite 2. For example, when the navigation message from the GPS satellite 2 has succeeded in NMA authentication in FIG. 5, the NMA related information about the GPS satellite 2c is updated from "F" to "T".

[0061]

The memory 220a is the backup memory, and retains the storage of the temporarily stored information even when, for example, the ignition power of a vehicle A is turned OFF to turn OFF the power of the first vehicle onboard apparatus 200. The memory 220a corresponds to a storage portion in the present disclosure. When the power of the first vehicle onboard apparatus 200 is turned OFF, and the NMA authentication has completed only for some of all the target GPS satellites 2 in the authentication related process, a situation where the NMA authentication information about some of the GPS satellites 2 is "F" occurs.

[0062]

<Restart method selection process>

The restart method selection process in the control portion 220 of the first vehicle onboard apparatus 200 will be explained with reference to the flowchart shown in FIG. 6. The flowchart in FIG. 6 may be configured appropriately to be started when, for example, the power of the first vehicle onboard apparatus 200 is turned OFF once and then turned ON again.

[0063]

In S21, the period during which the power of the first vehicle onboard apparatus 200 is OFF is specified. The period (hereinafter referred to as the power OFF period) during which the power of the first vehicle onboard apparatus 200 is OFF may appropriately be specified from a count in an RTC (Real Time Clock).

[0064]

In S22, when the power OFF period falls within a first predetermined period (YES in S22), the process shifts to S23. On the other hand, when the power OFF period does not fall within the first predetermined period (NO in S22), the process shifts to S25. It is sufficient for the first predetermined period mentioned to have a value that does not exceed the expiration date of the Ephemeris data. For example, the first predetermined period may be fifteen minutes, two hours, or the like.

[0065]

In S23, to perform a hot start is selected, and the process shifts to S24. In S24, a GPS wave from the GPS satellite 2 regarding which the temporarily stored information exists in the memory 220a is acquired using the Ephemeris data of the orbit information included in the temporarily stored information, and the process in FIG. 6 terminates. S24 corresponds to an acquisition portion in the present disclosure.

[0066]

In S25, when the power OFF period does not fall within the first predetermined period in S22, the process shifts to S26 when the power OFF period falls within a second predetermined period (YES in S25). On the other hand, when the power OFF period does not fall within the second predetermined period (NO in S25), the process shifts to S28. The second

predetermined period mentioned herein is a period longer than the first predetermined period and may appropriately have a value which does not exceed the expiration date of the Almanac data. For example, the second predetermined period may be two hours, one day, one week, or the like.

5 [0067]

In S26, to make a warm start is selected, and the process shifts to S27. In S27, a GPS wave from the GPS satellite 2 regarding which the temporarily stored information exists in the memory 220a is acquired using the Almanac data of the orbit information included in the temporarily stored information, and the process in FIG. 6 terminates. S27 also corresponds to the acquisition portion in the present disclosure.

[0068]

In S28, when the power OFF period does not fall within the second predetermined period in S25, to make a cold start is selected, and the process shifts to S29. S29 attempts to acquire GPS waves from all the GPS satellites 2 without using the orbit information. Then, the process in FIG. 6 terminates.

[0069]

<Initial positioning related process>

20 The initial positioning related process in the control portion 220 of the first vehicle onboard apparatus 200 will be explained with reference to the flowchart shown in FIG. 7. The flowchart in FIG. 7 may be configured appropriately to be started when either of the hot start and the warm start is selected in the restart method selection process.

25 [0070]

In S31, based on the temporarily stored information stored in the memory 220a, the GPS satellite 2 (hereinafter referred to as the NMA authenticated GPS satellite 2) that had succeeded in NMA authentication of the navigation message before the power of the first vehicle onboard apparatus 200 has turned OFF is extracted.

[0071]

In S32, when the NMA authenticated GPS satellite 2 exists (YES in S31), the process shifts to S33. On the other hand, when the NMA

authenticated GPS satellite 2 does not exist (NO in S31), the process shifts to S40.

[0072]

5 In S33, from the temporarily stored information stored in the memory 220a, the transmission time of the navigation message with respect to the NMA authenticated GPS satellite 2 extracted in S31 and the reception time when the navigation message is received by the first vehicle onboard apparatus 200 are acquired.

[0073]

10 In S34, the control portion 220 acquires the navigation message received by the satellite receiver 230 from the same GPS satellite 2 as the NMA authenticated GPS satellite 2 extracted in S31 after the power of the first vehicle onboard apparatus 200 is turned ON again (that is, restarted). The navigation message received by the satellite receiver 230 after the
15 restart is hereinafter referred to as a NMA pre-authentication navigation message.

[0074]

In S35, the reception time when the NMA pre-authentication navigation message acquired in S34 is received is specified. The
20 transmission time of the navigation message is specified from the navigation message. The reception time when the NMA pre-authentication navigation message is received may be specified from the value counted in the RTC, which is not shown.

[0075]

25 In S36, it is determined for the NMA authenticated GPS satellite 2 extracted in S31 whether the navigation message that has succeeded in NMA authentication has a consistency according to elapsed time with the NMA pre-authentication navigation message. Accordingly, S36 corresponds to a consistency determination portion in the present disclosure.

30 [0076]

For example, when the difference between the transmission time difference between the transmission time acquired from the temporarily stored information in S33 (that is, the transmission time of the navigation

message that has succeeded in NMA authentication that is stored in the memory 220a) and the transmission time of the NMA pre-authentication navigation message specified in S35 and the reception time difference between the respective reception times when the two navigation messages
5 have been received is less than a threshold value, it is determined that the navigation message has the consistency.

[0077]

The threshold value mentioned herein may appropriately have a value corresponding to a propagation time lag resulting from the movement
10 of the NMA authenticated GPS satellite 2 extracted in S31 during a time period corresponding to the transmission time difference. The threshold value may be set on the assumption that the position of the first vehicle onboard apparatus 200 is fixed.

[0078]

15 When the NMA pre-authentication navigation message specified in S35 is made by the repeater or the simulator, the relationship between the transmission time and the reception time has variance for an authentic navigation message. Consequently, the difference between the transmission time difference and the reception time difference is equal to or
20 greater than the threshold value. Therefore, it is likely that the navigation message determined to have the consistency in S36 is authentic even when the NMA authentication has not been performed.

[0079]

In S36, when the difference between the transmission time
25 difference and the reception time difference coincides with the threshold value (in other words, substantially match within the margin of error), it may be determined that the navigation message has the consistency.

[0080]

In S37, when it is determined that there is the consistency (YES in
30 S37), the process shifts to S38. On the other hand, when it is determined that there is no consistency (NO in S37), the process shifts to S39.

[0081]

In S38, the GPS satellite 2 as the transmitter of the navigation message determined to have the consistency is selected as the GPS satellite 2 for positioning. Accordingly, S38 corresponds to a selection portion in the present disclosure. It is likely that the navigation message determined to have the consistency in S36 is an authentic navigation message even when the NMA authentication has not been performed. Therefore, the GPS satellite 2 as the transmitter of the navigation message determined to have the consistency in S36 is selected as the GPS satellite 2 for positioning, supposing that the GPS satellite 2 as the transmitter of the navigation message determined to have the consistency in S36 allows more reliable positioning to be performed similarly to the GPS satellite 2 that has succeeded in NMA authentication of the navigation message. The GPS satellite 2 selected in S38 is referred to as a GPS satellite that has succeeded in deemed authentication.

[0082]

In S39, it is determined whether the number of the GPS satellites 2 that have succeeded in the deemed authentication has reached the number of the GPS satellites 2 required for positioning (hereinafter referred to as the number required for positioning). For example, the number required for positioning may be three, four, or the like. When it is determined that the number required for positioning has been reached (YES in S39), the process shifts to S42. On the other hand, when it is determined that the number required for positioning has not been reached (NO in S39), the process shifts to S40.

[0083]

In S40, when the process in S33 to S38 has completed for all the NMA authenticated GPS satellites 2 extracted in S31 (YES in S40), the process shifts to S41. On the other hand, when the process in S33 to S38 has not been completed even for some of the NMA authenticated GPS satellites 2 extracted in S31 (NO in S40), the process returns to S33, and the process in S33 to S38 is performed for the NMA authenticated GPS satellites 2 for which the process in S33 to S38 has not been completed.

[0084]

In S41, the NMA authentication is performed for the acquired GPS satellites 2 other than the NMA authenticated GPS satellites 2 until the GPS satellites 2 which have succeeded in NMA authentication and the number of which corresponds to the number required for positioning are obtained, and
5 the process shifts to S42.

[0085]

In S42, the initial positioning after the restart is performed, and the process in FIG. 7 terminates. The positioning itself is performed in accordance with a known method using the navigation messages received
10 from the GPS satellites 2 which have been selected for positioning and the number of which corresponds to the number required for positioning. S42 corresponds to a positioning portion in the present disclosure.

[0086]

When the number required for positioning can be satisfied only with
15 the GPS satellites 2 that have succeeded in the deemed authentication, the initial positioning can be started without the NMA authentication after the restart. Accordingly, it may be possible to suppress a delay in initial positioning since the NMA authentication after the restart need not be performed. Even when the number of the GPS satellites 2 that have
20 succeeded in the deemed authentication accounts for only a part of the number required for positioning, a delay in the initial positioning can be suppressed since the NMA authentication after the restart need not be performed for the GPS satellites 2 the number of which accounts for only a part of the number required for positioning.

25 [0087]

Incidentally, when the initial positioning after the restart is performed, and when a hot start is made, the positioning can be started without collecting the Ephemeris data. However, when a warm start is made, it is necessary to collect the Ephemeris data and then start positioning. Accordingly, when
30 a warm start is made, a start time of the initial positioning is delayed than a case when a hot start is made.

[0088]

<Authentication information storage process>

When positioning is performed, the control portion 220 of the first vehicle onboard apparatus 200 performs, for the GPS satellite 2 used for the positioning, an authentication information storage process which stores, in the memory 220a, the authentication information list including the NMA authentication information showing whether the NMA authentication has succeeded and information (hereinafter referred to as deemed authentication information) showing whether the deemed authentication has succeeded.

[0089]

An example of the authentication information list will be explained with reference to FIG. 8. It is supposed that, in the example of FIG. 8, the first vehicle onboard apparatus 200 has performed positioning using the GPS satellites 2a to 2d as the GPS satellites 2 for positioning. It is supposed that PRN ID of the GPS satellite 2a is "1", PRN ID of the GPS satellite 2b is "3", PRN ID of the GPS satellite 2c is "5", and PRN ID of the GPS satellite 2d is "10".

[0090]

As shown in FIG. 8, the authentication information list may be configured appropriately such that each of the GPS satellites 2 as the transmitters of the navigation messages is associated with PRN ID, the NMA authentication information showing whether the GPS satellite 2 shown by PRN ID has succeeded in NMA authentication, and the deemed authentication information showing whether the GPS satellite 2 shown by PRN ID has succeeded in deemed authentication.

[0091]

As shown in, for example, FIG. 8, the deemed authentication information may appropriately be a binary flag representing either one of the two states where authentication has succeeded ("T" in the drawing) and where authentication has failed or has not succeeded yet ("F" in the drawing). Alternatively, the deemed authentication information may also be information showing any of the three states where authentication has succeeded, where authentication has failed, and authentication has not succeeded yet. When only the GPS satellites 2 that have succeeded in deemed authentication are not sufficient to satisfy the required number for positioning and the GPS

satellites 2 that have succeeded in NMA authentication are also used for positioning, the GPS satellite 2 has "T" as the NMA authentication information and "F" as the deemed authentication information.

[0092]

5 For the authentication information list stored in the memory 220a, it may also be possible to update the information by performing the NMA authentication after the initial positioning, for the GPS satellites 2 that have not been subjected to the NMA authentication but have succeeded in deemed authentication. For example, when the GPS satellite 2 that had
10 succeeded in the deemed authentication has also succeeded in NMA authentication, each of the NMA authentication information and the deemed authentication information becomes "T".

[0093]

 The authentication information list stored in the memory 220a may
15 also be configured appropriately to be not only stored when initial positioning is performed, but also sequentially updated every time positioning is newly performed. Even when positioning is newly performed, the GPS satellites 2 that have succeeded in the deemed authentication may be continuously used as the GPS satellites 2 for positioning without performing the NMA
20 authentication.

[0094]

<Positioning information transmission process>

 The positioning information transmission process in the control
portion 220 of the first vehicle onboard apparatus 200 will be described with
25 reference to the flowchart shown in FIG. 9. The positioning information transmission process shown in FIG. 9 may be configured appropriately to be started at, for example, a constant period.

[0095]

 In the positioning information transmission process in the flowchart
30 in FIG. 9, the positioning information including the position determined by the first vehicle onboard apparatus 200 and the information in the authentication information list about the GPS satellites 2 used for the determination of the position is transmitted.

[0096]

In S51, the position calculated by the first vehicle onboard apparatus 200 in the immediately previous positioning is acquired. In S52, the information of the authentication information list stored in the memory
5 220a is acquired. In S53, the positioning information including the position acquired in S51 and information such as PRN ID of each of the GPS satellites 2, the NMA authentication, and the deemed authentication information included in the authentication list is transmitted using the narrow area communication function of the transmission portion 212, and the
10 process terminates. Accordingly, S53 corresponds to a determined position transmission processing portion in the present disclosure.

[0097]

Hereinafter, it is supposed that, in the present embodiment, the positioning information transmitted from the transmission portion 212 is
15 received by the second vehicle onboard apparatus 300.

[0098]

<Detailed configuration of second vehicle onboard apparatus 300>

The second vehicle onboard apparatus 300 receiving the positioning information transmitted from the first vehicle onboard apparatus
20 200 will be explained with reference to FIG. 10. As shown in FIG. 10, the second vehicle onboard apparatus 300 includes a communication portion 310, a control portion 320, and a satellite receiver 330. The communication portion 310 performs wireless communication with the communication portion 210 included in the first vehicle onboard apparatus 200.

25 [0099]

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
30 receiver 230, the satellite receiver 330 receives electric waves transmitted from the GPS satellites 2 and the QZS satellite 3 at a constant period.

[0100]

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. It is supposed that the memories include a ROM, a RAM, or the like, and the memory 220a is a nonvolatile temporary storage memory such as a backup RAM. In the same manner as in the first vehicle onboard apparatus 200, the CPU executes the program stored in the ROM using the temporary storing function of the RAM to perform various processes such as the authentication related process, the temporary storage process, the restart method selection process, the initial positioning related process, the authentication information storage process, and the positioning information transmission process.

[0101]

The control portion 320 acquires the positioning information received by the reception portion 311 from the first vehicle onboard apparatus 200 and performs a process (hereinafter referred to as position information utilization process) which utilizes the position of the first vehicle onboard apparatus 200 (that is, the position of the vehicle A) included in the acquired positioning information. Examples of the position information utilization process include a following drive process which performs a following drive, while keeping a proper inter-vehicular distance with the vehicle A using the first vehicle onboard apparatus 200, a process which reports the degree of congestion showing how many vehicles are present around the vehicle B using the second vehicle onboard apparatus 300, or the like.

[0102]

The control portion 320 may determine the degree of reliability of the position included in the positioning information based on the authentication information included in the positioning process and determine whether the position information utilization process is to be performed in accordance with the determined degree of reliability.

[0103]

For example, the following drive process, which requires a high reliability, is to be performed when all the GPS satellites 2 used to determine

the position have succeeded in NMA authentication but is not to be performed when the GPS satellites 2 used to determine the position include one which has not succeeded in NMA authentication. On the other hand, a configuration may be used appropriately which determines that, even when
5 there is the GPS satellite 2 that has not succeeded in NMA authentication, a process which needs no high reliability such as the process which reports the degree of congestion is to be performed as long as the GPS satellite 2 has succeeded in the deemed authentication.

[0104]

10 <Summarization of first embodiment>

According to the first embodiment, at the time of a hot start or a warm start, the navigation message that had been received from the GPS satellite 2 and succeeded in authentication before the power of the first vehicle onboard apparatus 200 is turned OFF has a consistency in
15 accordance with an elapsed time with the navigation message received from the same GPS satellite 2 after the restart, the GPS satellite 2 is selected as the GPS satellite 2 for positioning. The navigation message determined to have the consistency in accordance with the elapsed time has the high possibility of being authentic. Accordingly, when the navigation message
20 received from the GPS satellite 2 as the transmitter of the navigation message after the restart is used, it may be possible to perform more reliable positioning. Therefore, according to the first embodiment, it may be possible to perform more reliable initial positioning when a hot start or a warm start is made.

25 [0105]

According to the first embodiment, the GPS satellite 2 that has succeeded in the deemed authentication is used for positioning. It may be possible to reduce the time required to perform the NMA authentication after the restart. Consequently, it may be possible to suppress a delay in
30 positioning start time when a hot start or a warm start is made.

[0106]

According to the first embodiment, when the position determined in the first vehicle onboard apparatus 200 is transmitted to the second vehicle

onboard apparatus 300 by vehicle-to-vehicle communication, the authentication information about the GPS satellites 2 used for positioning such as the NMA authentication information and the deemed authentication information is also added to the determined position and the determined position is transmitted. This allows the second vehicle onboard apparatus 300 to determine how high the reliability of the position determined by the first vehicle onboard apparatus 200 is using the authentication information. Thus, it may be possible to determine whether the position information utilization process is to be performed based on the determined degree of reliability and depending on the degree of reliability required by the position information utilization process.

[0107]

<First modification>

The configuration in which it is determined in the initial positioning related process in the first vehicle onboard apparatus 200 that, when the difference between the transmission time difference between the transmission time of the navigation message succeeded in NMA authentication and stored in the memory 220a and the transmission time of the NMA pre-authentication navigation message and the reception time difference between the respective reception times when the two navigation messages have been received is less than the threshold value, the navigation message has the consistency is described. The configuration is not limited to this configuration. A configuration (hereinafter referred to as a first modification) may also be used appropriately in which it is determined that the navigation message that has succeeded in NMA authentication has a consistency with the NMA pre-authentication navigation message when the difference between the pseudo distances determined from the transmission time and the reception time of the navigation message is less than a threshold value.

[0108]

The navigation message authentication system 1 in a first modification will be explained with reference to the drawings. For the convenience of description, members having the same functions as those of

the members shown in the drawings used to describe the above embodiment are designated by the same reference numerals and a description is omitted.

[0109]

5 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 initial positioning related process is different.

[0110]

<Initial positioning related process in first modification>

10 The initial positioning related process in the control portion 220 of the first vehicle onboard apparatus 200 in the first modification will be explained with reference to the flowchart shown in FIG. 11. The flowchart in FIG. 11 is obtained by replacing only the process in S36 in the flowchart in FIG. 7 and shows only the extracted part of the process in S36a to S36c as a
15 replacement for the process in S36.

[0111]

In S36a subsequent to S35, the pseudo distance is calculated from the transmission time and the reception time (that is, the transmission time of the navigation message that had succeeded in NMA authentication, which is
20 stored in the memory 220a, and the reception time when the navigation message is received) acquired from the temporarily stored information in S33. The 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
25 GPS satellite 2 and from the time of reception by the first vehicle onboard apparatus 200.

[0112]

In S36b, the pseudo distance is calculated from the transmission time of the NMA pre-authentication navigation message and the reception
30 time when the navigation message is received, which have been specified in S35.

[0113]

In S36c, for the NMA authenticated GPS satellite 2 extracted in S31, it is determined from the pseudo distance calculated in S36a and from the pseudo distance calculated in S36b whether the navigation message that has succeeded in NMA authentication has a consistency with the NMA pre-authentication navigation message, and the process shifts to S37. Accordingly, S36c corresponds to the consistency determination portion in the present disclosure.

[0114]

As a specific example, it is determined that the navigation message has the consistency when the difference between the pseudo distance calculated in S36a and the pseudo distance calculated in S36b is less than a threshold value. Incidentally, the threshold value may be defined appropriately as a pseudo distance deviation corresponding to a propagation time lag due to the movement of the NMA authenticated GPS satellite 2 extracted in S31 during the time period corresponding to the transmission time difference. The threshold value may be set on the assumption that the position of the first vehicle onboard apparatus 200 is fixed.

[0115]

When a hot start or a warm start is made, the position of the first vehicle onboard apparatus 200 could not have moved since the power of the first vehicle onboard apparatus 200 is turned OFF. Accordingly, when the NMA pre-authentication navigation message specified in S35 is authentic, the distance between the pseudo distance determined from the transmission time and the reception time of the NAM pre-authentication navigation message and the pseudo distance determined from the transmission time and the reception time of the NAM authenticated navigation message should be less than a threshold value. Thus, it is likely that the navigation message determined to have the consistency in S36c is authentic even when the NMA authentication has not been performed therefor.

[0116]

In S36c, when the difference between the pseudo distance calculated in S36a and the pseudo distance calculated in S36b coincide with the threshold value (in other words, substantially match within the margin of

error), it may be determined that the navigation message has the consistency.

[0117]

<Summarization of first modification>

5 When there is a match between the pseudo distances determined from the transmission time and the reception time of the navigation message between the navigation message that has succeeded in authentication and the NMA pre-authentication navigation message, it is likely that the navigation message is authentic. In the first modification, when such a
10 condition is satisfied, the GPS satellite 2 that has transmitted the NMA pre-authentication navigation message is selected as the GPS satellite 2 for positioning. Therefore, according to the first modification, it may be possible to suppress a delay in positioning start time when a hot start or warm start is made, while allowing more reliable positioning to be performed.

15 [0118]

<Second modification>

The configuration of first modification may be applied to the initial positioning related process in the second vehicle onboard apparatus 300.

[0119]

20 <Third modification>

In the first embodiment, the positioning information transmitted from the first vehicle onboard apparatus 200 is received by the second vehicle onboard apparatus 300, but the configuration is not limited to this. A configuration (hereinafter referred to as a third modification) may be used in
25 which the positioning information transmitted from the first vehicle onboard apparatus 200 using the narrow area communication function is received by a roadside apparatus.

[0120]

In the configuration of third modification, it is supposed that the
30 roadside apparatus is a terminal of a system that performs the process of providing a predetermined service using the position transmitted from the first vehicle onboard apparatus 200. Process providing a service includes a billing process in which, when it is determined that the vehicle A using the

first vehicle onboard apparatus 200 is parked in a toll parking area or when the vehicle A has traveled along a toll road, the user of the vehicle is automatically charged or the like. Besides, there is also a game which uses position information or the like.

5 [0121]

In third modification, the roadside apparatus determines the degree of reliability of the position included in the positioning information based on the authentication information included in the positioning information to determine whether the process of providing the predetermined service is to be performed in accordance with the determined degree of reliability.

10 [0122]

For example, a billing process which requires a high reliability is determined to be performed when all the GPS satellites 2 used to determine the position have succeeded in NMA authentication, but a following drive process is determined not to be performed when the GPS satellites 2 include the one which has not succeeded in NMA authentication. On the other hand, in a game which needs no high reliability or the like, even when there is the GPS satellite 2 which has not succeeded in NMA authentication, the game is determined to be performed as long as the GPS satellite 2 has succeeded in deemed authentication.

20 [0123]

<Summarization of third modification>

According to third modification, when the position determined by the first vehicle onboard apparatus 200 is transmitted to the roadside apparatus, authentication information about the GPS satellite 2 used for positioning, such as the NMA authentication information and the deemed authentication information, is also added to the determined position and the determined position is transmitted. This allows the roadside apparatus to determine how high the reliability of the positioning in the first vehicle onboard apparatus 200 is using the authentication information. Thus, it may be possible to determine whether the process of providing the predetermined service using the position transmitted from the first vehicle onboard apparatus 200 is to be performed based on the determined degree of

reliability, in accordance with the degree of reliability required by the position information utilization process.

[0124]

<Fourth modification>

5 A configuration (hereinafter referred to as a fourth modification) may also be used appropriately which confirms that the result of performing the deemed authentication in the second vehicle onboard apparatus 300 is correct using the result of the NMA authentication in the first vehicle onboard apparatus 200.

10 [0125]

 The navigation message authentication system 1 in the fourth modification will be explained with reference to 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
15 embodiment are designated by the same reference numerals and a description is omitted.

[0126]

 The navigation message authentication system 1 in the fourth modification is the same as the navigation message authentication system 1
20 in the first embodiment except that an authentication confirmation information transmission process transmitting authentication confirmation information including the NMA authentication information and an authentication completion certificate for certifying that NMA authentication is performed and a confirmation process which confirms the result of performing the deemed
25 authentication using the authentication confirmation information transmitted from another apparatus are performed.

[0127]

<Authentication confirmation information Transmission Process>

 An authentication confirmation information transmission process in
30 the control portion 220 of the first vehicle onboard apparatus 200 will be explained with reference to the flowchart shown in FIG. 12. The authentication confirmation information transmission process shown in FIG. 12 may be started at, for example, a constant period.

[0128]

In S61, the information in the authentication information list stored in the memory 220a is acquired. In S62, for each of those of the GPS satellites 2 which are included in the authentication information list acquired in S61 and have succeeded in NMA authentication, the authentication completion certificate for certifying that NMA authentication is performed is acquired. As the authentication completion certificate, information obtained as the authentication information from the authentication center 120 or information which can be generated from the information may be used in NMA authentication. For example, an H matrix as a cryptography key may be used appropriately as the authentication completion certificate or a hash value produced from a hash function using each of the H matrix and the parity data as an input key may also be used appropriately as the authentication completion certificate. In the present embodiment, a case where the H matrix is used as the authentication completion certificate will be explained, for example.

[0129]

The H matrix used as the authentication completion certificate may be acquired from the authentication center 120 when the NMA authentication is performed, associated with the corresponding PRN ID in the authentication information list, and stored in the memory 220a.

[0130]

In S63, the authentication confirmation information including PRN ID of each of the GPS satellites 2, the NMA authentication information, and the deemed authentication information, which are included in the authentication information list acquired in S61, and the authentication completion certificate acquired in S62 is transmitted using the narrow area communication function of the transmission portion 212, and the process is completed. Accordingly, PRN ID corresponds to identification information in the present disclosure and S63 corresponds to the authentication information transmission processing portion in the present disclosure.

[0131]

An example of the authentication confirmation information will be explained with reference to FIG. 13. In the example of FIG. 13, the same information as shown in FIG. 8 is included in the authentication information list. Here, since the GPS satellites 2 which have succeeded in NMA authentication (each having "T" as the NMA authentication information in the drawing) are the GPS satellite 2a (having "1" as PRN ID in the drawing) and the GPS satellite 2d (having "10" as PRN ID in the drawing), the H matrices (Key1 and Key4 in the drawing) each as the authentication completion certificate are incorporated in authentication completion information about the GPS satellites 2a and 2d and then the authentication confirmation information sets are transmitted.

[0132]

The following description will be given on the assumption that the authentication confirmation information transmitted from the transmission portion 212 is received by the second vehicle onboard apparatus 300 in the present embodiment.

[0133]

<Authentication process>

A confirmation process in the control portion 320 of the second vehicle onboard apparatus 300 will be explained with reference to the flowchart shown in FIG. 14. The confirmation process shown in FIG. 14 may be started when the authentication confirmation information transmitted from the first vehicle onboard apparatus 200 is received by the reception portion 311.

[0134]

In S71, the authentication confirmation information received by the reception portion 311 from the first vehicle onboard apparatus 200 is acquired. Accordingly, S71 corresponds to an authentication information reception processing portion in the present disclosure. In S72, the authentication information list stored in a memory 320a is acquired. The memory 320a corresponds to the storage portion in the present disclosure.

[0135]

An example of the authentication information list stored in the memory 320a will be explained with reference to FIG. 15. In the example of FIG. 15, it is supposed that the second vehicle onboard apparatus 300 has performed positioning using the GPS satellites 2a to 2c and 2e as the GPS satellites 2 for positioning. It is supposed herein that PRN ID of the GPS satellite 2a is "1", PRN ID of the GPS satellite 2b is "3", PRN ID of the GPS satellite 2c is "5", and PRN ID of the GPS satellite 2e is "13". The items of the authentication information list are the same as those shown in FIG. 8.

[0136]

10 In the example of FIG. 15, the GPS satellites 2a and 2c have not succeeded in NMA authentication but have succeeded only in deemed authentication. The GPS satellite 2b has succeeded in NMA authentication but has not been subjected to the deemed authentication. The GPS satellite 2e has succeeded in each of NMA authentication and deemed authentication.

[0137]

In S73, from the authentication information list about the second vehicle onboard apparatus 300 acquired in S72, information about the GPS satellites 2 which have succeeded only in deemed authentication of the NMA authentication and the deemed authentication is extracted. In the example of FIG. 15, the information about the GPS satellites 2a and 2c corresponds to this.

[0138]

25 In S74, when the extraction has succeeded in S73 (YES in S74), the process shifts to S75. On the other hand, when the information is not extracted in S73 (NO in S74), the process in FIG. 14 terminates.

[0139]

30 In S75, from the authentication confirmation information acquired in S71, information about the GPS satellite 2 which has the same PRN ID as that of the GPS satellite 2 extracted in S73 and which has succeeded in NMA authentication is extracted. In the example in FIG. 13, information about the GPS satellite 2a corresponds to this.

[0140]

In S76, when the extraction has succeeded in S75 (YES in S76), the process shifts to S77. On the other hand, when the information is not extracted in S75 (NO in S76), the process in FIG. 14 terminates.

[0141]

5 In the process in S73 to S75, from among the GPS satellites 2 that have succeeded in the deemed authentication in the second vehicle onboard apparatus 300, the GPS satellites 2 succeeded in NMA authentication in the first vehicle onboard apparatus 200 are extracted.

[0142]

10 In S77, the H matrix for each of the GPS satellites 2 extracted in S75 is specified. For example, the H matrix is acquired from the authentication center 120 or is acquired at a previous time to be used. The previous time corresponds to the time of the NMA authentication performed before the deemed authentication is performed for the target GPS satellite 2. In the
15 case of acquiring the H matrix from the authentication center 120, a configuration may be used appropriately which uses PRN ID of the target GPS satellite 2 and TOW included in the navigation message received when the deemed authentication is performed for the GPS satellite 2 in the second vehicle onboard apparatus 300.

20 [0143]

In S78, it is determined whether the H matrix included in the authentication confirmation information about the GPS satellite 2 extracted in S75 matches the H matrix specified in S77. In S79, when there is a match (YES in S79), the process shifts to S80. On the other hand, when there is
25 no match (NO in S79), the process in FIG. 14 terminates.

[0144]

In S80, it is determined that the deemed authentication in the second vehicle onboard apparatus 300 is proper for that one of the GPS satellites 2 extracted in S75 for which the H matrix included in the
30 authentication confirmation information matches the H matrix specified in S77, and the process in FIG. 14 terminates. Accordingly, S80 corresponds to a confirmation portion in the present disclosure.

[0145]

A configuration may be used appropriately in which the GPS satellites 2 that have succeeded only in the deemed authentication of the NMA authentication and the deemed authentication in the second vehicle onboard apparatus 300 are subjected to the NMA authentication in the
5 second vehicle onboard apparatus 300 except for the GPS satellite 2 for which it is determined in S80 that the deemed authentication is proper.

[0146]

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

[0147]

<Summarization of fourth modification>

According to the fourth modification, for each of the GPS satellites 2
15 other than the GPS satellite 2 for which it is determined that the deemed authentication is proper, the reliability can be confirmed by performing the NMA authentication. This allows the second vehicle onboard apparatus 300 to perform more reliable positioning. On the other hand, for the GPS satellite 2 for which it is determined that the deemed authentication is proper,
20 the reliability is confirmed by the confirmation process. From this viewpoint also, it may be possible for the second vehicle onboard apparatus 300 to perform more reliable positioning.

[0148]

< Fifth modification and sixth modification>

25 In the fourth modification, the configuration is shown in which the authentication confirmation information includes the deemed authentication information and the authentication completion certificate. However, the configuration is not limited to this. A configuration (hereinafter referred to as a fifth modification) may also be used appropriately in which the
30 authentication confirmation information includes neither the deemed authentication information nor the authentication completion certificate. In the case of using the configuration in which the authentication confirmation information includes neither the deemed authentication information nor the

authentication completion certificate, the process in S77 to S79 in the flowchart in FIG. 14 is omitted and the process shifts to S80 when YES is given in S76.

[0149]

5 In the fourth modification, the configuration is shown in which, in an authentication information transmission process, the authentication confirmation information is transmitted separately from the positioning information transmitted in the positioning information transmission process. However, the configuration is not limited to this. A configuration (hereinafter referred to as a sixth modification) may be used appropriately which performs
10 the positioning information transmission process and the authentication confirmation information transmission process as one common process by using common information obtained by combining the positioning information and the authentication confirmation information with each other.

15 [0150]

<Seventh modification>

 In the embodiment, the configuration is shown in which the first vehicle onboard apparatus 200 transmits the positioning information and the authentication confirmation information to the second vehicle onboard
20 apparatus 300 by vehicle-to-vehicle communication. However, the configuration is not necessarily limited to this. By using a roadside apparatus as a relay, the positioning information and the authentication confirmation information may be transmitted from the first vehicle onboard apparatus 200 to the second vehicle onboard apparatus 300 by
25 road-to-vehicle communication. Alternatively, by using a public communication network, the positioning information and the authentication confirmation information may be transmitted from the first vehicle onboard apparatus 200 to the second vehicle onboard apparatus 300.

[0151]

30 <Eighth modification>

 In the embodiment, a case where only the navigation messages received from the GPS satellites 2 are used for positioning is described as an example. However, 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.

[0152]

5 In an example of an 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 sent to the master control station 130, and transmitted from the master
10 control station 130 to the QZS satellite 3. The QZS satellite 3 broadcasts the navigation message including the parity data toward the ground.

[0153]

The first vehicle onboard apparatus 200 and the second vehicle onboard apparatus 300 in each of the embodiments including and
15 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 comparing the parity data received from QZS satellite 3 to the produced
20 comparison parity data.

[0154]

<Ninth modification>

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

[0155]

<Tenth modification>

In the embodiment, the description is given using the first vehicle
30 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.

[0156]

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 uses the authentication information acquired by the authentication information acquisition portion to authenticate that the navigation message received by the satellite receiver is authentic, and a positioning portion that determines a position of the navigation message authentication type positioning apparatus based on the navigation messages received by the satellite receiver from multiple artificial satellites. The navigation message authentication type positioning apparatus also includes a storage portion that stores satellite information including at least orbit information about the artificial satellite included in the navigation message received by the satellite receiver and a result of the authentication of the navigation message in the authentication portion even during a power OFF period of the navigation message authentication type positioning apparatus, an acquisition portion that acquires, when the navigation message authentication type positioning apparatus is restarted, the artificial satellites using the orbit information stored in the storage portion, a consistency determination portion that determines, when the navigation message having a successful result of the authentication stored in the storage portion is present, whether the navigation message has a consistency with a navigation message received from the artificial satellite as the transmitter of the navigation message after the restart of the navigation message authentication type positioning apparatus using information included in the satellite information of the navigation message stored in the storage portion, and a selection portion that selects, when the consistency determination portion determines that the navigation message has the

consistency, the artificial satellite as the transmitter of the navigation message determined to have the consistency as the artificial satellite used for the positioning in the positioning portion. The positioning portion determines the position of the navigation message authentication type positioning apparatus using the navigation message received from the artificial satellite which is among the artificial satellites acquired in the acquisition portion and selected by the selection portion.

[0157]

In the message authenticating positioning apparatus according to the example of the present disclosure, when the host apparatus is restarted, the acquisition portion acquires the artificial satellites using the orbit information stored in the storage portion. It may be possible to perform a hot start or a warm start. When the navigation message that had been succeeded in authentication in the authentication portion before the power of the host apparatus is turned OFF has a consistency with the navigation message received from the identical artificial satellite after the restart of the apparatus, it is likely that the navigation message received after the restart is also authentic. Accordingly, the navigation message determined to have the consistency in the consistency determination portion also has the high probability of being authentic. The use of the navigation message received after the restart from the artificial satellite as the transmitter of the navigation message allows more reliable positioning to be performed. Therefore, by using the navigation message received from the artificial satellite selected by the selection portion, it may be possible to perform more reliable positioning.

[0158]

In addition, the positioning portion determines the position of the host apparatus using the navigation message received from the artificial satellite selected by the selection portion from among the artificial satellites acquired by the acquisition portion. This allows more reliable positioning to be performed when a hot start or a warm start is made. According to the present disclosure, by using the navigation message received from the artificial satellite selected by the selection portion, more reliable positioning can be performed without performing authentication in the authentication

portion using the authentication information acquired by the authentication information acquisition portion. Therefore, for the artificial satellite selected by the selection portion, it may be possible to reduce the time required for performing authentication in the authentication portion using the authentication information acquired by the authentication information acquisition portion and suppress a delay in positioning start time when a hot start or a warm start is made.

[0159]

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.

[0160]

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 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 one or more navigation messages from a one or more 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 one or more navigation messages received from the one or more artificial satellites;

10 an authentication portion that authenticates that the one or more navigation messages received by the satellite receiver are authentic, by using the authentication information acquired by the authentication information acquisition portion;

15 a positioning portion that determines a position of the navigation message authentication type positioning apparatus based on the one or more navigation messages received by the satellite receiver from the one or more of artificial satellites;

20 a storage portion that stores satellite information including at least orbit information about the one or more artificial satellites of the one or more navigation messages received by the satellite receiver, and an authentication result of the one or more navigation messages by the authentication portion even during power OFF period of the navigation message authentication type positioning apparatus;

25 an acquisition portion that acquires, when the navigation message authentication type positioning apparatus is restarted, the one or more artificial satellites by using the orbit information stored in the storage portion;

30 a consistency determination portion that determines, when the one or more navigation messages having the authentication result of a succeeded authentication stored in the storage portion exists, whether the one or more navigation messages have a consistency with one or more navigation messages received from the one or more artificial satellites as one or more transmitters of the one or more navigation messages after restart of the navigation message authentication type positioning apparatus by using

information included in the satellite information of the one or more navigation messages stored in the storage portion;

a selection portion that selects, when the consistency determination portion determines that the consistency exists, the one or more artificial satellites as the one or more transmitters of the one or more navigation messages determined to have the consistency with the one or more artificial satellites used for positioning in the positioning portion; and

a determination portion of a number of artificial satellites that determines whether a number of the one or more artificial satellites selected by the selection portion, of the one or more artificial satellites acquired by the acquisition portion, has reached a predetermined number of artificial satellites required for positioning of the navigation message authentication type positioning apparatus,

wherein:

when the determination portion of the number of artificial satellites determines that the number of the one or more artificial satellites selected by the selection portion, of the one or more artificial satellites acquired by the acquisition portion, is less than the predetermined number, the authentication portion authenticates the one or more navigation messages corresponding to a shortage number of artificial satellites in the positioning of the navigation message authentication type positioning apparatus; and

the positioning portion determines the position of the navigation message authentication type positioning apparatus by using the one or more navigation messages received from the one or more artificial satellites that are selected by the selection portion among the one or more artificial satellites acquired by the acquisition portion.

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

the storage portion also stores, as the satellite information, a transmission time when the one or more artificial satellites have transmitted the one or more navigation messages of the one or more navigation messages received by the satellite receiver; and

the consistency determination portion determines that the consistency exists

when a difference between

5 a time difference between the transmission time of the one or more navigation messages stored in the storage portion and a transmission time included in the one or more navigation messages received from the one or more artificial satellites as the one or more transmitters of the one or more navigation messages after the restart, and

10 a time difference between a reception time of the one or more navigation messages stored in the storage portion and a reception time of the one or more navigation messages received from the one or more artificial satellites as the one or more transmitters of the one or more navigation messages after the restart

is less than a threshold value.

15

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

20 the storage portion also stores, as the satellite information, a transmission time when the one or more artificial satellites have transmitted the one or more navigation messages of the one or more navigation messages received by the satellite receiver; and

the consistency determination portion determines that the consistency exists

when a difference between

25 a pseudo distance determined from the transmission time of the one or more navigation messages stored in the storage portion and a reception time when the one or more navigation messages are received, and

30 a pseudo distance determined from the transmission time included in the one or more navigation messages received from the one or more artificial satellites as the one or more transmitters of the navigation messages after the restart and a reception time when the one or more navigation messages are received after the restart

is less than a threshold value.

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

5 the positioning portion can also use, for positioning, the one or more navigation messages received from the one or more artificial satellites as the one or more transmitters of the one or more navigation messages that have succeeded in authentication in the authentication portion,

the navigation message authentication type positioning apparatus
10 further comprising:

a determined position transmission processing portion that transmits the position determined in the positioning portion to an outside of the navigation message authentication type positioning apparatus,

wherein:

15 the determined position transmission processing portion adds, to the position determined in the positioning portion, information showing

whether the one or more artificial satellites used to determine the position are the one or more artificial satellites that are the one or more transmitters of the one or more navigation messages that have succeeded in authentication in the authentication portion, and
20

whether the one or more artificial satellites used to determine the position is the one or more artificial satellites selected by the selection portion are the one or more artificial satellites used for the positioning in the positioning portion

25 and transmits the position determined in the positioning portion.

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

30 the positioning portion can also use, for positioning, the one or more navigation messages received from the one or more artificial satellites as the one or more transmitters of the one or more navigation messages that have succeeded in authentication in the authentication portion,

the navigation message authentication type positioning apparatus further comprising:

- 5 an authentication information transmission processing portion that transmits, to an outside of the navigation message authentication type positioning apparatus, identification information about the one or more artificial satellites which allow the one or more artificial satellites to be identified, and authentication information showing whether the one or more artificial satellites are the one or more artificial satellites that are the one or more transmitters of the one or more navigation messages that have
10 succeeded in authentication in the authentication portion;
- an authentication information reception processing portion that receives the identification information and the authentication information each transmitted from the authentication information transmission processing portion of a different navigation message authentication type positioning
15 apparatus that is different from the navigation message authentication type positioning apparatus; and
- a confirmation portion that determines that, when one or more artificial satellites selected as the one or more artificial satellites used for positioning in the positioning portion by the selection portion of the navigation
20 message authentication type positioning apparatus is specified as an identical artificial satellite as the one or more artificial satellites as the one or more transmitters of the one or more navigation messages that have succeeded in authentication in the authentication portion of the different navigation message authentication type positioning apparatus based on the
25 identification information and the authentication information each received by the authentication information reception processing portion, the one or more artificial satellites selected by the selection portion of the navigation message authentication type positioning apparatus is proper as one or more artificial satellites used for positioning.