

DESCRIPTION

TITLE OF INVENTION: NAVIGATION MESSAGE AUTHENTICATION
SYSTEM, RECEPTION TERMINAL, AND AUTHENTICATION
PROCESSING APPARATUS

5 CROSS REFERENCE TO RELATED APPLICATIONS

[0001]

The present application is based on Japanese Patent Application
No. 2014-21631 filed on February 6, 2014, the disclosure of which is
incorporated herein by reference.

10 TECHNICAL FIELD

[0002]

The present disclosure relates to a navigation message
authentication system that enables to authenticate a navigation message
received by a reception terminal, a reception terminal included in the
15 navigation message authentication system, and an authentication processing
apparatus.

BACKGROUND ART

[0003]

Conventionally, a reception terminal has been known which
20 receives a navigation message transmitted from an artificial satellite used in a
satellite positioning system and calculates the present position thereof based
on the navigation message.

[0004]

However, due to the recent development of a simulator or the like
25 capable of artificially generating a signal as with the signal transmitted from
an artificial satellite, a malicious person may cause a reception terminal to
calculate an erroneous position using the simulator.

[0005]

Patent Literature 1 proposes a navigation message authentication system which performs an authentication process of authenticating whether the navigation message received by a reception terminal is the navigation message transmitted from an artificial satellite used in a satellite positioning system. More specifically, the navigation message authentication system causes a quasi-zenith satellite used in a quasi-zenith satellite system to transmit data used to authenticate a navigation message.

[0006]

The reception terminal performs numerical calculation using the data acquired from the quasi-zenith satellite and the navigation message received thereby to determine whether the received navigation message is an authentic navigation message from the artificial satellite used in the satellite positioning system.

[0007]

A possibility that the position information calculated based on the navigation message authenticated in the authentication process has been falsified by a simulator or the like is relatively low. That is, by introducing the navigation message authentication system, it is possible to improve the reliability of the position information calculated by the reception terminal.

[0008]

It can be considered that an improvement in the reliability of the position information calculated by the reception terminal allows various services using the position information of the reception terminal to be provided. Examples of the services using the position information include a service which automatically charges a toll on a toll road based on the position of a reception terminal.

[0009]

However, according to the study conducted by the inventors of the present application, the navigation message authentication process performed by the reception terminal in Patent Literature 1 requires the numerical calculation. Accordingly, it is assumed that, even when the authentication process is performed for only one navigation message, a corresponding processing load is placed on a CPU. In addition, the

reception terminal needs to perform the navigation message authentication process for each of the navigation messages received thereby. To perform the authentication process for all the navigation messages, a larger processing load is placed. Thus, a wait time which is unacceptable by a service provider or a receiver of the provided service may occur before the authentication of each of the navigation messages is completed.

[0010]

When a CPU having a relatively high arithmetic processing ability is mounted in the reception terminal, the wait time can be reduced. However, as a CPU has a higher arithmetic processing ability, the CPU is more costly to disadvantageously increase the cost of the reception terminal.

PRIOR ART LITERATURE

PATENT LITERATURE

[0011]

Patent Literature 1: JP 2013-130395 A

SUMMARY OF INVENTION

[0012]

It is an object of the present disclosure to provide a navigation message authentication system that can suppress an increase in the cost of a reception terminal for authenticating the navigation message received by the reception terminal, the reception terminal, and an authentication processing apparatus.

[0013]

A navigation message authentication system according to an example of the present disclosure includes: at least one first satellite that transmits a first navigation message; a second satellite that transmits a second navigation message including an inspection data used for an authentication process for the first navigation message; a reception terminal that receives the first navigation message and the second navigation message. The navigation message authentication system performs the authentication process of authenticating whether the first navigation message

received by the reception terminal is the first navigation message transmitted from the first satellite by using the inspection data included in the second navigation message. The navigation message authentication system further includes an authentication processing apparatus that is provided outside the reception terminal and communicates with the reception terminal. The reception terminal includes: a terminal-side satellite receiver that receives the first navigation message transmitted from the first satellite and the second navigation message transmitted from the second satellite; an inspection data extraction section that extracts the inspection data from the second navigation message received by the terminal-side satellite receiver; an authentication relation data extraction section that extracts, from the first navigation message received by the terminal-side satellite receiver, an authentication relation data required for the authentication process for the first navigation message; an authentication request signal generation section that generates an authentication request signal which includes the inspection data extracted by the inspection data extraction section and the authentication relation data extracted by the authentication relation data extraction section, and requests the authentication process to be performed for the first navigation message received by the terminal-side satellite receiver, and an authentication request signal transmission processing section that transmits the authentication request signal generated by the authentication request signal generation section. The authentication processing apparatus includes: an authentication request signal reception processing section that receives the authentication request signal transmitted from the authentication request signal transmission processing section; and an authentication arithmetic operation section that performs the authentication process for the first navigation message received by the reception terminal, based on the inspection data and the authentication relation data each included in the authentication request signal.

[0014]

According to another example of the present disclosure, a reception terminal comprising: a terminal-side satellite receiver that receives a first navigation message transmitted from a first satellite and a second navigation

message transmitted from a second satellite and including inspection data used for an authentication process for the first navigation message; an inspection data extraction section that extracts the inspection data from the second navigation message received by the terminal-side satellite receiver; 5 an authentication relation data extraction section that extracts, from the first navigation message received by the terminal-side satellite receiver, an authentication relation data as a portion required for the authentication process for the first navigation message; an authentication request signal generation section that generates an authentication request signal which 10 includes the inspection data extracted by the inspection data extraction section and the authentication relation data extracted by the authentication relation data extraction section and requests the authentication process for the first navigation message received by the terminal-side satellite receiver to be performed; and an authentication request signal transmission processing 15 section that transmits the authentication request signal generated by the authentication request signal generation section is provided.

[0015]

According to still another example of the present disclosure, an authentication processing apparatus comprising: an authentication request 20 signal reception processing section that receives an authentication request signal including an authentication relation data as a portion required for an authentication process for the first navigation message and inspection data used for the authentication process for the first navigation message of a first navigation message transmitted from a first satellite; and an authentication 25 arithmetic operation section that performs the authentication process for the first navigation message received by a reception terminal based on the inspection data and the authentication relation data each included in the authentication request signal is provided.

[0016]

30 According to the navigation message authentication system, the reception terminal, and the authentication processing apparatus in the present disclosure, the reception terminal need not perform an authentication process. The authentication processing apparatus performs the

authentication process in place of the reception terminal. That is, since the reception terminal does not need a CPU having a high arithmetic processing ability for performing numerical calculation resulting from the authentication process at a high speed, it may be possible to suppress an increase in the cost of the reception terminal.

BRIEF DESCRIPTION OF DRAWINGS

[0017]

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 block 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 a control segment;

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

FIG. 4 is a flowchart showing an example of the flow of an authentication request relation process performed by the control portion of the vehicle onboard apparatus;

FIG. 5 is a block diagram showing an example of a schematic configuration of an NMA information management center;

FIG. 6 is a flowchart showing an example of the flow of an authentication relation process performed by the control portion of the NMA information management center;

FIG. 7 is a flowchart showing an example of the flow of an authentication arithmetic operation process performed by the control portion of the NMA information management center;

FIG. 8 is a block diagram showing an example of a schematic configuration of the navigation message authentication system in a second embodiment;

FIG. 9 is a block diagram showing an example of a schematic configuration of a service center in the second embodiment;

FIG. 10 is a flowchart showing an example of the flow of an SC-side authentication relation process performed by the control portion of the service center;

FIG. 11 is a block diagram showing an example of a schematic configuration of the service center in a second modification; and

FIG. 12 is a schematic diagram for illustrating the function included in the control portion of the vehicle onboard apparatus in a third modification.

10 PREFERRED EMBODIMENTS FOR CARRYING OUT INVENTION

[0018]

<First embodiment>

A first embodiment of the present disclosure will be explained with reference to the drawings. FIG. 1 is a view showing an example of a schematic configuration of a navigation message authentication system 1 in the present embodiment. As shown in FIG. 1, the navigation message authentication system 1 includes a GPS satellite 2, a quasi-zenith satellite (hereinafter referred to as QZS satellite) 3, a control segment (CS) 100, a vehicle onboard apparatus 200, and an NMA information management center 300. The control segment 100 includes a monitor station (MS) 110, an authentication center (AC) 120, and a master control station (MCS) 130.

[0019]

The GPS satellite 2 corresponds to a first satellite of the present disclosure. The QZS satellite 3 corresponds to a second satellite of the present disclosure. The NMA information management center 300 corresponds to an authentication processing apparatus of the present disclosure. The vehicle onboard apparatus 200 corresponds to a reception terminal of the present disclosure. The control segment 100 corresponds to an authentication center apparatus of the present disclosure.

[0020]

<Schematic configuration of navigation message authentication system 1>

The outline of each of the components included in the navigation message authentication system 1 will be described herein. The monitor station 110 receives the electric wave (so-called a GPS wave) transmitted from the GPS satellite 2 included in a GPS (Global Positioning System) as one of satellite positioning systems. FIG. 1 shows only one GPS satellite 2, but it should be appreciated that the navigation message authentication system 1 includes multiple GPS satellites 2.

[0021]

As is known, the signal carried by the GPS wave transmitted from the GPS satellite 2 has been subjected to phase modulation using a C/A code. The value of the pseudo random noise (PRN) used in the C/A code differs from one GPS satellite 2 to another. Accordingly, the C/A code also differs from one GPS satellite 2 to another. The GPS satellite 2 that serves as the transmitter of the GPS wave can be specified using a PRN value (that is, PRN ID) used in the C/A code. The following description will be given using PRN ID as a satellite number that identifies the GPS satellite 2.

[0022]

The GPS wave also includes a navigation message M. The navigation message M transmitted from each of the GPS satellites 2 includes a TOW (Time Of Week) that shows an elapsed time within a week, a clock correction parameter for a satellite clock, detailed orbit information (that is, Ephemeris data) about the GPS satellite 2, an ionization layer correction parameter, general orbit information (that is, Almanac data) about all the GPS satellites 2, or the like. The navigation message M transmitted from the GPS satellite 2 corresponds to a first navigation message of the present disclosure.

[0023]

The monitor station 110 demodulates the received GPS wave and extracts the navigation message M therefrom. Then, the monitor station 110 sequentially sends the extracted navigation message M to the authentication center 120. The monitor station 110 corresponds to a first navigation message reception portion of the present disclosure.

[0024]

The authentication center 120 generates a reference authentication navigation data (RAND) message based on the navigation message M acquired from the monitor station 110. The details of RAND message will be described later. The RAND message includes at least PRN ID and TOW to be able to specify the correspondence between the GPS satellite 2 transmitted the navigation message M and the time when the GPS satellite 2 has transmitted the navigation message M. The authentication center 120 produces, from the produced RAND message and an H matrix as an encryption key, parity data corresponding to the navigation message M and RAND message. The parity data corresponds to an inspection data of the present disclosure.

[0025]

The authentication center 120 is configured to be intercommunicative with the monitor station 110, the master control station 130, the vehicle onboard apparatus 200, or the like. For example, the authentication center 120 sends a signal including the produced parity data to the master control station 130.

[0026]

The master control station 130 transmits the parity data received from the authentication center 120 to the QZS satellite 3. The QZS satellite 3 broadcasts a navigation message N including the parity data toward the ground. Data showing RAND message to which the data corresponds has been added to the parity data. The navigation message N transmitted from the QZS satellite 3 corresponds to a second navigation message of the present disclosure. The master control station 130 corresponds to an inspection data transmission portion of the present disclosure.

[0027]

The vehicle onboard apparatus 200 is configured to be able to receive the electric waves transmitted from the GPS satellites 2 and the QZS satellite 3 and communicate with the NMA information management center 300. The vehicle onboard apparatus 200 detects (that is, determines) the position of the host apparatus from the electric waves transmitted from the GPS satellites 2 and the QZS satellite 3.

[0028]

The vehicle onboard apparatus 200 acquires the navigation message M from the GPS wave received by the host apparatus, and further extracts information (referred to as GPS-side NMA information) used for a navigation message authentication (NMA) process from the navigation message M. Herein, RAND message is generated as the GPS-side NMA information. The RAND message is used as the GPS-side NMA information herein, but the GPS-side NMA information is not limited to this. The GPS-side NMA information may be the navigation message M. The GPS-side NMA information may appropriately include information for specifying the GPS satellite 2 as the transmitter of the navigation message M and the transmission time. The GPS-side NMA information corresponds to authentication relation data of the present disclosure.

[0029]

The vehicle onboard apparatus 200 further acquires, from the navigation message N transmitted from the QZS satellite 3, the parity data as information to be used for the NMA process.

[0030]

Incidentally, the vehicle onboard apparatus 200 acquires, from the QZS satellite 3, multiple types of the parity data corresponding to the number of the GPS satellites 2. Among the multiple parity data sets, the parity data corresponding to the RAND message produced as the GPS-side NMA information is specified from PRN ID and TOW of the RAND message. Then, the vehicle onboard apparatus 200 generates an NMA request data Rq including the RAND message produced by the host apparatus and the parity data received from the QZS satellite 3 and transmits the NMA request data Rq to the NMA information management center 300.

[0031]

The NMA information management center 300 is configured to be communicative with the vehicle onboard apparatus 200 and the authentication center 120 via a known communication network. On acquiring the NMA request data Rq from the vehicle onboard apparatus 200, the NMA information management center 300 extracts, from the NMA

request data Rq, the RAND message generated by the vehicle onboard apparatus 200 and the parity data corresponding to this.

[0032]

Then, the NMA information management center 300 accesses a
5 data memory portion 124 of the authentication center 120 and acquires the H matrix corresponding to the RAND message from PRN ID and TOW each included in the RAND message. For example, the NMA information management center 300 transmits an H matrix request signal that includes PRN ID and TOW each included in the RAND message and requests the H
10 matrix corresponding to PRN ID and TOW to be transmitted to the authentication center 120. Then, using the H matrix acquired from the authentication center 120, the NMA information management center 300 performs an authentication relation process. By performing the authentication relation process, it is possible to perform the authentication
15 process of authenticating whether the navigation message M received by the vehicle onboard apparatus 200 is an authentic navigation message, that is, an NMA process.

[0033]

The vehicle onboard apparatus 200 may receive not only the signals
20 transmitted from the authentic GPS satellites 2, but also an electric wave transmitted from a simulator which simulatively generates a signal transmitted from the GPS satellite 2. When the position information of the vehicle onboard apparatus 200 has been falsified by such an inauthentic signal, a problem may occur such that, for example, in the provision of a
25 service by a service provider using the position information, proper billing cannot be performed.

[0034]

The NMA information management center 300 performs the NMA process to allow the service provider to know whether the vehicle onboard
30 apparatus 200 has received the signal transmitted from an authentic transmitter (that is, the GPS satellite 2). Among the transmitters of the navigation messages M received by the vehicle onboard apparatus 200, the GPS satellites 2 that transmit the navigation messages M that has been

authenticated will be hereinafter referred to as an authenticated GPS satellites 2.

[0035]

<Detailed configuration of authentication center 120>

5 A description will be given of a more detailed configuration of the authentication center 120. As shown in FIG. 2, the authentication center 120 includes a control portion 122, the data memory portion 124, and a communication portion 126.

[0036]

10 The control portion 122 is a computer including a CPU, a ROM, a RAM, or the like, and controls the data memory portion 124 and the communication portion 126. The CPU executes the program stored in the ROM using the temporary storing function of the RAM to thus implement various functions. More specifically, the control portion 122 includes, as
15 functional blocks, a RAND message generation portion 1221, a SEED value generation portion 1222, an H matrix generation portion 1223, a parity generation portion 1224, and a signal processing portion 1225. Incidentally, the functions of the individual portions 1221 to 1225 may appropriately be the same as those disclosed in Patent Literature 1.

20 [0037]

The RAND message generation portion 1221 produces the RAND message from the navigation message M acquired from the monitor station 110. The RAND message corresponds to an authentication data of the present disclosure, and the RAND message generation portion 1221
25 corresponds to an authentication data generation portion of the present disclosure.

[0038]

The RAND message includes TOW (Time Of Week) showing an elapsed time within a week, and TOC, AF0 and AF1 as a clock correction
30 parameter, having been extracted from the bit strings of the navigation message M. Incidentally, TOW is updated every 6 seconds and reset when a time period corresponding to one week has elapsed. TOW corresponds to a satellite time of the present disclosure. TOC, AF0, and AF1 correspond to

a satellite time correction parameter of the present disclosure. The clock correction parameters are information used to specify the satellite time and intrinsic to a satellite. That is, PRN ID and the clock correction parameters correspond to transmitter specific information of the present disclosure.

5 TOW corresponds to transmission time information.

[0039]

In the RAND message, AS Flag, which is an anti-spoof flag, and PRN ID have been added subsequently to AF1. TOW, PRN ID, TOC, AF0, AF1, AS Flag, or the like are placed in the bit strings forming the RAND
10 message in accordance with a format designed appropriately.

[0040]

As described above, the RAND message includes PRN ID and TOW. Accordingly, the RAND message is data showing when and which one of the GPS satellites 2 transmitted the navigation message. In addition,
15 since TOW is updated every 6 seconds, the RAND message generation portion 1221 generates a RAND message every 6 seconds for each of all the GPS satellites 2 from which the monitor station 110 receives the navigation messages M.

[0041]

20 The SEED value generation portion 1222 receives a PC clock as an input to cause a random number to be generated, and thus generates the SEED value.

[0042]

The H matrix generation portion 1223 uses the SEED value
25 generated by the SEED value generation portion 1222 to generate the H matrix for generating the parity bit which is uniquely determined from the input data. The H matrix is a matrix, and the numbers of rows and columns therein have values corresponding to the number of bits of the input data and the number of parity bits. As the H matrix, a known hash function may be
30 used appropriately. For example, a parity check matrix for performing LDPC (Low Density Parity Check) coding may be used appropriately as the H matrix. The H matrix corresponds to an encryption key of the present disclosure.

The H matrix generation portion 1223 corresponds to an encryption key generation portion of the present disclosure.

[0043]

5 The parity generation portion 1224 calculates the parity data based on the RAND message produced by the RAND message generation portion 1221 and the H matrix calculated by the H matrix generation portion 1223. That is, by multiplying the RAND message by the H matrix, the parity data is calculated. The parity generation portion 1224 corresponds to an inspection data generation portion of the present disclosure.

10 [0044]

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

[0045]

20 Incidentally, in the present embodiment, by way of example, the navigation message N transmitted from the QZS satellite 3 is configured to include the parity data sets and RAND messages corresponding to the individual GPS satellites 2 acquired by the monitor station 110. That is, the signal processing portion 1225 associates the parity data sets and RAND messages which correspond to the multiple GPS satellites 2 with each other
25 and inserts the parity data sets and the RAND messages into the navigation message N.

[0046]

30 Simultaneously with the insertion of the signals, the signal processing portion 1225 further associates the parity data calculated by the parity generation 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 the parity data, the RAND message, the H matrix, and the SEED value in the data memory portion 124.

The data memory portion 124 corresponds to a storage portion of the present disclosure.

[0047]

5 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 N to be transmitted from the QZS satellite 3. Consequently, every time the RAND message generation portion 1221 generates the RAND message, each of the RAND message generation portion 1221, the SEED value generation portion 1222, 10 the H matrix generation portion 1223, and the parity generation portion 1224 also performs the process.

[0048]

15 On receiving the H matrix request signal transmitted from the NMA information management center 300, the communication portion 126 selects, from among the H matrices stored in the data memory portion 124, the H matrix corresponding to the received H matrix request signal. Then, the communication portion 126 transmits the selected H matrix back to the NMA information management center 300.

[0049]

20 The transmission-and-reception of the H matrix between the authentication center 120 and the NMA information management center 300 is performed by an encrypted secure communication. For example, the authentication center 120 may appropriately use the public key issued by the NMA information management center 300 to encrypt the H matrix and 25 transmit the H matrix to the NMA information management center 300. The secrecy of communication may also be ensured by using a common public key encryption system or the like.

[0050]

<Detailed configuration of vehicle onboard apparatus 200>

30 A description will be given of a configuration of the vehicle onboard apparatus 200 using FIG. 3. As shown in FIG. 3, the vehicle onboard apparatus 200 includes a communication portion 210, a control portion 220, and a satellite receiver 230.

[0051]

The communication portion 210 includes a reception portion 211 that performs the demodulation of a reception signal or the like and a transmission portion 212 that modulates the data as an input from the control portion 220 and transmits the data. The transmission portion 212 corresponds to a terminal-side transmission portion of the present disclosure.

[0052]

The communication portion 210 also includes a narrow range communication function and a wide range communication function. The wide range communication function covers a communication distance of, for example, several kilometers. By performing communication with a base station in a public communication network, the communication portion 210 can communicate with another communication device present within communicating distance in the public communication network. It is assumed that the wide range communication function is implemented by a communication module used in, for example, a third generation mobile communication system. Using the wide range communication function, the communication portion 210 communicates with the NMA information management center 300. On the other hand, the narrow range communication function covers a communication distance of, for example, several hundreds of meters. When the vehicle onboard apparatus 200 is assumedly configured to communicate with the authentication center 120 and the service center 400 via a roadside apparatus not shown, the vehicle onboard apparatus 200 communicates with the roadside apparatus using the narrow range communication function.

[0053]

The satellite receiver 230 receives the electric waves transmitted from the GPS satellites 2 and the QZS satellite 3 at a fixed period. The satellite receiver 230 demodulates the received electric waves and outputs the electric waves to the control portion 220. That is, the satellite receiver 230 sequentially receives the navigation messages M transmitted from the GPS satellites 2 and the navigation message N transmitted from the QZS satellite 3 and outputs the navigation messages M and N to the control

portion 220. The satellite receiver 230 corresponds to a terminal-side satellite receiver of the present disclosure.

[0054]

The control portion 220 is a computer including a CPU, a ROM, a RAM, or the like, and controls the communication portion 210 and the satellite receiver 230. The CPU executes the program stored in the ROM using the temporary storing function of the RAM to thus perform an authentication request relation process or the like.

[0055]

The memory 221 is a rewritable storage medium, and implemented by, for example, EEPROM, RAM, or the like included in the control portion 220. The memory 221 stores the navigation messages M and N sequentially acquired from the satellite receiver 230 and the sequentially calculated present position. Incidentally, when the storage capacity is fully occupied, the stored navigation messages may appropriately be discarded in succession beginning with the chronologically oldest navigation message. The present position is represented by, for example, a known geodetic coordinate system, an ECEF coordinate system, or the like.

[0056]

Using the flowchart shown in FIG. 4, a sequence of process steps (referred to as the authentication request relation process) which requests the NMA information management center 300 to authenticate the navigation message M received by the satellite receiver 230 will be explained.

Authenticating the navigation message M received by the satellite receiver 230 indicates authenticating that the received navigation message M is not a navigation message falsified by a simulator, but the authentic navigation message M transmitted from the GPS satellite 2.

[0057]

As described above, the authentication request relation process is performed by the control portion 220 of the vehicle onboard apparatus 200. The control portion 220 sequentially (for example, every 100 milliseconds) performs the authentication request relation process shown in the flowchart in FIG. 4 when, for example, electric power is supplied to the vehicle onboard

apparatus 200. Alternatively, the control portion 220 may also be configured appropriately to perform the authentication request relation process when, for example, the navigation message M is input thereto from the satellite receiver 230.

5 [0058]

In S1, the navigation message N received by the satellite receiver 230 from the QZS satellite 3 is acquired. In S2, from the navigation message N acquired in S1, the parity data and the RAND message corresponding to the parity data are extracted. Then, as information for specifying the RAND message to which the parity data corresponds, PRN ID and TOW are extracted from the RAND message and stored in association with the parity data in the memory 221. S2 corresponds to an inspection data extraction section of the present disclosure.

[0059]

15 Incidentally, the navigation message N in the present embodiment includes the RAND messages for the individual GPS satellites 2 and the parity data sets corresponding to the RAND messages. Consequently, according to S2, the control portion 220 acquires the parity data sets corresponding to the navigation messages M transmitted from the individual GPS satellites 2, and stores the parity data sets in the memory 221. The parity data sets extracted from the navigation message N will be referred to as a reception parity data, so as to be distinguished from comparison parity data.

[0060]

25 In S3, the navigation message M received by the satellite receiver 230 from the GPS satellite 2 is acquired. In S4, it is determined whether the navigation message M needs to be authenticated. Whether the received navigation message M needs to be authenticated may be determined appropriately in response to, for example, a request from an application using the position information of the vehicle onboard apparatus 200.

[0061]

As an example of the application using the position information, an application which automatically charges the user of a vehicle in which the

vehicle onboard apparatus 200 is mounted when determining that the vehicle has been parked in a toll parking area, a game using the position information, an application for providing routing assistance, or the like can be assumed. Such an application which charges a fee using the position information needs
5 the authentication of the navigation message M so as to ensure that the position information has not been falsified. On the other hand, when the position information is provided to the application for providing routing assistance or the like, it can be considered that the authentication of the navigation message M is voluntary.

10 [0062]

That is, in S4, it is determined whether the authentication process is necessary based on the type of the application to which the position information is provided or a request from the application. When the navigation message M needs to be authenticated, YES is given in S4, and
15 the process moves to S5. On the other hand, when the navigation message M need not be authenticated, NO is given in S4, and the present flow terminates.

[0063]

In S5, from the navigation message M received in S3, the RAND
20 message is produced by the same method as used by the RAND message generation portion 1221 of the authentication center 120, and the process moves to S6. S5 corresponds to an authentication relation data extraction section of the present disclosure.

[0064]

Incidentally, the control portion 220 generates the RAND message from the navigation message M by the same method as used by the RAND message generation portion 1221. Accordingly, when the respective navigation messages M used to generate the RAND messages in the control
25 portion 220 and the RAND message generation portion 1221 are the same, the RAND messages generated therefrom also have the same content.
30

[0065]

That is, when the navigation message M received by the satellite receiver 230 in S3 is the authentic navigation message M, the RAND

message generated in S5 matches the RAND message generated by the RAND message generation portion 1221.

[0066]

In S6, from the navigation message M acquired in S3, PRN ID and
5 TOW are extracted and the reception parity data corresponding to the combination thereof is read from the memory 221, and the process moves to S7. In S7, the NMA request data Rq including the RAND message generated in S5 and the reception parity data read in S6 is generated, and the process moves to S8. The NMA request data Rq corresponds to an
10 example of an authentication request signal of the present disclosure. S7 corresponds to an authentication request signal generation section of the present disclosure.

[0067]

In S8, the NMA request data Rq is transmitted to the NMA
15 information management center 300. S8 corresponds to an authentication request signal transmission processing section of the present disclosure.

[0068]

Incidentally, communication between the vehicle onboard apparatus
200 and the NMA information management center 300 is performed by
20 encrypted secure communication. For example, the NMA request Rq may be encrypted appropriately using the public key issued by the NMA information management center 300 and transmitted to the NMA information management center 300. Needless to say, the secrecy of communication may also be ensured by using a common key encryption method or the like.

25 [0069]

<Detailed configuration of NMA information management center
300>

A configuration of the NMA information management center 300 will
be explained with reference to FIG. 5. As shown in FIG. 5, the NMA
30 information management center 300 includes a communication portion 310, a control portion 320, and an NMA information database (hereinafter referred to as NMA information DB) 340.

[0070]

The communication portion 310 includes a reception portion 311 that performs the demodulation of a reception signal or the like and a transmission portion 312 that modulates the data input thereto from the control portion 320 and transmits the data. The NMA information management center 300 can communicate with the vehicle onboard apparatus 200 and the authentication center 120 via the communication portion 310.

[0071]

The control portion 320 is a computer including a CPU, a ROM, a RAM, or the like, and controls the operation of the communication portion 310 and performs the addition, deletion, and reading of the data stored in the NMA information DB 340 or the like. The CPU of the control portion 320 executes the program stored in the ROM using the temporary storing function of the RAM to thus perform the authentication relation process described later or the like.

[0072]

The NMA information DB 340 is a rewritable large capacity storage device and implemented by, for example, a HDD or the like. The NMA information DB 340 stores information (assumed to be NMA information) used to authenticate the navigation messages M received by the vehicle onboard apparatus 200 based on an instruction from the control portion 320. More specifically, the NMA information DB 340 stores, as the NMA information, combinations of the RAND messages determined to have succeeded in authentication in an authentication arithmetic operation process described later and the parity data sets. The NMA information corresponds to authenticated data of the present disclosure and the NMA information DB 340 corresponds to an authenticated data memory portion of the present disclosure.

[0073]

The NMA information DB 340 stores the combinations of the RAND messages and the parity data sets so as to allow each of the combinations to be specified from PRN ID and TOW each included in the RAND message. That is, by specifying PRN ID and TOW, the control portion 320 is allowed to

access the parity data set and the RAND message which correspond to the combination of PRN ID and TOW. The RAND messages and the parity data sets corresponding to the RAND messages stored in the NMA information DB 340 are hereinafter referred to as authenticated RAND messages and
5 authenticated parity data sets, respectively.

[0074]

Using the flowchart shown in FIG. 6, a sequence of process steps (referred to as the authentication relation process) performed by the control portion 320 to authenticate the navigation message M received by the
10 satellite receiver 230 will be explained. The flowchart shown in FIG. 6 is implemented when, for example, the NMA request data Rq is received from the vehicle onboard apparatus 200.

[0075]

In S11, the encrypted NMA request data Rq transmitted from the
15 vehicle onboard apparatus 200 is acquired from the communication portion 310. Then, the encrypted NMA request data Rq is decrypted using a secret key corresponding to the public key used for the encryption thereof, and the process moves to S12. S11 corresponds to an authentication request signal reception processing section of the present disclosure.

[0076]

In S12, from the NMA request data Rq decrypted in S11, the RAND message and the parity data are extracted. The parity data is the data received by the vehicle onboard apparatus 200 from the QZS satellite 3, that is, the reception parity data. From the RAND message extracted from the
25 NMA request data Rq, PRN ID and TOW are further extracted.

[0077]

In S13, the NMA information DB 340 is accessed and the authenticated RAND message and the authenticated parity data which correspond to PRN ID and TOW each acquired in S12 are searched for.

30 When the authenticated RAND message and the authenticated parity data which correspond to PRN ID and TOW each acquired in S12 are present in the NMA information DB 340, YES is given in S13, and the process moves to S14. On the other hand, when the authenticated parity data acquired in S12

is not present in the NMA information DB 340, NO is given in S13, and the process moves to S20. S13 corresponds to an authentication completion determination section of the present disclosure. The NMA information corresponding to PRN ID and TOW acquired in S12 corresponds to
5 authenticated data corresponding to the authentication relation data of the present disclosure.

[0078]

In S14, it is determined whether the authenticated RAND message found in S13 matches the RAND message extracted from the NMA request
10 data Rq in S12. When the two RAND messages match, YES is given in S14, and the process moves of S15. In S15, it is determined that authentication has succeeded, and the present flow terminates. The successful authentication means that the navigation message M received by the vehicle onboard apparatus 200 in S3 in FIG. 4 is not a signal generated by a
15 simulator or the like, but the authentic navigation message M transmitted from the GPS satellite 2.

[0079]

Incidentally, in this configuration, it is determined that authentication has succeeded when the authenticated RAND message matches the RAND
20 message extracted from the NMA request data Rq in S12. However, the configuration is not limited to this. A configuration may also be used appropriately which determines that authentication has succeeded when the authenticated parity data matches the reception parity data.

[0080]

On the other hand, when the authenticated RAND message found in S13 does not match the RAND message extracted from the NMA request
25 data Rq in S12, NO is given in S14. The process moves to S16 to determine that authentication has failed, and the present flow terminates. S14 to S16 correspond to an authenticated data comparison authentication
30 section of the present disclosure.

[0081]

In S20, using the RAND message and the reception parity data each extracted from the NMA request data Rq, the authentication arithmetic

operation process is performed. A description will be given separately of the authentication arithmetic operation process using the flowchart shown in FIG. 7. Incidentally, S20 corresponds to an authentication arithmetic operation section of the present disclosure.

5 [0082]

The flowchart in FIG. 7 is executed when the process moves to S20 in FIG. 4. In S21, the reception parity data extracted from the NMA request data Rq is acquired, and the process moves to S22. In S22, the RAND message extracted from the NMA request data Rq is acquired, and the
10 process moves to S23.

[0083]

In S23, PRN ID and TOW each included in the RAND message are transmitted together with the public key used for secret communication from the transmission portion 312 to the authentication center 120. As described
15 above, the authentication center 120 encrypts the H matrix determined by PRN ID and TOW using the public key distributed from the NMA information management center 300, and transmits the encrypted H matrix to the NMA information management center 300.

[0084]

20 In S24, the encrypted H matrix transmitted from the authentication center 120 is acquired from the reception portion 311. In S25, the encrypted H matrix acquired in S24 is decrypted using the secret key, and the process moves to S26. S24 and S25 correspond to an encryption key acquisition section of the present disclosure.

25 [0085]

In S26, from the RAND message acquired in S22 and the H matrix decrypted in S25, parity data (referred to as the comparison parity data) is produced by the same process as the process performed by the parity generation portion 1224. The comparison parity data corresponds to a
30 comparison inspection data of the present disclosure. S26 corresponds to a comparison inspection data generation section of the present disclosure.

[0086]

In S27, it is determined whether the comparison parity produced in S26 matches the reception parity data acquired in S21. When the two parity data sets match, it is authenticated that the navigation message M received by the vehicle onboard apparatus is authentic (S28) for the reason described below.

[0087]

That is, the H matrix decrypted in S25 is the same H matrix as used when the authentication center 120 produced the parity data from the RAND message. The parity data generated by the authentication center 120 is the parity data transmitted from the QZS satellite 3, that is, the reception parity data.

[0088]

Accordingly, when the comparison parity data produced in S26 matches the reception parity data acquired in S21, it can be considered that the RAND message produced in S26 is the same as the RAND message produced by the authentication center 120.

[0089]

A match between the two RAND messages represents that the navigation message M on which the RAND message acquired in S22 is based, that is, the navigation message acquired in S3 in FIG. 4 matches the navigation message M used when the authentication center 120 produced the RAND message.

[0090]

That is, when the comparison parity data produced in S26 matches the reception parity data acquired in S21, a match between the two parity data sets represents that the navigation message M acquired in S3 in FIG. 4 is the authentic navigation message M acquired also by the authentication center 120.

[0091]

For this reason, when the comparison parity data produced in S26 matches the reception parity data acquired in S21 (YES in S27), the process advances to S28 to determine that authentication has succeeded. On the other hand, when the two parity data sets do not match (NO in S27), the

process advances to S29 to determine that authentication has failed. After S28 or S29 is performed, the result of the authentication is held, and then the process returns to the invoker of the authentication arithmetic operation process (S20 in FIG. 6).

5 [0092]

Referring back to FIG. 6, the description of the authentication relation process will be continued. The foregoing has described the process preceding and including S20. When S20 is completed, the process moves to S40. In S40, it is determined whether authentication has succeeded as a
10 result of the authentication arithmetic operation process. When authentication has succeeded, YES is given in S40, and the process moves to S41. On the other hand, when authentication has failed, NO is given in S40, and the process moves to S42.

[0093]

15 In S41, a combination of the RAND data extracted from the NMA request data Rq and the reception parity data is additionally newly stored as NMA information in the NMA information DB 340. Consequently, when the NMA request data Rq including the same RAND message and the same reception parity data is transmitted from another vehicle onboard apparatus,
20 YES is given in each of S13 and S14, and therefore it can be considered that authentication has succeeded. That is, the authentication arithmetic operation process in S20 can be omitted from the next time. When the additional storage process in S41 is completed, the present flow terminates.

[0094]

25 In S42, the RAND data and the reception parity data each extracted from the NMA request data Rq are discarded. In other words, the RAND data and the reception parity data that have failed in authentication are not stored in the NMA information DB 340. When the process in S42 is completed, the present flow terminates.

30 [0095]

(Summarization of first embodiment)

According to this configuration, on receiving the navigation message M, the vehicle onboard apparatus 200 generates the NMA request data Rq

which requests the authentication of whether the navigation message M is the navigation message M transmitted from the GPS satellite 2 to be performed, and transmits the NMA request data Rq to the NMA information management center 300. The NMA request data includes the RAND message and the reception parity data corresponding to the RAND message.

[0096]

That is, on receiving a first navigation message, a reception terminal in a navigation message authentication system according to an example of the present disclosure extracts the authentication data required for the authentication process from the first navigation message. The reception terminal also extracts the inspection data used for the authentication of the first navigation message from the second navigation message. Then, the reception terminal transmits an authentication request signal including the authentication data and the inspection data to the authentication processing apparatus.

[0097]

The NMA information management center 300 uses the RAND message and the reception parity data each included in the NMA request data Rq, and performs an authentication process that authenticates whether the navigation message M received by the vehicle onboard apparatus 200 is an authentic navigation message.

[0098]

That is, on receiving the authentication request signal, the authentication processing apparatus in the navigation message authentication system according to an example of the present disclosure performs the authentication process based on the authentication data and the inspection data each included in the authentication request signal.

[0099]

More specifically, the authentication processing apparatus accesses the NMA information DB 340 to search for the NMA information corresponding to PRN ID and TOW each included in the NMA request data Rq (S13). When there is the NMA information corresponding to PRN ID and TOW each included in the NMA request data Rq, the authentication process

using the NMA information and the RAND message included in the NMA request data Rq is performed (S14 to S16).

[0100]

When the NMA information corresponding to PRN ID and TOW
5 each included in the NMA request data Rq does not exist in the NMA information DB 340, the authentication arithmetic operation process (S20) using the RAND message and the reception parity data each included in the NMA request data Rq is performed.

[0101]

10 That is, in the present embodiment, the authentication arithmetic operation process for determining whether the navigation message M received by the vehicle onboard apparatus 200 is an authentic navigation message is performed by the NMA information management center 300. Accordingly, the vehicle onboard apparatus 200 need not perform the
15 authentication arithmetic operation process.

[0102]

Therefore, according to the above configuration, it may be possible to authenticate the navigation message M received by the vehicle onboard apparatus 200, while suppressing an increase in the cost of the vehicle
20 onboard apparatus 200.

[0103]

The reception terminal need not perform the authentication process. The authentication processing apparatus performs the authentication process in place of the reception terminal. That is, since the reception
25 terminal does not need a CPU having a high arithmetic processing ability for performing numerical calculation resulting from the authentication process at a high speed, it may be possible to suppress an increase in the cost of the reception terminal.

[0104]

30 In addition, the NMA information management center 300 intensively performs the authentication of the navigation messages M received by multiple vehicle onboard apparatuses 200, which are used in the navigation message authentication system 1. Also, a combination of the

RAND message and the parity data which has been once subjected to the authentication arithmetic operation process is stored in the NMA information DB 340. Accordingly, it is possible that the NMA request data Rq including the same PRN ID and the same TOW as included in the NMA request data Rq that has already succeeded in authentication is authenticated by being compared to the NMA information stored in the NMA information DB 340. It is possible to omit the authentication arithmetic operation process. Thus the NMA information management center 300 intensively performs the authentication process and consequently the navigation message M received by the vehicle onboard apparatus 200 is authenticated in a shorter time.

[0105]

While the embodiment of the present disclosure has been described, the present disclosure is not limited to the embodiment. The following embodiments are also included in the technical scope of the present disclosure. In addition, various changes and modifications other than those shown below can be made in the present disclosure, which can be implemented within a scope not departing from the gist thereof.

[0106]

<First modification>

Incidentally, in the first embodiment, the NMA information management center 300 is configured to acquire, from the vehicle onboard apparatus 200, the parity data to be compared to the parity data (that is, a comparison parity data) generated from the navigation message received by the vehicle onboard apparatus 200. However, the configuration of the NMA information management center 300 is not limited to this.

[0107]

The NMA information management center 300 may also acquire the parity data to be compared to the comparison parity data from the data memory portion 124. That is, the NMA information management center 300 may also acquire the parity data corresponding to the RAND message included in the NMA request data Rq from the authentication center 120 in the same manner as in the procedure of the acquisition of the H matrix (S23 to S25 in FIG. 7). Since the reception parity data received by the vehicle

onboard apparatus 200 from the QZS satellite 3 is the same as the parity data stored in the data memory portion 124, even when the data acquired as the parity data to be compared to the comparison parity data from the data memory portion 124 is used, the same result of determination can be
5 obtained in S27.

[0108]

Such a variation also eliminates the need to incorporate the reception parity data in the NMA request data R_q transmitted from the vehicle onboard apparatus 200 to the NMA information management center 300. It
10 may be possible to reduce the amount of data transmitted from the vehicle onboard apparatus 200 to the NMA information management center 300.

[0109]

<Second embodiment>

A second embodiment of the present disclosure will be explained
15 with reference to the drawings. Incidentally, for the sake of convenience, members having the same functions as those of the members shown in the drawings used to describe the first embodiment above are designated by the same reference numerals and a description thereof is omitted. In addition, when only a part of the configuration is described, the first embodiment
20 described previously is applicable to the description of the other part of the configuration.

[0110]

A navigation message authentication system 1a in the second embodiment includes, in addition to the configuration of the navigation
25 message authentication system 1 in the first embodiment, a service center 400 performing communication with each of the vehicle onboard apparatus 200 and the NMA information management center 300, as shown in FIG. 8. The vehicle onboard apparatus 200 in the second embodiment transmits the NMA request data R_q to the service center 400 and also transmits the result
30 of the positioning by the vehicle onboard apparatus 200 (that is, position information) to the service center 400.

[0111]

The service center 400 is provided outside a vehicle and managed by a service provider who provides a service using the position information transmitted from the vehicle onboard apparatus 200. As examples of the service using the position information, a service which automatically charges the user of the vehicle in which the vehicle onboard apparatus 200 is mounted when it is determined that the vehicle has been parked in a toll parking area or when it is determined that the vehicle has traveled along a toll road, or the like are assumed.

[0112]

Besides, as the service using the position information, a service which provides routing assistance or proposes a sightseeing spot around the present position, a game which uses the position information, or the like can be considered. By way of example, a service which is provided by a parking area management company and which charges a fee when it is determined that the vehicle in which the vehicle onboard apparatus 200 is mounted has been parked in a toll parking area is supposed.

[0113]

In a service using position information and involving billing, an important precondition is that the position information about the vehicle onboard apparatus 200 has not been falsified. That is, depending on whether the position information acquired from the vehicle onboard apparatus 200 is based on the authenticated navigation message M, the service provider determines whether the service is to be provided to the customer using the vehicle onboard apparatus 200.

[0114]

A configuration of the service center 400 will be explained with reference to FIG. 9. The service center 400 includes a communication portion 410, a control portion 420, an NMA information DB 440, and a customer database (hereinafter referred to as customer DB) 450.

[0115]

The communication portion 410 includes a reception portion 411 that performs the demodulation of a reception signal or the like and a transmission portion 412 that modulates the data inputted from the control

portion 420 and transmits the data. The service center 400 can perform communication with the vehicle onboard apparatus 200 and the NMA information management center 300 via the communication portion 410. The reception portion 411 corresponds to a service-center-side reception portion of the present disclosure. Incidentally, in the present disclosure, the service center may also be referred to as SC for the sake of simplicity.

[0116]

The NMA information DB 440 is a large scale rewritable storage device and stores the NMA information, similarly to the NMA information DB 340 included in the NMA information management center 300. More specifically, in the NMA information DB 340, as the NMA information, the RAND message and the parity data which allow for successful authentication are associated with each other and stored so as to be able to be specified from PRN ID and TOW each included in the RAND message.

[0117]

The NMA information stored in the NMA information DB 440 is added as necessary in a service-center-side authentication relation process (hereinafter referred to as SC-side authentication relation process). The NMA information DB 440 corresponds to an SC-side authenticated data memory portion of the present disclosure.

[0118]

The customer DB 450 is a large capacity rewritable storage device and stores information (referred to as customer information) about customers who use the service provided by the service center 400. The customer information is distinctively managed on a per customer basis. In the customer information, information (referred to as registered vehicle onboard apparatus information) about each of the vehicle onboard apparatuses 200 used by the customers and the position information acquired from the vehicle onboard apparatuses 200 are associated with each other and stored.

[0119]

The vehicle onboard apparatus information includes an identification number for distinguishing the vehicle onboard apparatus 200 from another vehicle onboard apparatus and authentication state information. Examples

of the authentication state information include whether the vehicle onboard apparatus 200 of concern has received an authenticated navigation message, the number of the authenticated GPS satellites 2, the ratio of the number of the authenticated GPS satellites 2 to the number of the GPS satellites 2 used
5 by the vehicle onboard apparatus 200 for positioning, or the like. As the identification number of the vehicle onboard apparatus, for example, the production number of the vehicle onboard apparatus 200, the MAC address thereof, or the like may be used appropriately.

[0120]

10 The service center 400 determines whether the service using the position information is to be provided to the customer who uses the vehicle onboard apparatus 200 based on the vehicle onboard apparatus information. For example, when positioning has been performed using the signal transmitted from the authenticated GPS satellite 2 or when the ratio of the
15 number of the authenticated GPS satellites 2 to the number of the GPS satellites 2 used for the positioning is not less than a fixed threshold (for example, 75%), the service center 400 determines that the service is to be provided.

[0121]

20 The control portion 420 is a computer including a CPU, a ROM, a RAM, or the like, and controls the operation of the communication portion 410 and performs the addition, deletion, and reading of the data stored in the NMA information DB 440 or the like. The CPU of the control portion 420 executes the program stored in the ROM using the temporary storing function
25 of the RAM to thus perform the SC-side authentication relation process described later or the like.

[0122]

A major difference between the service center 400 and the NMA information management center 300 lies in that the service center 400 is the
30 facility managed by the service provider and also does not have the function of performing the authentication arithmetic operation process. That is, authentication using the NMA information stored in the NMA information DB 440 can be performed, but a combination of PRN ID and TOW which is not

stored in the NMA information DB 440 cannot be authenticated in the facility of the service center 400. The process in this case will be mentioned in the description of the SC-side authentication relation process.

[0123]

5 A sequence of process steps for authenticating the navigation message M received by the vehicle onboard apparatus 200 in the second embodiment will be explained. On receiving the navigation message M, the vehicle onboard apparatus 200 performs the authentication request relation process shown in FIG. 4. In the second embodiment, the flow of the
10 authentication request relation process is the same as in the first embodiment. However, the destination of the NMA request data Rq transmitted in S8 is not the NMA information management center 300, but the service center 400.

[0124]

15 Then, the service center 400 that has received the NMA request data Rq from the vehicle onboard apparatus 200 performs the SC-side authentication relation process. Incidentally, the communication between the vehicle onboard apparatus 200 and the service center 400 is performed by encrypted secure communication.

[0125]

20 A description will be given of the SC-side authentication relation process performed by the control portion 420 of the service center 400 using the flowchart shown in FIG. 10. The flowchart shown in FIG. 10 may be performed appropriately when the NMA request data Rq is received from the vehicle onboard apparatus 200.

[0126]

25 In S51, the encrypted NMA request data Rq transmitted from the vehicle onboard apparatus 200 is acquired from the communication portion 410. Then, the encrypted NMA request data Rq is decrypted using the secret key corresponding to the public key used for the encryption, and the
30 process moves to S52. S51 corresponds to an SC-side authentication request signal reception processing section of the present disclosure.

[0127]

In S52, from the NMA request data Rq decrypted in S51, the RAND message and the parity data are extracted. The parity data is the data received by the vehicle onboard apparatus 200 from the QZS satellite 3, that is, the reception parity data. From the RAND message extracted from the NMA request data Rq, PRN ID and TOW are further extracted.

[0128]

In S53, the NMA information DB 440 is accessed and the NMA information corresponding to PRN ID and TOW each acquired in S52 is searched for. When the NMA information corresponding to PRN ID and TOW each acquired in S52 is present in the NMA information DB 440, S53 is YES, and the process moves to S54. On the other hand, when the NMA information corresponding to PRN ID and TOW each acquired in S52 is not present in the NMA information DB 440, S53 is NO, and the process moves to S57. S53 corresponds to an SC-side authentication completion determination section of the present disclosure.

[0129]

In S54, it is determined whether the authenticated RAND message of the NMA information found in S53 matches the RAND message extracted from the NMA request data Rq in S52. When the two RAND messages match, S54 is YES, and the process moves to S55. In S55, it is determined that authentication has succeeded, and the process moves to S62.

[0130]

Incidentally, in this configuration, in the same manner as in the first embodiment, it is determined that authentication has succeeded when the authenticated RAND message matches the RAND message extracted from the NMA request data Rq in S52. However, the configuration is not limited to this. A configuration may also be used appropriately which determines that authentication has succeeded when the reception parity data matches the authenticated parity data.

[0131]

On the other hand, when the authenticated RAND message found in S53 does not match the RAND message extracted from the NMA request data Rq, S54 is NO, and the process moves to S56 to determine that

authentication has failed and then moves to S62. S54 to S56 correspond to an SC-side authenticated data comparison-and-authentication section of the present disclosure.

[0132]

5 In S57, the NMA request data Rq acquired and decrypted in S51 is encrypted again using the public key distributed by the NMA information management center 300 and transmitted to the NMA information management center 300. That is, the NMA request data Rq transmitted from the vehicle onboard apparatus 200 is transferred to the NMA information
10 management center 300 (this is referred to as a secondary NMA request process). S57 corresponds to an SC-side authentication request signal transmission processing section of the present disclosure.

[0133]

On receiving the NMA request data Rq from the service center 400,
15 the NMA information management center 300 performs the NMA authentication relation process shown in FIG. 6. The NMA authentication relation process is the same as in the first embodiment. However, the results of authentication in S15, S16, S28, and S29 are transmitted to the service center 400. Thus, the NMA information management center 300
20 returns successful authentication or failed authentication as a response to the NMA request data Rq from the service center 400. The data showing the result of the authentication transmitted from the NMA information management device corresponds to authentication result data of the present disclosure.

25 [0134]

Referring back to FIG. 10, when the control portion 420 of the service center 400 receives the result of the authentication process from the NMA information management center 300 in S58, the process moves to S59. S58 corresponds to an authentication result acquisition section of the present
30 disclosure.

[0135]

In S59, it is determined whether the authentication result received from the NMA information management center 300 is successful

authentication. When the authentication result is successful authentication, S59 is YES, and the process moves to S60. On the other hand, when the authentication result is failed authentication, S59 is NO, and the process moves to S61.

5 [0136]

In S60, a combination of RAND data and the reception parity data each extracted from the NMA request data Rq acquired in S51 is additionally newly stored as the NMA information in the NMA information DB 440.

Consequently, when the NMA request data Rq including the same RAND
10 message and the same reception parity data is transmitted from another vehicle onboard apparatus, each of S53 and S54 is YES, and therefore it can be determined that authentication has succeeded. That is, the secondary NMA request process in S57 can be omitted from the next time. S60 corresponds to an SC-side authenticated data addition processing section of
15 the present disclosure. When the storage process in S60 is completed, the process moves to S62.

[0137]

In S61, the RAND data and the reception parity data each from the NMA request data are discarded. In other words, the RAND data and the
20 reception parity data that have failed in authentication are not stored in the NMA information DB 440. When the process in S61 is completed, the process moves to S62.

[0138]

In S62, the result of the authentication process requested by the
25 NMA request data Rq, that is, whether the authentication of the navigation message M received by the vehicle onboard apparatus 200 has succeeded is transmitted to the vehicle onboard apparatus 200, and the process moves to S63. S62 corresponds to an authentication result transmission processing section of the present disclosure.

30 [0139]

In S63, the authentication state information about the vehicle onboard apparatus 200 is updated, and the present flow terminates. For example, when the authentication process has succeeded, the vehicle

onboard apparatus 200 stores, in the authentication state information, the reception of the authentic navigation message M transmitted from the GPS satellite 2 and specified from PRN ID included in the NMA request data Rq.

[0140]

5 On acquiring the result of the authentication requested by the NMA request data Rq via the reception portion 211, the control portion 220 of the vehicle onboard apparatus 200 stores the authentication result in association with PRN ID in the memory 221. According to this configuration, it may be possible that the control portion 220 recognizes the authentication state (that
10 is, whether authentication has been completed) of the GPS satellite 2 by referencing the storage area of the memory 221 where the result of authentication is stored on a per PRN ID basis.

[0141]

Incidentally, in the present embodiment, the vehicle onboard
15 apparatus 200 acquires the authentication result from the service center 400. However, the vehicle onboard apparatus 200 may also acquire the authentication result from the NMA information management center 300.

[0142]

(Summarization of second embodiment)

20 According to the configuration, on receiving the navigation message M from the GPS satellite 2, the vehicle onboard apparatus 200 generates the NMA request data Rq asking whether the navigation message M is the navigation message M actually transmitted from the GPS satellite 2, and transmits the NMA request data Rq to the service center 400. The NMA
25 request data Rq includes the RAND message and the reception parity data that corresponds to the RAND message.

[0143]

The service center 400 authenticates whether the navigation
message M received by the vehicle onboard apparatus 200 is an authentic
30 navigation message by using the RAND message and the reception parity data each included in the NMA request data Rq and using the NMA information stored in the NMA information DB 440. When the NMA information corresponding to the RAND message and the reception parity

data each included in the NMA request data Rq is not present in the NMA information DB 440, the service center 400 transmits the NMA request data Rq to the NMA information management center 300 to acquire the authentication result.

5 [0144]

Thus, according to the configuration, it may be possible to authenticate the navigation message M received by the vehicle onboard apparatus 200, while suppressing an increase in the cost of the vehicle onboard apparatus 200.

10 [0145]

Since the service provider can recognize the authentication state of the vehicle onboard apparatus 200 used by the customer, it may be possible for the service provider to determine whether the service is to be provided based on the authentication state.

15 [0146]

In addition, the service center 400 returns the result of the authentication requested by the NMA request data Rq to the vehicle onboard apparatus 200 (S63 in FIG. 10). This allows the vehicle onboard apparatus 200 to recognize the credibility of the transmitter of the signal used in the positioning arithmetic operation, that is, whether the transmitter is the GPS satellite 2 or a simulator. For example, it may be possible to suppose that the transmitter of the navigation message M that has failed in authentication is a simulator. Since this shows that the signal from the simulator is used in the arithmetic operation, it may be possible to be prepared for a next positioning arithmetic operation by not using the signal from the transmitter of the navigation message M that has failed in authentication.

[0147]

<Second modification>

In the second embodiment, the configuration is used in which, when the NMA information corresponding to PRN ID and TOW each included in the NMA request data Rq acquired from the vehicle onboard apparatus 200 is not present in the NMA information DB 440 (NO in S53), the NMA request

data Rq is transmitted to the NMA information management center 300.
However, the configuration is not limited to this.

[0148]

As shown in FIG. 11, it may also be possible that the service center
5 400 includes the same satellite receiver 430 as the satellite receiver 230 and
the control portion 420 sequentially acquires the navigation messages M
transmitted from the GPS satellites 2 and the navigation message N
transmitted from the QZS satellite 3 (which is assumed to be the second
modification). The satellite receiver 430 corresponds to an SC-side satellite
10 receiver of the present disclosure.

[0149]

On receiving the navigation message M and the parity data that
result in a combination of PRN ID and TOW which is not present in the NMA
information DB 440, the control portion 420 in the second modification
15 generates the NMA request data Rq corresponding to the navigation
message M and transmits the NMA request data Rq to the NMA information
management center 300.

[0150]

When the result of the authentication requested by the NMA request
20 data Rq is successful authentication, the authenticated RAND message and
the authenticated parity data each corresponding to the combination of PRN
ID and TOW are additionally stored in the NMA information DB 440.

[0151]

According to this configuration, even when the NMA request data
25 Rq is not received from the vehicle onboard apparatus 200, the data included
in the NMA information DB 440 is updated as necessary. Consequently, it
may be possible that the control portion 420 reduces the possibility of
performing the secondary NMA request process (S57) in response to the
NMA request data Rq from the vehicle onboard apparatus 200 and more
30 promptly obtain the result of the authentication requested by the NMA
request data Rq from the vehicle onboard apparatus 200.

[0152]

<Third modification>

In the second embodiment, the control portion 220 of the vehicle onboard apparatus 200 may also have the function (transmission destination selection portion) 222 of selecting at least one destination to which the NMA request data Rq is to be transmitted from the multiple service centers 400a and 400b, as shown in FIG. 12.

[0153]

The transmission destination selection portion 222 selects the more preferable service center 400 as a destination to which the NMA request data Rq is to be transmitted based on the present position information, a currently active application, or the like. For example, when it is determined that the vehicle is currently present in a toll parking area from the present position information and map data, the NMA request data Rq is transmitted to the service center 400 of the service provider who manages the toll parking area. Alternatively, when the application of the game using the position information is active, the NMA request data Rq may be transmitted appropriately to the service center 400 managed by the service provider who provides the game.

[0154]

When a user can use the services each using the position information which are provided by the multiple service providers, the vehicle onboard apparatus 200 used by the user may need to be authenticated in the service centers 400 managed by the individual service providers. In such a case also, the configuration of a third modification allows the vehicle onboard apparatus 200 to be authenticated in the service center 400 which is more suitable for the purpose of the user.

[0155]

<Fourth modification>

In the configuration shown above, the vehicle onboard apparatus 200 communicates with the service center 400 and the NMA information management center 300 using the wide range communication function. However, communication may also be performed via a roadside apparatus or the like. The control portion 220 may also have the function of properly selecting a communication means such that, when there is no roadside apparatus in a communicable area formed by the narrow range

communication function of the communication portion 210, the wide range communication function is used.

[0156]

Each of the flowcharts or the processes in the flowcharts shown in
5 the present application may include multiple steps (or referred to also as sections). Each of the steps is represented as, for example, S1. Each of the steps may further be divided into sub-steps. Furthermore, several steps may be combined to form one step.

[0157]

10 The present disclosure is not intended to be limited to each of the embodiments described above and can variously be changed within the scope shown in the present disclosure. An embodiment obtained by properly combining the technical means disclosed in the different
15 embodiments is also included in the technical scope of the present disclosure.

CLAIMS

1. A navigation message authentication system (1), comprising:
at least one first satellite (2) that transmits a first navigation
message;

5 a second satellite (3) that transmits a second navigation message
including an inspection data used for an authentication process for the first
navigation message;

a reception terminal (200) that receives the first navigation message
and the second navigation message, wherein the navigation message

10 authentication system (1) performs the authentication process of
authenticating whether the first navigation message received by the reception
terminal (200) is the first navigation message transmitted from the first
satellite (2) by using the inspection data included in the second navigation
message; and

15 an authentication processing apparatus (300) that is provided
outside the reception terminal (200) and communicates with the reception
terminal (200),

wherein:

the reception terminal (200) includes

20 a terminal-side satellite receiver (230) that receives the first
navigation message transmitted from the first satellite (2) and the second
navigation message transmitted from the second satellite (3),

an inspection data extraction section (S2) that extracts the
inspection data from the second navigation message received by the

25 terminal-side satellite receiver (230),

an authentication relation data extraction section (S5) that
extracts, from the first navigation message received by the terminal-side
satellite receiver (230), an authentication relation data required for the
authentication process for the first navigation message,

30 an authentication request signal generation section (S7) that
generates an authentication request signal which includes the inspection
data extracted by the inspection data extraction section (S2) and the
authentication relation data extracted by the authentication relation data

extraction section (S5), and requests the authentication process to be performed for the first navigation message received by the terminal-side satellite receiver (230), and

an authentication request signal transmission processing section (S8) that transmits the authentication request signal generated by the authentication request signal generation section (S7); and

the authentication processing apparatus (300) includes

an authentication request signal reception processing section (S11) that receives the authentication request signal transmitted from the

authentication request signal transmission processing section (S8), and

an authentication arithmetic operation section (S20) that performs the authentication process for the first navigation message received by the reception terminal (200), based on the inspection data and the authentication relation data each included in the authentication request

signal.

2. The navigation message authentication system according to claim 1, wherein:

the inspection data included in the second navigation message is generated by an authentication center apparatus (100) that acquires the first navigation message;

the authentication center apparatus (100) includes

a first navigation message reception portion (110) that receives the first navigation message,

an authentication data generation portion (1221) that generates an authentication data from the authentication relation data of the first navigation message received by the first navigation message reception portion (110),

an encryption key generation portion (1223) that generates an encryption key corresponding to the authentication data generated by the authentication data generation portion (1221),

an inspection data generation portion (1224) that generates the inspection data by using the authentication data generated by the

authentication data generation portion (1221) and the encryption key corresponding to the authentication data,

a storage portion (124) that stores the encryption key generated by the encryption key generation portion (1223) in association with the authentication data using the encryption key,

an inspection data transmission portion (130) that transmits the inspection data generated by the inspection data generation portion (1224) to the second satellite (3), and

a communication portion (126) that communicates with the authentication processing apparatus (300);

the storage portion (124) stores the encryption key in association with the inspection data and the first navigation message;

the authentication processing apparatus (300) further includes

an encryption key acquisition section (S24 and S25) that acquires, from the storage portion (124), the encryption key corresponding to the authentication relation data included in the authentication request signal, and

a comparison inspection data generation section (S26) that generates a comparison inspection data from the authentication relation data included in the authentication request signal and from the encryption key acquired by the encryption key acquisition section (S24 and S25); and

the authentication arithmetic operation section (S20)

determines that the first navigation message received by the reception terminal (200) has succeeded in authentication when the comparison inspection data generated by the comparison inspection data generation section (S26) matches the inspection data included in the authentication request signal, and

determines that the first navigation message has failed in authentication when the comparison inspection data generated by the comparison inspection data generation section (S26) does not match the inspection data included in the authentication request signal.

3. The navigation message authentication system according to claim 1 or 2, wherein:

the authentication processing apparatus (300) further includes

an authenticated data memory portion (340) that stores, as an authenticated data, a combination of the authentication relation data and the inspection data, the combination being determined to have succeeded in authentication as a result of the authentication process performed by the authentication arithmetic operation section (S20),

an authentication completion determination section (S13) that determines whether the authenticated data stored in the authenticated data memory portion (340) includes the authenticated data corresponding to the authentication relation data included in the authentication request signal, and

an authenticated data comparison-and-authentication section (S14 to S16) that performs, when the authentication completion

determination section (S13) determines that the authenticated data stored in the authenticated data memory portion (340) include the authenticated data corresponding to the authentication relation data included in the authentication request signal, the authentication process for the first navigation message received by the reception terminal (200) based on the authentication relation data and the authenticated data corresponding to the authentication relation data; and

the authentication arithmetic operation section (S20) performs the authentication process when the authentication completion determination section (S13) determines that the authenticated data stored in the authenticated data memory portion (340) does not include the authenticated data corresponding to the authentication relation data included in the authentication request signal.

4. The navigation message authentication system according to claim 3, further comprising:

at least one service center (400, 400a, 400b) that performs communication with the authentication processing apparatus (300) and the reception terminal (200),

wherein:

the service center (400, 400a, 400b) includes

a service-center-side authentication request signal reception processing section (S51) that receives the authentication request signal transmitted from the authentication request signal transmission processing section (S8),

a service-center-side authenticated data memory portion (440) that stores, as the authenticated data, the combination of the authentication relation data and the inspection data, the combination being determined to have succeeded in authentication in the authentication process performed by the authentication arithmetic operation section (S20), and

a service-center-side authenticated data comparison-and-authentication section (S54 to S56) that performs the authentication process for the first navigation message received by the reception terminal (200) based on the authentication relation data included in the authentication request signal and the authenticated data corresponding to the authentication relation data.

5. The navigation message authentication system according to claim 4, wherein:

the service center (400, 400a, 400b) further includes

a service-center-side authentication completion determination section (S53) that determines whether the authenticated data stored in the service-center-side authenticated data memory portion (440) includes the authenticated data corresponding to the authentication relation data included in the authentication request signal, and

a service-center-side authentication request signal transmission processing section (S57) that transmits the authentication request signal to the authentication processing apparatus (300) when the service-center-side authentication completion determination section (S53) determines that the authenticated data stored in the service-center-side authenticated data memory portion (440) does not include the authenticated

data corresponding to the authentication relation data included in the authentication request signal;

the authentication request signal reception processing section (S11) of the authentication processing apparatus (300) receives the authentication request signal transmitted from the service-center-side authentication request signal transmission processing section (S57);

either one of the authentication arithmetic operation section (S20) and the authenticated data comparison-and-authentication section (S14 to S16) of the authentication processing apparatus (300) performs the authentication process based on the authentication relation data and the inspection data each included in the authentication request signal;

the authentication processing apparatus (300) transmits an authentication result data showing a result of the authentication process to the service center (400, 400a, 400b); and

the service center (400, 400a, 400b) further includes an authentication result acquisition section (S58) that acquires the authentication result data transmitted from the authentication processing apparatus (300), and

a service-center-side authenticated data addition processing section (S60) that adds, as the authenticated data, the combination of the authentication relation data and the inspection data to the service-center-side authenticated data memory portion (440) when a result shown by the authentication result data acquired by the authentication result acquisition section (S58) is successful authentication.

6. The navigation message authentication system according to claim 5, wherein:

the service center (400, 400a, 400b) includes an authentication result transmission processing section (S62) that transmits a result of authentication requested by the authentication request signal to the reception terminal (200).

7. The navigation message authentication system according to any one of claims 1 to 6, wherein:

the reception terminal (200) includes

5 a reception portion (211) that receives a result of the authentication process requested by the authentication request signal.

8. The navigation message authentication system according to any one of claims 5 to 7, wherein:

the service center (400, 400a, 400b) includes

10 a service-center-side satellite receiver (430) that receives the first navigation message transmitted from the first satellite (2) and the second navigation message;

the service-center-side authentication request signal transmission processing section (S57) extracts the inspection data from the second
15 navigation message received by the service-center-side satellite receiver, while extracting the authentication relation data from the first navigation message received by the service-center-side satellite receiver, generates the authentication request signal including the inspection data and the authentication relation data, and transmits the authentication request signal
20 to the authentication processing apparatus (300).

9. The navigation message authentication system according to any one of claims 4 to 8, further comprising:

a plurality of the service centers (400, 400a, 400b),

25 wherein:

the reception terminal (200) includes

a transmission destination selection portion (222) that selects a transmission destination of the authentication request signal from among the plurality of service centers (400, 400a, 400b); and

30 the authentication request signal transmission processing section (S8) transmits the authentication request signal to the service center (400, 400a, 400b) selected by the transmission destination selection portion.

10. The navigation message authentication system according to any one of claims 4 to 8, wherein:

the reception terminal (200) includes

a terminal-side transmission portion (212) that determines a position of the reception terminal (200) based on a signal from the first satellite (2) and also transmits position information showing a result of positioning to the service center (400, 400a, 400b); and

the service center (400, 400a, 400b) includes

a service-center-side reception portion (411) that receives the position information transmitted from the reception terminal (200), and implements a service using the position information received by the service-center-side reception portion (411).

11. The navigation message authentication system according to any one of claims 1 to 10, wherein:

the authentication relation data includes information for specifying a transmitter of the first navigation message, which is intrinsic to the transmitter, and transmission time information for specifying a transmission time of the first navigation message.

12. A reception terminal, comprising:

a terminal-side satellite receiver (230) that receives

a first navigation message transmitted from a first satellite (2)

and

a second navigation message transmitted from a second satellite (3) and including inspection data used for an authentication process for the first navigation message;

an inspection data extraction section (S2) that extracts the inspection data from the second navigation message received by the terminal-side satellite receiver (230);

an authentication relation data extraction section (S5) that extracts, from the first navigation message received by the terminal-side satellite

receiver (230), an authentication relation data as a portion required for the authentication process for the first navigation message;

an authentication request signal generation section (S7) that generates an authentication request signal which includes the inspection data extracted by the inspection data extraction section (S2) and the authentication relation data extracted by the authentication relation data extraction section (S5) and requests the authentication process for the first navigation message received by the terminal-side satellite receiver (230) to be performed; and

an authentication request signal transmission processing section (S8) that transmits the authentication request signal generated by the authentication request signal generation section (S7).

13. An authentication processing apparatus, comprising:

an authentication request signal reception processing section (S11) that receives an authentication request signal including an authentication relation data as a portion required for an authentication process for the first navigation message and inspection data used for the authentication process for the first navigation message of a first navigation message transmitted from a first satellite (2); and

an authentication arithmetic operation section (S20) that performs the authentication process for the first navigation message received by a reception terminal (200) based on the inspection data and the authentication relation data each included in the authentication request signal.