

DESCRIPTION

TITLE OF INVENTION: POSITION INFORMATION AUTHENTICATION
SYSTEM, POSITIONING TERMINAL, AND POSITION INFORMATION
ACQUISITION APPARATUS

5 CROSS REFERENCE TO RELATED APPLICATIONS

[0001]

The present application is based on Japanese Patent Application No. 2014-8904 filed on January 21, 2014, the disclosure of which is incorporated herein by reference.

10 TECHNICAL FIELD

[0002]

The present disclosure relates to a position information authentication system capable of authenticating a navigation message received from a navigation satellite in order to calculate position information,
15 and a positioning terminal and a position information acquisition apparatus included in the authentication system.

BACKGROUND ART

[0003]

A widely known positioning terminal receives a satellite electric
20 wave from a navigation satellite included in a navigation satellite system such as a global positioning system (GPS), and uses a navigation message included in the satellite electric wave so as to compute a present position.

[0004]

There is a false satellite electric wave generator that generates and broadcasts a false satellite electric wave. A malicious person may use the false satellite electric wave generator to cause the positioning terminal to compute an incorrect position.

5 [0005]

As disclosed in Patent Literature 1, a proposed position information authentication system is capable of authenticating a navigation message in order to determine reliability of the navigation message that is received from a navigation satellite to compute position information.

10 [0006]

According to the position information authentication system, the positioning terminal can determine whether the navigation message received by the positioning terminal itself corresponds to a navigation message authenticated by an authentication center. The positioning terminal can
15 determine that the navigation message has been transmitted by the navigation satellite when it is determined that the navigation message received by the positioning terminal itself corresponds to the navigation message authenticated by the authentication center.

[0007]

20 Based on the technology according to Patent Literature 1, the positioning terminal receiving navigation messages can reliably compute a present position.

[0008]

The inventors of the present application have found the following.

25 [0009]

The position information computed by the positioning terminal may be used to allow a user carrying the positioning terminal to know the present position or may be used to circumferentially transmit position information indicating the present position computed by the positioning terminal. For
30 example, the position information may be used for automatic charging by transmitting the position information to a charge management apparatus that manages toll parking areas or toll roads. In this case, the positioning terminal may transmit position information representing a position different

from the computed present position to a position information acquisition apparatus that receives the position information and performs a charging process. Correct charging is impossible even when the positioning terminal reliably computes the present position.

5 [0010]

The capability for the positioning terminal to correctly compute positions is insufficient in a system in which the positioning terminal computes a position and the position information acquisition apparatus acquires the computed position and performs a particular process such as
10 charging. The positioning terminal needs to indicate that the positioning terminal itself does not falsify the position information. The position information acquisition apparatus that acquires the position information needs to determine that the positioning terminal is a reliable terminal that does not falsify the position information.

15 PRIOR ART LITERATURES

PATENT LITERATURE

[0011]

Patent Literature 1: JP 2013-130395 A

SUMMARY OF INVENTION

20 [0012]

It is an object of the present disclosure to provide a position information authentication system, a positioning terminal, and a position information acquisition apparatus so that the position information acquisition apparatus acquiring position information from the positioning terminal can
25 determine that the positioning terminal complies with the position information authentication system.

[0013]

A position information authentication system according to one aspect of the present disclosure comprises: a positioning terminal that

receives a navigation message, and when the navigation message that has been received corresponds to a navigation message to be authenticated, wirelessly transmits position information indicating a present position outside, the present position being computed by using the navigation message; an
5 authentication center apparatus that transmits a center-generated authentication data to a communication satellite transmitting the center-generated authentication data used by the positioning terminal for authentication; and a position information acquisition apparatus that receives the position information, which is wirelessly transmitted by the positioning
10 terminal.

[0014]

The authentication center apparatus includes: a center-side satellite reception portion that receives from a navigation satellite included in a navigation satellite system, a satellite electric wave including the navigation
15 message; a center-side authentication data generation portion that generates a cryptography key, and generates the center-generated authentication data based on the cryptography key and the navigation message, which is included in the satellite electric wave received by the center-side satellite reception portion; and an authentication data transmission portion that
20 transmits the center-generated authentication data, which is generated by the center-side authentication data generation portion, to the communication satellite.

[0015]

The positioning terminal includes: a terminal-side satellite reception
25 portion that receives the center-generated authentication data from the communication satellite, and receives the satellite electric wave from the navigation satellite; a key reception portion that receives a key-related data from the authentication center apparatus, the key-related data being one of the cryptography key and a key generation data capable of generating the
30 cryptography key; a terminal-side authentication data generation portion that generates a terminal-generated authentication data based on the key-related data, which is received by the key reception portion, and the navigation message, which is extracted from the satellite electric wave received by the

terminal-side satellite reception portion; an authentication determination portion that compares the center-generated authentication data with the terminal-generated authentication data and, when the center-generated authentication data and the terminal-generated authentication data are
5 matched, determines that the navigation message included in the satellite electric wave received by the terminal-side satellite reception portion is authenticated; an authenticated data generation portion that generates an authenticated data indicating the navigation message included in the satellite electric wave received by the terminal-side satellite reception portion is
10 authenticated, based on the key-related data received by the key reception portion from the authentication center apparatus; and a terminal-side transmission portion that transmits the position information computed based on the navigation message and the authenticated data, which is generated by the authenticated data generation portion.

15 [0016]

The position information acquisition apparatus includes: a terminal data acquisition portion that acquires the position information and the authenticated data transmitted by the terminal-side transmission portion from a communication portion; a key acquisition portion that acquires the
20 key-related data from the authentication center apparatus through the communication portion; a comparative data generation portion that, based on the key-related data acquired by the key acquisition portion, generates an authenticated comparative data to be compared with the authenticated data; and a terminal determination portion that compares the authenticated data,
25 which is acquired by the terminal data acquisition portion, with the authenticated comparative data, which is generated by the comparative data generation portion and, when the authenticated data acquired by the terminal data acquisition portion is matched with the authenticated comparative data generated by the comparative data generation portion, determines that the
30 positioning terminal corresponds to a regular positioning terminal.

[0017]

According to the present disclosure, the positioning terminal authenticates a navigation message included in a satellite electric wave

received from the navigation satellite. For this authentication, the key reception portion receives key-related data from the authentication center apparatus. The key-related data corresponds to a cryptography key or key generation data. The cryptography key is used by the authentication center
5 apparatus to generate center-generated authentication data. The key generation data is capable of generating the cryptography key. When the authentication is successful, the positioning terminal uses the key-related data received from the authentication center apparatus to generate authenticated data indicating completion of the authentication, and transmits
10 the authenticated data along with position information.

[0018]

The positioning terminal generates the authenticated data using the key-related data, which is acquired from the authentication center apparatus, and transmits the key-related data along with the position information.
15 Accordingly, it may be possible to prove that the positioning terminal itself is a regular positioning terminal that is capable of communication with the authentication center apparatus and is trusted by the authentication center apparatus.

[0019]

20 The key-related data generating the authenticated data is acquired from the authentication center apparatus in order to authenticate a navigation message included in a satellite electric wave which is received by the positioning terminal itself. It may be possible to simplify a process generating the authenticated data since another data generating the
25 authenticated data need not be acquired from the authentication center apparatus separately.

[0020]

The position information acquisition apparatus receives the authenticated data along with the position information. The position
30 information acquisition apparatus itself also acquires the key-related data from the authentication center apparatus. The position information acquisition apparatus generates an authenticated comparative data to be compared with the authenticated data based on the key-related data, which

has been acquired. The terminal determination portion compares the authenticated comparative data with the authenticated data acquired by the terminal data acquisition portion, so that it may be possible to determine whether the positioning terminal transmitted the position information is a regular positioning terminal.

[0021]

A positioning terminal according to another aspect of the present disclosure receives a navigation message and, when the navigation message that has been received corresponds to a navigation message to be authenticated, wirelessly transmits position information indicating a present position outside, the present position being computed by using the navigation message. The positioning terminal comprises: a terminal-side satellite reception portion that receives a center-generated authentication data from a communication satellite, the center-generated authentication data being generated by an authentication center apparatus and transmitted to the communication satellite to be used for authentication in the positioning terminal, and receives a satellite electric wave including the navigation message from a navigation satellite included in a navigation satellite system; a key reception portion that receives a key-related data from the authentication center apparatus, the key-related data being one of a cryptography key to generate the center-generated authentication data and a key generation data capable of generating the cryptography key; a terminal-side authentication data generation portion that generates a terminal-generated authentication data based on the key-related data received by the key reception portion and the navigation message extracted from the satellite electric wave received by the terminal-side satellite reception portion; an authentication determination portion that compares the center-generated authentication data with the terminal-generated authentication data and, when the center-generated authentication data is matched with the terminal-generated authentication data, determines the navigation message included in the satellite electric wave received by the terminal-side satellite reception portion is authenticated; an authenticated data generation portion that generates an authenticated data indicating the

navigation message included in the satellite electric wave received by the terminal-side satellite reception portion is authenticated, based on the key-related data received by the key reception portion from the authentication center apparatus; and a terminal-side transmission portion that transmits the position information computed based on the navigation message and the authenticated data generated by the authenticated data generation portion.

[0022]

A position information acquisition apparatus according to another aspect of the present disclosure receives a navigation message and, when the navigation message that has been received corresponds to a navigation message to be authenticated, receives position information and an authenticated data from a positioning terminal that wirelessly transmit the position information and the authenticated data outside, the position information indicating the present position computed using the navigation message, the authenticated data indicating the navigation message that has been received is authenticated. The position information acquisition apparatus comprises: a terminal data acquisition portion that acquires the position information and the authenticated data transmitted by the positioning terminal from a communication portion; a key acquisition portion that allows the communication portion to acquire a key-related data from an authentication center apparatus, wherein the key-related data corresponds to one of a cryptography key and a key generation data, the cryptography key being used by the authentication center apparatus to generate a center-generated authentication data that is used by the positioning terminal for authentication, the key generation data being capable of generating the cryptography key; a comparative data generation portion that generates an authenticated comparative data to be compared with the authenticated data based on the key-related data acquired by the key acquisition portion; and a terminal determination portion that compares the authenticated data acquired by the terminal data acquisition portion with the authenticated comparative data generated by the comparative data generation portion and, when the authenticated data acquired by the terminal data acquisition portion is matched with the authenticated comparative data generated by the

comparative data generation portion, determines that the positioning terminal is a regular positioning terminal.

[0023]

5 According to the position information authentication system, the positioning terminal, and the position information acquisition apparatus of the present disclosure, it may be possible that the position information acquisition apparatus acquiring the position information from the positioning terminal determines that the positioning terminal complies with the position information authentication system.

10 BRIEF DESCRIPTION OF DRAWINGS

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:

15 [0024]

FIG. 1 is a diagram illustrating a configuration of a position information authentication system as a first embodiment;

FIG. 2 is a block diagram illustrating in detail the configuration of an authentication center processor in FIG. 1;

20 FIG. 3 is a block diagram illustrating in detail the configuration of a vehicle onboard apparatus in FIG. 1;

FIG. 4 is a diagram illustrating a relation between a navigation message included in a satellite electric wave and a RAND message;

25 FIG. 5 is a flowchart illustrating a process performed by a control portion of the vehicle onboard apparatus;

FIG. 6 is a flowchart illustrating in detail a navigation message authentication process of S4 in FIG. 5;

FIG. 7 is a flowchart illustrating a process performed by a control portion of the roadside apparatus;

30 FIG. 8 is a diagram illustrating a configuration of a roadside apparatus of a second embodiment;

FIG. 9 is a flowchart illustrating a preparatory process performed by a control portion included in the roadside apparatus; and

FIG. 10 is a flowchart illustrating a process performed by the control portion of the roadside apparatus when receiving position information from the vehicle onboard apparatus.

PREFERRED EMBODIMENTS FOR CARRYING OUT INVENTION

[0025]

(First embodiment)

Embodiments of the present disclosure will be described with reference to the drawings. As illustrated in FIG. 1, a position information authentication system 1 of a first embodiment includes an authentication center apparatus 100, a vehicle onboard apparatus 200 that corresponds to a positioning terminal of the present disclosure, and a roadside apparatus 300 that corresponds to a position information acquisition apparatus of the present disclosure.

[0026]

(Outline configuration of the position information authentication system 1)

The authentication center apparatus 100 includes a monitor station apparatus 110, an authentication center processor 120, and a master control station apparatus 130. The description below omits the terms apparatus and processor, and simply expresses the monitor station apparatus 110 as the monitor station, the authentication center processor 120 as the authentication center 120, and the master control station apparatus 130 as the master control station 130.

[0027]

The monitor station 110 corresponds to a center-side satellite reception portion of the present disclosure. The monitor station 110 receives a GPS electric wave transmitted by a GPS satellite 2 included in a GPS, which is one of navigation satellite systems. The GPS satellite 2 corresponds to a navigation satellite of the present disclosure. The GPS

electric wave corresponds to a satellite electric wave of the present disclosure. As is well known, the GPS electric wave includes a navigation message. The monitor station 110 demodulates the received GPS electric wave to extract the navigation message, and transmits the navigation
5 message to the authentication center 120. When receiving GPS electric waves from multiple GPS satellites 2, the monitor station 110 extracts navigation messages from the corresponding GPS electric waves, and transmits the navigation messages to the authentication center 120.

[0028]

10 The authentication center 120 generates a parity data from a navigation message and an H matrix that is a cryptography key. The parity data corresponds to a center-generated authentication data of the present disclosure. The authentication center 120 sends a signal including the generated parity data to the master control station 130. The authentication
15 center 120 communicates with the vehicle onboard apparatus 200 and the roadside apparatus 300. The authentication center 120 will be described in detail with reference to FIG. 2.

[0029]

20 The master control station 130 corresponds to an authentication data transmission portion of the present disclosure. The master control station 130 receives the parity data from the authentication center 120, and transmits the parity data to a quasi-zenith satellite (hereinafter, referred to as a QZS satellite) 3.

[0030]

25 The QZS satellite 3 corresponds to a communication satellite of the present disclosure. The QZS satellite 3 broadcasts a navigation message including the parity data to the earth.

[0031]

30 The vehicle onboard apparatus 200 is provided by a vehicle onboard apparatus of a navigation message authentication type. The vehicle onboard apparatus 200 determines whether the navigation message received from the GPS satellite 2 can be authenticated by using the parity data included in the navigation message received from the QZS satellite 3.

During the authentication, the vehicle onboard apparatus 200 communicates with the authentication center 120. The vehicle onboard apparatus 200 computes a present position using the navigation message received from the GPS satellite 2. The vehicle onboard apparatus 200 wirelessly transmits position information indicating the computed present position along with a hash value, which is described later. The hash value indicates that the navigation message has been authenticated. The hash value corresponds to an authenticated data of the present disclosure. The vehicle onboard apparatus 200 will be described with reference to FIG. 3, FIG. 5, and FIG. 6.

10 [0032]

The roadside apparatus 300 is managed by a service provider that provides a specified service using the position information transmitted from the vehicle onboard apparatus 200. For example, the service includes charging a user of a vehicle mounted with the vehicle onboard apparatus 200 when the vehicle parks at a toll parking area or travels a toll road.

15 [0033]

The roadside apparatus 300 includes a communication portion 310 and a control portion 320. The communication portion 310 wirelessly communicates with a communication portion 126 (referring to FIG. 2) included in the authentication center 120 or a communication portion 210 (referring to FIG. 3) included in the vehicle onboard apparatus 200.

20 [0034]

The control portion 320 is provided as a computer including a CPU, ROM, RAM, or the like. The CPU controls the communication portion 310 by performing a program stored in the ROM while using a temporary storage function of the RAM. The control portion 320 acquires the hash value transmitted from the vehicle onboard apparatus 200 via the communication portion 310, and determines whether the vehicle onboard apparatus 200 corresponds to a regular vehicle onboard apparatus, based on the hash value. During the determination, the control portion 320 communicates with the authentication center 120.

25 [0035]

(Detailed configuration of the authentication center 120)

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

[0036]

5 The control portion 122 is provided as a computer including a CPU, ROM, RAM, or the like, and controls the data storage portion 124 and the communication portion 126. The CPU performs a program stored in the ROM while using a temporary storage function of the RAM to provide functions as a RAND message generation portion 1221, a SEED value
10 generation portion 1222, an H matrix computation portion 1223, a parity computation portion 1224, and a signal processing portion 1225. Functions of the portions 1221 through 1225 may be the same functions disclosed in Patent Literature 1. In addition, the control portion 122 also includes an H matrix selection portion 1226. The control portion 122 corresponds to a
15 center-side authentication data generation portion of the present disclosure.

[0037]

RAND in the RAND message generation portion 1221 signifies Reference Authentication Navigation Data that is generated from a navigation message acquired from the monitor station 110.

20 [0038]

FIG. 4 illustrates relation between the RAND message and the navigation message. As is well known, the navigation message is divided into sub-frames 1 through 5. Each of the sub-frames 4, 5 includes 1 to 25 pages. Each sub-frame is divided into words 1 through 10.

25 [0039]

The RAND message sequentially includes elapsed time TOW (time of week, corresponding to time information of the present disclosure) included in word 2 of the sub-frame 1, TOC included in words 8 through 10, and AF0 and AF1. The RAND message is further followed by AS Flag as an
30 anti-spoof flag and PRN (Pseudo Random Noise) ID as a satellite number. In FIG. 4, each data included in the RAND message is followed by a numeric value in parentheses. The numeric value signifies the number of bits in each data.

[0040]

TOW varies every six seconds. The RAND message including TOW and PRNID can indicate when the GPS electric wave is transmitted from which GPS satellite. The RAND message is generated every six
5 seconds correspondingly to the GPS satellite 2 from which the monitor station 110 receives the GPS electric wave since TOW varies every six seconds and PRNID is included.

[0041]

The SEED value generation portion 1222 generates a unique SEED
10 value using a PC clock as input. The SEED value generation portion 1222 generates a SEED value by generating a random number using a PC clock as input, for example. The SEED value in the present embodiment is equal to 36 bits.

[0042]

15 The H matrix computation portion 1223 uses the SEED value generated by the SEED value generation portion 1222 to compute an H matrix that maintains one-to-one correspondence to the SEED value. The H matrix corresponds to a cryptography key of the present disclosure. The SEED value corresponds to a key generation data of the present disclosure
20 since settling the SEED value can generate the H matrix. A known hash function may be used as the H matrix. A parity check matrix to encode LDPC (Low Density Parity Check) may be used, for example. Further, a generator matrix that is determined from the parity check matrix may be used.

[0043]

25 The H matrix corresponds to an example of the cryptography key of the present disclosure. The H matrix or the SEED value corresponds to an example of a key-related data of the present disclosure.

[0044]

The parity computation portion 1224 computes the parity data based
30 on the RAND message generated by the RAND message generation portion 1221 and the H matrix computed by the H matrix computation portion 1223. Namely, the H matrix is multiplied by the RAND message to compute the parity data.

[0045]

The signal processing portion 1225 inserts the parity data, which is computed by the parity computation portion 1224, and the RAND message, which is used for the computation, into a navigation message that is
5 transmitted to the QZS satellite 3. The signal processing portion 1225 sends the navigation message after the insertion to the master control station 130.

[0046]

In addition to the insertion of the signal, the signal processing
10 portion 1225 stores the parity data computed by the parity computation portion 1224, the RAND message, the H matrix used for the parity data computation, and the SEED value used for the H matrix computation in the data storage portion 124.

[0047]

The signal processing portion 1225 inserts the RAND message and
15 the parity data into a navigation message to be transmitted to the QZS satellite 3 each time the RAND message generation portion 1221 generates a RAND message. Thus, the SEED value generation portion 1222, the H matrix computation portion 1223, and the parity computation portion 1224
20 also perform processes each time the RAND message generation portion 1221 generates a RAND message.

[0048]

When the communication portion 126 receives PRNID, TOW, and a public key transmitted from the vehicle onboard apparatus 200, the H matrix
25 selection portion 1226 selects an H matrix corresponding to the received PRNID and TOW from H matrix stored in the data storage portion 124. The H matrix selection portion 1226 encrypts the selected H matrix using the public key, and transmits the encrypted H matrix to the vehicle onboard apparatus 200 that transmitted the PRNID, or the like.

30 [0049]

When the communication portion 126 receives PRNID, TOW, and a public key transmitted from the roadside apparatus 300, the H matrix selection portion 1226 selects an H matrix and parity data corresponding to

the received PRNID and TOW from H matrix and parity data stored in the data storage portion 124. The H matrix selection portion 1226 encrypts the selected H matrix and parity data using the public key, and transmits the encrypted H matrix and parity data to the roadside apparatus 300 that
5 transmitted PRNID, or the like.

[0050]

The communication portion 126 communicates with the communication portion 210 included in the vehicle onboard apparatus 200 and the communication portion 310 included in the roadside apparatus 300.

10 [0051]

The master control station 130 transmits the navigation message generated by the signal processing portion 1225 to the QZS satellite 3.

[0052]

The QZS satellite 3 broadcasts the navigation message received
15 from the master control station 130 to the earth.

[0053]

(Configuration of the vehicle onboard apparatus 200)

A satellite reception portion 230 of the vehicle onboard apparatus 200 receives the navigation message broadcasted from the QZS satellite 3.

20 The vehicle onboard apparatus 200 includes the communication portion 210 and a control portion 220 in addition to the satellite reception portion 230.

[0054]

The communication portion 210 includes a reception portion 211 and a transmission portion 212. The reception portion 211 corresponds to a
25 key reception portion of the present disclosure. The transmission portion 212 corresponds to a terminal-side transmission portion of the present disclosure. The communication portion 210 includes a broad communication function and a narrow communication function. The narrow communication function ensures a communication distance of several
30 hundreds of meters, for example. The broad communication function ensures a communication distance of several kilometers, for example. The broad communication function communicates with a base station of a public communication channel network to enable communication with other

communication apparatus within the communication range of the public communication channel network. The communication portion 210 uses the narrow communication function to communicate with the communication portion 310 of the roadside apparatus 300. The communication portion 210
5 uses the broadband communication function to communicate with the communication portion 126 of the authentication center 120.

[0055]

The satellite reception portion 230 corresponds to a terminal-side satellite reception portion of the present disclosure. The satellite reception
10 portion 230 receives electric wave transmitted from the GPS satellite 2 and the QZS satellite 3 at a constant cycle.

[0056]

The control portion 220 is provided as a computer including a CPU, ROM, RAM, or the like, and controls the communication portion 210 and the
15 satellite reception portion 230. The CPU performs a program stored in the ROM while using a temporary storage function of the RAM to perform a process as illustrated in FIG. 5.

[0057]

The control portion 220 performs the process illustrated in FIG. 5
20 each time the satellite reception portion 230 receives GPS electric waves from four or more GPS satellites 2. Four or more GPS satellites 2 are used since computation of the present position requires receiving GPS electric waves from four or more GPS satellites 2.

[0058]

25 At S2, the control portion 220 computes the present position based on a GPS electric wave. At S4, the control portion 220 performs a navigation message authentication process. The process is illustrated in FIG. 6 in detail.

[0059]

30 At S42, the control portion 220 acquires from the reception portion 211, a navigation message received from the QZS satellite 3.

[0060]

At S44, the control portion 220 extracts PRNID, TOW, and parity data from the navigation message acquired at S42. PRNID, TOW, and parity data to be extracted correspond to the navigation message used to compute the present position. PRNID and TOW may be extracted from the navigation message used to compute the present position.

[0061]

At S46, the control portion 220 transmits PRNID and TOW extracted at S44 along with a public key to the authentication center 120 from the transmission portion 212. As described above, the authentication center 120 encrypts an H matrix determined by PRNID and TOW using the public key, and transmits the H matrix to the vehicle onboard apparatus 200.

[0062]

At S48, the control portion 220 receives the encrypted H matrix from the reception portion 211. The H matrix is transmitted from the authentication center 120. At S50, the control portion 220 uses a private key (also referred to as a secret key) to decrypt the encrypted H matrix acquired at S48.

[0063]

At S52, the control portion 220 generates a RAND message from the GPS electric wave whose navigation message includes the same PRNID as that transmitted at S46.

[0064]

At S54, the control portion 220 generates comparative parity data from the RAND message generated at S52 and the H matrix decrypted at S50. The generated comparative parity data corresponds to terminal-generated authentication data of the present disclosure. The process at S54 corresponds to a terminal-side authentication data generation portion of the present disclosure.

[0065]

The control portion 220 then performs S56 to S60 that correspond to an authentication determination portion of the present disclosure. At S56, the control portion 220 determines whether the comparative parity data generated at S54 matches the parity data extracted at S44.

[0066]

The H matrix decrypted at S50 is identical with the H matrix which the authentication center 120 has used to generate the parity data. The parity computation portion 1224 of the authentication center 120 computes
5 parity data based on the H matrix and the RAND message.

[0067]

When the comparative parity data generated at S54 matches the parity data extracted at S44, the RAND message generated at S52 can be assumed to be the same as the RAND message generated by the
10 authentication center 120. When the comparative parity data generated at S54 matches the parity data extracted at S44, the control portion 220 proceeds to S58, and determines that the authentication is successful. When the two pieces of parity data do not match, the control portion 220 proceeds to S60, and determines that the authentication is unsuccessful.

15 [0068]

Return to the description of FIG. 5. After performing the process at S4, the control portion 220 performs the process at S6 through S10 that correspond to an authenticated data generation portion of the present disclosure. At S6, the control portion 220 determines whether the result of
20 the navigation message authentication process represents the authentication success.

[0069]

When the determination corresponds to No, namely, the authentication is unsuccessful, the control portion 220 terminates the process
25 of FIG. 4. When the determination at S6 corresponds to Yes, the control portion 220 proceeds to S8.

[0070]

At S8, the control portion 220 determines whether position information needs to be transmitted. A case where the position information
30 needs to be transmitted corresponds to a case where a signal to request the position information is received from the communication portion 310 of the roadside apparatus 300, for example. The position information may be transmitted at a specified transmission cycle. When the determination at S8

results in No, the control portion 220 terminates the process in FIG. 4. When the determination at S8 also results in Yes, the control portion 220 proceeds to S10.

[0071]

5 At S10, the control portion 220 generates a hash value from the hash function using the H matrix as data generated by the authentication center 120 and the parity data, as input keys. The hash value corresponds to authenticated data of the present disclosure.

[0072]

10 At S12, the control portion 220 transmits the position information indicating the present position computed at S2, the hash value generated at S10, and PRNID and TOW extracted at S44 to the communication portion 310 of the roadside apparatus 300 from the transmission portion 212.

[0073]

15 (Processes in the roadside apparatus 300)

 The control portion 320 of the roadside apparatus 300 cyclically transmits a request signal that requests to transmit position information around the roadside apparatus 300. When the vehicle onboard apparatus 200 receives the request signal, the vehicle onboard apparatus 200 transmits
20 the position information, the hash value, or the like as described above.

[0074]

 The control portion 320 of the roadside apparatus 300 performs a process illustrated in FIG. 7 when the communication portion 310 of the roadside apparatus 300 receives the position information, the hash value, or
25 the like from the vehicle onboard apparatus 200.

[0075]

 At S70, the control portion 320 acquires the position information, the hash value, PRNID, and TOW received by the communication portion 310 from the communication portion 310. The process at S70 corresponds to a
30 terminal data acquisition portion of the present disclosure.

[0076]

 At S72, the control portion 320 transmits PRNID and TOW acquired at S70 along with a public key to the authentication center 120 from the

communication portion 310. The roadside apparatus 300 uniquely stores this public key. The public key differs from a public key the vehicle onboard apparatus 200 transmits to the authentication center 120.

[0077]

5 As described above, the authentication center 120 uses the public key to encrypt the H matrix and the parity data determined by the PRNID and TOW, and transmits the H matrix and the parity data to the roadside apparatus 300. The H matrix and the parity data correspond to input keys to generate a hash value.

10 [0078]

At S74, the control portion 320 acquires the encrypted H matrix and parity data from the communication portion 310 when the H matrix and the parity data are transmitted from the authentication center 120. The process at S74 corresponds to a key acquisition portion of the present disclosure.

15 [0079]

At S76, the control portion 320 uses the private key to decrypt the encrypted H matrix and parity data that are acquired at S74.

[0080]

20 At S78, the control portion 320 uses the H matrix and the parity data decrypted at S76 as input keys to generate a comparative hash value from the hash function that is stored in advance as being used by the regular vehicle onboard apparatus 200. The comparative hash value corresponds to authenticated comparative data of the present disclosure. The process at S78 corresponds to a comparative data generation portion of the present disclosure.

25 [0081]

The control portion 320 then performs S80 through S84 that correspond to a terminal determination portion of the present disclosure. At S80, the control portion 320 determines whether the comparative hash value generated at S78 matches the hash value acquired at S70.

30 [0082]

When the two hash values match each other, it may be considered that the hash value transmitted by the vehicle onboard apparatus 200 uses

the H matrix generated by the authentication center 120 as an input key. When the two hash values match, the control portion 320 proceeds to S82 and assumes that the vehicle onboard apparatus 200 having transmitted the position information, the hash value, or the like to be an approved vehicle
5 onboard apparatus. When the two hash values do not match, the control portion 320 proceeds to S84 and assumes that the vehicle onboard apparatus 200 having transmitted the position information and the hash value to be an invalid vehicle onboard apparatus.

[0083]

10 According to the first embodiment, the vehicle onboard apparatus 200 authenticates the navigation message included in the satellite electric wave received from the GPS satellite 2 (S4). For the authentication, the H matrix that the authentication center 120 has used for generation of the parity data is received from the authentication center 120 (S48). When the
15 authentication is successful, the control portion 220 uses the H matrix acquired from the authentication center 120 to generate a hash value to indicate that the authentication is completed (S10). The control portion 220 transmits the hash value along with the position information (S12).

[0084]

20 The vehicle onboard apparatus 200 transmits the hash value along with the position information, the hash value indicating that the authentication is successful and being generated using the H matrix acquired from the authentication center 120. Accordingly, it may be possible to prove that the vehicle onboard apparatus 200 itself corresponds to a regular vehicle
25 onboard apparatus that is capable of communication with the authentication center 120 and is trusted by the authentication center 120.

[0085]

The H matrix to generate the hash value is acquired from the authentication center 120 in order to authenticate the navigation message
30 included in the satellite electric wave received by the vehicle onboard apparatus 200 itself. Thus, it is unnecessary to acquire additional data to generate a hash value from the authentication center 120, so that it may be possible to simplify the process generating the hash value.

[0086]

The control portion 220 transmits the hash value generated from the H matrix using the hash function without transmitting the H matrix itself. The hash function is an irreversible one-way function, so that it may be possible to prevent the H matrix from being known to a third party.

[0087]

The roadside apparatus 300 receives the hash value along with the position information. The roadside apparatus 300 itself also acquires the H matrix from the authentication center 120 and the parity data (S74). The control portion 320 generates comparative hash value from the H matrix, the parity data, and the hash function that is stored in advance as being used by the regular vehicle onboard apparatus 200 (S78). Comparison between the comparative hash value and the hash value acquired from the vehicle onboard apparatus 200 enables to determine whether the vehicle onboard apparatus 200 to have transmitted the position information is a regular vehicle onboard apparatus.

[0088]

(Second embodiment)

A second embodiment will be described. An element marked with the same reference numeral as that used hitherto may be included in the description of the second embodiment or later and, in such a case, equals the element marked with the same reference numeral described in the preceding embodiment, unless otherwise specified. When only part of a configuration is described, the other parts of the configuration may conform to the embodiment that is already described.

[0089]

As illustrated in FIG. 8, a roadside apparatus 300A according to the second embodiment includes a satellite reception portion 330. The satellite reception portion 330 corresponds to an acquirer-side satellite reception portion of the present disclosure. In the second embodiment, a control portion 320A according to the second embodiment performs a process that partially differs from the process performed by the control portion 320 of the first embodiment. The process of the control portion 320A will be described

with reference to FIG. 9 and FIG. 10. The control portion 320A performs the process in FIG. 9 at a specified cycle to acquire GPS electric waves, and also performs the process in FIG. 10 at a specified cycle.

[0090]

5 FIG. 9 illustrates a preparatory process that is performed before acquiring position information from the vehicle onboard apparatus 200. FIG. 9 will be described. At S90, the control portion 320A acquires a navigation message from the satellite reception portion 330. The navigation message is included in a GPS electric wave received by the satellite reception portion
10 330. The control portion 320A acquires navigation messages in all GPS electric waves received by the satellite reception portion 330 when the satellite reception portion 330 receives GPS electric waves from the several GPS satellites 2.

[0091]

15 At S92, the control portion 320A extracts PRNID and TOW from all the navigation messages acquired at S90. The process at S92 corresponds to an electric wave information extraction portion of the present disclosure.

[0092]

 At S94, the control portion 320A transmits PRNID and TOW
20 extracted at S92 along with a public key to the authentication center 120 from the communication portion 310. The process at S94 corresponds to an electric wave information transmission portion of the present disclosure. The authentication center 120 encrypts the H matrix and the parity data determined by PRNID and TOW with a public key, and transmits the H matrix
25 and the parity data to the roadside apparatus 300.

[0093]

 At S96, the control portion 320A acquires the encrypted H matrix and the encrypted parity data from the communication portion 310. The H matrix and the parity data are transmitted from the authentication center 120.

30 [0094]

 At S98, the control portion 320A decrypts the encrypted H matrix and parity data acquired at S96 with a private key. The process at S96 corresponds to a key acquisition portion of the present disclosure.

[0095]

At S100, the control portion 320A uses the H matrix and the parity data decrypted at S98 as input keys to generate a comparative hash value from the hash function that is stored in advance as being used by the approved vehicle onboard apparatus 200. The comparative hash value is generated for all GPS electric waves received by the satellite reception portion 330.

[0096]

At S102, the control portion 320A generates a comparative hash value table. The comparative hash value table represents the correspondence relation between the comparative hash value generated at S100, and PRNID and TOW transmitted to the authentication center 120 in order to acquire the H matrix and the parity data used to generate the comparative hash value.

[0097]

FIG. 10 will be described. At S110, the control portion 320A determines whether the communication portion 310 receives data such as the position information transmitted by the vehicle onboard apparatus 200 by performing the process at S12 in FIG. 5. When the determination results in No, the control portion 320A terminates the process in FIG. 10. When the determination results in Yes, the control portion 320A proceeds to S112.

[0098]

At S112, the control portion 320A acquires the position information, the hash value, PRNID, and TOW that the communication portion 310 has received from the vehicle onboard apparatus 200.

[0099]

The control portion 320A then performs S114 through S120. The process at S114 through S120 corresponds to a terminal determination portion of the present disclosure. Suppose that PRNID and TOW acquired at S112 are included in the comparative hash value table generated by the preparatory process in FIG. 9. At S114, the control portion 320A determines that comparative hash values corresponding to PRNID and TOW are used for the comparison at this time. The preparatory process in FIG. 9 generates

comparative hash values for all GPS electric waves received by the satellite reception portion 230. Therefore, the comparative hash value table is highly likely to include hash values corresponding to PRNID and TOW acquired at S112. Depending on the position or the size of an electric wave shielding object around the roadside apparatus 300, the satellite reception portion 330 of the roadside apparatus 300 may not be able to receive a satellite electric wave received by the satellite reception portion 230 of the vehicle onboard apparatus 200. In this case, the comparative hash value table does not include hash values corresponding to PRNID and TOW acquired at S112.

5 The control portion 320A performs the process at S72 through S78 in FIG. 7 to generate a comparative hash value when the comparative hash value table does not include hash values corresponding to PRNID and TOW acquired at S112.

[0100]

15 At S116, the control portion 320A determines whether the hash value acquired at S112 matches the comparative hash value determined at S114.

[0101]

When the two hash values match, the control portion 320A proceeds to S118 and assumes that the vehicle onboard apparatus 200 having transmitted the position information and the hash value is a regular vehicle onboard apparatus. When the two hash values do not match, the control portion 320A proceeds to S120 and assumes that the vehicle onboard apparatus 200 having transmitted the position information and the hash value is an invalid vehicle onboard apparatus.

20

25

[0102]

According to the second embodiment described above, the roadside apparatus 300 includes the satellite reception portion 230. The roadside apparatus 300 can receive a satellite electric wave from the GPS satellite 2 equal to the vehicle onboard apparatus 200 that is likely to exist around the roadside apparatus 300 and transmit the hash value to the roadside apparatus 300.

30

[0103]

According to the first embodiment, the authentication center apparatus 100 receives PRNID and TOW from the vehicle onboard apparatus 200, transmits the received PRNID and TOW to the authentication center 120, and acquires the H matrix and the parity data. According to the
5 second embodiment, the authentication center apparatus 100 can receive satellite electric waves from the GPS satellite 2 identical with the vehicle onboard apparatus 200. The authentication center apparatus 100 extracts PRNID and TOW from the navigation message received by the satellite
10 reception portion 330 without waiting for the reception of PRNID and TOW from the vehicle onboard apparatus 200. The authentication center apparatus 100 transmits the extracted PRNID and TOW to the authentication center 120, acquires the H matrix and the parity data, and generates the comparative hash value table (FIG. 9).

[0104]

15 Accordingly, after receiving the position information or the like from the vehicle onboard apparatus 200 (S110: Yes), the authentication center apparatus 100 references the comparative hash value table, which has been generated in advance, and determines a comparative hash value
20 corresponding to PRNID and TOW received from the vehicle onboard apparatus 200 (S112, S114). It may be possible for the authentication center apparatus 100 to fast determine whether the vehicle onboard apparatus 200 is approved since the authentication center apparatus 100 is highly likely to omit the process at S72 through S78 in the first embodiment after receiving PRNID and TOW from the vehicle onboard apparatus 200.

25 [0105]

Specifically, suppose that the roadside apparatus 300 authenticates the vehicle onboard apparatus 200 as being a regular vehicle onboard apparatus, and a process based on the authentication result is then
30 performed while the vehicle onboard apparatus 200 is traveling. In such a case, the authentication center apparatus 100 highly requires fast determining whether the vehicle onboard apparatus 200 corresponds to be a regular vehicle onboard apparatus. The process based on the authentication result includes notifying the vehicle onboard apparatus 200

that the vehicle onboard apparatus 200 is a regular vehicle onboard apparatus, or opening or closing a gate provided for a vehicle traveling route based on that the vehicle onboard apparatus 200 is authenticated as being approved, for example. The second embodiment may be especially useful
5 when the authentication center apparatus 100 requires fast determining whether the vehicle onboard apparatus is approved.

[0106]

While there have been described the embodiments of the present disclosure, the disclosure is not limited to the above-mentioned embodiments.
10 Modifications described below are also included in the technical scope of the disclosure. Furthermore, the disclosure may be embodied in various modifications other than those described below without departing from the spirit and scope of the invention.

[0107]

15 (First modification and second modification)

According to the above mentioned embodiments, for example, the control portion generates the hash value and the comparative hash value using the H matrix and the parity data as input keys for the hash function (the authenticated data generation portion: S10, and the comparative data
20 generation portion: S100). However, the disclosure is not limited thereto. The control portion may generate a hash value and a comparative hash value using only the H matrix as an input key for the hash function (a first modification). Alternatively, the control portion may generate a hash value and a comparative hash value using a SEED value corresponding to key
25 generation data as an input key for the hash function instead of the H matrix as a cryptography key (a second modification).

[0108]

(Third modification)

An H matrix can be generated from a SEED value. The
30 authenticated data generation portion or the comparative data generation portion may not use the SEED value as an input key even when the SEED value is acquired as a key related data. Instead, the authenticated data generation portion or the comparative data generation portion may generate

an H matrix from the SEED value and generate a hash value using the H matrix as an input key.

[0109]

(Fourth modification)

5 The authenticated data generation portion or the comparative data generation portion may not use a hash value for authenticated data or authenticated comparative data, but may use an H matrix or a SEED value used to generate the hash value for authenticated data or authenticated comparative data.

10 [0110]

(Fifth modification)

 According to the second embodiment, the control portion generates comparative hash values for all GPS electric waves received by the satellite reception portion 330. The control portion may generate comparative hash values for a part of GPS electric waves received by the satellite reception portion 330. For example, the control portion may generate comparative hash values for only GPS electric waves received from a predetermined number of GPS satellites 2 capable of successful reception.

15

[0111]

20 (Sixth modification)

 The above mentioned embodiments have described the roadside apparatus 300, 300A as a position information acquisition apparatus. However, the disclosure is not limited thereto. The position information acquisition apparatus may be provided as a mobile apparatus that is mounted on a vehicle to crack down on the invalid use of a toll parking or a toll road.

25

[0112]

(Seventh modification)

 The above mentioned embodiments have described the vehicle onboard apparatus 200 as a positioning terminal. However, the disclosure is not limited thereto. The positioning terminal may be provided as a portable terminal carried by a user or as a terminal mounted on a mobile object other than a vehicle.

30

[0113]

A flowchart or a process corresponding to the flowchart described in the present application includes several steps (or referred to as sections). Each step is represented as S2, for example. Each step may be divided into
5 sub-steps. Several steps may be combined into one step.

[0114]

In the embodiments, the inside of the control portion 122 is classified into portions from the viewpoint of the functions of the control portion 122 for descriptive purposes. This does not signify that the inside of
10 the control portion 122 is physically divided into parts corresponding to the respective portions. Therefore, each "portion" may be embodied as software such as part of a computer program or may be embodied as hardware such as an IC chip or a large-scale integrated circuit.

[0115]

15 While the embodiments, the configurations, and the modes according to the present disclosure have been described with reference to embodiments thereof, it is to be understood that the disclosure is not limited to the embodiments and constructions. The present disclosure is intended to cover various modification and equivalent arrangements. In addition,
20 while the various combinations and configurations, other combinations and configurations, including more, less or only a single element, are also within the spirit and scope of the present disclosure.

CLAIMS

1. A position information authentication system comprising:
 - a positioning terminal that receives a navigation message, and
when the navigation message that has been received corresponds to a
5 navigation message to be authenticated, wirelessly transmits position
information indicating a present position outside, the present position being
computed by using the navigation message;
 - an authentication center apparatus that transmits a center-
generated authentication data to a communication satellite transmitting the
10 center-generated authentication data used by the positioning terminal for
authentication; and
 - a position information acquisition apparatus that receives the
position information, which is wirelessly transmitted by the positioning
terminal ,
 - 15 wherein
 - the authentication center apparatus includes:
 - a center-side satellite reception portion that receives from a
navigation satellite included in a navigation satellite system, a satellite
electric wave including the navigation message;
 - 20 a center-side authentication data generation portion that
generates a cryptography key, and generates the center-generated
authentication data based on the cryptography key and the navigation
message, which is included in the satellite electric wave received by the
center-side satellite reception portion; and
 - 25 an authentication data transmission portion that transmits the
center-generated authentication data, which is generated by the center-side
authentication data generation portion, to the communication satellite,
 - the positioning terminal includes:
 - a terminal-side satellite reception portion that receives the
30 center-generated authentication data from the communication satellite, and
receives the satellite electric wave from the navigation satellite;

a key reception portion that receives a key-related data from the authentication center apparatus, the key-related data being one of the cryptography key and a key generation data capable of generating the cryptography key;

5 a terminal-side authentication data generation portion that generates a terminal-generated authentication data based on the key-related data, which is received by the key reception portion, and the navigation message, which is extracted from the satellite electric wave received by the terminal-side satellite reception portion ;

10 an authentication determination portion that compares the center-generated authentication data with the terminal-generated authentication data and, when the center-generated authentication data and the terminal-generated authentication data are matched, determines that the navigation message included in the satellite electric wave received by the
15 terminal-side satellite reception portion is authenticated;

an authenticated data generation portion that generates an authenticated data indicating the navigation message included in the satellite electric wave received by the terminal-side satellite reception portion is authenticated, based on the key-related data received by the key reception
20 portion from the authentication center apparatus; and

a terminal-side transmission portion that transmits the position information computed based on the navigation message and the authenticated data, which is generated by the authenticated data generation portion, and

25 the position information acquisition apparatus includes:

a terminal data acquisition portion that acquires the position information and the authenticated data transmitted by the terminal-side transmission portion from a communication portion;

a key acquisition portion that acquires the key-related data
30 from the authentication center apparatus through the communication portion;

a comparative data generation portion that, based on the key-related data acquired by the key acquisition portion , generates an authenticated comparative data to be compared with the authenticated data; and

5 a terminal determination portion that compares the authenticated data, which is acquired by the terminal data acquisition portion, with the authenticated comparative data, which is generated by the comparative data generation portion and, when the authenticated data acquired by the terminal data acquisition portion is matched with the
10 authenticated comparative data generated by the comparative data generation portion, determines that the positioning terminal corresponds to a regular positioning terminal.

2. The position information authentication system according to
15 claim 1, wherein:

the authenticated data generation portion generates the authenticated data by a hash function using the key-related data received by the key reception portion .

20 3. The position information authentication system according to claim 2, wherein:

the authenticated data generation portion generates the authenticated data by the hash function using the terminal-generated authentication data along with the key-related data received by the key
25 reception portion .

4. The position information authentication system according to any one of claims 1-3, wherein:

the position information acquisition apparatus includes
30 an acquirer-side satellite reception portion that receives the satellite electric wave from the navigation satellite,

an electric wave information extraction portion that extracts a satellite number and time information from the satellite electric wave received by the acquirer-side satellite reception portion, and

an electric wave information transmission portion that allows
5 the communication portion to periodically transmit the satellite number and the time information extracted by the electric wave information extraction portion to the authentication center apparatus;

the key acquisition portion acquires the key-related data transmitted from the authentication center apparatus based on transmission of the
10 satellite number and the time information from the communication portion to the authentication center apparatus from the communication portion;

the comparative data generation portion generates the authenticated comparative data, and determines in advance a correspondence relation among the authenticated comparative data, the
15 satellite number, and the time information before receiving the authenticated data; and

when the authenticated comparative data determined by the correspondence relation, the satellite number, and the time information acquired by the terminal data acquisition portion exists, the terminal
20 determination portion compares the authenticated comparative data with the authenticated data acquired by the terminal data acquisition portion.

5. A positioning terminal that receives a navigation message and, when the navigation message that has been received corresponds to a
25 navigation message to be authenticated, wirelessly transmits position information indicating a present position outside, the present position being computed by using the navigation message, the positioning terminal comprising:

a terminal-side satellite reception portion that receives a center-
30 generated authentication data from a communication satellite, the

center-generated authentication data being generated by an authentication center apparatus and transmitted to the communication satellite to

5

10

15

20

25

30

be used for authentication in the positioning terminal, and receives a satellite electric wave including the navigation message from a navigation satellite included in a navigation satellite system;

5 a key reception portion that receives a key-related data from the authentication center apparatus, the key-related data being one of a cryptography key to generate the center-generated authentication data and a key generation data capable of generating the cryptography key;

10 a terminal-side authentication data generation portion that generates a terminal-generated authentication data based on the key-related data received by the key reception portion and the navigation message extracted from the satellite electric wave received by the terminal-side satellite reception portion ;

15 an authentication determination portion that compares the center-generated authentication data with the terminal-generated authentication data and, when the center-generated authentication data is matched with the terminal-generated authentication data, determines the navigation message included in the satellite electric wave received by the terminal-side satellite reception portion is authenticated;

20 an authenticated data generation portion that generates an authenticated data indicating the navigation message included in the satellite electric wave received by the terminal-side satellite reception portion is authenticated, based on the key-related data received by the key reception portion from the authentication center apparatus; and

25 a terminal-side transmission portion that transmits the position information computed based on the navigation message and the authenticated data generated by the authenticated data generation portion.

30 6. A position information acquisition apparatus that receives a navigation message and, when the navigation message that has been received corresponds to a navigation message to be authenticated,

receives position information and an authenticated data from a positioning terminal that wirelessly transmits the position information and the authenticated data outside, the position information indicating the present position computed using the navigation message, the authenticated data
5 indicating the navigation message that has been received is authenticated, the position information acquisition apparatus comprising:
a terminal data acquisition portion that acquires the position information and the authenticated data transmitted by the positioning terminal from a communication portion;
10 a key acquisition portion that allows the communication portion to acquire a key-related data from an authentication center apparatus, wherein the key-related data corresponds to one of a cryptography key and a key generation data, the cryptography key being used by the authentication center apparatus to generate a center-generated authentication data that is
15 used by the positioning terminal for authentication, the key generation data being capable of generating the cryptography key;
a comparative data generation portion that generates an authenticated comparative data to be compared with the authenticated data based on the key-related data acquired by the key acquisition portion; and
20 a terminal determination portion that compares the authenticated data acquired by the terminal data acquisition portion with the authenticated comparative data generated by the comparative data generation portion and, when the authenticated data acquired by the terminal data acquisition portion is matched with the authenticated comparative data generated by the comparative data generation portion, determines that the positioning
25 terminal is a regular positioning terminal.

7. The position information authentication system according to claim 2, wherein:
30 the authenticated data generation portion generates the authenticated data by the hash function using the center-generated authentication data along with the key-related data received by the key reception portion.