DESCRIPTION

TITILE OF INVENTION: NAVIGATION MESSAGE RECEPTION DEVICE AND SIMPLIFIED AUTHENTICATION SYSTEM

CROSS REFERENCE TO RELATED APPLICATION

[0001]

This application is based on Japanese Patent Application No. 2014-37044 filed on February 27, 2014, the disclosure of which is incorporated herein by reference.

TECHNICAL FIELD

[0002]

The present disclosure relates to a navigation message reception device to receive a navigation message from an artificial satellite used for a satellite positioning system and a simplified authentication system including the navigation message reception device.

BACKGROUND ART

[0003]

Conventionally, there is known a technology that uses a receiver to receive a navigation message for positioning transmitted from an artificial satellite used for a satellite positioning system.

[0004]

Recently, however, a malicious person's falsification or impersonation of position information is increasing in response to development of a repeater which

duplicates signals from the artificial satellite or a simulator which is capable of imitatively generating signals from the artificial satellite.

[0005]

Patent literature 1 discloses the technology to authenticate whether a receiver receives an authentic navigation message from an artificial satellite used for the satellite positioning system. According to the technology disclosed in patent literature 1, the receiver accesses a database in an authentication center and acquires data used to authenticate a targeted artificial satellite from a satellite number and the satellite time contained in a navigation message received from the artificial satellite. The receiver uses the data acquired from the authentication center to authenticate whether the received navigation message conforms to an authenticated navigation message from the artificial satellite used for the satellite positioning system.

PRIOR ART LITERATURES

PATENT LITERATURE

[0006]

Patent Literature 1: JP-2013-130395A

SUMMARY OF INVENTION

[0007]

The inventors of the present application found the following concerning the technology disclosed in patent literature 1.

[0008]

According to the technology disclosed in patent literature 1, each of receivers, if available, needs to communicate with the authentication center and

authenticate each of navigation messages from multiple satellites used for positioning every time the positioning is performed. Each receiver needs to frequently communicate with the authentication center and causes an excessive amount of communication processing load on the authentication center.

[0009]

The present disclosure has been made in consideration of the foregoing. It is an object of the present disclosure to provide a navigation message reception device and a simplified authentication system capable of determining whether a navigation message from an artificial satellite is authentic while suppressing a communication processing load at an authentication center used to authenticate a navigation message from an artificial satellite used for a satellite positioning system.

[0010]

A navigation message reception device according to an example of the present disclosure comprises: a satellite receiver for receiving a navigation message from an artificial satellite used for a satellite positioning system; a satellite information acquisition portion for acquiring authenticated satellite information from a positioning device that performs authentication by receiving authentication information corresponding to a navigation message received from the artificial satellite, wherein the authenticated satellite information is information about the artificial satellite that is a source of the successfully authenticated navigation message; and a simplified determination portion for determining whether the navigation message received by the satellite receiver is authentic, by using the authenticated satellite information acquired by the satellite information acquisition portion.

[0011]

The above-mentioned navigation message reception device determines whether a navigation message received by the satellite receiver is authentic, using authenticated satellite information about an artificial satellite that is a source of originating a navigation message successfully authenticated by the positioning device that receives authentication information from the authentication center, the authentication information corresponding to the navigation message received from the artificial satellite. Therefore, the navigation message reception device can determine whether a navigation message received by the satellite receiver is authentic, without receiving the authentication information from the authentication center. Accordingly, the navigation message reception device need not receive the authentication information from the authentication center, reducing a communication processing load on the authentication center.

[0012]

A simplified authentication system according to an example of the present disclosure comprises: a first navigation message reception device used for a first mobile object; a roadside device arranged to a road; and a second navigation message reception device used for a second mobile object. The first navigation message reception device includes: a first satellite receiver for receiving a navigation message from an artificial satellite used for a satellite positioning system; an authentication information receiver for receiving, from an authentication center, authentication information corresponding to the navigation message received by the first satellite receiver; a center usage authentication portion for authenticating whether the navigation message received by the first satellite receiver is authentic, by using the authentication information received by the authentication information receiver; and a satellite information transmitter for transmitting authenticated satellite information, the authenticated satellite

information being information about the artificial satellite that is a source of the navigation message successfully authenticated by the center usage authentication portion. The roadside device includes: a satellite information receiver for receiving the authenticated satellite information transmitted from the satellite information transmitter; an accumulation portion for accumulating the authenticated satellite information received by the satellite information receiver; and a delivery portion for delivering information accumulated in the accumulation portion. The second navigation message reception device includes: a second satellite receiver for receiving a navigation message from an artificial satellite used for the satellite positioning system; a satellite information acquisition portion for acquiring the authenticated satellite information by receiving the authenticated satellite information delivered from the delivery portion of the roadside device; and a simplified determination portion for determining whether the navigation message received by the satellite receiver is authentic, by using the authenticated satellite information acquired by the satellite information acquisition portion.

[0013]

According to the above-mentioned simplified authentication system, the second navigation message reception device determines whether a navigation message received by the satellite receiver is authentic, using the authenticated satellite information which is information about the artificial satellite that is a source of the navigation message successfully authenticated in the first navigation message reception device by using the authentication information received from the authentication center. Therefore, the second navigation message reception device can determine whether a navigation message received by the satellite receiver is authentic, without receiving the authentication information from the authentication center. The second navigation message reception device need

not receive the authentication information from the authentication center, reducing a communication processing load on the authentication center.

[0014]

The first navigation message reception device used for the first mobile object transmits the authentication information. The roadside device temporarily accumulates the authentication information and transmits the authentication information to the second navigation message reception device used for the second mobile object. Therefore, the second navigation message reception device can acquire the authentication information transmitted from the first navigation message reception device even when the first mobile object and the second mobile object are not located near the roadside device at the same time after the second navigation message reception device later reaches the vicinity of the roadside device.

[0015]

As the roadside device is arranged to a road, the authentication information that the roadside device receives from the first navigation message reception device equals the authentication information about an artificial satellite whose navigation message is receivable near the roadside device. Therefore, the second navigation message reception device can receive the authentication information about only the artificial satellite whose navigation messages are receivable near the roadside device out of artificial satellites used for the satellite positioning system.

BRIEF DESCRIPTION OF DRAWINGS

[0016]

The foregoing and other objects, features and advantages of the present

disclosure will become more apparent from the detailed description given below with reference to the accompanying drawings in which:

FIG. 1 is a diagram illustrating a schematic configuration of a simplified authentication system according to a first embodiment;

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

FIG. 3 is a block diagram illustrating a schematic configuration of a first onboard device;

FIG. 4 is a flowchart illustrating a flow of an authentication-related process on the first onboard device according to the first embodiment;

FIG. 5 is a flowchart illustrating a flow of an authenticated satellite information transmission process on the first onboard device according to the first embodiment;

FIG. 6 is a block diagram illustrating a schematic configuration of a second onboard device;

FIG. 7 is a flowchart illustrating a flow of a first simplified determination process on the second onboard device according to the first embodiment;

FIG. 8 is a diagram illustrating a schematic configuration of the simplified authentication system according to a first modification;

FIG. 9 is a flowchart illustrating a flow of an accumulation process on the roadside device according to the first modification;

FIG. 10 is a flowchart illustrating a flow of a delivery process on the roadside device according to the first modification;

FIG. 11 is a flowchart illustrating a flow of the first simplified determination process on the second onboard device according to a third modification;

FIG. 12 is a schematic diagram illustrating a process at S65;

FIG. 13 is a diagram illustrating a schematic configuration of the simplified authentication system according to a second embodiment;

FIG. 14 is a flowchart illustrating a flow of the authentication-related process on the second onboard device according to the second embodiment;

FIG. 15 is a flowchart illustrating a flow of a second simplified determination process on the second onboard device according to the second embodiment;

FIG. 16 is a schematic diagram illustrating a process at S94;

FIG. 17 is a flowchart illustrating a flow of the second simplified determination process on the second onboard device according to a fourth modification;

FIG. 18 is a schematic diagram illustrating a process at S105;

FIG. 19 is a flowchart illustrating a flow of a third simplified determination process on the second onboard device according to a third embodiment;

FIG. 20 is a schematic diagram illustrating a process at S112; and

FIG. 21 is a flowchart illustrating a flow of the third simplified determination process on the second onboard device according to a fifth modification.

EMBODIMENTS FOR CARRYING OUT INVENTION

[0017]

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

[0018]

(First Embodiment)

As illustrated in FIG. 1, a simplified authentication system 1 according to the first embodiment includes a monitor station 110, an authentication center 120, a master control station 130, a first onboard device 200, and a second onboard device 300. Vehicle A is assumed to use the first onboard device 200. Vehicle B is assumed to use the second onboard device 300. The first onboard device 200 corresponds to a positioning device. The second onboard device 300 corresponds to a navigation message reception device.

[0019]

<Schematic Configuration of the Simplified Authentication System 1>

The monitor station 110 receives GPS radio waves originated from GPS satellites 2a through 2c included in a GPS, one of satellite positioning systems. The GPS satellites 2a through 2c correspond to artificial satellites. The GPS satellites 2a through 2c are hereafter represented as a GPS satellite 2 if the GPS satellites need not be distinguished from each other. As publicly known, the GPS radio wave contains a navigation message. The monitor station 110 demodulates the received GPS radio wave, extracts a navigation message, and transmits it to the authentication center 120. The monitor station 110 may receive GPS radio waves from multiple GPS satellites 2. In this case, the monitor station 110 extracts navigation messages from respective GPS radio waves and transmits the navigation messages to the authentication center 120.

[0020]

The authentication center 120 generates parity data from the navigation message and an H matrix serving as an encryption key. The authentication center 120 transmits a signal containing the parity data to the master control station 130. The authentication center 120 also communicates with the first onboard device 200. The authentication center 120 will be described in detail

later with reference to FIG. 2.

[0021]

The master control station 130 transmits the parity data received from the authentication center 120 to a quasi-zenith satellite (hereinafter referred to as a QZS satellite) 3. The QZS satellite 3 broadcasts the navigation message containing the parity data to the earth.

[0022]

The first onboard device 200 represents a navigation message authentication (NMA) onboard device. The first onboard device 200 communicates with the authentication center 120 to authenticate that the navigation message received from the GPS satellite 2 is authentic. The authentication will be described in detail later with reference to FIG. 4.

[0023]

The first onboard device 200 determines a current position of the first onboard device 200 using the navigation messages received from the multiple GPS satellites 2. The determination of the current position uses navigation messages received from at least three GPS satellites 2.

[0024]

The first onboard device 200 uses wireless communication to externally transmit information (hereinafter referred to as authenticated satellite information) about the GPS satellite 2 that is a source of the successfully authenticated navigation message (hereinafter referred to as authenticated satellite information). The first onboard device 200 will be described in detail later with reference to FIG. 3.

[0025]

The second onboard device 300 receives the authenticated satellite

information transmitted from the first onboard device 200. Using the authenticated satellite information, the second onboard device 300 determines whether a navigation message received from the GPS satellite 2 is authentic, without using the authentication center 120. The second onboard device 300 will be described in detail later with reference to FIG. 6.

[0026]

<Detailed Configuration of the Authentication Center 120>

As illustrated in FIG. 2, the authentication center 120 includes a controller 122, a data storage 124, and a communicator 126.

[0027]

The controller 122 is provided as a computer including a CPU, ROM, and RAM. The controller 122 controls the data storage 124 and the communicator 126. The CPU executes a program stored in the ROM while using a temporary storage function of the RAM, thereby functioning as a RAND message generator 1221, a SEED value generator 1222, an H matrix calculator 1223, a parity calculator 1224, and a signal processor 1225. The functions of the portions 1221 through 1225 may include functions disclosed in patent literature 1.

[0028]

The RAND message generator 1221 generates a RAND message from a navigation message acquired from the monitor station 110. The RAND message contains TOW, TOC, AF0, and AF1 in order. TOW (time of week) is bit string data contained in bit strings of the navigation message. TOC, AF0, and AF1 are clock correction parameters in ephemeris data. TOW, TOC, AF0, and AF1 are provided as data to specify a signal transmission time and correspond to a transmission time. The data is followed by AS Flag acting as an anti-spoof flag and PRN (Pseudo Random Noise) ID acting as a satellite number.

[0029]

RAND containing TOW and PRN ID can be provided as data to indicate which GPS satellite is used as the source at which time. TOW varies every six seconds. RAND contains PRN ID. Therefore, RAND is generated every six seconds for each GPS satellite 2 from which the monitor station 110 receives a GPS radio wave.

[0030]

The SEED value generator 1222 generates a random number using a PC clock as input to generate a SEED value.

[0031]

The H matrix calculator 1223 uses the SEED value generated by the SEED value generator 1222 to calculate an H matrix that maintains one-to-one correspondence to the SEED value. The publicly known hash function can be used for the H matrix. For example, the H matrix may be available as a parity check matrix for LDPC (Low Density Parity Check) coding. The H matrix may be also available as a generator matrix resulting from the parity check matrix.

[0032]

The parity calculator 1224 calculates parity data based on the RAND message generated by the RAND message generator 1221 and the H matrix calculated by the H matrix calculator 1223.

[0033]

The signal processor 1225 inserts the parity data and the RAND message into a navigation message originated from the QZS satellite 3. The parity data is calculated by the parity calculator 1224. The RAND message is used for this calculation. The signal processor 1225 transmits the navigation message after the insertion to the master control station 130.

[0034]

In addition to the signal insertion, the signal processor 1225 causes the data storage 124 to store the parity data calculated by the parity calculator 1224, the RAND message used for the parity data calculation, the H matrix, and the SEED value used for the H matrix calculation so that these are associated with each other.

[0035]

The signal processor 1225 inserts the RAND message and the parity data into a navigation message transmitted from the QZS satellite 3 each time the RAND message generator 1221 generates a RAND message. Therefore, the RAND message generator 1221, the SEED value generator 1222, the H matrix calculator 1223, and the parity calculator 1224 also perform the processes each time the RAND message generator 1221 generates a RAND message.

[0036]

Suppose that the communicator 126 receives PRN ID, TOW, and a public key transmitted from the first onboard device 200. In this case, an H matrix selector 1226 selects an H matrix corresponding to the received PRN ID and TOW from H matrices stored in the data storage 124. The H matrix selector 1226 encrypts the selected H matrix using the public key and returns the encrypted H matrix to the first onboard device 200.

[0037]

<Detailed Configuration of the First Onboard Device 200>

The first onboard device 200 includes a communicator 210 that includes a receiver 211. The receiver 211 receives a navigation message broadcast from the QZS satellite 3. As illustrated in FIG. 3, the first onboard device 200 includes the communicator 210, a controller 220, and a satellite receiver 230.

[0038]

The communicator 210 includes the receiver 211 and a transmitter 212. The communicator 210 includes a dedicated short range communication function and a wide area communication function. The dedicated short range communication function supports several hundred meters of communication distance, for example. The wide area communication function supports several kilometers of communication distance and performs communication with a base station in the public network to enable communication with other communication devices available within a communication range of the public network. The dedicated short range communication function enables inter-vehicle communication with a communicator 310 of the second onboard device 300. The wide area communication function enables the communicator 210 to communicate with the communicator 126 of the authentication center 120.

[0039]

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

[0040]

The controller 220 is provided as a computer including a CPU, ROM, and RAM. The controller 220 controls the communicator 210 and the satellite receiver 230. The CPU executes a program stored in the ROM while using a temporary storage function of the RAM, thereby executing an authentication-related process in FIG. 4 and an authenticated satellite information transmission process in FIG. 5.

[0041]

<Authentication-Related Process>

The controller 220 of the first onboard device 200 performs the

authentication-related process to be described with reference to a flowchart in FIG. 4. The authentication-related process relates to the authentication proving that a signal received by the satellite receiver 230 conforms to an authentic navigation message received from the GPS satellite 2. The flowchart in FIG. 4 may be performed each time the satellite receiver 230 receives GPS radio waves from three or more GPS satellites 2.

[0042]

Suppose that the satellite receiver 230 may receive a signal from a repeater or a simulator and incorrectly assume that the signal is a navigation message contained in the GPS radio wave. In the above, the repeater is one that duplicates a signal from the GPS satellite 2. The simulator is one that can imitatively generate a signal from the GPS satellite 2.

[0043]

At S1, a current position is determined based on navigation messages contained in the GPS radio waves received from three or more GPS satellites 2.

[0044]

At S2, a navigation message received from the QZS satellite 3 is acquired from the receiver 211. At S3, PRN ID and TOW are extracted from the navigation message acquired at S1.

[0045]

At S4, PRN ID and TOW extracted at S3 are transmitted along with a public key to the authentication center 120 from the transmitter 212. The H matrix is determined from PRN ID and TOW. The authentication center 120 encrypts the H matrix using the public key and transmits the H matrix to the first onboard device 200. The H matrix, which is determined from PRN ID and TOW transmitted from the first onboard device 200 to the authentication center 120,

corresponds to authentication information.

[0046]

At S5, the H matrix transmitted from the authentication center 120 is acquired from the receiver 211. Namely, the H matrix corresponding to the navigation message received from the GPS satellite 2 is received from the authentication center 120. At S6, the encrypted H matrix acquired at S5 is decrypted using a private key.

[0047]

At S7, a RAND message is generated from, of the navigation messages contained in the GPS radio waves received from the GPS satellites 2, a navigation message containing the same PRN ID as that transmitted at S4.

[0048]

At S8, comparison parity data is generated based on the RAND message generated at S7 and the H matrix decrypted at S6. At S9, it is determined whether the comparison parity data generated at S8 matches the parity data extracted at S3.

[0049]

The H matrix decrypted at S6 equals the H matrix that the authentication center 120 uses to generate the parity data. The parity calculator 1224 of the authentication center 120 calculates parity data based on this H matrix and the RAND message.

[0050]

Accordingly, when the comparison parity data generated at S8 matches the parity data extracted at S3, the RAND message generated at S7 can be assumed to equal the RAND message generated by the authentication center 120.

[0051]

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

[0052]

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

[0053]

<Authenticated Satellite Information Transmission Process>

The controller 220 of the first onboard device 200 performs a process (hereinafter referred to as an authenticated satellite information transmission process) related to transmission of authenticated satellite information to the second onboard device 300. The authenticated satellite information transmission process will be described with reference to a flowchart in FIG. 5. The process according to the flowchart in FIG. 5 and the process according to the

flowchart in FIG. 4 are performed in parallel. The flowchart in FIG. 5 starts even when the authentication according to the flowchart in FIG. 4 is not completed on all navigation messages used for positioning. The flowchart in FIG. 5 may start at a predetermined cycle, for example.

[0054]

The authenticated satellite information transmission process according to the flowchart in FIG. 5 transmits authenticated satellite information containing a satellite number or a transmission time about the GPS satellite 2 that is a source of the successfully authenticated navigation message. The second onboard device 300 uses the authenticated satellite information transmitted from the first onboard device 200 to determine whether the received navigation message is authentic.

[0055]

At S21, PRN ID (i.e., satellite number), TOW, TOC, AF0, and AF1 (i.e., transmission time) are extracted from the navigation message that is successfully authenticated according to the flowchart in FIG. 4. At S22, the dedicated short range communication function of the transmitter 212 is used to transmit the authenticated satellite information containing the satellite number and the transmission time extracted at S21, and then the process is ended. The description of the embodiment below assumes that the second onboard device 300 receives the authenticated satellite information transmitted from the transmitter 212.

[0056]

The transmitter 212 may transmit the current position measured at S1 as well as the authenticated satellite information. In this case, the transmitter 212 may transmit the current position in association with the authenticated satellite

information about the GPS satellite 2 used to determine the current position.

[0057]

<Detailed Configuration of the Second Onboard Device 300>

As illustrated in FIG. 6, the second onboard device 300 includes the communicator 310, a controller 320, and a satellite receiver 330. The communicator 310 wirelessly communicates with the communicator 210 included in the first onboard device 200.

[0058]

The communicator 310 includes a receiver 311 and a transmitter 312. The communicator 310 includes the dedicated short range communication function mentioned above. The communicator 310 uses the dedicated short range communication function to communicate with the communicator 210 of the first onboard device 200.

[0059]

The satellite receiver 330 receives radio waves originated from the GPS satellite 2 and the QZS satellite 3 at a specified cycle. For the purpose of illustration, the description below explains an example of receiving a radio wave originated from the GPS satellite 2.

[0060]

The controller 320 is provided as a computer including a CPU, ROM, and RAM. The controller 320 controls the communicator 310 and the satellite receiver 330. The CPU executes a program stored in the ROM while using a temporary storage function of the RAM, thereby executing a first simplified determination process in FIG. 7.

[0061]

<First Simplified Determination Process>

The description below explains the first simplified determination process performed by the controller 320 of the second onboard device 300 with reference to a flowchart in FIG. 7. The first simplified determination process uses the authenticated satellite information transmitted from the first onboard device 200 to determine whether a navigation message received by the satellite receiver 330 of the second onboard device 300 is authentic, without access to the authentication center 120. For example, the flowchart in FIG. 7 may start when the communicator 310 of the second onboard device 300 receives the authenticated satellite information transmitted from the first onboard device 200.

[0062]

At S31, the authenticated satellite information received by the communicator 310 is acquired from the communicator 310. S31 corresponds to a satellite information acquisition portion. The authenticated satellite information contains a satellite number and a transmission time about the GPS satellite 2 that is a source of the successfully authenticated navigation message.

[0063]

At S32, a navigation message is acquired that the satellite receiver 330 receives from the GPS satellite 2 and outputs most recently. The satellite receiver 330 outputs multiple navigation messages if received from the multiple GPS satellites 2 within a specified period of time.

[0064]

At S33, it is determined whether a satellite number contained in the authenticated satellite information acquired at S31 matches a satellite number contained in the navigation message received at S32. Namely, it is determined whether there is a match between the satellite number of the GPS satellite 2 that is a source of the navigation message successfully authenticated by the first

onboard device 200 and the satellite number of the GPS satellite 2 from which the second onboard device 300 receives the navigation message. The satellite number corresponds to identification information.

[0065]

At S34, it may be determined that the satellite numbers match (S34: YES). In this case, the process proceeds to S35 and determines that, of the navigation messages received by the satellite receiver 330 from the GPS satellite 2, the navigation message containing the satellite number matching the satellite number contained in the authenticated satellite information is authentic. The process is then ended. It may be determined that the satellite numbers do not match (S34: NO). In this case, it is determined that the navigation message determined as having the mismatch in the satellite number is unauthentic. The process is then ended. S33 through S35 correspond to a simplified determination portion.

[0066]

In determining the current position of the device based on a navigation message contained in the GPS radio wave received from the GPS satellite 2, the navigation message determined to be authentic during the first simplified determination process may be treated as a successfully authenticated navigation message. As an example, it may be determined that the current position of the second onboard device 300 positioned based on the navigation message determined to be authentic during the first simplified determination process is not falsified.

[0067]

<Summary of the First Embodiment>

According to the first embodiment, the second onboard device 300

determines whether a navigation message received by the satellite receiver 330 is authentic, based on where there is a match between a satellite number in the navigation message received by the satellite receiver 330 and the satellite number for the GPS satellite 2 that is a source of the navigation message that the first onboard device 200 receives from the authentication center 120 and successfully authenticates using an H matrix that cannot be acquired in advance.

[0068]

A navigation message received from the GPS satellite 2 that is the source of the already authenticated navigation message is more likely to be authentic than a navigation message received from the GPS satellite 2 that is the source of a navigation message not authenticated. Therefore, the second onboard device 300 can determine whether a navigation message received by the satellite receiver 330 is authentic, without receiving the H matrix from the authentication center 120. Because the second onboard device 300 need not receive the H matrix from the authentication center 120, it is possible to reduce a communication processing load on the authentication center 120.

[0069]

As a result, the second onboard device 300 can determine whether a navigation message from the GPS satellite 2 is authentic, while suppressing a communication processing load on the authentication center 120 used to authenticate a navigation message from the GPS satellite 2 used for the satellite positioning system.

[0070]

<First Modification>

There has been described the first embodiment in which the second onboard device 300 directly receives the authenticated satellite information

transmitted from the first onboard device 200. However, this is limiting. For example, according to a configuration (hereinafter referred to as a first modification), a roadside device 400 may receive and accumulate the authenticated satellite information transmitted from the first onboard device 200 and may deliver the accumulated authenticated satellite information to the second onboard device 300.

[0071]

The description below explains a simplified authentication system 1a according to the first modification with reference to the accompanying drawings. For the purpose of illustration, elements having the same functions as those shown in the drawings used to explain the above-mentioned embodiment are given the same references and their detailed description is omitted.

[0072]

The simplified authentication system 1a is similar to the simplified authentication system 1 according to the first embodiment except the following. The simplified authentication system 1a includes the roadside device 400. The roadside device 400 relays and delivers the authenticated satellite information transmitted from the first onboard device 200. The second onboard device 300 receives the delivered authenticated satellite information.

[0073]

<Schematic Configuration of the Simplified Authentication System 1a According to the First Modification>

As illustrated in FIG. 8, the simplified authentication system 1a according to the first modification includes the monitor station 110, the authentication center 120, the master control station 130, the first onboard device 200, the second onboard device 300, and the roadside device 400.

[0074]

The first onboard device 200 performs the authentication-related process in FIG. 4 and the authenticated satellite information transmission process in FIG. 5 as above. The first onboard device 200 corresponds to a first navigation message reception device. The satellite receiver 230 of the first onboard device 200 corresponds to a first satellite receiver. S5 corresponds to an authentication information receiver. S9 through S11 correspond to a center usage authentication portion. S22 corresponds to a satellite information transmitter.

[0075]

The second onboard device 300 performs the first simplified determination process in FIG. 7. The second onboard device 300 corresponds to a second navigation message reception device. The satellite receiver 330 of the second onboard device 300 corresponds to a second satellite receiver. According to the first modification, the communicator 310 of the second onboard device 300 receives the authenticated satellite information relayed by the roadside device 400. S31 corresponds to the satellite information acquisition portion. S33 through S35 correspond to a simplified determination portion.

[0076]

<Detailed Configuration of the Roadside Device 400 According to the First Modification>

The roadside device 400 is arranged to a road and includes a communicator 410, a controller 420, and a storage 430 as illustrated in FIG. 8. The communicator 410 uses the dedicated short range communication function to enable the so-called road-to-vehicle communication with the communicator 210 included in the first onboard device 200 and the communicator 310 included in the second onboard device 300.

[0077]

The controller 420 is provided as a computer including a CPU, ROM, and RAM. The controller 420 controls the communicator 410 and allows the storage 430 to accumulate the authenticated satellite information received from the first onboard device 200. The CPU executes a program stored in the ROM while using a temporary storage function of the RAM, thereby executing an accumulation process in FIG. 9 or a delivery process in FIG. 10.

[0078]

<Accumulation Process>

The controller 420 of the roadside device 400 performs the accumulation process to accumulate the authenticated satellite information received from the first onboard device 200. The accumulation process will be described with reference to a flowchart in FIG. 9. The flowchart in FIG. 9 may start when the communicator 410 of the roadside device 400 receives the authenticated satellite information from the first onboard device 200, for example.

[0079]

At S41, the authenticated satellite information transmitted from the first onboard device 200 is received via the communicator 410. S41 corresponds to a satellite information receiver.

[0080]

At S42, the storage 430 accumulates the authenticated satellite information received at S41 and the process is terminated. The storage 430 corresponds to an accumulation portion. For example, the storage 430 may already accumulate the authenticated satellite information that contains the same satellite number. In such a case, the authenticated satellite information corresponding to an earlier transmission time may be deleted. The authenticated

satellite information corresponding to a more recent transmission time may be accumulated in the storage 430.

[0081]

Another possible example is to delete the authenticated satellite information whose transmission time is longer than or equal to a specified time period such as one hour. The storage 430 may be limited to accumulating relatively recent authenticated satellite information so that the first simplified determination process in the second onboard device 300 can improve the accuracy of determining a navigation message to be authentic. This is because a navigation message is less likely to be impersonated and is more likely to be authentic if the navigation message is received from the GPS satellite 2 that is a source of the successfully authenticated navigation message during a relatively short period of time within an area comparable to a range of the road-to-vehicle communication.

[0082]

<Delivery Process>

The controller 420 of the roadside device 400 performs a delivery process to deliver the authenticated satellite information accumulated by the accumulation process. The delivery process will be described with reference to a flowchart in FIG. 10. The flowchart in FIG. 10 may start in response to a power-on sequence on the roadside device 400 and may end in response to a power-off sequence on the roadside device 400.

[0083]

At S51, it is determined whether a delivery timing to deliver the authenticated satellite information accumulated in the storage 430 is reached. The delivery timing for the authenticated satellite information may be defined as a

specified cycle, for example. The process proceeds to S52 if it is determined that the delivery timing is reached (S51: YES). The process repeats S51 if it is determined that the delivery timing is not reached (S51: NO).

[0084]

At S52, the communicator 410 delivers the authenticated satellite information accumulated in the storage 430 and the process returns to S51. The storage 430 may accumulate the authenticated satellite information about the multiple GPS satellites 2. In such a case, the authenticated satellite information about the GPS satellites 2 may be delivered.

[0085]

<Summary of the First Modification>

According to the first modification, similarly to the first embodiment, the second onboard device 300 can also determine whether a navigation message received by the satellite receiver 330 is authentic, without receiving the H matrix from the authentication center 120. Because the second onboard device 300 need not receive the H matrix from the authentication center 120, a communication processing load on the authentication center 120 is reduced.

[0086]

According to the first modification, the first onboard device 200 and the second onboard device 300 need not maintain a distance capable of the inter-vehicle communication. The roadside device 400 temporarily accumulates the authenticated satellite information transmitted from the first onboard device 200 and delivers the authenticated satellite information. This enables the second onboard device 300 to acquire the authenticated satellite information when the second onboard device 300 arrives near the roadside device 400 later than the first onboard device 200.

[0087]

Because the roadside device 400 is arranged to the road, the authenticated satellite information received by the roadside device 400 from the first onboard device 200 is narrowed down to o the authenticated satellite information about the GPS satellite 2 whose navigation message is receivable near the roadside device 400. Therefore, the roadside device 400 can deliver only the authenticated satellite information about the GPS satellite 2 whose navigation messages is receivable near the roadside device 400. As a result, the second onboard device 300, which receives the authenticated satellite information from the roadside device 400, can efficiently receive the authenticated satellite information about the GPS satellite 2 whose navigation messages is receivable near the vehicle.

[0088]

<Second Modification>

According to the first modification, the roadside device 400 receives the authenticated satellite information transmitted from the first onboard device 200 and accumulates the authenticated satellite information and the roadside device 400 delivers the accumulated authenticated satellite information. However, this is not limiting. For example, the roadside device 400 may perform the authentication-related process similarly to the first onboard device 200. The roadside device 400 may deliver the authenticated satellite information about the GPS satellite 2 that is a source of the successfully authenticated navigation message. The second onboard device 300 may receive the delivered authenticated satellite information.

[0089]

Further, the first onboard device 200 or the roadside device 400 may

transmit the authenticated satellite information via the public network. The second onboard device 300 may receive the transmitted authenticated satellite information. In this case, the communicator 310 of the second onboard device 300 may also include the wide area communication function to receive the authenticated satellite information via the public network.

[0090]

<Third Modification>

The first embodiment determines whether a received navigation message is authentic, based on whether there is match between the satellite number contained in the authenticated satellite information received from the first onboard device 200 and the satellite number contained in the navigation message received by the satellite receiver 330. However, this is not limiting. It may be preferable that the third modification described below be adopated to further improve the accuracy of determining a navigation message to be authentic.

[0091]

The third modification is similar to the first embodiment except differences in the process on the controller 220 of the first onboard device 200 and the process on the controller 320 of the second onboard device 300. More specifically, the third modification differs from the first embodiment in that the third modification determines whether a received navigation message is authentic, depending on presence and absence of the continuity between the transmission time contained in the authenticated satellite information received from the first onboard device 200 and the transmission time contained in the navigation message received by the satellite receiver 330.

[0092]

<Authenticated Satellite Information Transmission Process According to

the Third Modification>

The authentication-related process on the controller 220 of the first onboard device 200 in the third modification is similar to that in the first embodiment but is different in part. The description below explains the authenticated satellite information transmission process in the third modification.

[0093]

The authenticated satellite information transmission process according to the third modification transmits the authenticated satellite information that contains not only the satellite number and the transmission time extracted from a successfully authenticated navigation message, but also the reception time when the satellite receiver 230 of the first onboard device 200 receives the navigation message successfully authenticated.

[0094]

<First Simplified Determination Process According to the Third Modification>

The controller 320 of the second onboard device 300 according to the third modification performs the first simplified determination process. The description below explains the first simplified determination process with reference to a flowchart in FIG. 11. The flowchart in FIG. 11 may also start when the communicator 310 of the second onboard device 300 receives the authenticated satellite information transmitted from the first onboard device 200. The controller 320 may perform the process according to the flowchart in FIG. 11 on each of the multiple GPS satellites 2 when the authenticated satellite information transmitted from the first onboard device 200 contains information about the GPS satellites 2.

[0095]

At S61, the authenticated satellite information received by the

communicator 310 is acquired from the communicator 310. S61 also corresponds to the satellite information acquisition portion. The authenticated satellite information contains the transmission time, the reception time, and the satellite number about the GPS satellite 2 that is a source of the successfully authenticated navigation message.

[0096]

At S62, a navigation message and the reception time of the navigation message are acquired. In the above, the navigation message is the navigation message that the satellite receiver 330 receives from the GPS satellite 2 and most recently outputs The satellite receiver 330 outputs multiple navigation messages if received from the multiple GPS satellites 2 within a specified period of time.

[0097]

At S63, it is determined whether where is match between the satellite number contained in the authenticated satellite information acquired at S61 and the satellite number contained in the navigation message received at S62.

[0098]

At S64, it is determined whether the satellite numbers match. The process proceeds to S65 if the satellite numbers match (S64: YES). The process is ended if the satellite numbers do not match (S64: NO).

[0099]

At S65, with regard to the authenticated satellite information and the navigation message determined at S64 as containing the matching satellite number, it is determined whether there is continuity between the transmission time contained in the authenticated satellite information acquired at S61 and the transmission time contained in the navigation message received at S62. In other words, with regard to the same GPS satellite 2, it is determined whether the

transmission time contained in the authenticated satellite information received from the first onboard device 200 and the transmission time contained in the navigation message received by the second onboard device 300 have continuity that corresponds to a reception time difference between the reception time contained in the authenticated satellite information and the reception time of the navigation message. S65 corresponds to a first continuity determination portion.

[0100]

An example of the process at S65 will be described with reference to FIG. 12. According to the example in FIG. 12, the first onboard device 200 uses the authentication center 120 to successfully authenticate a navigation message originated from the GPS satellite 2a. The first onboard device 200 transmits the authenticated satellite information about the navigation message to the second onboard device 300. The second onboard device 300 thereafter receives a navigation message originated from the GPS satellite 2a.

[0101]

The GPS satellite 2a originates a navigation message successfully authenticated by the first onboard device 200 at transmission time Ti1. The first onboard device 200 receives the navigation message at reception time To1. The second onboard device 300 thereafter receives a navigation message from the GPS satellite 2a at reception time To2 when the GPS satellite 2a originates the navigation message at transmission time Ti2.

[0102]

In the process at S65, the reception time (To1) contained in the authenticated satellite information acquired at S61 is subtracted from the reception time (To2) of the navigation message acquired at S62 to find a reception time difference (To2 - To1) which is a difference from the reception time contained

in the authenticated satellite information acquired at S61 to the reception time of the navigation message acquired at S62.

[0103]

It is then determined whether there is match between the time (Ti1 + (To2 - To1)) resulting from adding the calculated reception time difference (To2 - To1) to the transmission time (Ti1) contained in the authenticated satellite information acquired at S61 and the transmission time (Ti2) contained in the navigation message acquired at S62. The match here signifies not only a complete match but also an approximate match within a range of an error.

[0104]

If a match is determined between the time (Ti1 + (To2 - To1)) and the transmission time (Ti2), the presence of the continuity is determined between the transmission time contained in the authenticated satellite information acquired at S61 and the transmission time contained in the navigation message acquired at S62. If no match is determined, the absence of the continuity is determined.

[0105]

The process at S65 may determine whether there is a match between the time (To2 - To1) resulting from subtracting the reception time (To1) contained in the authenticated satellite information acquired at S61 from the reception time (To2) of the navigation message acquired at S62 and the time (Ti2 - Ti1) resulting from subtracting the transmission time (Ti1) contained in the authenticated satellite information acquired at S61 from the transmission time (Ti2) contained in the navigation message acquired at S62.

[0106]

If a match is determined between the time (To2 - To1) and the time (Ti2 - Ti1), the presence of the continuity is determiend between the transmission time

contained in the authenticated satellite information acquired at S61 and the transmission time contained in the navigation message acquired at S62. If no match is determined, the absence of the continuity is determined.

[0107]

At S66 in FIG. 11, when it is determine that there is the continuity between the transmission time contained in the authenticated satellite information acquired at S61 and the transmission time contained in the navigation message acquired at S62 (S66: YES), the process proceeds to S67. At S67, it is determined the navigation message containing the transmission time determined to have the continuity with the transmission time contained in the authenticated satellite information is authentic. The process is then ended.

[0108]

When the absence of the continuity is determined between the transmission time contained in the authenticated satellite information acquired at S61 and the transmission time contained in the navigation message acquired at S62 (S66: NO, it is determined the navigation message containing the transmission time determined not to have the continuity with the transmission time contained in the authenticated satellite information is unauthentic. The process is then ended. S66 and S67 correspond to a simplified determination portion.

[0109]

If the determination results in NO at S66, it may be determined that the navigation message containing the transmission time determined not to have the continuity with the transmission time contained in the authenticated satellite information is unauthentic.

[0110]

<Summary of the Third Modification>

According to the third modification, like the first embodiment, the second onboard device 300 can determine, without receiving the H matrix from the authentication center 120, that a navigation message received by the satellite receiver 330 is authentic. Therefore, the second onboard device 300 need not receive the H matrix from the authentication center 120, reducing a communication processing load on the authentication center 120.

[0111]

When a repeater duplicating a signal from the GPS satellite 2 is used, a delay in the reception time of a navigation message occurs with respect to the authentic navigation message. When a simulator capable of imitatively generating a signal from the GPS satellite 2 is used, a discrepancy in the transmission time or the reception time of a navigation message occurs with respect to the authentic navigation message. Specifically, the use of a repeater or a simulator nullifies the continuity corresponding to a reception time difference between the transmission time contained in the authenticated satellite information and the transmission time contained in the navigation message received by the second onboard device 300.

[0112]

The third modification does not determine that a newly received navigation message is authentic if the continuity corresponding to a reception time difference is absent between the transmission time contained in the authenticated satellite information and the transmission time contained in the navigation message received by the second onboard device 300. Therefore, the third modification can prevent a received navigation message from being determined to be authentic when a repeater or a simulator is used, and can improve the accuracy to determine a navigation message to be authentic.

[0113]

(Second Embodiment)

The following describes the second embodiment with reference to the appended drawings. Elements having the same functions as those illustrated in the drawings used to describe the first embodiment are depicted by the same reference numerals and a description is omitted for simplicity.

[0114]

A simplified authentication system 1b according to the second embodiment equals the simplified authentication system 1 according to the first embodiment, except that the second onboard device 300 accesses the authentication center 120 to authenticate a received navigation message at least once and that a navigation message successfully authenticated on the second onboard device 300 in the past is used to determine authenticity of a navigation message received by the satellite receiver 330 of the second onboard device 300 without access to the authentication center 120.

[0115]

<Schematic Configuration of the Simplified Authentication System 1b According to the Second Embodiment>

As illustrated in FIG. 13, the simplified authentication system 1b according to the second embodiment includes the monitor station 110, the authentication center 120, the master control station 130, the first onboard device 200, and the second onboard device 300.

[0116]

The first onboard device 200 performs the authentication-related process in FIG. 4 and the authenticated satellite information transmission process in FIG. 5 as above.

[0117]

The second onboard device 300 performs not only the first simplified determination process in FIG. 7, but also the authentication-related process in FIG. 14 and the second simplified determination process in FIG. 15. The authentication-related process from S71 to S82 in FIG. 14 is assumed to equal the authentication-related process from S1 to S12 in FIG. 4. Therefore, S75 corresponds to the authentication information receiver. S79 through S81 correspond to the center usage authentication portion.

[0118]

The second onboard device 300 uses nonvolatile memory such as backup RAM of the controller 320 to store the reception time of an authenticated navigation message in association with the authenticated navigation message. The authenticated navigation message signifies a navigation message that the authentication-related process in FIG. 14 authenticates successfully. Only the satellite number and the transmission time contained in the authenticated navigation message may be stored in association with the reception time.

[0119]

<Second Simplified Determination Process According to the Second Embodiment>

The controller 320 of the second onboard device 300 according to the second embodiment performs a second simplified determination process. The second simplified determination process will be described with reference to a flowchart in FIG. 15. The flowchart in FIG. 15 may start when the satellite receiver 330 of the second onboard device 300 receives a navigation message from the GPS satellite 2, for example. The flowchart in FIG. 15 may be performed on each of navigation messages from the multiple GPS satellites 2

when the satellite receiver 330 receives the navigation messages from the GPS satellites 2 within one cycle of successive output from the satellite receiver 330 to the controller 320.

[0120]

At S91, a navigation message received by the satellite receiver 330 is acquired from the satellite receiver 330.

[0121]

At S92, it is determined whether there is a match between the satellite number contained in the navigation message acquired at S91 and the satellite number contained in an authenticated navigation message already stored in the memory of the controller 320.

[0122]

The process proceeds to S94 if the satellite numbers are determined to match at S93 (S93: YES). The process is ended if the satellite numbers are determined to differ from each other at S93 (S93: NO). The satellite numbers may be also determined to differ from each other when no authenticated navigation message is stored in the memory of the controller 320.

[0123]

At S94, it is determined whether there is continuity between the authenticated navigation message and the navigation message that is acquired at S91 and is determined at S93 to contain the matching satellite number. In detail, it is determined whether the transmission time contained in the navigation message newly received by the satellite receiver 330 and the transmission time contained in the authenticated navigation message contains the transmission time have the continuity that corresponds to a reception time difference which is a difference from the reception time of the authenticated navigation message to the

reception time of the newly received navigation message. S94 corresponds to a second continuity determination portion.

[0124]

An example of the process at S94 will be described using FIG. 16. As a precondition for the example in FIG. 16, the second onboard device 300 successfully authenticates a navigation message originated from the GPS satellite 2a using the authentication center 120. The second onboard device 300 thereafter receives a navigation message originated from the GPS satellite 2a.

[0125]

Transmission time Ti3 is assumed to be a transmission time of the authenticated navigation message, namely, the navigation message that the second onboard device 300 successfully authenticates using the authentication center 120. Reception time To3 is assumed to be a reception time of the navigation message by the second onboard device 300. Transmission time Ti4 and reception time To4 are assumed to be a transmission time and a reception time of a navigation message that the second onboard device 300 newly receives from the GPS satellite 2a thereafter.

[0126]

In the process at S94, the reception time (To3) of the authenticated navigation message is subtracted from reception time (To4) of the navigation message acquired at S91 to find a reception time difference (To4 - To3) which is a difference from the reception time of the authenticated navigation message to the reception time of the navigation message acquired at S91.

[0127]

It is then determined whether there is a match between the time (Ti3 + (To4 - To3)) resulting from adding the calculated reception time difference (To4 -

To3) to the transmission time (Ti3) contained in the authenticated navigation message and the transmission time (Ti4) contained in the navigation message acquired at S91. The match here signifies not only a complete match but also an approximate match within a range of an error. The match here can be rephrased as consistency.

[0128]

If a match is determined between the time (Ti3 + (To4 - To3)) and the transmission time (Ti4), it is determined that there is the continuity between the transmission time contained in the authenticated navigation message and the transmission time contained in the navigation message acquired at S91. It is determined that there is no continuity if no match is determined.

[0129]

The process at S94 may determine whether there is a match between the time (To4 - To3) resulting from subtracting the reception time (To3) for the authenticated navigation message from the reception time (To4) for the navigation message acquired at S91 and the time (Ti4 - Ti3) resulting from subtracting the transmission time (Ti3) contained in the authenticated navigation message from the transmission time (Ti4) contained in the navigation message acquired at S91.

[0130]

It may be determined that there is the continuity between the transmission time contained in the authenticated navigation message and the transmission time contained in the navigation message acquired at S91 if a match is determined between the time (To4 - To3) and the time (Ti4 - Ti3). The controller 320 may determine that there is no continuity if no match is determined.

[0131]

At S95 in FIG. 15, when it is determined that there is the continuity

between the transmission time contained in the authenticated navigation message and the transmission time contained in the navigation message acquired at S91 (S95: YES), the process proceeds to S96. At S96, it is determined that the navigation message acquired at S91 is authentic and the process is ended.

[0132]

When it is determined that there is no continuity between the transmission time contained in the authenticated navigation message and the transmission time contained in the navigation message acquired at S91 (S95: NO), it is determined that the navigation message acquired at S91 is unauthentic and the process is ended. S95 and S96 correspond to a simplified determination portion.

[0133]

If the determination results in NO at S95, it may be determined that the navigation message acquired at S91 is unauthentic.

[0134]

In the second embodiment, for example, the second simplified determination process may not acquire an authenticated navigation message that contains the satellite number matching the satellite number contained in the navigation message acquired at S91. In this case, the controller 320 may perform the first simplified determination process using the authenticated satellite information transmitted from the first onboard device 200.

[0135]

The second embodiment may delete the authenticated navigation message stored in the memory of the controller 320 when a timer to measure the reception time, i.e., the time the satellite receiver 330 receives a navigation message, indicates a lapse of time that causes a time lag in excess of a range

within which the time or an interval of time is determined to be consistent at S94. After the authenticated navigation message is deleted, the authentication of a navigation message newly received from the same GPS satellite may be performed using the authentication center 120 and the successfully authenticated navigation message may be stored as an authenticated navigation message in the memory.

[0136]

<Summary of the Second Embodiment>

According to the second embodiment, once the second onboard device 300 successfully authenticates a navigation message using the authentication center 120, the second onboard device 300 can determine whether a navigation message newly received from the GPS satellite 2 that is the source of the successfully authenticated navigation message is authentic, based on the authenticated navigation message and the reception time stored in the memory. Therefore, the second onboard device 300 need not receive the H matrix from the authentication center 120 in terms of a newly received navigation message, reducing a communication processing load on the authentication center 120.

[0137]

When a repeater or a simulator is used, the continuity corresponding to a reception time difference is not ensured between the transmission time contained in the authenticated navigation message and the transmission time of the navigation message newly received by the second onboard device 300.

[0138]

According to the second embodiment, when the continuity corresponding to a reception time difference is absent between the transmission time contained in the authenticated navigation message and the transmission time of the

navigation message newly received by the second onboard device 300, the newly received navigation message is not determined to be authentic. Therefore, the embodiment can prevent a navigation message from being determined to be authentic when a repeater or a simulator is used, and can improve the accuracy to determine a navigation message to be authentic.

[0139]

<Fourth Modification>

There has been described the second embodiment that determines whether a received navigation message is authentic depending on whether the continuity corresponding to a reception time difference exists between the transmission time contained in the authenticated navigation message and the transmission time of a navigation message newly received by the second onboard device 300 in terms of the same GPS satellite 2. However, this is not limiting.

[0140]

For example, a configuration (hereinafter referred to as a fourth modification) may determine whether a received navigation message is authentic depending on whether the continuity exists between two pseudo-distances, namely, one pseudo-distance determined from the transmission time and the reception time of the authenticated navigation message and the other pseudo-distance determined from the transmission time and the reception time of a newly received navigation message. The fourth modification equals the second embodiment except that the controller 320 of the second onboard device 300 performs a partially different process. In detail, the fourth modification differs from the second embodiment in part of the second simplified determination process performed by the controller 320.

[0141]

<Second Simplified Determination Process in the Fourth Modification>

The controller 320 of the second onboard device 300 according to the fourth modification performs the second simplified determination process to be described with reference to a flowchart in FIG. 17. The flowchart in FIG. 17 may also start when the satellite receiver 330 of the second onboard device 300 receives a navigation message from the GPS satellite 2, for example. The flowchart in FIG. 17 may be also performed on each of navigation messages from the multiple GPS satellites 2 when the satellite receiver 330 receives the navigation messages from the GPS satellites 2 within one cycle of successive output from the satellite receiver 330 to the controller 320.

[0142]

At S101, a reception time difference is determined which is difference between the reception time of the authenticated navigation message stored in the memory of the controller 320 and the reception time of a navigation message newly received by the satellite receiver 330. The controller 320 proceeds to S102 if the reception time difference is within a specified time period (S101: YES). When the reception time difference exceeds the specified time period (S101: NO), it is determined that the navigation message newly received by the satellite receiver 330 is unauthentic and the process is ended.

[0143]

The specified time period is so estimated that the pseudo-distance determined from the transmission time of a navigation message from the GPS satellite 2 and the reception time of the navigation message at the satellite receiver 230 when a repeater duplicating a signal from the GPS satellite 2 or a simulator capable of imitatively generating a signal from the GPS satellite 2 is not used is unlikely to cause a difference greater than or equal to a threshold value

used for S105 described later. The specified time period can be set to any value.

[0144]

The pseudo-distance signifies a distance between the GPS satellite 2 and the satellite receiver 330 calculated by multiplying the light speed and the propagation time that is determined from the transmission time at the GPS satellite 2 and the reception time at the satellite receiver 330.

[0145]

The process at S102 through S104 equals that at S91 through S93. At S105, it is determined whether the continuity exists between the authenticated navigation message and the navigation message that is newly acquired by the satellite receiver 330 and is determined at S104 to contain the matching satellite number. In detail, the controller 320 determines whether the continuity exists between two pseudo-distances. One pseudo-distance is determined from the transmission time contained in the authenticated navigation message and the reception time of the authenticated navigation message. The other pseudo-distance is determined from the transmission time contained in the navigation message newly received by the satellite receiver 330 and the reception time of the navigation message. S105 also corresponds to a second continuity determination portion.

[0146]

The pseudo-distance signifies a distance between the GPS satellite 2 and the satellite receiver 330 calculated by multiplying the light speed and the propagation time that is determined from the transmission time at the GPS satellite 2 and the reception time at the satellite receiver 330.

[0147]

An example of the process at S105 will be described using FIG. 18. As

a precondition for the example in FIG. 18, the second onboard device 300 successfully authenticates a navigation message originated from the GPS satellite 2a using the authentication center 120. The second onboard device 300 thereafter receives the navigation message originated from the GPS satellite 2a.

[0148]

Pseudo-distance ρ1 is determined from the transmission time of the authenticated navigation message and the reception time of the authenticated navigation message. Pseudo-distance ρ2 is determined from the transmission time of a navigation message thereafter newly received by the satellite receiver 330 from the GPS satellite 2a and the reception time of the navigation message.

[0149]

At S105, the pseudo-distance (ρ1) is calculated by multiplying the light speed and the propagation time that is determined from the transmission time of the authenticated navigation message and the reception time of the authenticated navigation message. The pseudo-distance (ρ2) is calculated by multiplying the light speed and the propagation time that is determined from the transmission time of a navigation message newly received by the satellite receiver 330 and the reception time of the navigation message.

[0150]

The pseudo-distance (ρ2) is subtracted from the pseudo-distance (ρ1) to find the absolute value of the difference (|ρ1 - ρ2|), and it is determined whether the absolute value is smaller than a threshold value. The threshold value here approximates to the upper limit of a change in the pseudo-distance between the GPS satellite 2 and the satellite receiver 330 when a repeater or a simulator is not used. The change is supposed to occur due to a lapse of the specified time period at S101.

[0151]

If the difference is smaller than the threshold value, it is determined that there is the continuity between the authenticated navigation message and the navigation message newly received by the satellite receiver 330. If the difference is greater than or equal to the threshold value, it is determined that there is no continuity.

[0152]

At S106 in FIG. 17, when it is determined that there is the continuity between the authenticated navigation message and the navigation message newly received by the satellite receiver 330 (S106: YES), the process proceeds to S107. At S107, it is determined that the navigation message newly received by the satellite receiver 330 is authentic and the process is ended.

[0153]

The specified time period at S101 is provided as a condition that allows S106 to determine the presence and absence of the continuity for a navigation message when a repeater or a simulator is not used as above.

[0154]

When it is determined that there is no continuity between the authenticated navigation message and the navigation message newly received by the satellite receiver 330 (S106: NO), it is determined the navigation message newly received by the satellite receiver 330 is unauthentic and the process is ended. S106 and S107 also correspond to the simplified determination portion.

[0155]

<Summary of the Fourth Modification>

According to the fourth modification, like the second embodiment, once the second onboard device 300 successfully authenticates a navigation message

using the authentication center 120, the second onboard device 300 can determine whether a navigation message newly received from the GPS satellite 2 equal to the source of the successfully authenticated navigation message is authentic, based on the authenticated navigation message and the reception time stored in the memory. Therefore, the second onboard device 300 need not receive the H matrix from the authentication center 120 in terms of a newly received navigation message, reducing a communication processing load on the authentication center 120.

[0156]

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

[0157]

The fourth modification does not determine a newly received navigation message to be authentic if no continuity is found between two pseudo-distances, namely, one pseudo-distance determined from the transmission time contained in the authenticated navigation message and the reception time of the authenticated navigation message and the other pseudo-distance determined from the transmission time of a newly received navigation message and the reception time of the navigation message. The fourth modification can prevent a navigation message from being determined to be authentic when a repeater or a simulator is

used, and can improve the accuracy to determine a navigation message to be authentic.

[0158]

(Third Embodiment)

The following describes the third embodiment with reference to the appended drawings. Elements having the same functions as those illustrated in the drawings used to describe the foregoing embodiments are depicted by the same reference numerals and a description is omitted for simplicity.

[0159]

The simplified authentication system 1b according to the third embodiment equals the simplified authentication system 1b according to the second embodiment, except that the satellite receiver 330 uses a navigation message successfully authenticated by the second onboard device 300 to determine authenticity of a navigation message received from the other GPS satellite 2 at almost the same timing as that for the successfully authenticated navigation message, without access to the authentication center 120.

[0160]

<Schematic Configuration of the Simplified Authentication System 1b According to the Third Embodiment>

Similarly to the second embodiment, the simplified authentication system 1b according to the third embodiment also includes the monitor station 110, the authentication center 120, the master control station 130, the first onboard device 200, and the second onboard device 300.

[0161]

The first onboard device 200 performs the authentication-related process in FIG. 4 and the authenticated satellite information transmission process in FIG. 5.

The second onboard device 300 performs the authentication-related process in FIG. 14 as well as the first simplified determination process in FIG. 7. The second onboard device 300 performs a third simplified determination process in FIG. 19 instead of the second simplified determination process described in the second embodiment.

[0162]

The satellite receiver 330 of the second onboard device 300 cyclically outputs a navigation message received from the GPS satellite 2 within one cycle to the controller 320 of the second onboard device 300. The satellite receiver 330 may receive navigation messages from three or more GPS satellites 2 within one cycle. In this case, the satellite receiver 330 outputs the navigation messages concerning these GPS satellites 2 to the controller 320.

[0163]

The second onboard device 300 according to the third embodiment performs positioning based on navigation messages that are received by the satellite receiver 330 from three or more GPS satellites 2 within one cycle. The second onboard device 300 performs the authentication-related process until at least one of the navigation messages used for the positioning is successfully authenticated. When one navigation message is successfully authenticated, the second onboard device 300 performs the third simplified determination process to determine whether the other navigation messages are authentic, without access to the authentication center 120. The navigation messages received within one cycle may signify those received at almost the same timing.

[0164]

<Third Simplified Determination Process According to the Third Embodiment>

The controller 320 of the second onboard device 300 according to the third embodiment performs the third simplified determination process to be described with reference to a flowchart in FIG. 19. The flowchart in FIG. 19 may start when the authentication-related process successfully authenticates at least one of navigation messages used for positioning. The flowchart in FIG. 19 may be performed on each of navigation messages that are used for positioning and are not authenticated by the authentication-related process.

[0165]

At S111, of navigation messages used for positioning, an unauthenticated navigation message different from a navigation message (authenticated navigation message) successfully authenticated by the authentication-related process is acquired.

[0166]

At S112, it is determined whether there is a match between the transmission time contained in the unauthenticated navigation message acquired at S111 and the transmission time contained in the authenticated navigation message. The match here signifies not only a complete match but also an approximate match within a range of an error. The transmission time contained in the authenticated navigation message corresponds to consistency information. S112 corresponds to a consistency determination portion.

[0167]

An example of the process at S112 will be described with reference to FIG. 20. According to the example in FIG. 20, GPS satellites are used for positioning. The second onboard device 300 uses the authentication center 120 to successfully authenticate a navigation message originated from the GPS satellite 2a. A navigation message originated from the GPS satellite 2b is not

authenticated yet.

[0168]

The GPS satellite 2a originates the navigation message (i.e., authenticated navigation message) at transmission time Ti5. The GPS satellite 2b originates the navigation message (i.e., unauthenticated navigation message) at transmission time Ti6. The process at S112 determines whether there is a match between the transmission time (Ti5) of the authenticated navigation message and the transmission time (Ti6) of the unauthenticated navigation message.

[0169]

Multiple navigation messages received by the satellite receiver 330 within one cycle guarantee their transmission times to match when a repeater duplicating a signal from the GPS satellite 2 or a simulator capable of imitatively generating a signal from the GPS satellite 2 is not used.

[0170]

At S113, if it is determined that the transmission times match (S113: YES), it is determined that the unauthenticated navigation message contains the transmission time consistent with the transmission time contained in the authenticated navigation message, and the process proceeds to S114. At S114, it is determined the unauthenticated navigation message acquired at S111 is authentic and then the process is ended. If it is determined that the transmission times do not match (S113: NO), the process is ended. In this case, it is not determined that the unauthenticated navigation message acquired at S111 is authentic. S113 and S114 also correspond to the simplified determination portion.

[0171]

If the determination results in NO at S113, it may be determined that the unauthenticated navigation message acquired at S111 is unauthentic.

[0172]

In the third embodiment, for example, the third simplified determination process may be performed to reinforce a determination result from the first simplified determination process. The first simplified determination process may be performed to reinforce a determination result from the third simplified determination process. The third embodiment may also perform the second simplified determination process. In this case, the third simplified determination process may be performed to reinforce a determination result from the second simplified determination process. The second simplified determination process may be performed to reinforce a determination result from the third simplified determination process.

[0173]

<Summary of the Third Embodiment>

According to the third embodiment, when the second onboard device 300 successfully authenticates one of navigation messages used for positioning by using the authentication center 120, the other navigation messages used for positioning can be determined to be authentic or unauthentic based on the transmission times. Therefore, the second onboard device 300 need not receive the H matrix from the authentication center 120 in terms of the other navigation messages used for positioning, reducing a communication processing load on the authentication center 120.

[0174]

The transmission times of the navigation messages used for positioning match when no repeater or simulator is used. The third embodiment determines

a navigation message to be authentic or unauthentic based on whether the transmission time matches the successfully authenticated navigation message. Therefore, the third embodiment can prevent a navigation message from being determined to be authentic when a repeater or a simulator is used. Therefore, the third embodiment can improve the accuracy to determine a navigation message to be authentic.

<Fifth Modification>

There has been described the third embodiment that determines an unauthenticated navigation message to be authentic or unauthentic based on whether, of the navigation messages used for positioning, the transmission time contained in the authenticated navigation message matches the transmission time contained in the unauthenticated navigation message. However, this is not limiting.

[0175]

For example, there may be a configuration (fifth modification) that determines an unauthenticated navigation message to be authentic or unauthentic based on where there is a match between satellite positions. Of the satellite positions, one satellite position is determined from orbit information about the GPS satellite 2 contained in the authenticated navigation message and the transmission time contained in the authenticated navigation message. Another satellite position is determined from orbit information about the GPS satellite 2 contained in the unauthenticated navigation message and the transmission time contained in the unauthenticated navigation message. The fifth modification equals the third embodiment except a partial difference in the process on the controller 320 of the second onboard device 300. In detail, the fifth modification differs from the third embodiment in part of the third simplified determination

process the controller 320 performs.

[0176]

As publicly known, a navigation message contains ephemeris data and almanac data. The almanac data contains the orbit information about not only the GPS satellite 2 that is a source of the navigation message but also all GPS satellites 2 in orbit. Satellite positions of all the GPS satellites 2 can be calculated from the orbit information and the transmission time of the navigation message. The ephemeris data contains the orbit information about the GPS satellite 2 that is a source of the navigation message. A satellite position of the GPS satellite 2 that is a source of this navigation message can be calculated more accurately from the orbit information and the transmission time of the navigation message.

[0177]

The fifth modification uses, of the orbit information contained in the almanac data and the ephemeris data, the orbit information contained in the almanac data. The orbit information contained in the almanac data is hereinafter simply referred to as the orbit information.

[0178]

<Third Simplified Determination Process According to the Fifth Modification>

The controller 320 of the second onboard device 300 according to the fifth modification performs the third simplified determination process to be described with reference to a flowchart in FIG. 21. The flowchart in FIG. 21 may also start when the authentication-related process successfully authenticates at least one of navigation messages used for positioning. The flowchart in FIG. 21 may be also performed on each of navigation messages that are used for

positioning and are not authenticated by the authentication-related process.

[0179]

According to the example in FIG. 21, the GPS satellite 2a represents the GPS satellite 2 that is a source of an authenticated navigation message.

[0180]

At S121, like S111 above, an unauthenticated navigation message except the authenticated navigation message out of navigation messages used for positioning is acquired.

[0181]

At S122, a position of the GPS satellite 2a is calculated using the transmission time contained in the authenticated navigation message used for positioning and the orbit information about the GPS satellite 2a contained in the authenticated navigation message. The transmission time and the orbit information correspond to satellite position calculation information.

[0182]

At S123, a position of the GPS satellite 2a is calculated using the transmission time contained in the unauthenticated navigation message used for positioning and the orbit information about the GPS satellite 2a contained in the unauthenticated navigation message. The description below explains why a satellite position of the GPS satellite 2a can be calculated from the orbit information contained in the unauthenticated navigation message received from the GPS satellite 2 other than the GPS satellite 2a that is a source of the authenticated navigation message. The GPS satellite 2 other than the GPS satellite 2a that is a source of the authenticated navigation message corresponds to an unauthenticated satellite.

[0183]

The orbit information contained in the almanac data also contains the orbit information about the GPS satellite 2a other than the GPS satellite 2 that is a source of the unauthenticated navigation message. As above, multiple navigation messages received by the satellite receiver 330 within one cycle guarantee their transmission times to match when the repeater or the simulator is not used. Therefore, a satellite position of the GPS satellite 2a can be calculated also from the transmission time and the orbit information contained in the unauthenticated navigation message.

[0184]

At S124, it is determined whether there is a match between the satellite position of the GPS satellite 2a calculated at S122 and the satellite position of the GPS satellite 2a calculated at S123. The match here signifies not only a complete match but also an approximate match within a range of an error. S124 corresponds to the consistency determination portion.

[0185]

The transmission times of the unauthenticated navigation message and the authenticated navigation message used for positioning are supposed to match when the repeater or the simulator is not used. The satellite position of the GPS satellite 2a is calculated from the transmission time and the orbit information contained in the authenticated navigation message. Therefore, the same satellite position as the satellite position of the GPS satellite 2a can be calculated from the transmission time and the orbit information contained in the unauthenticated navigation message when the repeater or the simulator is not used. Therefore, the satellite position of the GPS satellite 2a calculated at S122 matches the satellite position of the GPS satellite 2a calculated at S123 when the repeater or the simulator is not used.

[0186]

When it is determined at S125 that the satellite positions match (S125: YES), it is determined that the unauthenticated navigation message contains the orbit information and the transmission time consistent with the orbit information and the transmission time contained in the authenticated navigation message, and the process proceeds to S126. At S126, it is determined that the unauthenticated navigation message acquired at S121 is authentic, and then the process is ended. When it is determined that the satellite positions do not match (S125: NO), it is determined that the unauthenticated navigation message acquired at S121 is unauthentic, and the process is ended. S113 and S114 also correspond to the simplified determination portion.

[0187]

If the determination results in NO at S125, it may be determined that the unauthenticated navigation message acquired at S121 is unauthentic.

[0188]

In the fifth modification, for example, the third simplified determination process may be performed to reinforce a determination result from the first simplified determination process. The first simplified determination process may be performed to reinforce a determination result from the third simplified determination process. The fifth modification may also perform the second simplified determination process. In this case, the third simplified determination process may be performed to reinforce a determination result from the second simplified determination process. The second simplified determination process may be performed to reinforce a determination result from the third simplified determination process.

[0189]

<Summary of the Fifth Modification>

According to the fifth modification similarly to the third embodiment, when the second onboard device 300 successfully authenticates one of navigation messages used for positioning by using the authentication center 120, the other navigation messages used for positioning can be determined to be authentic or unauthentic based on a satellite position calculated from the orbit information and the transmission time. Therefore the second onboard device 300 need not receive the H matrix from the authentication center 120 in terms of the other navigation messages used for positioning, reducing a communication processing load on the authentication center 120.

[0190]

The use of a repeater or a simulator causes a difference between transmission times contained in the navigation messages used for positioning and consequently a difference between satellite positions of the same GPS satellite 2 calculated from the transmission time and the orbit information. The third embodiment determines a navigation message to be authentic or unauthentic based on whether the satellite position matches the successfully authenticated navigation message. Therefore, the fifth embodiment can prevent a navigation message from being determined to be authentic when a repeater or a simulator is used, and accordingly, the fifth embodiment can improve the accuracy to determine a navigation message to be authentic.

[0191]

The fifth modification has described the example in which a satellite position of the GPS satellite 2a that is a source of an authenticated navigation message is used for the match between satellite positions. Alternatively, a satellite position of the GPS satellite 2 other than the GPS satellite 2a may be

used as long as the GPS satellite 2 is a source of a navigation message used for positioning.

[0192]

<Sixth Modification>

There has been described the embodiment that uses only navigation messages received from the GPS satellite 2 for positioning. However, a navigation message received from the QZS satellite 3 may be used for positioning. In this case, the navigation message received from the QZS satellite 3 may be also authenticated similarly to the case of the GPS satellite 2.

[0193]

An example of the sixth modification is to generate a RAND message from the navigation message that the monitor station 110 receives from the QZS satellite 3. The authentication center 120 generates parity data based on the RAND message. The generated parity data is transmitted to the master control station 130. The master control station 130 transmits the parity data to the QZS satellite 3. The QZS satellite 3 broadcasts a navigation message containing the parity data to the earth.

[0194]

The first onboard device 200 or the second onboard device 300 according to the second or subsequent embodiments may generate a RAND message from the navigation message received from the QZS satellite 3. The first onboard device 200 or the second onboard device 300 may generate comparison parity data from the RAND message and the H matrix acquired from the authentication center 120. The first onboard device 200 or the second onboard device 300 may authenticate navigation messages by comparing the generated comparison parity data with the parity data received from the QZS

satellite 3.

[0195]

<Seventh Modification>

Although the authentication method in the above embodiment is of a type of authenticating a navigation message, this is a mere example. As long as an authentication method is of a type requiring an access to a certification organization, other configurations may be employed in the authentication method (seventh modification).

[0196]

<Eighth Embodiment>

Although the above embodiment illustrates the first onboard device 200 and the second onboard device 300 used for vehicles, this is not limiting. For example, a navigation message reception device comparable to the first onboard device 200 or the second onboard device 300 may be applied to a mobile terminal carried by a user.

[0197]

Although embodiments and the configurations have been illustrated, embodiments and the configurations of the present disclosure are not limited to those illustrated above. For example, the scope of embodiments and configurations according to the present disclosure also includes an embodiment and a configuration resulting from any combination of technical elements disclosed in different embodiments and configurations.

CLAIMS

1. A navigation message reception device comprising:

a satellite receiver for receiving a navigation message from an artificial satellite used for a satellite positioning system;

a satellite information acquisition portion for acquiring authenticated satellite information from a positioning device that performs authentication by receiving authentication information corresponding to a navigation message received from the artificial satellite, wherein the authenticated satellite information is information about the artificial satellite that is a source of the successfully authenticated navigation message; and

a simplified determination portion for determining whether the navigation message received by the satellite receiver is authentic, by using the authenticated satellite information acquired by the satellite information acquisition portion.

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

the navigation message contains identification information for identifying the artificial satellite;

the authenticated satellite information contains identification information for identifying the artificial satellite that is a source of the successfully authenticated navigation message;

the simplified determination portion determines that the navigation message received by the satellite receiver is authentic when the identification information contained in the navigation message received by the

satellite receiver matches the identification information contained in the authenticated satellite information acquired by the satellite information acquisition portion; and

the simplified determination portion does not determine that the navigation message received by the satellite receiver is authentic when the identification information contained in the navigation message received by the satellite receiver does not match the identification information contained in the authenticated satellite information acquired by the satellite information acquisition portion.

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

the authenticated satellite information contains a transmission time at which the artificial satellite originates the successfully authenticated navigation message, and a reception time at which the positioning device receives the successfully authenticated navigation message,

the navigation message reception device further comprising:

a first continuity determination portion for determining whether the transmission time contained in the authenticated satellite information acquired by the satellite information acquisition portion and the transmission time contained in the navigation message received by the satellite receiver from the artificial satellite that is the source of the successfully authenticated navigation message have there between continuity that corresponds to a reception time difference which is a difference between a navigation message reception time contained in the authenticated satellite information and a reception time of the navigation message by the satellite receiver from the artificial satellite that is the

source of the successfully authenticated navigation message,

wherein:

when the first continuity determination portion determines that there is the continuity, the simplified determination portion determines that the navigation message received by the satellite receiver is authentic; and

when the first continuity determination portion determines that there is no continuity, the simplified determination portion does not determine that the navigation message received by the satellite receiver is authentic.

4. The navigation message reception device according to claim 1 or 2, further comprising:

an authentication information receiver for receiving the authentication information from the authentication center;

a center usage authentication portion for authenticating the navigation message received by the satellite receiver using the authentication information received by the authentication information receiver; and

a second continuity determination portion for determining whether there is continuity between the navigation message successfully authenticated by the center usage authentication portion and a new navigation message that the satellite receiver receives from the artificial satellite that is the source of the navigation message successfully authenticated by the center usage authentication portion,

wherein:

when the second continuity determination portion determines that there is the continuity, the simplified determination portion determines that the navigation message received by the satellite receiver is

authentic; and

when the second continuity determination portion determines that there is no continuity, the simplified determination portion does not determine that the navigation message received by the satellite receiver is authentic.

5. The navigation message reception device according to claim 4, wherein:

the navigation message contains a transmission time thereof; and

the second continuity determination portion determines whether a transmission time contained in the navigation message successfully authenticated by the center usage authentication portion and a transmission time contained in the new navigation message have there between continuity that corresponds to a reception time difference between a reception time of the successfully authenticated navigation message and a reception time of the new navigation message.

6. The navigation message reception device according to claim 4, wherein:

the navigation message contains a transmission time thereof;

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

the second continuity determination portion determines that there is the continuity between the navigation message successfully authenticated by the center usage authentication portion and the new navigation message when a

difference between a pseudo-distance determined from the transmission time and the reception time of the navigation message successfully authenticated by the center usage authentication portion and a pseudo-distance determined from the transmission time and the reception time of the new navigation message is smaller than a threshold value.

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

the navigation message contains consistency information ensuring consistency between a plurality of the artificial satellites,

the navigation message reception device further comprising:

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

a center usage authentication portion for authenticating the navigation message received by the satellite receiver using the authentication information received by the authentication information receiver according to the navigation message; and

a consistency determination portion for determining whether information ensuring consistency with the consistency information contained in the navigation message successfully authenticated by the center usage authentication portion is contained in a navigation message received by the satellite receiver from an unauthenticated satellite, wherein the unauthenticated satellite is the artificial satellite other than the source of the navigation message successfully authenticated by the center usage authentication portion,

wherein:

when the consistency determination portion determines that the information ensuring the consistency is contained in the navigation message received from the unauthenticated satellite, the simplified determination portion determines that the navigation message received by the satellite receiver is authentic; and

when the consistency determination portion determines that the information ensuring the consistency is not contained in the navigation message received from the unauthenticated satellite, the simplified determination portion does not determine that the navigation message received by the satellite receiver is authentic.

8. The navigation message reception device according to claim 7, wherein:

the consistency information is a transmission time thereof; and

based on whether there is a match between a transmission time contained in the navigation message successfully authenticated by the center usage authentication portion and a transmission time contained in the navigation message received by the satellite receiver from the unauthenticated satellite, the consistency determination portion determines whether the information ensuring the consistency is contained.

9. The navigation message reception device according to claim 7, wherein:

the navigation message contains satellite position calculation information enabling to calculate satellite positions of not only the artificial satellite that is a source of the navigation message but also another artificial satellite;

the consistency information is the satellite position calculation information; and

based on whether there is a match between a satellite position of the unauthenticated satellite calculated from the satellite position calculation information contained in the navigation message successfully authenticated by the center usage authentication portion and a satellite position of the unauthenticated satellite calculated from the satellite position calculation information contained in a navigation message received by the satellite receiver from the unauthenticated satellite, the consistency determination portion determines whether the information ensuring the consistency is contained.

10. A simplified authentication system comprising:

a first navigation message reception device used for a first mobile object;

a roadside device arranged to a road; and

a second navigation message reception device used for a second mobile object,

wherein the first navigation message reception device includes:

a first satellite receiver for receiving a navigation message from an artificial satellite used for a satellite positioning system;

an authentication information receiver for receiving, from an authentication center, authentication information corresponding to the navigation message received by the first satellite receiver;

a center usage authentication portion for authenticating whether the navigation message received by the first satellite receiver is authentic, by using the authentication information received by the authentication information

receiver; and

a satellite information transmitter for transmitting authenticated satellite information, wherein the authenticated satellite information is information about the artificial satellite that is a source of the navigation message successfully authenticated by the center usage authentication portion,

wherein the roadside device includes:

a satellite information receiver for receiving the authenticated satellite information transmitted from the satellite information transmitter;

an accumulation portion for accumulating the authenticated satellite information received by the satellite information receiver; and

a delivery portion for delivering information accumulated in the accumulation portion,

wherein the second navigation message reception device includes:

a second satellite receiver for receiving a navigation message from an artificial satellite used for the satellite positioning system;

a satellite information acquisition portion for acquiring the authenticated satellite information by receiving the authenticated satellite information delivered from the delivery portion of the roadside device; and

a simplified determination portion for determining whether the navigation message received by the satellite receiver is authentic, by using the authenticated satellite information acquired by the satellite information acquisition portion.