US Patent & Trademark Office
Patent Public Search | Text View

United States Patent	12395840
Kind Code	B2
Date of Patent	August 19, 2025
Inventor(s)	Suyama; Yojiro et al.

Relay device and vehicle communication method

Abstract

A relay device mounted to a vehicle includes a plurality of function units. The relay device includes: an authentication processing unit configured to acquire authentication information of a function unit from an external device outside the vehicle, and perform an authentication process regarding the function unit by using the acquired authentication information; and a relay processing unit configured to, on the basis of a result of the authentication process performed by the authentication processing unit, relay information between the function unit and another function unit. When a validity time limit of the authentication information has expired, the authentication processing unit acquires, from the external device, the authentication information that is new.

Inventors:	**Suyama; Yojiro (Osaka, JP), Yabuuchi; Yasuhiro (Yokkaichi, JP), Go; Darmawan (Yokkaichi, JP), Shimizu; Yosuke (Yokkaichi, JP), Hagihara; Takeshi (Yokkaichi, JP)**

Applicant:	**SUMITOMO ELECTRIC INDUSTRIES, LTD.** (Osaka, JP);
	SUMITOMO WIRING SYSTEMS, LTD. (Yokkaichi, JP);
	AUTONETWORKS TECHNOLOGIES, LTD. (Yokkaichi, JP)

Family ID:	**1000008762280**

Assignee:	**SUMITOMO ELECTRIC INDUSTRIES, LTD. (Osaka, JP);
	SUMITOMO WIRING SYSTEMS, LTD. (Mie, JP);
	AUTONETWORKS TECHNOLOGIES, LTD. (Mie, JP)**

Appl. No.:	**17/624784**
Filed (or PCT Filed):	**June 11, 2020**
PCT No.:	**PCT/JP2020/022988**
PCT Pub. No.:	**WO2021/005949**
PCT Pub. Date:	January 14, 2021

Prior Publication Data

Document Identifier	Publication Date
US 20220264293 A1	Aug. 18, 2022

Foreign Application Priority Data

JP	2019-126255	Jul. 05, 2019

Publication Classification

Int. Cl.: **H04W12/06** (20210101); **G07C5/00** (20060101); **H04W4/40** (20180101); **H04W76/10** (20180101)

U.S. Cl.:

CPC **H04W12/06** (20130101); **G07C5/008** (20130101); **H04W4/40** (20180201); **H04W76/10** (20180201);

Field of Classification Search

CPC: H04W (12/06); H04W (4/40); H04W (76/10); G07C (5/008)

USPC: 726/4

References Cited

U.S. PATENT DOCUMENTS

Patent No.	Issued Date	Patentee Name	U.S. Cl.	CPC
2002/0146002	12/2001	Sato	N/A	N/A
2007/0185624	12/2006	Duddles et al.	N/A	N/A
2008/0059806	12/2007	Kishida et al.	N/A	N/A
2010/0002710	12/2009	Isoyama	N/A	N/A
2010/0302974	12/2009	Niiyama et al.	N/A	N/A
2010/0313242	12/2009	Sato	N/A	N/A
2012/0054835	12/2011	Oda et al.	N/A	N/A
2012/0277949	12/2011	Ghimire et al.	N/A	N/A
2013/0010640	12/2012	Higuchi et al.	N/A	N/A
2014/0068099	12/2013	Komori	709/236	H04L 45/745
2015/0145648	12/2014	Winkelman	N/A	N/A
2015/0172298	12/2014	Otsuka	N/A	N/A
2016/0315766	12/2015	Ujiie et al.	N/A	N/A
2016/0373449	12/2015	Haga et al.	N/A	N/A
2017/0134164	12/2016	Haga et al.	N/A	N/A
2017/0331767	12/2016	Zinner	N/A	N/A
2017/0352210	12/2016	Maiwand	N/A	G07C 9/00571
2018/0009446	12/2017	Ricci	N/A	H04W 4/46
2018/0077062	12/2017	Park et al.	N/A	N/A
2018/0115490	12/2017	Kawasaki	N/A	H04L 7/2441

2018/0367546	12/2017	Miyashita	N/A	N/A
2019/0044730	12/2018	Woo et al.	N/A	N/A
2019/0173912	12/2018	Ujiie et al.	N/A	N/A
2019/0197468	12/2018	Endo	N/A	G06Q 10/0832
2019/0334897	12/2018	Anzai et al.	N/A	N/A
2019/0356608	12/2018	Tanaka et al.	N/A	N/A
2019/0394065	12/2018	Okubo et al.	N/A	N/A
2020/0029213	12/2019	Nölscher et al.	N/A	B60R 25/24
2020/0084025	12/2019	Ujiie et al.	N/A	N/A
2020/0106704	12/2019	Iwata et al.	N/A	N/A
2020/0137049	12/2019	Ogawa et al.	N/A	N/A
2020/0220716	12/2019	Haga et al.	N/A	N/A
2020/0366529	12/2019	Park	N/A	H04L 69/22
2021/0028925	12/2020	Ujiie et al.	N/A	N/A
2021/0329002	12/2020	Huh	N/A	G06F 21/32

FOREIGN PATENT DOCUMENTS

Patent No.	Application Date	Country	CPC
102333118	12/2011	CN	N/A
106961436	12/2016	CN	N/A
2002-314573	12/2001	JP	N/A
2003-046536	12/2002	JP	N/A
2003-244185	12/2002	JP	N/A
2008-059450	12/2007	JP	N/A
2010-183204	12/2009	JP	N/A
2010-283607	12/2009	JP	N/A
2013-017021	12/2012	JP	N/A
2013-193598	12/2012	JP	N/A
2016-127299	12/2015	JP	N/A
2016-134170	12/2015	JP	N/A
2016-152429	12/2015	JP	N/A
2017-005617	12/2016	JP	N/A
2017-059210	12/2016	JP	N/A
2017-212728	12/2016	JP	N/A
2017-220220	12/2016	JP	N/A
2018-117254	12/2017	JP	N/A
2018113505	12/2017	JP	N/A
2018-152758	12/2017	JP	N/A
2018-174481	12/2017	JP	N/A
2018-192876	12/2017	JP	N/A
2019-016247	12/2018	JP	N/A
2013/161873	12/2012	WO	N/A
2016/075865	12/2015	WO	N/A
2016/075869	12/2015	WO	N/A
2016/204081	12/2015	WO	N/A

OTHER PUBLICATIONS

Sep. 7, 2023 U.S. Office Action issued U.S. Appl. No. 17/615,174. cited by applicant
The U.S. Appl. No. 17/615,174, filed Nov. 30, 2021 in the name of Yusuke Yamamoto et al. cited by applicant

The U.S. Appl. No. 17/612,136, filed Nov. 17, 2021 in the name of Yusuke Yamamoto et al. cited by applicant
The U.S. Appl. No. 17/622,892, filed Dec. 27, 2021 in the name of Yojiro Suyama et al. cited by applicant
Jun. 28, 2023 Office Action issued in U.S. Appl. No. 17/622,892. cited by applicant
Feb. 15, 2023 Office Action issued in U.S. Appl. No. 17/622,892. cited by applicant
Oct. 20, 2023 Notice of Allowance issued in U.S. Appl. No. 17/622,892. cited by applicant
Mar. 16, 2023 Office Action Issued In U.S. Appl. No. 17/615,174. cited by applicant
Apr. 10, 2024 Office Action issued in U.S. Appl. No. 17/615,174. cited by applicant
Apr. 15, 2024 Office Action issued in U.S. Appl. No. 17/612,136. cited by applicant
Jan. 4, 2024 Office Action issued in U.S. Appl. No. 17/612,136. cited by applicant
Apr. 26, 2024 Notice of Allowance issued in U.S. Appl. No. 17/622,892. cited by applicant
Aug. 30, 2024 Office Action issued in U.S. Appl. No. 18/403,973. cited by applicant
Sep. 29, 2024 Office Action issued in U.S. Appl. No. 17/612,136. cited by applicant
Oct. 23, 2024 Office Action issued in U.S. Appl. No. 17/615,174. cited by applicant
Dec. 9, 2024 Notice of Allowance issued in U.S. Appl. No. 18/403,973. cited by applicant
Jan. 10, 2025 Ex-Parte Quayle Action issued in U.S. Appl. No. 17/615,174. cited by applicant
Jan. 27, 2025 Notice of Allowance issued in U.S. Appl. No. 17/612,136. cited by applicant
Feb. 26, 2025 Notice of Allowance issued in U.S. Appl. No. 17/615,174. cited by applicant
May 15, 2025 Notice of Allowance received in U.S. Appl. No. 18/403,973. cited by applicant
May 20, 2025 Notice of Allowance issued in U.S. Appl. No. 17/612,136. cited by applicant
U.S. Appl. No. 18/403,973, filed May 15, 2025, in the name of Yamamoto. cited by applicant

Primary Examiner: Jean; Frantz B

Attorney, Agent or Firm: Oliff PLC

Background/Summary

TECHNICAL FIELD
(1) The present disclosure relates to a relay device and a vehicle communication method.
(2) This application claims priority on Japanese Patent Application No. 2019-126255 filed on Jul. 5, 2019, the entire content of which is incorporated herein by reference.
BACKGROUND ART
(3) PATENT LITERATURE 1 (Japanese Laid-Open Patent Publication No. 2013-193598) discloses a vehicle authentication device as below. That is, the vehicle authentication device is a vehicle authentication device (**11**) mounted to a vehicle and provided to an electronic control device (**1**) connected via an in-vehicle network to an in-vehicle communication device (**2**) that can perform communication by using an internet protocol with an external device (**3**) outside the vehicle, through at least a wireless manner out of a wireless manner or a wired manner. The vehicle authentication device (**11**) includes: identification information acquisition means (**11**, S**1**) that, when information including identification information for specifying the external device has been transmitted from the external device to the communication device, acquires this identification information; state determination means (**11**, S**5**) that determines whether or not the state of the vehicle corresponds to a security securing state, which is a state where an authentic user whose operation of the vehicle is permitted operates or has operated the vehicle; registration means (**11**, S**7**) that registers the identification information acquired by the identification information acquisition means into a storage device (**12**) mounted to the vehicle, when the state determination

means has determined that the state of the vehicle corresponds to the security securing state, and that does not register the identification information into the storage device when the state determination means has determined that the state of the vehicle does not correspond to the security securing state; registration determination means (**11**, S**2**) that determines, when identification information has been acquired by the identification information acquisition means, whether or not the identification information has been registered in the storage device; and authentication means (**11**, S**3**, S**6**) that, when the registration determination means has determined that the identification information has been registered in the storage device, permits exchange of information between the electronic control device and the external device specified by the identification information, and that prohibits exchange of information between the electronic control device and the external device specified by the identification information, on the basis of a fact that the registration determination means has determined that the identification information has not been registered in the storage device.

CITATION LIST

Patent Literature

(4) PATENT LITERATURE 1: Japanese Laid-Open Patent Publication No. 2013-193598

SUMMARY OF INVENTION

(5) A relay device of the present disclosure is mounted to a vehicle including a plurality of function units. The relay device includes: an authentication processing unit configured to acquire authentication information of a function unit from an external device outside the vehicle, and perform an authentication process regarding the function unit by using the acquired authentication information; and a relay processing unit configured to, on the basis of a result of the authentication process performed by the authentication processing unit, relay information between the function unit and another function unit. When a validity time limit of the authentication information has expired, the authentication processing unit acquires, from the external device, the authentication information that is new.

(6) A vehicle communication method of the present disclosure is to be performed in a relay device mounted in a vehicle including a plurality of function units. The vehicle communication method includes the steps of: acquiring authentication information of a function unit from an external device outside the vehicle; performing an authentication process regarding the function unit by using the acquired authentication information; relaying, on the basis of a result of the authentication process, information between the function unit and another function unit; and acquiring, when a validity time limit of the authentication information has expired, the authentication information that is new, from the external device.

(7) One mode of the present disclosure can be realized as a semiconductor integrated circuit that realizes a part or the entirety of the relay device or can be realized as a system that includes the relay device. One mode of the present disclosure can be realized as a program for causing a computer to execute process steps performed in the relay device.

Description

BRIEF DESCRIPTION OF DRAWINGS

(1) FIG. **1** shows a configuration of a communication system according to an embodiment of the present disclosure.

(2) FIG. **2** shows a configuration of an in-vehicle communication system according to the embodiment of the present disclosure.

(3) FIG. **3** shows a configuration of an in-vehicle ECU according to the embodiment of the present disclosure.

(4) FIG. **4** shows a configuration of a relay device according to the embodiment of the present

disclosure.

(5) FIG. **5** is a flow chart describing an operation procedure according to which the relay device in the communication system according to the embodiment of the present disclosure relays information between in-vehicle ECUs on the basis of a result of an authentication process.

(6) FIG. **6** shows an example of a sequence of an extra-vehicular authentication process performed in the communication system according to the embodiment of the present disclosure.

(7) FIG. **7** shows an example of a sequence of an extra-vehicular authentication process and an intra-vehicular authentication process performed in the communication system according to the embodiment of the present disclosure.

(8) FIG. **8** shows an example of a sequence of the intra-vehicular authentication process performed in the communication system according to the embodiment of the present disclosure.

(9) FIG. **9** shows another example of a sequence of the extra-vehicular authentication process and the intra-vehicular authentication process performed in the communication system according to the embodiment of the present disclosure.

DESCRIPTION OF EMBODIMENTS

(10) To date, in-vehicle network systems for improving security in in-vehicle networks have been developed.

Problems to be Solved by the Present Disclosure

(11) A technology that exceeds the technology described in PATENT LITERATURE 1 and that can improve security in in-vehicle networks is desired.

(12) The present disclosure has been made in order to solve the above problem. An object of the present disclosure is to provide a relay device and a vehicle communication method that are capable of improving security in an in-vehicle network.

Effects of the Present Disclosure

(13) According to the present disclosure, security in the in-vehicle network can be improved.

DESCRIPTION OF EMBODIMENT OF THE PRESENT DISCLOSURE

(14) First, the contents of an embodiment of the present disclosure are listed and described.

(15) (1) A relay device according to an embodiment of the present disclosure is mounted to a vehicle including a plurality of function units. The relay device includes: an authentication processing unit configured to acquire authentication information of a function unit from an external device outside the vehicle, and perform an authentication process regarding the function unit by using the acquired authentication information; and a relay processing unit configured to, on the basis of a result of the authentication process performed by the authentication processing unit, relay information between the function unit and another function unit. When a validity time limit of the authentication information has expired, the authentication processing unit acquires, from the external device, the authentication information that is new.

(16) Thus, with the configuration in which authentication information of a function unit is acquired from the external device outside the vehicle, even when a new unknown function unit has been added to the in-vehicle network, the authentication information of the function unit can be acquired. Further, when the validity time limit has expired, new authentication information is acquired, the authentication process regarding the function unit is performed by using the acquired authentication information, and on the basis of the result of the authentication process, information between function units is relayed. With this configuration, security in the in-vehicle network can be ensured. In addition, even in a situation where the communication environment between the relay device and the external device is bad due to the traveling environment of the vehicle and it is difficult to acquire new authentication information from the external device, the authentication process regarding the function unit can be performed by continuously using the authentication information. Therefore, security in the in-vehicle network can be improved.

(17) (2) Preferably, when the validity time limit of the authentication information has expired and the relay device is not able to communicate with the external device, the authentication processing

unit performs an extension process of maintaining validity of the authentication information, and performs, by using extended authentication information being the authentication information of which the validity has been maintained, an authentication process regarding the function unit corresponding to the authentication information.

(18) With this configuration, even in a case where, when the validity time limit of the authentication information has expired, the communication environment between the relay device and the external device is bad due to the traveling environment of the vehicle and new authentication information cannot be acquired, it is possible to perform an authentication process and continue relay of information between function units based on the authentication result. Accordingly, for example, in a configuration in which security is improved by updating the content of the authentication information at the outside of the vehicle, it is possible to manage stable communication in the in-vehicle network, irrespective of the traveling environment of the vehicle.

(19) (3) Preferably, the relay processing unit determines, in accordance with a type of the function unit, a content of information that should be relayed when the authentication process using the extended authentication information by the authentication processing unit has been successful.

(20) With this configuration, a part of information to be relayed when the extension process has been performed can be restricted in accordance with the type of the function unit. Therefore, for example, by continuing relay of information between function units that will influence traveling of the vehicle, and at the same time, by stopping relay of information between function units that will not influence traveling of the vehicle, it is possible to suppress decrease in security in the in-vehicle network while maintaining favorable traveling of the vehicle.

(21) (4) Preferably, the relay processing unit determines, in accordance with a type of information received from the function unit, whether or not to perform relay when the authentication process using the extended authentication information by the authentication processing unit has been successful.

(22) With this configuration, a part of information to be relayed when the extension process has been performed can be restricted in accordance with the type of information received from the function unit. Therefore, for example, by continuing relay of information that will influence traveling of the vehicle, and at the same time, by stopping relay of information that will not influence traveling of the vehicle, it is possible to suppress decrease in security in the in-vehicle network while maintaining favorable traveling of the vehicle.

(23) (5) Preferably, the authentication processing unit acquires, from the external device, the authentication information that has a content that is different every time the authentication information is acquired.

(24) With this configuration, every time the validity time limit has expired, authentication information that has a new content can be acquired, and an authentication process regarding the function unit can be performed by using the authentication information. Therefore, security in the in-vehicle network can be further improved.

(25) (6) Preferably, when the vehicle is traveling in a state where communication between the relay device and the external device is possible and where the validity time limit of the authentication information has expired, the authentication processing unit performs an extension process of maintaining validity of the authentication information without acquiring, from the external device, the authentication information that is new.

(26) With this configuration, for example, a situation where an authentication error occurs as a result of performing an authentication process by using new authentication information, and relay of a part or all of information between function units is stopped during traveling of the vehicle, can be avoided. Thus, favorable traveling of the vehicle can be maintained.

(27) (7) A vehicle communication method according to an embodiment of the present disclosure is to be performed in a relay device mounted in a vehicle including a plurality of function units. The vehicle communication method includes the steps of: acquiring authentication information of a

function unit from an external device outside the vehicle; performing an authentication process regarding the function unit by using the acquired authentication information; relaying, on the basis of a result of the authentication process, information between the function unit and another function unit; and acquiring, when a validity time limit of the authentication information has expired, the authentication information that is new, from the external device.

(28) Thus, with the method in which authentication information of a function unit is acquired from the external device outside the vehicle, even when a new unknown function unit has been added to the in-vehicle network, the authentication information of the function unit can be acquired. Further, when the validity time limit has expired, new authentication information is acquired, the authentication process regarding the function unit is performed by using the acquired authentication information, and on the basis of the result of the authentication process, information between function units is relayed. With this method, security in the in-vehicle network can be ensured. In addition, even in a situation where the communication environment between the relay device and the external device is bad due to the traveling environment of the vehicle and it is difficult to acquire new authentication information from the external device, the authentication process regarding the function unit can be performed by continuously using the authentication information. Therefore, security in the in-vehicle network can be improved.

(29) Hereinafter, an embodiment of the present disclosure will be described with reference to the drawings. In the drawings, the same or corresponding parts are denoted by the same reference signs, and description thereof is not repeated. At least some parts of the embodiment described below may be combined as desired.

(30) [Communication System]

(31) FIG. **1** shows a configuration of a communication system according to an embodiment of the present disclosure.

(32) With reference to FIG. **1**, a communication system **401** includes a server **181** and an in-vehicle communication system **301**. The in-vehicle communication system **301** is mounted to a vehicle **1**.

(33) FIG. **2** shows a configuration of the in-vehicle communication system according to the embodiment of the present disclosure.

(34) With reference to FIG. **2**, the in-vehicle communication system **301** includes in-vehicle ECUs (Electronic Control Units) **200**A to **200**D and a relay device **100**.

(35) Hereinafter, each of the in-vehicle ECUs **200**A to **200**D will also referred to as an in-vehicle ECU **200**. The in-vehicle ECU **200** and the relay device **100** are an example of an in-vehicle device.

(36) The in-vehicle communication system **301** need not necessarily be provided with four in-vehicle ECUs **200** and may be provided with three or less or five or more in-vehicle ECUs **200**. The in-vehicle communication system **301** need not necessarily be provided with one relay device **100** and may be provided with two or more relay devices **100**.

(37) Each in-vehicle ECU **200** and the relay device **100** form an in-vehicle network **12**. The in-vehicle ECU **200** is an example of a function unit in the in-vehicle network **12**.

(38) In the in-vehicle network **12**, the in-vehicle ECU **200** is connected to the relay device **100** via an Ethernet (registered trademark) cable **13**.

(39) The relay device **100** is a switch device, for example, and can relay information between a plurality of in-vehicle ECUs **200** connected to the relay device **100**. More specifically, the relay device **100** can perform a relay process according to a layer **2**, and a layer **3**, which is of a higher order than the layer **2**, for example.

(40) The in-vehicle ECU **200**A is a TCU (Telematics Communication unit), for example. Hereinafter, the in-vehicle ECU **200**A will also be referred to as a TCU **200**A.

(41) The in-vehicle ECUs **200**B to **200**D are an automated driving ECU (Electronic Control Unit), a sensor, a navigation device, an accelerator control ECU, a brake control ECU, a steering control ECU, a human machine interface, and the like, for example.

(42) For example, the in-vehicle ECU **200**D is not connected to the relay device **100** in the initial state. For example, at any of a manufacturing factory for the vehicle **1**, a dealer for the vehicle **1**, a retailer for replacement parts for the vehicle **1**, etc., the in-vehicle ECU **200**D is mounted to the vehicle **1** and connected to the relay device **100** via an Ethernet cable.

(43) The relay device **100** performs a relay process of an Ethernet frame in accordance with an Ethernet communication standard. Specifically, the relay device **100** relays an Ethernet frame that is sent and received between in-vehicle ECUs **200**, for example. An IP packet is stored in the Ethernet frame.

(44) The configuration of the in-vehicle communication system **301** is not limited to a configuration in which relay of the Ethernet frame is performed in accordance with the Ethernet communication standard, and may be a configuration in which relay of data is performed in accordance with another communication standard such as CAN (Controller Area Network) (registered trademark), FlexRay (registered trademark), MOST (Media Oriented Systems Transport) (registered trademark), or LIN (Local Interconnect Network), for example.

(45) With reference to FIG. **1** and FIG. **2**, the TCU **200**A can communicate with the server **181** outside the vehicle **1**. Specifically, the TCU **200**A can communicate with the server **181** via a wireless base station device **161** by using an IP packet, for example.

(46) More specifically, for example, the TCU **200**A can perform wireless communication with the wireless base station device **161** outside the vehicle **1** in accordance with a communication standard such as LTE (Long Term Evolution) or 3G.

(47) Specifically, when the wireless base station device **161** has received an IP packet via an external network **11** from the server **181** outside the vehicle **1**, the wireless base station device **161** causes the received IP packet to be included in a radio signal, and transmits the radio signal to the TCU **200**A.

(48) For example, when the TCU **200**A has received, from the wireless base station device **161**, a radio signal including an IP packet from the server **181**, the TCU **200**A acquires the IP packet from the received radio signal, stores the acquired IP packet into an Ethernet frame, and transmits the Ethernet frame to the relay device **100**.

(49) Meanwhile, when the TCU **200**A has received an Ethernet frame from the relay device **100**, the TCU **200**A acquires an IP packet from the received Ethernet frame, causes the acquired IP packet to be included in a radio signal, and transmits the radio signal to the wireless base station device **161**.

(50) Upon receiving the radio signal from the TCU **200**A, the wireless base station device **161** acquires the IP packet from the received radio signal, and transmits the acquired IP packet to the server **181** via the external network **11**.

(51) [On-Vehicle ECU]

(52) FIG. **3** shows a configuration of an in-vehicle ECU according to the embodiment of the present disclosure.

(53) With reference to FIG. **3**, the in-vehicle ECU **200** includes a communication unit **210**, a processing unit **220**, an authentication request unit **230**, and a storage unit **240**. The storage unit **240** is a flash memory, for example.

(54) When the communication unit **210** has received an Ethernet frame from the relay device **100** via a corresponding Ethernet cable **13**, the communication unit **210** outputs the received Ethernet frame to the processing unit **220**.

(55) The processing unit **220** acquires information included in the Ethernet frame received from the communication unit **210**, and performs a predetermined process by using the acquired information.

(56) In addition, the processing unit **220** generates an Ethernet frame addressed to another in-vehicle ECU **200**, and outputs the generated Ethernet frame to the communication unit **210**.

(57) Upon receiving the Ethernet frame from the processing unit **220**, the communication unit **210** transmits the received Ethernet frame to the relay device **100** via a corresponding Ethernet cable

13.

(58) Meanwhile, when the processing unit **220** acquires a common key described later from an Ethernet frame received from the communication unit **210**, the processing unit **220** outputs the acquired common key to the authentication request unit **230**.

(59) Upon receiving the common key from the processing unit **220**, the authentication request unit **230** stores the received common key into the storage unit **240**.

(60) When the in-vehicle ECU **200** to which the authentication request unit **230** belongs has been connected to the relay device **100** via an Ethernet cable **13**, the authentication request unit **230** generates an Ethernet frame having stored therein authentication request information that includes the ID of the in-vehicle ECU **200**, e.g., a MAC address, and transmits the generated Ethernet frame to the relay device **100** via the communication unit **210**.

(61) [Relay Device]

(62) FIG. **4** shows a configuration of the relay device according to the embodiment of the present disclosure.

(63) With reference to FIG. **4**, the relay device **100** includes communication ports **52**A, **52**B, **52**C, **52**D, a communication unit **110**, a relay processing unit **120**, a detection unit **130**, an authentication processing unit **140**, a storage unit **150**, and timers **160**. The storage unit **150** is a flash memory, for example.

(64) For example, the relay device **100** includes timers **160** the number of which corresponds to the communication ports **52**A, **52**B, **52**C, **52**D. Specifically, the relay device **100** includes timers **160**A, **160**B, **160**C, **160**D as the timers **160**.

(65) Hereinafter, each of the communication ports **52**A, **52**B, **52**C, **52**D will also be referred to as a communication port **52**. The communication port **52** is a terminal to which an Ethernet cable can be connected, for example.

(66) In this example, the communication ports **52**A, **52**B, **52**C are connected to the TCU **200**A, the in-vehicle ECU **200**B, and the in-vehicle ECU **200**C, respectively.

(67) When the communication unit **110** has received an Ethernet frame via a corresponding communication port **52** from a certain in-vehicle ECU **200**, the communication unit **110** outputs the received Ethernet frame to the relay processing unit **120**.

(68) When the communication unit **110** has received, from the relay processing unit **120**, an Ethernet frame addressed to a certain in-vehicle ECU **200**, the communication unit **110** transmits the received Ethernet frame to the in-vehicle ECU **200** via a corresponding communication port **52**.

(69) The relay processing unit **120** performs a relay process of an Ethernet frame between in-vehicle ECUs **200**. Specifically, for example, upon receiving an Ethernet frame from the communication unit **110**, the relay processing unit **120** performs a relay process for the layer **2** or a relay process for the layer **3**, onto the received Ethernet frame.

(70) Meanwhile, when the relay processing unit **120** has received an Ethernet frame having stored therein authentication request information from an in-vehicle ECU **200** that is newly added to the in-vehicle network **12**, the relay processing unit **120** acquires the authentication request information from the received Ethernet frame, and outputs the acquired authentication request information to the detection unit **130**.

(71) [Detection Unit]

(72) The detection unit **130** detects a new function unit that has been newly added to the in-vehicle network **12**. For example, the detection unit **130** detects, as the new function unit, the in-vehicle ECU **200**D that has newly been added to the in-vehicle network **12**.

(73) With reference to FIG. **2** and FIG. **4**, the in-vehicle ECU **200**D is connected to the communication port **52**D in the relay device **100** via an Ethernet cable **13**.

(74) The detection unit **130** in the relay device **100** receives authentication request information from the in-vehicle ECU **200**D via the relay processing unit **120**, thereby detecting addition of the in-vehicle ECU **200**D to the in-vehicle network **12**.

(75) The detection unit **130** outputs the authentication request information received from the relay processing unit **120**, to the authentication processing unit **140**.

(76) [Authentication Processing Unit]

(77) The authentication processing unit **140** acquires authentication information of an in-vehicle ECU **200** from an external device outside the vehicle **1**.

(78) More specifically, when the authentication processing unit **140** has received authentication request information from the detection unit **130**, the authentication processing unit **140** acquires authentication information of the in-vehicle ECU **200**D serving as a new function unit indicated by the authentication request information, from the server **181** in accordance with a procedure conforming to IEEE802.1X, for example.

(79) The server **181** performs an authentication process regarding an in-vehicle ECU **200** by using an authentication protocol in accordance with the procedure conforming to IEEE802.1X, for example, thereby generating authentication information of the in-vehicle ECU **200**. Hereinafter, the authentication process regarding an in-vehicle ECU **200** performed by the server **181** will also be referred to as an extra-vehicular authentication process.

(80) Here, for example, as an authentication scheme to be used in the extra-vehicular authentication process by the server **181**, EAP (Extended Authentication Protocol)-MD (Message Digest algorithm) **5**, EAP-TLS (Transport Layer Security), PEAP (Protected EAP), LEAP (Lightweight EAP), EAP-TTLS (EAP-Tunneled Transport Layer Security), or the like can be used in accordance with the type of the authentication protocol to be used in the authentication process.

(81) For example, the storage unit **150** has stored therein an authentication scheme to be used in the extra-vehicular authentication process by the server **181**.

(82) When the authentication processing unit **140** has received authentication request information from the detection unit **130**, the authentication processing unit **140** acquires, from the storage unit **150**, the authentication scheme to be used in the extra-vehicular authentication process by the server **181**, and transmits authentication scheme information indicating the acquired authentication scheme, to the in-vehicle ECU **200**D serving as the new function unit indicated by the authentication request information, via the relay processing unit **120** and the communication unit **110**.

(83) The in-vehicle ECU **200**D and the server **181** send and receive, via the relay device **100**, an EAP message that includes information necessary for the extra-vehicular authentication process.

(84) The authentication processing unit **140** in the relay device **100** relays the EAP message and the like sent and received between the server **181** and the in-vehicle ECU **200**D.

(85) More specifically, when the authentication processing unit **140** has received an Ethernet frame having stored therein an EAP message from the in-vehicle ECU **200**D via the communication unit **110** and the relay processing unit **120**, the authentication processing unit **140** converts the received Ethernet frame into a RADIUS (Remote Authentication Dial In User Service) frame and transmits the converted RADIUS frame to the server **181** via the communication unit **110** and the TCU **200**A.

(86) When the authentication processing unit **140** has received a RADIUS frame from the server **181** via the TCU **200**A, the communication unit **110**, and the relay processing unit **120**, the authentication processing unit **140** converts the received RADIUS frame into an Ethernet frame, and transmits the converted Ethernet frame to the in-vehicle ECU **200**D via the communication unit **110**.

(87) The server **181** performs the extra-vehicular authentication process regarding the in-vehicle ECU **200**D by using the EAP message received from the in-vehicle ECU **200** via the relay device **100**. Then, when the server **181** has succeeded in authentication of the in-vehicle ECU **200**D through the extra-vehicular authentication process, the server **181** generates authentication information that indicates an authentication success, and transmits the generated authentication information to the relay device **100** via the wireless base station device **161** and the TCU **200**A.

(88) Meanwhile, when the server **181** has failed in authentication of the in-vehicle ECU **200**D, the server **181** generates authentication information that indicates an authentication failure, and transmits the generated authentication information to the relay device **100** via the wireless base station device **161** and the TCU **200**A.

(89) When the authentication processing unit **140** has received the authentication information indicating the authentication success from the server **181** via the TCU **200**A, the communication unit **110**, and the relay processing unit **120**, the authentication processing unit **140** generates extra-vehicular authentication success information indicating that the extra-vehicular authentication process has been successful, and outputs the generated extra-vehicular authentication success information to the relay processing unit **120**.

(90) Upon receiving the extra-vehicular authentication success information from the authentication processing unit **140**, the relay processing unit **120** transmits the received extra-vehicular authentication success information to the in-vehicle ECU **200**D via the communication unit **110**.

(91) Here, when the authentication processing unit **140** has received authentication information that indicates an authentication success from the server **181** via the communication unit **110** and the relay processing unit **120**, the authentication processing unit **140** sets a valid time of the authentication information to a timer **160**, for each in-vehicle ECU **200**.

(92) For example, the authentication processing unit **140** sets, to the timer **160**A, a valid time of the authentication information of the TCU **200**A connected to the communication port **52**A; sets, to the timer **160**B, a valid time of the authentication information of the in-vehicle ECU **200**B connected to the communication port **52**B; sets, to the timer **160**C, a valid time of the authentication information of the in-vehicle ECU **200**C connected to the communication port **52**C; and sets, to the timer **160**D, a valid time of the authentication information of the in-vehicle ECU **200**D connected to the communication port **52**D.

(93) Meanwhile, when the authentication processing unit **140** has received authentication information that indicates an authentication failure from the server **181** via the TCU **200**A, the communication unit **110**, and the relay processing unit **120**, the authentication processing unit **140** outputs connection non-permitting information to the relay processing unit **120**.

(94) Upon receiving the connection non-permitting information from the authentication processing unit **140**, the relay processing unit **120** transmits the received connection non-permitting information to the in-vehicle ECU **200**D via the communication unit **110**.

(95) The authentication processing unit **140** performs an authentication process regarding the in-vehicle ECU **200** by using the authentication information that indicates an authentication success and that has been acquired from the server **181**. Hereinafter, the authentication process regarding the in-vehicle ECU **200** performed by the authentication processing unit **140** will also be referred to as intra-vehicular authentication process.

(96) The relay processing unit **120** relays information between in-vehicle ECUs **200** on the basis of the result of the intra-vehicular authentication process performed by the authentication processing unit **140**.

Authentication Example 1

(97) For example, authentication information that is received from the server **181** by the authentication processing unit **140** and that indicates an authentication success includes a common key.

(98) When the authentication processing unit **140** has received authentication information of an in-vehicle ECU **200** from the server **181** via the TCU **200**A, the communication unit **110**, and the relay processing unit **120**, the authentication processing unit **140** sets, to a corresponding timer **160**, a predetermined valid time of the received authentication information.

(99) Then, the authentication processing unit **140** acquires a common key from the received authentication information, and stores the acquired common key into the storage unit **150** in association with the in-vehicle ECU **200**. For example, the authentication processing unit **140**

stores the acquired common key into the storage unit **150** in association with a communication port **52**.

(100) The authentication processing unit **140** generates extra-vehicular authentication success information that includes the common key, and transmits the generated extra-vehicular authentication success information to the corresponding in-vehicle ECU **200** via the communication unit **110**.

(101) With reference to FIG. **3** again, when the authentication request unit **230** in the in-vehicle ECU **200** has received the extra-vehicular authentication success information from the authentication processing unit **140** in the relay device **100** via the communication unit **210**, the authentication request unit **230** acquires the common key from the received extra-vehicular authentication success information, and stores the acquired common key into the storage unit **240**.

(102) For example, periodically or non-periodically, the authentication processing unit **140** in the relay device **100** performs an intra-vehicular authentication process for each in-vehicle ECU **200** by using a corresponding common key in the storage unit **150**.

(103) Specifically, the authentication processing unit **140** generates a random number, for example, and transmits the generated random number to a corresponding in-vehicle ECU **200** via the communication unit **110**. In addition, the authentication processing unit **140** encrypts the generated random number by using the common key, to generate encrypted data.

(104) When the authentication request unit **230** in the in-vehicle ECU **200** has received the random number, the authentication request unit **230** encrypts the received random number by using the common key in the storage unit **240**, to generate encrypted data. The in-vehicle ECU **200** transmits the generated encrypted data to the relay device **100**.

(105) When the authentication processing unit **140** in the relay device **100** has received the encrypted data from the in-vehicle ECU **200** via the communication unit **110**, the authentication processing unit **140** collates the received encrypted data with the encrypted data generated by the authentication processing unit **140**.

(106) When the encrypted data received from the in-vehicle ECU **200** matches the encrypted data generated by the authentication processing unit **140**, the authentication processing unit **140** determines that the intra-vehicular authentication process regarding the in-vehicle ECU **200** has been successful. Then, the authentication processing unit **140** outputs, to the relay processing unit **120**, intra-vehicular authentication success information indicating that the authentication of the in-vehicle ECU **200** has been successful.

(107) Upon receiving the intra-vehicular authentication success information from the authentication processing unit **140**, the relay processing unit **120** starts or continues relay of information between the in-vehicle ECU **200** and another in-vehicle ECU **200**.

(108) More specifically, when the relay processing unit **120** has received intra-vehicular authentication success information from the authentication processing unit **140**, the relay processing unit **120** starts or continues relay of an Ethernet frame between the in-vehicle ECU **200** and another in-vehicle ECU **200**.

(109) Meanwhile, when the encrypted data received from the in-vehicle ECU **200** does not match the encrypted data generated by the authentication processing unit **140**, the authentication processing unit **140** determines that the intra-vehicular authentication process regarding the in-vehicle ECU **200** has failed. Then, the authentication processing unit **140** outputs, to the relay processing unit **120**, intra-vehicular authentication failure information indicating that the authentication of the in-vehicle ECU **200** has failed.

(110) Upon receiving the intra-vehicular authentication failure information from the authentication processing unit **140**, the relay processing unit **120** stops relay of information between the in-vehicle ECU **200** and another in-vehicle ECU **200**.

(111) More specifically, when the relay processing unit **120** has received the intra-vehicular authentication failure information from the authentication processing unit **140**, the relay processing

unit **120** starts discarding an Ethernet frame received from the in-vehicle ECU **200**, and an Ethernet frame addressed to the in-vehicle ECU **200** and received from another in-vehicle ECU **200**.

(112) When the intra-vehicular authentication process regarding the in-vehicle ECU **200** has failed, the authentication processing unit **140** acquires new authentication information of the in-vehicle ECU **200** from the server **181** in accordance with the procedure conforming to IEEE802.1X, for example.

(113) When the authentication processing unit **140** has received, from the server **181**, authentication information that indicates an authentication success, as new authentication information, the authentication processing unit **140** stores the common key included in the received authentication information into the storage unit **150** and sets, to a timer **160**, a predetermined valid time of the new authentication information. In addition, the authentication processing unit **140** transmits the common key to the in-vehicle ECU **200** via the relay processing unit **120** and the communication unit **110**.

(114) Then, the authentication processing unit **140** performs the intra-vehicular authentication process regarding the in-vehicle ECU **200** again, by using the common key. Specifically, the authentication processing unit **140** generates a random number and encrypted data, transmits the generated encrypted data to the in-vehicle ECU **200**, and collates the encrypted data received from the in-vehicle ECU **200** with the encrypted data generated by the authentication processing unit **140**.

(115) Meanwhile, when the authentication processing unit **140** has received, from the server **181**, authentication information that indicates an authentication failure, as new authentication information, the authentication processing unit **140** outputs connection non-permitting information to the relay processing unit **120**.

Authentication Example 2

(116) For example, the authentication information received from the server **181** by the authentication processing unit **140** includes a MAC address of an in-vehicle ECU **200** that has been authenticated by the server **181**. Hereinafter, the MAC address of an authenticated in-vehicle ECU **200** will also be referred to as an authenticated MAC address.

(117) When the authentication processing unit **140** has received authentication information of an in-vehicle ECU **200** from the server **181** via the TCU **200**A, the communication unit **110**, and the relay processing unit **120**, the authentication processing unit **140** sets a predetermined valid time of the received authentication information to a corresponding timer **160**.

(118) Then, the authentication processing unit **140** acquires the authenticated MAC address from the received authentication information, and stores the acquired authenticated MAC address into the storage unit **150** in association with the in-vehicle ECU **200**. For example, the authentication processing unit **140** stores the acquired authenticated MAC address into the storage unit **150** in association with a communication port **52**.

(119) The authentication processing unit **140** transmits extra-vehicular authentication success information to the corresponding in-vehicle ECU **200** via the communication unit **110**.

(120) For example, periodically or non-periodically, the authentication processing unit **140** performs an authentication process for each in-vehicle ECU **200** by using a corresponding authenticated MAC address in the storage unit **150**.

(121) For example, the authentication processing unit **140** acquires the transmission source MAC address included in an Ethernet frame received via a communication port **52** from a corresponding in-vehicle ECU **200** by the communication unit **110**, and collates the acquired transmission source MAC address with the authenticated MAC address associated with the communication port **52**.

(122) When the acquired transmission source MAC address matches the authenticated MAC address, the authentication processing unit **140** outputs, to the relay processing unit **120**, intra-vehicular authentication success information indicating that authentication of the in-vehicle ECU **200** has been successful.

(123) Upon receiving the intra-vehicular authentication success information from the authentication processing unit **140**, the relay processing unit **120** starts or continues relay of information between the in-vehicle ECU **200** and another in-vehicle ECU **200**.

(124) Meanwhile, when the acquired transmission source MAC address does not match the authenticated MAC address, the authentication processing unit **140** outputs, to the relay processing unit **120**, intra-vehicular authentication failure information indicating that authentication of the in-vehicle ECU **200** has failed.

(125) Upon receiving the intra-vehicular authentication failure information from the authentication processing unit **140**, the relay processing unit **120** starts discarding an Ethernet frame received from the in-vehicle ECU **200** and an Ethernet frame addressed to the in-vehicle ECU **200** received from another in-vehicle ECU **200**.

(126) When the intra-vehicular authentication process regarding the in-vehicle ECU **200** has failed, the authentication processing unit **140** acquires new authentication information of the in-vehicle ECU **200** connected to the communication port **52**, from the server **181**, in accordance with the procedure conforming to IEEE802.1X, for example.

(127) When the authentication processing unit **140** has received, from the server **181**, authentication information that indicates an authentication success, as new authentication information, the authentication processing unit **140** stores the authenticated MAC address included in the received authentication information into the storage unit **150**, and sets, to a timer **160**, a predetermined valid time of the new authentication information.

(128) Then, the authentication processing unit **140** performs the authentication process regarding the in-vehicle ECU **200** again, by using the authenticated MAC address. Specifically, the authentication processing unit **140** acquires the transmission source MAC address included in an Ethernet frame received via the communication port **52** by the communication unit **110**, and collates the acquired transmission source MAC address with the authenticated MAC address associated with the communication port **52**.

(129) Meanwhile, when the authentication processing unit **140** has received, from the server **181**, authentication information that indicates an authentication failure, as new authentication information, the authentication processing unit **140** outputs connection non-permitting information to the relay processing unit **120**.

(130) [Update of Authentication Information]

(131) When the validity time limit of authentication information of a certain in-vehicle ECU **200** has expired, the authentication processing unit **140** acquires new authentication information of the in-vehicle ECU **200** from the server **181**.

(132) More specifically, when the timer **160** of the corresponding in-vehicle ECU **200** has expired, the authentication processing unit **140** discards the common key or the authenticated MAC address in the storage unit **150**.

(133) Then, the authentication processing unit **140** acquires new authentication information of the in-vehicle ECU **200** from the server **181** in accordance with the procedure conforming to IEEE802.1X, for example.

(134) For example, every time the server **181** performs an extra-vehicular authentication process and succeeds in authentication, the server **181** generates authentication information that has a different content. More specifically, every time the server **181** performs an extra-vehicular authentication process and succeeds in authentication, the server **181** generates authentication information that includes a different common key.

(135) That is, the authentication processing unit **140** acquires, from the server **181**, authentication information that has a content that is different every time the authentication information is acquired. More specifically, the authentication processing unit **140** acquires, from the server **181**, authentication information of which the common key is updated every time the authentication information is acquired.

(136) When the authentication processing unit **140** has received new authentication information from the server **181**, the authentication processing unit **140** stores the common key included in the received authentication information into the storage unit **150**, and sets, to a timer **160**, a predetermined valid time of the authentication information. In addition, the authentication processing unit **140** transmits the common key to the in-vehicle ECU **200** via the relay processing unit **120** and the communication unit **110**.

(137) [Extension Process]

(138) When the validity time limit of authentication information has expired and the relay device **100** cannot communicate with the server **181**, the authentication processing unit **140** performs an extension process of maintaining the validity of the authentication information.

(139) For example, when the timer **160** has expired, the authentication processing unit **140** transmits, to the server **181**, a communication confirmation request via the communication unit **110** and the TCU **200**A in order to confirm whether or not the state is a state where communication with the server **181** is possible.

(140) Upon receiving the communication confirmation request, the server **181** transmits communication-possible information as a response to the communication confirmation request, to the relay device **100** via the wireless base station device **161** and the TCU **200**A.

(141) When the authentication processing unit **140** has received the communication-possible information from the server **181** via the communication unit **110** and the relay processing unit **120**, the authentication processing unit **140** deletes the common key or the authenticated MAC address of the corresponding in-vehicle ECU **200** in the storage unit **150**.

(142) Then, the authentication processing unit **140** acquires new authentication information of the in-vehicle ECU **200** from the server **181** in accordance with the procedure conforming to IEEE802.1X, for example.

(143) Meanwhile, when the authentication processing unit **140** has not received communication-possible information within a predetermined period from the transmission of the communication confirmation request, the authentication processing unit **140** determines that the state is a state where the relay device **100** and the server **181** cannot communicate with each other, and performs an extension process of maintaining the validity of the authentication information.

(144) More specifically, the authentication processing unit **140** sets, to a timer **160**, a predetermined extension time of the authentication information without discarding the common key or the authenticated MAC address of the corresponding in-vehicle ECU **200** in the storage unit **150**.

(145) Alternatively, for example, when the vehicle **1** is traveling in a state where communication between the relay device **100** and the server **181** is possible and where the validity time limit of the authentication information has expired, the authentication processing unit **140** performs the extension process without acquiring new authentication information from the server **181**.

(146) For example, the authentication processing unit **140** acquires information indicating whether or not the vehicle **1** is traveling, from an in-vehicle ECU **200** such as an automated driving ECU, via the communication unit **110** and the relay processing unit **120**.

(147) Even when the authentication processing unit **140** has received communication-possible information from the server **181** via the communication unit **110** and the relay processing unit **120**, if the vehicle **1** is traveling, the authentication processing unit **140** sets, to a timer **160**, a predetermined extension time of the authentication information without discarding the common key or the authenticated MAC address of the corresponding in-vehicle ECU **200** in the storage unit **150**.

(148) After the extension process, the authentication processing unit **140** performs an intra-vehicular authentication process regarding the corresponding in-vehicle ECU **200** by using extended authentication information being the authentication information of which the validity has been maintained. Specifically, the authentication processing unit **140** performs an authentication process regarding the in-vehicle ECU **200** by using the common key or the authenticated MAC

address, in the storage unit **150**, that corresponds to the extended authentication information.

(149) When the authentication processing unit **140** has succeeded in authentication of the in-vehicle ECU **200** as a result of performing the authentication process regarding the in-vehicle ECU **200** by use of the extended authentication information, the authentication processing unit **140** outputs extended authentication success information to the relay processing unit **120**.

(150) Upon receiving the extended authentication success information from the authentication processing unit **140**, the relay processing unit **120** continues relay of information between the in-vehicle ECU **200** and another in-vehicle ECU **200**.

(151) After performing the extension process, the authentication processing unit **140** transmits, periodically or non-periodically, a communication confirmation request to the server **181** and tries acquisition of new authentication information.

(152) Until acquiring new authentication information, the authentication processing unit **140** performs the authentication process regarding the in-vehicle ECU **200** by using the extended authentication information.

(153) [Relay Process Based on Extended Authentication Information]

(154) The relay processing unit **120** determines, in accordance with the type of the in-vehicle ECU **200**, the content of information that should be relayed when the authentication process using the extended authentication information by the authentication processing unit **140** has been successful.

(155) Alternatively, the relay processing unit **120** determines, in accordance with the type of information received from the in-vehicle ECU **200**, whether or not to perform relay when the authentication process using the extended authentication information by the authentication processing unit **140** has been successful.

(156) The relay processing unit **120** determines the content of information, among information received from an in-vehicle ECU **200** and information addressed to the in-vehicle ECU **200**, that should be relayed when extended authentication success information has been received from the authentication processing unit **140**.

(157) For example, the authentication information received from the server **181** by the authentication processing unit **140** includes the MAC address, the IP address, and the port number of an in-vehicle ECU **200** serving as a communication target of the corresponding in-vehicle ECU **200**, and the port number and the like of the corresponding in-vehicle ECU **200**.

(158) When the authentication processing unit **140** has acquired these pieces of information from the authentication information, the authentication processing unit **140** outputs the acquired information to the relay processing unit **120**.

(159) On the basis of the information received from the authentication processing unit **140**, the relay processing unit **120** determines the content of information that should be relayed when extended authentication success information has been received from the authentication processing unit **140**.

(160) For example, the relay processing unit **120** relays all of information between the in-vehicle ECU **200** and another in-vehicle ECU that will influence the driving state of the vehicle **1**, such as an automated driving ECU. Meanwhile, the relay processing unit **120** stops relay of information between the in-vehicle ECU **200** and another in-vehicle ECU that will not influence the driving state of the vehicle **1**.

(161) For example, on the basis of the port number included in the information from the corresponding in-vehicle ECU **200** and the port number included in the information from the in-vehicle ECU **200** serving as the communication target of the corresponding in-vehicle ECU **200**, the relay processing unit **120** discerns information that will influence the driving state of the vehicle **1**, and relays all of the information that will influence the driving state of the vehicle **1** out of information between the in-vehicle ECU **200** and another in-vehicle ECU.

(162) The relay processing unit **120** may be configured to determine, in accordance with both of the type of an in-vehicle ECU **200** and the type of information received from the in-vehicle ECU

200, whether or not to relay a part or all of information when the authentication process using the extended authentication information by the authentication processing unit **140** has been successful.

(163) [Operation Flow]

(164) Each device in the communication system according to the embodiment of the present disclosure includes a computer that includes a memory. An arithmetic processing unit such as a CPU in the computer reads out, from the memory, a program including a part or all of steps in the flow chart and sequence shown below, and executes the program. Programs of the plurality of devices can each be installed from outside. The programs of the plurality of devices are each distributed in a state of being stored in a storage medium.

(165) FIG. **5** is a flow chart describing an operation procedure according to which the relay device in the communication system according to the embodiment of the present disclosure relays information between in-vehicle ECUs on the basis of a result of an authentication process.

(166) With reference to FIG. **5**, first, the relay device **100** waits for addition of a new function unit to the in-vehicle network **12** (NO in step S**102**). Upon detecting addition of the in-vehicle ECU **200**D to the in-vehicle network **12** (YES in step S**102**), the relay device **100** acquires authentication information of the detected in-vehicle ECU **200**D from the server **181** (step S**104**).

(167) Next, when the relay device **100** has acquired, from the server **181**, the authentication information that indicates an authentication failure (NO in step S**106**), the relay device **100** transmits connection non-permitting information to the in-vehicle ECU **200**D (step S**108**).

(168) Next, the relay device **100** waits for new addition of a new function unit to the in-vehicle network **12** (NO in step S**102**).

(169) Meanwhile, when the relay device **100** has acquired, from the server **181**, authentication information that indicates an authentication success (YES in step S**106**), the relay device **100** transmits extra-vehicular authentication success information to the corresponding in-vehicle ECU **200**D (step S**110**).

(170) Next, the relay device **100** performs an intra-vehicular authentication process regarding the in-vehicle ECU **200**D by using the authentication information acquired from the server **181** (step S**112**).

(171) Next, when the relay device **100** has failed in the intra-vehicular authentication process regarding the in-vehicle ECU **200**D (YES in step S**114**), the relay device **100** stops relay of information between the in-vehicle ECU **200**D and another in-vehicle ECU **200** (step S**116**).

(172) Next, the relay device **100** acquires new authentication information of the in-vehicle ECU **200**D from the server **181** (step S**104**).

(173) Meanwhile, when the relay device **100** has succeeded in the intra-vehicular authentication process regarding the in-vehicle ECU **200**D (NO in step S**114**), the relay device **100** starts or continues relay of information between the in-vehicle ECU **200**D and another in-vehicle ECU **200** (step S**118**).

(174) Next, when the validity time limit of the authentication information of the in-vehicle ECU **200**D has not expired (NO in step S**120**), the relay device **100** performs, at the timing of the next intra-vehicular authentication process, the intra-vehicular authentication process regarding the in-vehicle ECU **200**D by using the authentication information (step S**112**).

(175) Meanwhile, when the validity time limit of the authentication information of the in-vehicle ECU **200**D has expired (YES in step S**120**), the relay device **100** confirms whether or not the state is a state where communication with the server **181** is possible (step S**122**).

(176) Next, when the state is a state where communication with the server **181** is possible (YES in step S**122**) and the vehicle **1** is not traveling (YES in step S**124**), the relay device **100** acquires new authentication information of the in-vehicle ECU **200**D from the server **181** (step S**104**).

(177) Meanwhile, when the state is a state where communication with the server **181** is not possible (NO in step S**122**) or when the state is a state where communication with the server **181** is possible (YES in step S**122**) and the vehicle **1** is traveling (NO in step S**124**), the relay device **100** performs

an extension process (step S**126**).

(178) Next, at the timing of the next intra-vehicular authentication process, the relay device **100** performs the intra-vehicular authentication process regarding the in-vehicle ECU **200**D by using extended authentication information being the authentication information of which the validity has been maintained by the extension process (step S**112**).

(179) FIG. **6** shows an example of a sequence of an extra-vehicular authentication process performed in the communication system according to the embodiment of the present disclosure.

(180) With reference to FIG. **6**, first, when the in-vehicle ECU **200**D serving as a new function unit newly added to the in-vehicle network **12** has been connected to the relay device **100**, the in-vehicle ECU **200**D transmits, to the relay device **100**, authentication request information including the MAC address of the in-vehicle ECU **200**D (step S**202**).

(181) Next, when having received the authentication request information from the in-vehicle ECU **200**D, the relay device **100** transmits, to the in-vehicle ECU **200**D, authentication scheme information indicating an authentication scheme to be used in the extra-vehicular authentication process (step S**204**).

(182) Next, the in-vehicle ECU **200**D and the server **181** send and receive, via the relay device **100**, an EAP message that includes information necessary for the extra-vehicular authentication process (step S**206**).

(183) Next, the server **181** performs the extra-vehicular authentication process regarding the in-vehicle ECU **200**D by using the EAP message received from the in-vehicle ECU **200** via the relay device **100** (step S**208**).

(184) Next, when the server **181** has succeeded in authentication of the in-vehicle ECU **200**D through the extra-vehicular authentication process, the server **181** generates authentication information that indicates an authentication success, and transmits the generated authentication information to the relay device **100** (step S**210**).

(185) Next, upon receiving the authentication information from the server **181**, the relay device **100** transmits extra-vehicular authentication success information to the in-vehicle ECU **200**D (step S**212**).

(186) FIG. **7** shows an example of a sequence of an extra-vehicular authentication process and an intra-vehicular authentication process performed in the communication system according to the embodiment of the present disclosure.

(187) With reference to FIG. **7**, first, the relay device **100** is relaying information between the in-vehicle ECU **200**C and the in-vehicle ECU **200**D on the basis of a result of an intra-vehicular authentication process using a common key. That is, the in-vehicle ECU **200**C and the in-vehicle ECU **200**D are communicating with each other via the relay device **100** on the basis of the result of the intra-vehicular authentication process performed by the relay device **100** (step S**302**).

(188) Next, when the validity time limit of authentication information of the in-vehicle ECU **200**D has expired, the relay device **100** transmits a communication confirmation request to the server **181** (step S**304**).

(189) Next, when the relay device **100** has not been able to receive communication-possible information from the server **181** within a predetermined time from the transmission of the communication confirmation request, the relay device **100** determines that the state is a state where the relay device **100** and the server **181** cannot communicate with each other, and performs an extension process of maintaining the validity of the authentication information including the common key (step S**306**).

(190) Next, the relay device **100** continues relay of information between the in-vehicle ECU **200**C and the in-vehicle ECU **200**D based on the result of the intra-vehicular authentication process using the common key. Then, on the basis of the result of the intra-vehicular authentication process performed by the relay device **100**, the in-vehicle ECU **200**C and the in-vehicle ECU **200**D perform communication with each other via the relay device **100** (step S**308**).

(191) Next, the relay device **100** transmits again a communication confirmation request to the server **181** (step S**310**).

(192) Next, upon receiving the communication confirmation request, the server **181** transmits, to the relay device **100**, communication-possible information as a response to the communication confirmation request (step S**312**).

(193) Next, the in-vehicle ECU **200**D and the server **181** send and receive, via the relay device **100**, an EAP message that includes information necessary for the extra-vehicular authentication process. Then, the server **181** performs the extra-vehicular authentication process regarding the in-vehicle ECU **200**D by using the EAP message received from the in-vehicle ECU **200** via the relay device **100** (step S**314**).

(194) Next, when the server **181** has succeeded in authentication of the in-vehicle ECU **200**D through the extra-vehicular authentication process, the server **181** generates authentication information that includes a new common key, and transmits the generated authentication information to the relay device **100** (step S**316**).

(195) Next, upon receiving the authentication information including the new common key from the server **181**, the relay device **100** transmits, to the in-vehicle ECU **200**D, extra-vehicular authentication success information that includes the new common key (step S**318**).

(196) Next, the relay device **100** starts relay of information between the in-vehicle ECU **200**C and the in-vehicle ECU **200**D based on the result of an intra-vehicular authentication process using the new common key. Then, on the basis of the result of the intra-vehicular authentication process performed by the relay device **100**, the in-vehicle ECU **200**C and the in-vehicle ECU **200**D perform communication with each other via the relay device **100** (step S**320**).

(197) FIG. **8** shows an example of a sequence of the intra-vehicular authentication process performed in the communication system according to the embodiment of the present disclosure. FIG. **8** shows details of the processes in steps S**302**, S**308**, S**320** in FIG. **7**.

(198) With reference to FIG. **8**, first, the relay device **100** generates a random number (step S**402**).

(199) Next, the relay device **100** transmits the generated random number to the in-vehicle ECU **200**D serving as the target of the intra-vehicular authentication process (step S**404**).

(200) Next, the relay device **100** encrypts the generated random number by using a common key, to generate encrypted data (step S**406**).

(201) The in-vehicle ECU **200**D encrypts the random number received from the relay device **100**, by using the common key, to generate encrypted data (step S**408**).

(202) Next, the in-vehicle ECU **200**D transmits the generated encrypted data to the relay device **100** (step S**410**).

(203) Upon receiving the encrypted data from the in-vehicle ECU **200**D, the relay device **100** collates the received encrypted data with the encrypted data generated by the relay device **100** (step S**412**).

(204) Next, when the encrypted data received from the in-vehicle ECU **200**D matches the encrypted data generated by the relay device **100**, the relay device **100** determines that the intra-vehicular authentication process regarding the in-vehicle ECU **200**D has been successful, and starts or continues relay of information between the in-vehicle ECU **200**D and another in-vehicle ECU **200** (step S**414**).

(205) FIG. **9** shows another example of a sequence of the extra-vehicular authentication process and the intra-vehicular authentication process performed in the communication system according to the embodiment of the present disclosure.

(206) With reference to FIG. **9**, first, the relay device **100** is relaying information between the in-vehicle ECU **200**C and the in-vehicle ECU **200**D on the basis of a result of an intra-vehicular authentication process using an authenticated MAC address. That is, the in-vehicle ECU **200**C and the in-vehicle ECU **200**D are communicating with each other via the relay device **100** on the basis of the result of the intra-vehicular authentication process performed by the relay device **100** (step

S**502**).

(207) Next, when the validity time limit of authentication information of the in-vehicle ECU **200**D has expired, the relay device **100** transmits a communication confirmation request to the server **181** (step S**504**).

(208) Next, when the relay device **100** has not been able to receive communication-possible information from the server **181** within a predetermined time from the transmission of the communication confirmation request, the relay device **100** determines that the state is a state where the relay device **100** and the server **181** cannot communicate with each other, and performs an extension process of maintaining the validity of the authentication information including the authenticated MAC address (step S**506**).

(209) Next, the relay device **100** continues relay of information between the in-vehicle ECU **200**C and the in-vehicle ECU **200**D based on the result of the intra-vehicular authentication process using the authenticated MAC address. Then, on the basis of the result of the intra-vehicular authentication process performed by the relay device **100**, the in-vehicle ECU **200**C and the in-vehicle ECU **200**D perform communication with each other via the relay device **100** (step S**508**).

(210) Next, the relay device **100** transmits again a communication confirmation request to the server **181** (step S**510**).

(211) Next, upon receiving the communication confirmation request, the server **181** transmits, to the relay device **100**, communication-possible information as a response to the communication confirmation request (step S**512**).

(212) Next, the in-vehicle ECU **200**D and the server **181** send and receive, via the relay device **100**, an EAP message that includes information necessary for the extra-vehicular authentication process. Then, the server **181** performs the extra-vehicular authentication process regarding the in-vehicle ECU **200**D by using the EAP message received from the in-vehicle ECU **200** via the relay device **100** (step S**514**).

(213) Next, when the server **181** has succeeded in authentication of the in-vehicle ECU **200**D through the extra-vehicular authentication process, the server **181** transmits, to the relay device **100**, new authentication information that includes an authenticated MAC address (step S**516**).

(214) Next, upon receiving the new authentication information from the server **181**, the relay device **100** transmits, to the in-vehicle ECU **200**D, extra-vehicular authentication success information that includes the authenticated MAC address that corresponds to the received authentication information (step S**518**).

(215) Next, the relay device **100** starts relay of information between the in-vehicle ECU **200**C and the in-vehicle ECU **200**D based on the result of an intra-vehicular authentication process using the new authenticated MAC address. Then, on the basis of the result of the intra-vehicular authentication process performed by the relay device **100**, the in-vehicle ECU **200**C and the in-vehicle ECU **200**D perform communication with each other via the relay device **100** (step S**520**).

(216) In the relay device **100** according to the embodiment of the present disclosure, when the validity time limit of the authentication information has expired and the relay device **100** cannot communicate with the server **181**, the authentication processing unit **140** performs an extension process of maintaining the validity of the authentication information, and performs an intra-vehicular authentication process regarding the corresponding in-vehicle ECU **200** by using extended authentication information being the authentication information of which the validity has been maintained. However, the present disclosure is not limited thereto. When the validity time limit of the authentication information has expired and the relay device **100** cannot communicate with the server **181**, the authentication processing unit **140** may stop the intra-vehicular authentication process until acquiring new authentication information, without performing the extension process. Alternatively, the relay processing unit **120** may stop relay of information between in-vehicle ECUs **200** until the authentication processing unit **140** acquires new authentication information and performs an intra-vehicular authentication process by using the

acquired new authentication information.

(217) In the relay device **100** according to the embodiment of the present disclosure, the relay processing unit **120** determines, in accordance with the type of the in-vehicle ECU **200**, the content of information that should be relayed when the authentication process using extended authentication information by the authentication processing unit **140** has been successful. However, the present disclosure is not limited thereto. Irrespective of the type of the in-vehicle ECU **200**, the relay processing unit **120** may relay all information including various types of content between the in-vehicle ECU **200** and another in-vehicle ECU **200** when the authentication process using extended authentication information by the authentication processing unit **140** has been successful.

(218) In the relay device **100** according to the embodiment of the present disclosure, the relay processing unit **120** determines, in accordance with the type of information received from an in-vehicle ECU **200**, whether or not to perform relay when the authentication process using extended authentication information by the authentication processing unit **140** has been successful. However, the present disclosure is not limited thereto. Irrespective of the type of information received from the in-vehicle ECU **200**, the relay processing unit **120** may relay all information received from the in-vehicle ECU **200** and addressed to another in-vehicle ECU **200**.

(219) In the relay device **100** according to the embodiment of the present disclosure, the authentication processing unit **140** acquires, from the server **181**, authentication information of which the common key is updated every time the authentication information is acquired. However, the present disclosure is not limited thereto. Every time the server **181** performs an extra-vehicular authentication process and succeeds in authentication, the server **181** may generate corresponding authentication information that includes the same common key, and transmit the generated authentication information to the relay device **100**.

(220) In the relay device **100** according to the embodiment of the present disclosure, when the vehicle **1** is traveling in a state where communication between the relay device **100** and the server **181** is possible and where the validity time limit of the authentication information has expired, the authentication processing unit **140** performs the extension process of maintaining the validity of the authentication information without acquiring new authentication information from the server **181**. However, the present disclosure is not limited thereto. Irrespective of whether or not the vehicle **1** is traveling in a state where communication between the relay device **100** and the server **181** is possible and where the validity time limit of the authentication information has expired, the authentication processing unit **140** may acquire new authentication information from the server **181**.

(221) Meanwhile, a technology that can improve security in in-vehicle networks is desired.

(222) Specifically, for example, in a case where a new in-vehicle network is configured by mounting a new in-vehicle ECU to an existing in-vehicle network, a technology that can improve security in the new in-vehicle network is desired.

(223) In this regard, the relay device **100** according to the embodiment of the present disclosure is mounted to the vehicle **1** including a plurality of in-vehicle ECUs **200**. The authentication processing unit **140** acquires authentication information of an in-vehicle ECU **200** from the server **181** outside the vehicle **1** and performs an authentication process regarding the in-vehicle ECU **200** by using the acquired authentication information. On the basis of the result of the authentication process performed by the authentication processing unit **140**, the relay processing unit **120** relays information between the in-vehicle ECU **200** and another in-vehicle ECU **200**. When the validity time limit of the authentication information has expired, the authentication processing unit **140** acquires new authentication information from the server **181**.

(224) Thus, with the configuration in which authentication information of an in-vehicle ECU **200** is acquired from the server **181** outside the vehicle **1**, even when a new unknown in-vehicle ECU **200** has been added to the in-vehicle network, the authentication information of the in-vehicle ECU can be acquired. Further, when the validity time limit has expired, new authentication information is

acquired, the authentication process regarding the in-vehicle ECU **200** is performed by using the acquired authentication information, and on the basis of the result of the authentication process, information between the in-vehicle ECU **200** and another in-vehicle ECU **200** is relayed. With this configuration, security in the in-vehicle network can be ensured. In addition, even in a situation where it is difficult to acquire new authentication information from the server **181** due to the traveling environment of the vehicle **1**, the authentication process regarding the in-vehicle ECU **200** can be performed by continuously using the authentication information.

(225) Therefore, in the relay device **100** according to the embodiment of the present disclosure, security in the in-vehicle network can be improved.

(226) In the relay device **100** according to the embodiment of the present disclosure, when the validity time limit of the authentication information has expired and the relay device **100** cannot communicate with the server **181**, the authentication processing unit **140** performs an extension process of maintaining the validity of the authentication information, and performs, by using extended authentication information being the authentication information of which the validity has been maintained, an authentication process regarding the in-vehicle ECU **200** corresponding to the authentication information.

(227) With this configuration, even in a case where, when the validity time limit of the authentication information has expired, the communication environment between the relay device **100** and the server **181** is bad due to the traveling environment of the vehicle **1** and new authentication information cannot be acquired, it is possible to perform an authentication process and continue relay of information between in-vehicle ECUs **200** based on the authentication result. Accordingly, for example, in a configuration in which security is improved by updating the content of the authentication information at the outside of the vehicle **1**, it is possible to manage stable communication in the in-vehicle network, irrespective of the traveling environment of the vehicle **1**.

(228) In the relay device **100** according to the embodiment of the present disclosure, the relay processing unit **120** determines, in accordance with the type of the in-vehicle ECU **200**, the content of information that should be relayed when the authentication process using extended authentication information by the authentication processing unit **140** has been successful.

(229) With this configuration, a part of information to be relayed when the extension process has been performed can be restricted in accordance with the type of the in-vehicle ECU **200**. Therefore, for example, by continuing relay of information between in-vehicle ECUs **200** that will influence traveling of the vehicle **1**, and at the same time, by stopping relay of information between in-vehicle ECUs **200** that will not influence traveling of the vehicle **1**, it is possible to suppress decrease in security in the in-vehicle network while maintaining favorable traveling of the vehicle **1**.

(230) In the relay device **100** according to the embodiment of the present disclosure, the relay processing unit **120** determines, in accordance with the type of information received from the in-vehicle ECU **200**, whether or not to perform relay when the authentication process using extended authentication information by the authentication processing unit **140** has been successful.

(231) With this configuration, a part of information to be relayed when the extension process has been performed can be restricted in accordance with the type of information received from the in-vehicle ECU **200**. Therefore, for example, by continuing relay of information that will influence traveling of the vehicle **1**, and at the same time, by stopping relay of information that will not influence traveling of the vehicle **1**, it is possible to suppress decrease in security in the in-vehicle network while maintaining favorable traveling of the vehicle **1**.

(232) In the relay device **100** according to the embodiment of the present disclosure, the authentication processing unit **140** acquires, from the server **181**, authentication information that has a content that is different every time the authentication information is acquired.

(233) With this configuration, every time the validity time limit has expired, authentication

information that has a new content can be acquired, and an authentication process regarding the in-vehicle ECU **200** can be performed by using the authentication information. Therefore, security in the in-vehicle network can be further improved.

(234) In the relay device **100** according to the embodiment of the present disclosure, when the vehicle **1** is traveling in a state where communication between the relay device **100** and the server **181** is possible and where the validity time limit of the authentication information has expired, the authentication processing unit **140** performs an extension process of maintaining the validity of the authentication information without acquiring new authentication information from the server **181**.

(235) With this configuration, for example, a situation where an authentication error occurs as a result of performing an authentication process by using new authentication information, and relay of a part or all of information between in-vehicle ECUs **200** is stopped during traveling of the vehicle **1**, can be avoided. Thus, favorable traveling of the vehicle **1** can be maintained.

(236) A vehicle communication method according to an embodiment of the present disclosure is performed in the relay device **100** mounted to the vehicle **1** including a plurality of in-vehicle ECUs **200**. In this vehicle communication method, first, authentication information of an in-vehicle ECU **200** is acquired from an external device outside the vehicle **1**. Next, an authentication process regarding the in-vehicle ECU **200** is performed by using the acquired authentication information. Next, on the basis of the result of the authentication process, information between the in-vehicle ECU **200** and another in-vehicle ECU **200** is relayed. Next, when the validity time limit of the authentication information has expired, new authentication information is acquired from the server **181**.

(237) Thus, with the method in which authentication information of an in-vehicle ECU **200** is acquired from the server **181** outside the vehicle **1**, even when a new unknown in-vehicle ECU **200** has been added to the in-vehicle network, the authentication information of the in-vehicle ECU can be acquired. Further, when the validity time limit has expired, new authentication information is acquired, the authentication process regarding the in-vehicle ECU **200** is performed by using the acquired authentication information, and on the basis of the result of the authentication process, information between the in-vehicle ECU **200** and another in-vehicle ECU **200** is relayed. With this method, security in the in-vehicle network can be ensured. In addition, even in a situation where it is difficult to acquire new authentication information from the server **181** due to the traveling environment of the vehicle **1**, the authentication process regarding the in-vehicle ECU **200** can be performed by continuously using the authentication information.

(238) Therefore, with the vehicle communication method according to the embodiment of the present disclosure, security in the in-vehicle network can be improved.

(239) The above embodiment is merely illustrative in all aspects and should not be recognized as being restrictive. The scope of the present disclosure is defined by the scope of the claims rather than by the description above, and is intended to include meaning equivalent to the scope of the claims and all modifications within the scope.

(240) The above description includes the features in the additional note below.

(241) [Additional Note 1]

(242) A relay device mounted to a vehicle including a plurality of function units, the relay device comprising: an authentication processing unit configured to acquire authentication information of a function unit from an external device outside the vehicle, and perform an authentication process regarding the function unit by using the acquired authentication information; and a relay processing unit configured to, on the basis of a result of the authentication process performed by the authentication processing unit, relay information between the function unit and another function unit, wherein when a validity time limit of the authentication information has expired, the authentication processing unit acquires, from the external device, the authentication information that is new, and the authentication processing unit acquires, from the external device, the authentication information that includes a common key that is different every time the

authentication information is acquired, and the authentication processing unit performs an authentication process regarding the function unit by using the common key included in the acquired authentication information.

REFERENCE SIGNS LIST

(243) **1** vehicle **11** external network **12** in-vehicle network **13** Ethernet cable **52** communication port **100** relay device **110** communication unit **120** relay processing unit **130** detection unit **140** authentication processing unit **150** storage unit **160** timer **161** wireless base station device **181** server **200** in-vehicle ECU **210** communication unit **220** processing unit **230** authentication request unit **240** storage unit **301** in-vehicle communication system **401** communication system

Claims

1. A relay device mounted to a vehicle including a plurality of function units, the relay device comprising: an authentication processing unit configured to acquire, from an external device outside the vehicle, first authentication information including a success result or a failure result of a first authentication process for a first function unit of the plurality of function units; and a relay processing unit configured to, on the basis of the acquired first authentication information including the success result of the first authentication process, relay information between the first function unit and a second function unit of the plurality of function units, wherein in response to a validity time limit of the first authentication information having expired, the authentication processing unit acquires, from the external device, second authentication information including a success result or a failure result of a second authentication process for the first function unit.
2. The relay device according to claim 1, wherein when the validity time limit of the first authentication information has expired and the relay device is not able to communicate with the external device, the authentication processing unit performs an extension process of maintaining validity of the first authentication information, and performs, by using extended authentication information being the first authentication information of which the validity has been maintained, a third authentication process regarding the first function unit corresponding to the first authentication information.
3. The relay device according to claim 2, wherein the relay processing unit determines, in accordance with a type of the first function unit, a content of information that should be relayed when the third authentication process using the extended authentication information by the authentication processing unit has been successful.
4. The relay device according to claim 2, wherein the relay processing unit determines, in accordance with a type of information received from the first function unit, whether or not to perform relay when the third authentication process using the extended authentication information by the authentication processing unit has been successful.
5. The relay device according to claim 1, wherein the authentication processing unit acquires, from the external device, the first authentication information that has a content that is different every time the first authentication information is acquired.
6. The relay device according to claim 1, wherein when the vehicle is traveling in a state where communication between the relay device and the external device is possible and where the validity time limit of the first authentication information has expired, the authentication processing unit performs an extension process of maintaining validity of the first authentication information without acquiring the second authentication information from the external device.
7. A vehicle communication method to be performed in a relay device mounted in a vehicle including a plurality of function units, the vehicle communication method comprising the steps of: acquiring, from an external device outside the vehicle, first authentication information including a success result or a failure result of a first authentication process for a first function unit of the plurality of function units; relaying, on the basis of, the acquired first authentication information

including the success result of the first authentication process, information between the first function unit and a second function unit of the plurality of function units; and acquiring, in response to a validity time limit of the first authentication information having expired, second authentication information including a success result or a failure result of a second authentication process for the first function unit, from the external device.